**Description**


The objective of this standard is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System.

**Disclaimer**

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

**Scan**

<table>
<thead>
<tr>
<th>URL</th>
<th><a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan date</td>
<td></td>
</tr>
<tr>
<td>Duration</td>
<td></td>
</tr>
<tr>
<td>Profile</td>
<td></td>
</tr>
</tbody>
</table>

**Compliance at a Glance**

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

- **Inventory of assets (8.1.1)**
  No alerts in this category

- **Handling of assets (8.2.3)**
  Total number of alerts in this category: 93

- **Access to networks and network services (9.1.2)**
  No alerts in this category

- **Management of privileged access rights (9.2.3)**
  Total number of alerts in this category: 23

- **Management of secret authentication information of users (9.2.4)**
  No alerts in this category

- **Use of secret authentication information (9.3.1)**
  No alerts in this category

- **Information access restriction (9.4.1)**
  Total number of alerts in this category: 92

- **Secure log-on procedures (9.4.2)**
  No alerts in this category

- **Password management system (9.4.3)**
  No alerts in this category
- Use of privileged utility programs (9.4.4)
  No alerts in this category

- Access control to program source code (9.4.5)
  Total number of alerts in this category: 6

- Separation of development, testing and operational environments (12.1.4)
  Total number of alerts in this category: 7

- Controls against malware (12.2.1)
  No alerts in this category

- Protection of log information (12.4.2)
  Total number of alerts in this category: 92

- Administrator and operator logs (12.4.3)
  Total number of alerts in this category: 92

- Installation of software on operational systems (12.5.1)
  Total number of alerts in this category: 29

- Security of network services (13.1.1)
  No alerts in this category

- Information transfer policies and procedures (13.2.1)
  Total number of alerts in this category: 3

- Electronic messaging (13.2.3)
  Total number of alerts in this category: 3

- Securing application services on public networks (14.1.2)
  Total number of alerts in this category: 95

- Protecting application services transactions (14.1.3)
  Total number of alerts in this category: 3

- Secure development policy (14.2.1)
  Total number of alerts in this category: 98

- Protection of test data (14.3.1)
  Total number of alerts in this category: 7

- Availability of information processing facilities (17.2.1)
  No alerts in this category

- Protection of records (18.1.3)
  Total number of alerts in this category: 159

- Privacy and protection of personally identifiable information (18.1.4)
  Total number of alerts in this category: 159

- Regulation of cryptographic controls (18.1.5)
  Total number of alerts in this category: 1
Compliance According to Categories: A Detailed Report

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

(8.1.1) Inventory of assets

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

No alerts in this category.

(8.2.3) Handling of assets

Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

Total number of alerts in this category: 93

Alerts in this category

Directory traversal (verified)

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Base Score: 5.3</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Target Distribution: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
</tbody>
</table>

CWE

CWE-22

Affected item
/showimage.php
**Macromedia Dreamweaver remote database scripts (verified)**

Macromedia Dreamweaver has created a directory (_mmServerScripts or _mmDBScripts) that contains scripts for testing database connectivity. One of these scripts (mmhttpdb.php or mmhttpdb.asp) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: High</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Official_fix</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Confirmed</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVE</th>
<th>CVE-2004-1893</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-16</th>
</tr>
</thead>
</table>

**Affected item**  
Web Server

**Affected parameter**  
file

.../.../.../.../.../.../.../proc/version

---

**Possible database backup**

Manual confirmation is required for this alert.

It looks like this file contains a database backup/dump. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

| CWE | CWE-538 |
.htaccess file readable (verified)

This directory contains an .htaccess file that is readable. This may indicate a server misconfiguration. .htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

CWE: CWE-16

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
### CVSS3
- Base Score: 5.3
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: Low
- Integrity Impact: None
- Availability Impact: None

### CWE
- CWE-200

### Affected item
- **Web Server**

### Affected parameter
- */[*].php*

### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2          |  
|----------------|---
| Base Score: 5.0 |  
| Access Vector: Network_accessable |  
| Access Complexity: Low |  
| Authentication: None |  
| Confidentiality Impact: Partial |  
| Integrity Impact: None |  
| Availability Impact: None |  
| Exploitability: Not_defined |  
| Remediation Level: Not_defined |  
| Report Confidence: Not_defined |  
| Availability Requirement: Not_defined |  
| Collateral Damage Potential: Not_defined |  
| Confidentiality Requirement: Not_defined |  
| Integrity Requirement: Not_defined |  
| Target Distribution: Not_defined |  

| CVSS3          |  
|----------------|---
| Base Score: 5.3 |  
| Attack Vector: Network |  
| Attack Complexity: Low |  
| Privileges Required: None |  
| User Interaction: None |  
| Scope: Unchanged |  
| Confidentiality Impact: Low |  
| Integrity Impact: None |  
| Availability Impact: None |  

| CWE          |  
|--------------|---
| CWE-200 |  

### Affected item
- **Web Server**

### Affected parameter
- 

### Application error message

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/cart.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>login</td>
</tr>
</tbody>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>5.0</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>5.3</td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Low</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/cart.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>Referer</td>
</tr>
</tbody>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| **CVSS3** | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CWE</strong></td>
<td>CWE-200</td>
</tr>
<tr>
<td><strong>Affected item</strong></td>
<td>/cart.php</td>
</tr>
<tr>
<td><strong>Affected parameter</strong></td>
<td>User-Agent</td>
</tr>
</tbody>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| **CVSS2** | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CWE</strong></td>
<td>CWE-200</td>
</tr>
<tr>
<td><strong>Affected item</strong></td>
<td>/cart.php</td>
</tr>
<tr>
<td><strong>Affected parameter</strong></td>
<td>X-Forwarded-For</td>
</tr>
</tbody>
</table>

**Application error message**
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | | Base Score: 5.0  
| | Access Vector: Network\_accessible  
| | Access Complexity: Low  
| | Authentication: None  
| | Confidentiality Impact: Partial  
| | Integrity Impact: None  
| | Availability Impact: None  
| | Exploitability: Not\_defined  
| | Remediation Level: Not\_defined  
| | Report Confidence: Not\_defined  
| | Availability Requirement: Not\_defined  
| | Collateral Damage Potential: Not\_defined  
| | Confidentiality Requirement: Not\_defined  
| | Integrity Requirement: Not\_defined  
| | Target Distribution: Not\_defined  
| CVSS3 | | Base Score: 5.3  
| | Attack Vector: Network  
| | Attack Complexity: Low  
| | Privileges Required: None  
| | User Interaction: None  
| | Scope: Unchanged  
| | Confidentiality Impact: Low  
| | Integrity Impact: None  
| | Availability Impact: None  
| CWE | | CWE-200  
| Affected item | /listproducts.php  
| Affected parameter | artist  
| Variants | 12345"\";\|\*%00\%0d%0a<%00>%bf%27\%20l  

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
CVSS2
Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3
Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE
CWE-200

Affected item
/listproducts.php

Affected parameter
cat

Variants
12345``\);]]*%00{%0d%0a<%00>%bf%27%0a%

Application error message
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/listproducts.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>User-Agent</td>
</tr>
</tbody>
</table>
CVSS2

| Base Score: 5.0 |
| Access Vector: Network_accessible |
| Access Complexity: Low |
| Authentication: None |
| Confidentiality Impact: Partial |
| Integrity Impact: None |
| Availability Impact: None |
| Exploitability: Not_defined |
| Remediation Level: Not_defined |
| Report Confidence: Not_defined |
| Availability Requirement: Not_defined |
| Collateral Damage Potential: Not_defined |
| Confidentiality Requirement: Not_defined |
| Integrity Requirement: Not_defined |
| Target Distribution: Not_defined |

CVSS3

| Base Score: 5.3 |
| Attack Vector: Network |
| Attack Complexity: Low |
| Privileges Required: None |
| User Interaction: None |
| Scope: Unchanged |
| Confidentiality Impact: Low |
| Integrity Impact: None |
| Availability Impact: None |

CWE

| CWE-200 |
| Affected item: /listproducts.php |
| Affected parameter: X-Forwarded-For |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| Base Score: 5.0 |
| Access Vector: Network_accessible |
| Access Complexity: Low |
| Authentication: None |
| Confidentiality Impact: Partial |
| Integrity Impact: None |
| Availability Impact: None |
| Exploitability: Not_defined |
| Remediation Level: Not_defined |
| Report Confidence: Not_defined |
| Availability Requirement: Not_defined |
| Collateral Damage Potential: Not_defined |
| Confidentiality Requirement: Not_defined |
| Integrity Requirement: Not_defined |
| Target Distribution: Not_defined |
| CVSS3          | Base Score: 5.3  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: Low  
|               | Integrity Impact: None  
|               | Availability Impact: None  
| CWE           | CWE-200  
| Affected item | /product.php  
| Affected parameter | pic  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2          | Base Score: 5.0  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

| CVSS3          | Base Score: 5.3  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: Low  
|               | Integrity Impact: None  
|               | Availability Impact: None  
| CWE           | CWE-200  
| Affected item | /secured/newuser.php  
| Affected parameter | login  

**Application error message**
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2          | Base Score: 5.0
|                | Access Vector: Network_accessible
|                | Access Complexity: Low
|                | Authentication: None
|                | Confidentiality Impact: Partial
|                | Integrity Impact: None
|                | Availability Impact: None
|                | Exploitability: Not_defined
|                | Remediation Level: Not_defined
|                | Report Confidence: Not_defined
|                | Availability Requirement: Not_defined
|                | Collateral Damage Potential: Not_defined
|                | Confidentiality Requirement: Not_defined
|                | Integrity Requirement: Not_defined
|                | Target Distribution: Not_defined
| CVSS3          | Base Score: 5.3
|                | Attack Vector: Network
|                | Attack Complexity: Low
|                | Privileges Required: None
|                | User Interaction: None
|                | Scope: Unchanged
|                | Confidentiality Impact: Low
|                | Integrity Impact: None
|                | Availability Impact: None

CWE               | CWE-200

Affected item       | /secured/newuser.php

Affected parameter  | signup

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Scope: Unchanged</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Affected item**

/secure/newuser.php

**Affected parameter**

uaddress

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /secured/newuser.php |
| Affected parameter | ucc |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /secured/newuser.php |
| Affected parameter | uemail |
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
</tr>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-200

Affected item

/secured/newuser.php

Affected parameter

uuname

Variants

12345"\";|]*%00[%0d%0a<%00>%%bf%27'}}

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE | CWE-200 |

| Affected item | /showimage.php |
| Affected parameter | file |
| Variants | acu4562%EF%BC%9Cs1%EF%B9%A5s2%CA%BA%As3%CA%B9uca4562 |

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE  | CWE-200 |
| Affected item | /userinfo.php |
| Affected parameter | script#text |
| Variants | 12345"\");||*%00{%0d%0a<%00>%bf%27\"\"i |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE  | CWE-200 |
| Affected item | /userinfo.php |
| Affected parameter | uaddress |
| Variants | 12345"\");||*%00{%0d%0a<%00>%bf%27\"\"i |
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /userinfo.php |
| Affected parameter | ucc |
| Variants | 12345"\"\";||%00(%0d%0a<%00>%%bf%27\x00i |

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item
/userinfo.php

Affected parameter
uemail

Variants
12345\\\');||%00(%0d%0a<%00>%bf%27ð¡

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application’s internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the ‘Attack details’ section for more information about the affected page.
**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

---

**CVSS3**

Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None

**CWE**

CWE-200

**Affected item**  
/userinfo.php

**Affected parameter**  
uname

**Variants**  
12345"\";||%00{%0d%0a<%00>%bf%270\470_i

---

**CVSS2**

Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

---

**CVSS3**

Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None

**CWE**

CWE-200

**Affected item**  
/userinfo.php

**Affected parameter**  
uphone

**Variants**  
12345"\";||%00{%0d%0a<%00>%bf%270\470_i
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  |

| CWE | CWE-200 |
| Affected item | /userinfo.php |
| Affected parameter | uname |
| Variants | 12345"\":[]]*%00(%0d%0a<%00>%bf%27%00>| |

Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.
### CVSS2

- **Base Score:** 5.0
- **Access Vector:** NetworkAccessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** NotDefined
- **Remediation Level:** NotDefined
- **Report Confidence:** NotDefined
- **Availability Requirement:** NotDefined
- **Collateral Damage Potential:** NotDefined
- **Confidentiality Requirement:** NotDefined
- **Integrity Requirement:** NotDefined
- **Target Distribution:** NotDefined

### CWE

- **CWE:** CWE-538

### Affected item

- **/index.bak**

### Affected parameter

---

#### Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Score:</strong> 5.0</td>
</tr>
<tr>
<td><strong>Access Vector:</strong> NetworkAccessible</td>
</tr>
<tr>
<td><strong>Access Complexity:</strong> Low</td>
</tr>
<tr>
<td><strong>Authentication:</strong> None</td>
</tr>
<tr>
<td><strong>Confidentiality Impact:</strong> Partial</td>
</tr>
<tr>
<td><strong>Integrity Impact:</strong> None</td>
</tr>
<tr>
<td><strong>Availability Impact:</strong> None</td>
</tr>
<tr>
<td><strong>Exploitability:</strong> NotDefined</td>
</tr>
<tr>
<td><strong>Remediation Level:</strong> NotDefined</td>
</tr>
<tr>
<td><strong>Report Confidence:</strong> NotDefined</td>
</tr>
<tr>
<td><strong>Availability Requirement:</strong> NotDefined</td>
</tr>
<tr>
<td><strong>Collateral Damage Potential:</strong> NotDefined</td>
</tr>
<tr>
<td><strong>Confidentiality Requirement:</strong> NotDefined</td>
</tr>
<tr>
<td><strong>Integrity Requirement:</strong> NotDefined</td>
</tr>
<tr>
<td><strong>Target Distribution:</strong> NotDefined</td>
</tr>
</tbody>
</table>

### CWE

- **CWE:** CWE-538

### Affected item

- **/index.zip**

### Affected parameter

---

#### Credit card number disclosed (verified)

This alert may be a false positive, manual confirmation is required.

The response contains one or more credit card numbers. The credit card numbers were validated using the Luhn algorithm to make sure they are real credit card numbers.
**CVSS2**

- **Base Score:** 4.3
- **Access Vector:** NetworkAccessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** NotDefined
- **Remediation Level:** NotDefined
- **Report Confidence:** NotDefined
- **Availability Requirement:** NotDefined
- **Collateral Damage Potential:** NotDefined
- **Confidentiality Requirement:** NotDefined
- **Integrity Requirement:** NotDefined
- **Target Distribution:** NotDefined

**CVSS3**

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

**CWE**

- **CWE-200**

**Affected item**

/userinfo.php

**Affected parameter**

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** NetworkAccessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** NotDefined
- **Remediation Level:** NotDefined
- **Report Confidence:** NotDefined
- **Availability Requirement:** NotDefined
- **Collateral Damage Potential:** NotDefined
- **Confidentiality Requirement:** NotDefined
- **Integrity Requirement:** NotDefined
- **Target Distribution:** NotDefined

**CVSS3**

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
<th>Access Vector: Network_accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Complexity: Low</td>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

**CWE**

CWE-538

**Affected item**

/.idea/

**Affected parameter**

/.idea/scopes/
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
</table>

| Affected item | /admin/ |

| Affected parameter | |

#### CVSS2

Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

#### CVSS3

Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
</table>

| Affected item | /Connections/ |

| Affected parameter | |
### CVSS2
- **Base Score**: 5.0
- **Access Vector**: Network accessible
- **Access Complexity**: Low
- **Authentication**: None
- **Confidentiality Impact**: Partial
- **Integrity Impact**: None
- **Availability Impact**: None
- **Exploitability**: Not_defined
- **Remediation Level**: Not_defined
- **Report Confidence**: Not_defined
- **Availability Requirement**: Not_defined
- **Collateral Damage Potential**: Not_defined
- **Confidentiality Requirement**: Not_defined
- **Integrity Requirement**: Not_defined
- **Target Distribution**: Not_defined

### CVSS3
- **Base Score**: 7.5
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Unchanged
- **Confidentiality Impact**: High
- **Integrity Impact**: None
- **Availability Impact**: None

### CWE
- **CWE**: CWE-538

#### Affected item
/CVS/

#### Affected parameter

---

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**Directory listing (verified)**

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Flash/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**CVSS2**

- Base Score: 5.0
- Access Vector: Network_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitation: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**

- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/images/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>
### CVSS2
- **Base Score**: 5.0
- **Access Vector**: Network accessible
- **Access Complexity**: Low
- **Authentication**: None
- **Confidentiality Impact**: Partial
- **Integrity Impact**: None
- **Availability Impact**: None
- **Exploitability**: Not defined
- **Remediation Level**: Not defined
- **Report Confidence**: Not defined
- **Availability Requirement**: Not defined
- **Collateral Damage Potential**: Not defined
- **Confidentiality Requirement**: Not defined
- **Integrity Requirement**: Not defined
- **Target Distribution**: Not defined

### CVSS3
- **Base Score**: 7.5
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Unchanged
- **Confidentiality Impact**: High
- **Integrity Impact**: None
- **Availability Impact**: None

### CWE
- **CWE-538**

**Affected item**
/Mod_Rewrite_Shop/images/

**Affected parameter**

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
| CVSS3          | Base Score: 7.5  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: High  
|               | Integrity Impact: None  
|               | Availability Impact: None  
| CWE           | CWE-538  
| Affected item | /pictures/  
| Affected parameter |  

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

| CVSS2          | Base Score: 5.0  
|               | Access Vector: Network_accessable  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

| CVSS3          | Base Score: 7.5  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: High  
|               | Integrity Impact: None  
|               | Availability Impact: None  
| CWE           | CWE-538  
| Affected item | /Templates/  
| Affected parameter |  

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### CVSS2
- Base Score: 5.0
- Access Vector: Networkaccessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

### CVSS3
- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

### CWE
- CWE-538

#### Affected item
/wvstests/

#### Affected parameter

---
**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

---

### CVSS2
- Base Score: 5.0
- Access Vector: Networkaccessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined
Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the
Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Base Score: 5.3</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CWE**

CWE-200

**Affected item**

AJAX/infoartist.php

**Affected parameter**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

This alert requires manual confirmation.

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

This alert requires manual confirmation.

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

This alert requires manual confirmation.

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.
**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

<table>
<thead>
<tr>
<th>CWE-200</th>
</tr>
</thead>
</table>

**Affected item**

<table>
<thead>
<tr>
<th>/AJAX/infocateg.php</th>
</tr>
</thead>
</table>

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

<table>
<thead>
<tr>
<th>CWE-200</th>
</tr>
</thead>
</table>

**Affected item**

<table>
<thead>
<tr>
<th>/AJAX/infotitle.php</th>
</tr>
</thead>
</table>

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
<tr>
<td>CVSS3</td>
<td>Base Score: 5.3</td>
</tr>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE       | CWE-200 |

Affected item       | /Connections/DB_Connection.php |

Affected parameter

Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-200</td>
</tr>
<tr>
<td>Affected item</td>
<td>/secured/database_connect.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**JetBrains .idea project directory**

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-538</td>
</tr>
<tr>
<td>Affected item</td>
<td>Web Server</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**PHP errors enabled (verified)**

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found that the PHP `display_errors` directive is enabled.
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE | CWE-16  
| Affected item | /secured/phpinfo.php |
| Affected parameter |  |

**PHPinfo page (verified)**

PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  |

| CWE   | CWE-200  |

**Affected item**  
/secured/phpinfo.php  

**Affected parameter**

---

**PHPinfo page found**

This script is using `phpinfo()` function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  |

| CWE   | CWE-200  |

**Affected item**  
/secured/phpinfo.php  

**Affected parameter**

---

**Source code disclosure**

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.
| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-538 |
| Affected item | /index.bak |
| Affected parameter | |

**Source code disclosure**

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.
### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-538

### Affected item

- **Affected item:** /pictures/wp-config.bak

### Affected parameter

---

**WS_FTP log file found (verified)**

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CWE

- **CWE:** CWE-538

### Affected item

- **Affected item:** /pictures/WS_FTP.LOG

### Affected parameter

---

**MySQL username disclosure**

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.
**MySQL username disclosure**

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

---

**Possible sensitive directories**

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS2</td>
<td>5.0</td>
<td>Network accessible</td>
<td>Low</td>
<td>None</td>
<td>Partial</td>
<td>None</td>
<td>None</td>
<td>Not_defined</td>
<td>Not_defined</td>
<td>Not_defined</td>
<td>Not_defined</td>
<td>Not_defined</td>
<td>Not_defined</td>
<td>Not_defined</td>
<td>Not_defined</td>
</tr>
<tr>
<td>CVSS3</td>
<td>7.5</td>
<td>Network</td>
<td>Low</td>
<td>None</td>
<td>High</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>Not_defined</td>
<td>Not_defined</td>
<td>Not_defined</td>
<td>Not_defined</td>
<td>Not_defined</td>
</tr>
<tr>
<td>CWE</td>
<td>CWE-200</td>
<td>/admin/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Possible sensitive directories**

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE   | CWE-200  
| Affected item | /CVS/  
| Affected parameter |  

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE   | CWE-200  
| Affected item | /hpp/test.php  
| Affected parameter |  

Possible virtual host found

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.
This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

| CWE                        | CWE-200 |

**Affected item**

**Web Server**

**Affected parameter**

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>
### CVSS3

| Base Score: 0.0 |
| Attack Vector: Network |
| Attack Complexity: Low |
| Privileges Required: None |
| User Interaction: None |
| Scope: Unchanged |
| Confidentiality Impact: None |
| Integrity Impact: None |
| Availability Impact: None |

### CWE

| CWE-200 |
| Affected item | Web Server |
| Affected parameter |

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### CVSS2

| Base Score: 0.0 |
| Access Vector: Network_accessible |
| Access Complexity: Low |
| Authentication: None |
| Confidentiality Impact: None |
| Integrity Impact: None |
| Availability Impact: None |
| Exploitability: Not_defined |
| Remediation Level: Not_defined |
| Report Confidence: Not_defined |
| Availability Requirement: Not_defined |
| Collateral Damage Potential: Not_defined |
| Confidentiality Requirement: Not_defined |
| Integrity Requirement: Not_defined |
| Target Distribution: Not_defined |

### CVSS3

| Base Score: 0.0 |
| Attack Vector: Network |
| Attack Complexity: Low |
| Privileges Required: None |
| User Interaction: None |
| Scope: Unchanged |
| Confidentiality Impact: None |
| Integrity Impact: None |
| Availability Impact: None |

### CWE

| CWE-200 |
| Affected item | /404.php |
| Affected parameter |

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS2 | Base Score: 0.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|-----|-----|
| CVSS3 | Base Score: 0.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /artists.php |
| Affected parameter | |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|-----|-----|


| CVSS3 | Base Score: 0.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: None  
| Integrity Impact: None  
| Availability Impact: None |

| CWE | CWE-200 |

**Affected item**  
/cart.php  

**Affected parameter**  

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
| Access Vector: Network_accessable  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: None  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CVSS3 | Base Score: 0.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: None  
| Integrity Impact: None  
| Availability Impact: None |

| CWE | CWE-200 |

**Affected item**  
/categories.php  

**Affected parameter**  

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
CVSS2

Base Score: 0.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 0.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item
/disclaimer.php

Affected parameter

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CVSS2

Base Score: 0.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
</table>
| Base Score: 0.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitation: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined | Base Score: 0.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None |

CWE  
CWE-200  
Affected item /index.php  
Affected parameter

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
</table>
| Base Score: 0.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitation: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-200</th>
</tr>
</thead>
</table>

**Affected item**

/`logout.php`

**Affected parameter**

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like `myname@mydomain.com` and then record any addresses found.
### CVSS3

- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

### Affected item

- **/product.php**

### Affected parameter

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE   | CWE-200  
| Affected item | /signup.php  
| Affected parameter | |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
<p>|       | Target Distribution: Not_defined |</p>
<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector:</td>
</tr>
<tr>
<td></td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Templates/main_dynamic_template.dwt.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector:</td>
</tr>
<tr>
<td></td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**Microsoft Office possible sensitive information**

This document has been converted to HTML using Microsoft Office. It seems that Office has included sensitive information during the conversion.
| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |

**Affected item**
/secured/office.htm

**Affected parameter**

---

### Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

| CVSS2 | Base Score: 0.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE   | CWE-200  
| Affected item | Web Server  
| Affected parameter | form1  

**Password type input with auto-complete enabled**

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessable  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE   | CWE-200  
| Affected item | Web Server  
| Affected parameter | loginform  

**Possible internal IP address disclosure**

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE-200**

**Affected item**

/404.php

**Affected parameter**

---

### Possible internal IP address disclosure

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | /pictures/ipaddresses.txt  
| Affected parameter |  

**Possible internal IP address disclosure**

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CWE | CWE-200  
| Affected item | /secured/phpinfo.php  
| Affected parameter |  

**Possible server path disclosure (Unix)**

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.
This alert may be a false positive, manual confirmation is required.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200  
Affected item | /pictures/path-disclosure-unix.html  
Affected parameter |

**Possible server path disclosure (Unix)**

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
**CVSS3**

Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None

**CWE**

CWE-200

**Affected item**

/secured/phpinfo.php

**Affected parameter**

**Possible username or password disclosure**

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

**CVSS2**

Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

**CVSS3**

Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None

**CWE**

CWE-200

**Affected item**

/pictures/credentials.txt

**Affected parameter**

**(9.1.2) Access to networks and network services**

Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

No alerts in this category.
Management of privileged access rights

The allocation and use of privileged access rights shall be restricted and controlled.

Total number of alerts in this category: 23

Alerts in this category

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

| CVSS2                  | Base Score: 2.6 |
|                       | Access Vector: Network_accessible |
|                       | Access Complexity: High |
|                       | Authentication: None |
|                       | Confidentiality Impact: None |
|                       | Integrity Impact: Partial |
|                       | Availability Impact: None |
|                       | Exploitability: Not_defined |
|                       | Remediation Level: Not_defined |
|                       | Report Confidence: Not_defined |
|                       | Availability Requirement: Not_defined |
|                       | Collateral Damage Potential: Not_defined |
|                       | Confidentiality Requirement: Not_defined |
|                       | Integrity Requirement: Not_defined |
|                       | Target Distribution: Not_defined |

| CVSS3                  | Base Score: 4.3 |
|                       | Attack Vector: Network |
|                       | Attack Complexity: Low |
|                       | Privileges Required: None |
|                       | User Interaction: Required |
|                       | Scope: Unchanged |
|                       | Confidentiality Impact: None |
|                       | Integrity Impact: Low |
|                       | Availability Impact: None |

CWE

CWE-352

Affected item /404.php

Affected parameter <empty>
Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: High</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 4.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: Required</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

CWE-352

**Affected item**

/artist.php

**Affected parameter**

<empty>

---

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.
### CVSS3
- **Base Score:** 4.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** Required
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE:** CWE-352

### Affected item
- **/categories.php**

### Affected parameter
- `<empty>`

---

**HTML form without CSRF protection**

This alert requires manual confirmation.

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

---

### CVSS2
- **Base Score:** 2.6
- **Access Vector:** Network accessible
- **Access Complexity:** High
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 4.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** Required
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE:** CWE-352

### Affected item
- **/comment.php**

### Affected parameter
- **fComment**

---

**HTML form without CSRF protection**
This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

| CVSS2         | Base Score: 2.6  
|              | Access Vector: Network_accessible  
|              | Access Complexity: High  
|              | Authentication: None  
|              | Confidentiality Impact: None  
|              | Integrity Impact: Partial  
|              | Availability Impact: None  
|              | Exploitability: Not_defined  
|              | Remediation Level: Not_defined  
|              | Report Confidence: Not_defined  
|              | Availability Requirement: Not_defined  
|              | Collateral Damage Potential: Not_defined  
|              | Confidentiality Requirement: Not_defined  
|              | Integrity Requirement: Not_defined  
|              | Target Distribution: Not_defined  

| CVSS3         | Base Score: 4.3  
|              | Attack Vector: Network  
|              | Attack Complexity: Low  
|              | Privileges Required: None  
|              | User Interaction: Required  
|              | Scope: Unchanged  
|              | Confidentiality Impact: None  
|              | Integrity Impact: Low  
|              | Availability Impact: None  

| CWE           | CWE-352  

| Affected item | /disclaimer.php  
| Affected parameter | <empty>  

### HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.
### CVSS2
- **Base Score:** 2.6
- **Access Vector:** Network_accessible
- **Access Complexity:** High
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 4.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** Required
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE-352**
- **Affected item:** `/guestbook.php`
- **Affected parameter:** `<empty>`

#### HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.
### CVSS3

- **Base Score:** 4.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** Required
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE

- **CWE-352**

### Affected item

- **/guestbook.php**

### Affected parameter

- **faddentry**

---

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim’s browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

### CVSS2

- **Base Score:** 2.6
- **Access Vector:** Network accessible
- **Access Complexity:** High
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 4.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** Required
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE

- **CWE-352**

### Affected item

- **/hpp/**

### Affected parameter

- **<empty>**
This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: High</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 4.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: Required</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-352</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/hpp/index.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>&lt;empty&gt;</td>
</tr>
</tbody>
</table>

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.
### CVSS2

- **Base Score**: 2.6
- **Access Vector**: Network accessible
- **Access Complexity**: High
- **Authentication**: None
- **Confidentiality Impact**: None
- **Integrity Impact**: Partial
- **Availability Impact**: None
- **Exploitability**: Not_defined
- **Remediation Level**: Not_defined
- **Report Confidence**: Not_defined
- **Availability Requirement**: Not_defined
- **Collateral Damage Potential**: Not_defined
- **Confidentiality Requirement**: Not_defined
- **Integrity Requirement**: Not_defined
- **Target Distribution**: Not_defined

### CVSS3

- **Base Score**: 4.3
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: Required
- **Scope**: Unchanged
- **Confidentiality Impact**: None
- **Integrity Impact**: Low
- **Availability Impact**: None

### CWE

- **CWE**: CWE-352

#### Affected item

/index.php

#### Affected parameter

<empty>

### HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.
### CVSS3
Base Score: 4.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: Required  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: Low  
Availability Impact: None

### CWE
CWE-352

### Affected item
/listproducts.php

### Affected parameter
<empty>

---

#### HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

---

### CVSS2
Base Score: 2.6  
Access Vector: Network_accessible  
Access Complexity: High  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: Partial  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

---

### CVSS3
Base Score: 4.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: Required  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: Low  
Availability Impact: None

### CWE
CWE-352

### Affected item
/login.php

### Affected parameter
<empty>
Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 2.6</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: High</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 4.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: Required</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

CWE       
CWE-352

Affected item /login.php 
Affected parameter loginform 

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
### CVSS2
- **Base Score**: 2.6
- **Access Vector**: Network accessible
- **Access Complexity**: High
- **Authentication**: None
- **Confidentiality Impact**: None
- **Integrity Impact**: Partial
- **Availability Impact**: None
- **Exploitability**: Not defined
- **Remediation Level**: Not defined
- **Report Confidence**: Not defined
- **Availability Requirement**: Not defined
- **Collateral Damage Potential**: Not defined
- **Confidentiality Requirement**: Not defined
- **Integrity Requirement**: Not defined
- **Target Distribution**: Not defined

### CVSS3
- **Base Score**: 4.3
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: Required
- **Scope**: Unchanged
- **Confidentiality Impact**: None
- **Integrity Impact**: Low
- **Availability Impact**: None

### CWE
- **CWE-352**

#### Affected item
/\logout.php

#### Affected parameter
<empty>

### HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.
Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim’s browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.
This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
<th>CWE</th>
<th>Affected item</th>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 2.6</td>
<td>Base Score: 4.3</td>
<td>CWE-352</td>
<td>/search.php</td>
<td>&lt;empty&gt;</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Complexity: High</td>
<td>Attack Complexity: Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td>User Interaction: Required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td>Scope: Unchanged</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Target Distribution: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.
# CVSS2

- **Base Score:** 2.6
- **Access Vector:** Network accessible
- **Access Complexity:** High
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

# CVSS3

- **Base Score:** 4.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** Required
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

# CWE

- **CWE:** CWE-352

## Affected item

- **/signup.php**

## Affected parameter

- `<empty>`

---

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

---

# CVSS2

- **Base Score:** 2.6
- **Access Vector:** Network accessible
- **Access Complexity:** High
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined
**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 2.6</td>
<td></td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>High</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 4.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>Required</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Low</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

CWE

CWE-352

Affected item /userinfo.php

Affected parameter <empty>

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.
| CVSS2 | Base Score: 2.6  
|       | Access Vector: Network_accessible  
|       | Access Complexity: High  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 4.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: Required  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None |

| CWE   | CWE-352  
|       | Affected item /userinfo.php  
|       | Affected parameter form1 |

### (9.2.4) Management of secret authentication information of users

The allocation of secret authentication information shall be controlled through a formal management process.

No alerts in this category.

### (9.3.1) Use of secret authentication information

Users shall be required to follow the organization's practices in the use of secret authentication information.

No alerts in this category.

### (9.4.1) Information access restriction

Access to information and application system functions shall be restricted in accordance with the access control policy.

Total number of alerts in this category: 92

**Alerts in this category**

Macromedia Dreamweaver remote database scripts (verified)
Macromedia Dreamweaver has created a directory (_mmServerScripts or _mmDBScripts) that contains scripts for testing database connectivity. One of these scripts (mmhttpdb.php or mmhttpdb.asp) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: High  
|       | Remediation Level: Official_fix  
|       | Report Confidence: Confirmed  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVE | CVE-2004-1893  
| CWE | CWE-16  

**Affected item**: Web Server

**Possible database backup**

Manual confirmation is required for this alert.

It looks like this file contains a database backup/dump. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CWE | CWE-538  
| Affected item | /admin/create.sql  
| Affected parameter |  

**.htaccess file readable (verified)**
This directory contains an `.htaccess` file that is readable. This may indicate a server misconfiguration. `.htaccess` files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/Mod_Rewrite_Shop/</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected parameter</th>
</tr>
</thead>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-200

**Affected item**

Web Server

**Affected parameter**

`/*`<s>/<s>/<n>/

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-200

**Affected item**

Web Server

**Affected parameter**

`/*`<s>/<s>/<n>/
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
</table>

**Affected item**
/cart.php

**Affected parameter**
login

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

### Affected item

- **/cart.php**

### Affected parameter

- **Referer**

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
| CVSS3                  | Base Score: 5.3  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: Low  
| Integrity Impact: None  
| Availability Impact: None |
| CWE                   | CWE-200 |
| Affected item         | /cart.php |
| Affected parameter    | User-Agent |

### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2                  | Base Score: 5.0  
| Access Vector: Network_accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CVSS3                  | Base Score: 5.3  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: Low  
| Integrity Impact: None  
| Availability Impact: None |
| CWE                   | CWE-200 |
| Affected item         | /cart.php |
| Affected parameter    | X-Forwarded-For |
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|-------|--------------------------------------------------|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE   | CWE-200 |
| Affected item | /listproducts.php |
| Affected parameter | artist |
| Variants | 12345\"\";]]*%00[%0d%0a<%00>%bf%27\|"" |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
<th>CWE</th>
</tr>
</thead>
</table>
| Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None | CWE-200 |
| Affected item | /listproducts.php | |
| Affected parameter | cat | |
| Variants | 12345\"\";\"%00\"%0d%0a<%00>%bf%27 tinder | |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

| CWE            | CWE-200           |

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/listproducts.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>login</td>
</tr>
</tbody>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

| CWE            | CWE-200           |

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/listproducts.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>Referer</td>
</tr>
</tbody>
</table>
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2                | Base Score: 5.0
|                     | Access Vector: Network_accessible
|                     | Access Complexity: Low
|                     | Authentication: None
|                     | Confidentiality Impact: Partial
|                     | Integrity Impact: None
|                     | Availability Impact: None
|                     | Exploitability: Not_defined
|                     | Remediation Level: Not_defined
|                     | Report Confidence: Not_defined
|                     | Availability Requirement: Not_defined
|                     | Collateral Damage Potential: Not_defined
|                     | Confidentiality Requirement: Not_defined
|                     | Integrity Requirement: Not_defined
|                     | Target Distribution: Not_defined

| CVSS3                | Base Score: 5.3
|                     | Attack Vector: Network
|                     | Attack Complexity: Low
|                     | Privileges Required: None
|                     | User Interaction: None
|                     | Scope: Unchanged
|                     | Confidentiality Impact: Low
|                     | Integrity Impact: None
|                     | Availability Impact: None

| CWE                  | CWE-200

| Affected item        | /listproducts.php
| Affected parameter   | User-Agent

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2          | Base Score: 5.0  
|               | Access Vector: Network_accessable  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  |
| CVSS3          | Base Score: 5.3  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: Low  
|               | Integrity Impact: None  
|               | Availability Impact: None  |
| CWE            | CWE-200  
| Affected item  | /listproducts.php  
| Affected parameter | X-Forwarded-For  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2          | Base Score: 5.0  
|               | Access Vector: Network_accessable  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  |
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

Application error message

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE
CWE-200
Affected item /product.php
Affected parameter pic

Application error message

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CWE
CWE-200
Affected item /secured/newuser.php
Affected parameter login
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
</table>

**Affected item** /secured/newuser.php

**Affected parameter** signup
**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

---

**CVSS2**

Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

**CVSS3**

Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None

**CWE**

CWE-200  
Affected item: /secured/newuser.php  
Affected parameter: uaddress

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

---

**CVSS2**

Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /secured/newuser.php |
| Affected parameter | ucc |

### Application error message

**This alert requires manual confirmation**

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not defined  
|       | Remediation Level: Not defined  
|       | Report Confidence: Not defined  
|       | Availability Requirement: Not defined  
|       | Collateral Damage Potential: Not defined  
|       | Confidentiality Requirement: Not defined  
|       | Integrity Requirement: Not defined  
|       | Target Distribution: Not defined |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /secured/newuser.php |
| Affected parameter | uemail |
Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

#### Affected item

/secured/newuser.php

#### Affected parameter

uuname

#### Variants

12345"\"%;j]%00[%0d%0a<%00>%bf%270%0a

### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

**CVSS3**

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

**CWE**

CWE-200

**Affected item**
/showimage.php

**Affected parameter**
file

**Variants**
acu4562%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca4562

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined
### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>uaddress</td>
</tr>
<tr>
<td>Variants</td>
<td>12345&quot;&quot;;]]*%00{%0d%0a%0a&gt;%%bf%27\0\0\0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>uaddress</td>
</tr>
<tr>
<td>Variants</td>
<td>12345&quot;&quot;;]]*%00{%0d%0a%0a&gt;%%bf%27\0\0\0</td>
</tr>
</tbody>
</table>
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>5.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>5.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CWE

CWE-200

Affected item /userinfo.php

Affected parameter ucc

Variants 12345\\x27%00%0d%0a<%00>%bf%27\0\0

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-200**

<table>
<thead>
<tr>
<th><strong>Affected item</strong></th>
<th>/userinfo.php</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Affected parameter</strong></td>
<td>uemail</td>
</tr>
<tr>
<td><strong>Variants</strong></td>
<td>12345&quot;&quot;;]]*%00(%0d%0a&lt;%00&gt;%bf%27[i</td>
</tr>
</tbody>
</table>
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | /userinfo.php  
| Affected parameter | uname  
| Variants | 12345"\";]|]*%00{%0d%0a<%00>%bf%27"[]i  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | /userinfo.php  
| Affected parameter | uphone  
| Variants | 12345"\";]|]*%00{%0d%0a<%00>%bf%27"[]i
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE-200**

### Affected item

- `/userinfo.php`

### Affected parameter

- `urname`

### Variants

- `12345"\"\";\[|]\*%00{%0d%0a<%00>%bf%27'ð¡`

### Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.
### CVSS2

<table>
<thead>
<tr>
<th>Base Score</th>
<th>5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not defined</td>
</tr>
</tbody>
</table>

### CWE

| CWE          | CWE-538 |

#### Affected item

| /index.bak |

#### Affected parameter

---

### Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

#### CVSS2

<table>
<thead>
<tr>
<th>Base Score</th>
<th>5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not defined</td>
</tr>
</tbody>
</table>

#### CWE

| CWE          | CWE-538 |

#### Affected item

| /index.zip |

#### Affected parameter

---

### Credit card number disclosed (verified)

This alert may be a false positive, manual confirmation is required.

The response contains one or more credit card numbers. The credit card numbers were validated using the Luhn algorithm to make sure they are real credit card numbers.
| CVSS2 | Base Score: 4.3  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | /userinfo.php  
| Affected parameter |  

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  

109
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 7.5</td>
</tr>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE (CWE-538)

<table>
<thead>
<tr>
<th>Affected item</th>
</tr>
</thead>
<tbody>
<tr>
<td>/.idea/</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>/idea/scopes/</td>
</tr>
</tbody>
</table>
CVSS2

**Base Score:** 5.0  
**Access Vector:** Network_accessible  
**Access Complexity:** Low  
**Authentication:** None  
**Confidentiality Impact:** Partial  
**Integrity Impact:** None  
**Availability Impact:** None  
**Exploitability:** Not_defined  
**Remediation Level:** Not_defined  
**Report Confidence:** Not_defined  
**Availability Requirement:** Not_defined  
**Collateral Damage Potential:** Not_defined  
**Confidentiality Requirement:** Not_defined  
**Integrity Requirement:** Not_defined  
**Target Distribution:** Not_defined

CVSS3

**Base Score:** 7.5  
**Attack Vector:** Network  
**Attack Complexity:** Low  
**Privileges Required:** None  
**User Interaction:** None  
**Scope:** Unchanged  
**Confidentiality Impact:** High  
**Integrity Impact:** None  
**Availability Impact:** None

CWE

**CWE-538**

**Affected item**
/_mmServerScripts/

**Affected parameter**

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/admin/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

#### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

#### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Connections/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>
**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

**CVSS3**

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

**CWE**

- **CWE-538**

**Affected item**

/CVS/

**Affected parameter**

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Flash/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**CVSS2**

- Base Score: 5.0
- Access Vector: Network_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**

- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |

CWE | CWE-538 |

**Affected item** | `/wvstests/` |
**Affected parameter** | |

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the
Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2          | Base Score: 5.0  |
|               | Access Vector: Network_accessible |
|               | Access Complexity: Low |
|               | Authentication: None |
|               | Confidentiality Impact: Partial |
|               | Integrity Impact: None |
|               | Availability Impact: None |
|               | Exploitability: Not_defined |
|               | Remediation Level: Not_defined |
|               | Report Confidence: Not_defined |
|               | Availability Requirement: Not_defined |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined |
|               | Target Distribution: Not_defined |

| CVSS3          | Base Score: 5.3  |
|               | Attack Vector: Network |
|               | Attack Complexity: Low |
|               | Privileges Required: None |
|               | User Interaction: None |
|               | Scope: Unchanged |
|               | Confidentiality Impact: Low |
|               | Integrity Impact: None |
|               | Availability Impact: None |

CWE: CWE-200

Affected item: /AJAX/infoartist.php

Affected parameter

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### CVSS3
- **Base Score**: 5.3
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Unchanged
- **Confidentiality Impact**: Low
- **Integrity Impact**: None
- **Availability Impact**: None

### CWE
- **CWE**: CWE-200

### Affected item
- **/AJAX/infocateg.php**

### Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

### CVSS2
- **Base Score**: 5.0
- **Access Vector**: Network_accessible
- **Access Complexity**: Low
- **Authentication**: None
- **Confidentiality Impact**: Partial
- **Integrity Impact**: None
- **Availability Impact**: None
- **Exploitability**: Not_defined
- **Remediation Level**: Not_defined
- **Report Confidence**: Not_defined
- **Availability Requirement**: Not_defined
- **Collateral Damage Potential**: Not_defined
- **Confidentiality Requirement**: Not_defined
- **Integrity Requirement**: Not_defined
- **Target Distribution**: Not_defined

### CVSS3
- **Base Score**: 5.3
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Unchanged
- **Confidentiality Impact**: Low
- **Integrity Impact**: None
- **Availability Impact**: None

### CWE
- **CWE**: CWE-200

### Affected item
- **/AJAX/infotitle.php**

### Error message on page
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
</table>

| Affected item | /Connections/DB_Connection.php |

| Affected parameter | |

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE   | CWE-200  
| Affected item | /pictures/path-disclosure-unix.html  
| Affected parameter |  

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**JetBrains .idea project directory**

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

**PHP errors enabled (verified)**

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found that the PHP `display_errors` directive is enabled.
### CVSS2
Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

### CVSS3
Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None

### CWE
CWE-16

Affected item  
/secured/phpinfo.php

Affected parameter

### PHPinfo page (verified)
PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE | CWE-200 |

| Affected item | /secured/phpinfo.php |
| Affected parameter |

**PHPinfo page found**

This script is using `phpinfo()` function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE | CWE-200 |

| Affected item | /secured/phpinfo.php |
| Affected parameter |

**Source code disclosure**

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-538**

**Affected item**
- `/index.bak`

**Affected parameter**

### Source code disclosure

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined
| CVSS3 | Base Score: 7.5  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: High  
| Integrity Impact: None  
| Availability Impact: None |
| CWE | CWE-538 |
| Affected item | /pictures/wp-config.bak |
| Affected parameter |

**WS_FTP log file found (verified)**

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

| CVSS2 | Base Score: 5.0  
| Access Vector: Network accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |
| CWE | CWE-538 |
| Affected item | /pictures/WS_FTP.LOG |
| Affected parameter |

**MySQL username disclosure**

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.
For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
| CVSS2          | Base Score: 5.0  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  
| CVSS3          | Base Score: 7.5  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: High  
|               | Integrity Impact: None  
|               | Availability Impact: None  
| CWE            | CWE-200  
| Affected item  | /admin/  
| Affected parameter |  

### Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

**Affected item**

- `/CVS/`

**Affected parameter**

**Possible sensitive files**

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

**Affected item**

- `/hpp/test.php`

**Affected parameter**

**Possible virtual host found**

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.
This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200|
| Affected item | Web Server |
| Affected parameter | |

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

CWE-200

### Affected item

Web Server

### Affected parameter

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### Email address found

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### Email address found

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

CWE-200

### Affected item

/404.php

### Affected parameter

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  

**CWE**

CWE-200

**Affected item**

/artists.php

**Affected parameter**

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3          | Base Score: 0.0  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: None  
|               | Integrity Impact: None  
|               | Availability Impact: None  
| CWE            | CWE-200  
| Affected item  | /cart.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2          | Base Score: 0.0  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: None  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

| CVSS3          | Base Score: 0.0  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: None  
|               | Integrity Impact: None  
|               | Availability Impact: None  
| CWE            | CWE-200  
| Affected item  | /categories.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS2 | Base Score: 0.0  
|    | Access Vector: Network_accessible  
|    | Access Complexity: Low  
|    | Authentication: None  
|    | Confidentiality Impact: None  
|    | Integrity Impact: None  
|    | Availability Impact: None  
|    | Exploitability: Not_defined  
|    | Remediation Level: Not_defined  
|    | Report Confidence: Not_defined  
|    | Availability Requirement: Not_defined  
|    | Collateral Damage Potential: Not_defined  
|    | Confidentiality Requirement: Not_defined  
|    | Integrity Requirement: Not_defined  
|    | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 0.0  
|    | Attack Vector: Network  
|    | Attack Complexity: Low  
|    | Privileges Required: None  
|    | User Interaction: None  
|    | Scope: Unchanged  
|    | Confidentiality Impact: None  
|    | Integrity Impact: None  
|    | Availability Impact: None  |

**CWE**  
CWE-200  

**Affected item**  
/disclaimer.php

**Affected parameter**

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-200 |

**Affected item**

/guestbook.php

**Affected parameter**

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-200 |

**Affected item**

/index.bak

**Affected parameter**

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-200**

**Affected item**
- `/index.php`

**Affected parameter**

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like `myname@mydomain.com` and then record any addresses found.

---

### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
| CVSS3 | Base Score: 0.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: None  
| Integrity Impact: None  
| Availability Impact: None |

| CWE | CWE-200 |

| Affected item | /listproducts.php |
| Affected parameter | |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
| Access Vector: Network_accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: None  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CWE | CWE-200 |

| Affected item | /login.php |
| Affected parameter | |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/product.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/search.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
## CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

## CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

## CWE

<table>
<thead>
<tr>
<th>CWE-200</th>
</tr>
</thead>
</table>

### Affected item

/signup.php

### Affected parameter

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

## CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
CVSS3

Base Score: 0.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item

/Templates/main_dynamic_template.dwt.php

Affected parameter

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CVSS2

Base Score: 0.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 0.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item

/userinfo.php

Affected parameter

Microsoft Office possible sensitive information

This document has been converted to HTML using Microsoft Office. It seems that Office has included sensitive information during the conversion.
**CVSS2**

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

---

**CVSS3**

Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

---

**CWE**

CWE-200

Affected item: /secured/office.htm

Affected parameter:

---

**Password type input with auto-complete enabled**

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

---

**CVSS2**

Base Score: 0.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined
**Password type input with auto-complete enabled**

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

**Possible internal IP address disclosure**

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: NotDefined
Report Confidence: Not_defined
Availability Requirement: NotDefined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

CWE-200

Possible internal IP address disclosure

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Possible server path disclosure (Unix)

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.
This alert may be a false positive, manual confirmation is required.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/pictures/path-disclosure-unix.html</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**Possible server path disclosure (Unix)**

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
### CVSS3

- **Base Score:** 7.5  
- **Attack Vector:** Network  
- **Attack Complexity:** Low  
- **Privileges Required:** None  
- **User Interaction:** None  
- **Scope:** Unchanged  
- **Confidentiality Impact:** High  
- **Integrity Impact:** None  
- **Availability Impact:** None  

### CWE

**CWE-200**

**Affected item:**  
/secured/phpinfo.php

**Affected parameter:**

---

### Possible username or password disclosure

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

---

### CVSS2

- **Base Score:** 5.0  
- **Access Vector:** Network_accessible  
- **Access Complexity:** Low  
- **Authentication:** None  
- **Confidentiality Impact:** Partial  
- **Integrity Impact:** None  
- **Availability Impact:** None  
- **Exploitability:** Not_defined  
- **Remediation Level:** Not_defined  
- **Report Confidence:** Not_defined  
- **Availability Requirement:** Not_defined  
- **Collateral Damage Potential:** Not_defined  
- **Confidentiality Requirement:** Not_defined  
- **Integrity Requirement:** Not_defined  
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 7.5  
- **Attack Vector:** Network  
- **Attack Complexity:** Low  
- **Privileges Required:** None  
- **User Interaction:** None  
- **Scope:** Unchanged  
- **Confidentiality Impact:** High  
- **Integrity Impact:** None  
- **Availability Impact:** None

### CWE

**CWE-200**

**Affected item:**  
/pictures/credentials.txt

**Affected parameter:**

---

### (9.4.2) Secure log-on procedures

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

No alerts in this category.
(9.4.3) Password management system

Password management systems shall be interactive and shall ensure quality passwords.

No alerts in this category.

(9.4.4) Use of privileged utility programs

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

No alerts in this category.

(9.4.5) Access control to program source code

Access to program source code shall be restricted.

Total number of alerts in this category: 6

Alerts in this category

Directory traversal (verified)

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE

CWE-22

Affected item /showimage.php
Affected parameter file
Variants ../../../../../../../../../../../../../proc/version

File inclusion

This script is possibly vulnerable to file inclusion attacks.

It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.

CVSS2

Base Score: 7.5
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CWE

CWE-20

Affected item /showimage.php
Affected parameter file
Variants showimage.php

JetBrains .idea project directory

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.
Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.
Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

| CVSS2 | Base Score: 5.0  
| Access Vector: Network_accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CVSS3 | Base Score: 7.5  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: High  
| Integrity Impact: None  
| Availability Impact: None |

| CWE | CWE-538 |

| Affected item | /pictures/wp-config.bak |
| Affected parameter |

---

WS_FTP log file found (verified)

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

| CVSS2 | Base Score: 5.0  
| Access Vector: Network_accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CWE | CWE-538 |

| Affected item | /pictures/WS_FTP.LOG |
| Affected parameter |
Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

Total number of alerts in this category: 7

Alerts in this category

Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Affected item</th>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>/index.bak</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CWE</td>
<td>CWE-538</td>
<td></td>
</tr>
</tbody>
</table>

Affected parameter

Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Affected item</th>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>/index.zip</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CWE</td>
<td>CWE-538</td>
<td></td>
</tr>
</tbody>
</table>

Affected parameter
**JetBrains .idea project directory**

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

| CVSS2          | Base Score: 5.0  
|                | Access Vector: Network_accessible  
|                | Access Complexity: Low  
|                | Authentication: None  
|                | Confidentiality Impact: Partial  
|                | Integrity Impact: None  
|                | Availability Impact: None  
|                | Exploitability: Not_defined  
|                | Remediation Level: Not_defined  
|                | Report Confidence: Not_defined  
|                | Availability Requirement: Not_defined  
|                | Collateral Damage Potential: Not_defined  
|                | Confidentiality Requirement: Not_defined  
|                | Integrity Requirement: Not_defined  
|                | Target Distribution: Not_defined  

**CWE**  
CWE-538  

**Affected item**  
**Web Server**

**Affected parameter**

---

**PHPinfo page (verified)**

PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

| CVSS2          | Base Score: 5.0  
|                | Access Vector: Network_accessible  
|                | Access Complexity: Low  
|                | Authentication: None  
|                | Confidentiality Impact: Partial  
|                | Integrity Impact: None  
|                | Availability Impact: None  
|                | Exploitability: Not_defined  
|                | Remediation Level: Not_defined  
|                | Report Confidence: Not_defined  
|                | Availability Requirement: Not_defined  
|                | Collateral Damage Potential: Not_defined  
|                | Confidentiality Requirement: Not_defined  
|                | Integrity Requirement: Not_defined  
|                | Target Distribution: Not_defined  

**CVSS3**

Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None

**CWE**

CWE-200

Affected item /secured/phpinfo.php

Affected parameter

---

**PHPinfo page found**

This script is using phpinfo() function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

**CVSS2**

Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

---

**WS_FTP log file found (verified)**

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.
### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-538</th>
</tr>
</thead>
</table>

**Affected item**  
/pictures/WS_FTP.LOG

**Affected parameter**

### Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-200</th>
</tr>
</thead>
</table>

**Affected item**  
/hpp/test.php

**Affected parameter**

(12.2.1) Controls against malware
Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

No alerts in this category.

(12.4.2) Protection of log information

Logging facilities and log information shall be protected against tampering and unauthorized access.

Total number of alerts in this category: 92

Alerts in this category

Macromedia Dreamweaver remote database scripts (verified)

Macromedia Dreamweaver has created a directory (_mmServerScripts or _mmDBScripts) that contains scripts for testing database connectivity. One of these scripts (mmhttpdb.php or mmhttpdb.asp) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: High  
|       | Remediation Level: Official_fix  
|       | Report Confidence: Confirmed  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVE   | CVE-2004-1893  
| CWE   | CWE-16  

Affected item: Web Server

Possible database backup

Manual confirmation is required for this alert.

It looks like this file contains a database backup/dump. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.
This directory contains an `.htaccess` file that is readable. This may indicate a server misconfiguration. `.htaccess` files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

---

**.htaccess file readable (verified)**

This directory contains an `.htaccess` file that is readable. This may indicate a server misconfiguration. `.htaccess` files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | Web Server  
| Affected parameter | /*].php  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

## CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

## CWE

- **CWE-200**

## Affected item

**Web Server**

## Affected parameter

/[*]/<s>/<s>/</n>/

### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

## CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: NotDefined</td>
</tr>
<tr>
<td>Confidentiality Requirement: NotDefined</td>
</tr>
<tr>
<td>Integrity Requirement: NotDefined</td>
</tr>
<tr>
<td>Target Distribution: NotDefined</td>
</tr>
</tbody>
</table>

## CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

## CWE

- **CWE-200**

## Affected item

/cart.php

## Affected parameter

login
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE  | CWE-200  
| Affected item | /cart.php  
| Affected parameter | Referer  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /cart.php |
| Affected parameter | User-Agent |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

Application error message

```
Variants
12345"\n\n);[|]*%00{%0d%0a<%00>%bf%27\d\n\n
```
Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  

CWE  
CWE-200  

| Affected item | /listproducts.php  
| Affected parameter | cat  
| Variants | 12345"\"%;]]*%00[%0d%0a<%00>%bf%27"[]|

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE   | CWE-200 |
| Affected item | /listproducts.php |
| Affected parameter | login |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE  | CWE-200 |
| Affected item | /listproducts.php |
| Affected parameter | Referer |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE  | CWE-200 |
| Affected item | /listproducts.php |
| Affected parameter | User-Agent |
Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the ‘Attack details’ section for more information about the affected page.

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**CVSS2**

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

**CVSS3**

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

**CWE**

CWE-200

**Affected item**

/listproducts.php

**Affected parameter**

X-Forwarded-For
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE | CWE-200 |

**Affected item**  
/product.php  

**Affected parameter**  
pic

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS3                      | Base Score: 5.3  
|                           | Attack Vector: Network  
|                           | Attack Complexity: Low  
|                           | Privileges Required: None  
|                           | User Interaction: None  
|                           | Scope: Unchanged  
|                           | Confidentiality Impact: Low  
|                           | Integrity Impact: None  
|                           | Availability Impact: None |
| CWE                       | CWE-200             |
| Affected item             | /secured/newuser.php |
| Affected parameter        | login               |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2                      | Base Score: 5.0  
|                           | Access Vector: Network_accessible  
|                           | Access Complexity: Low  
|                           | Authentication: None  
|                           | Confidentiality Impact: Partial  
|                           | Integrity Impact: None  
|                           | Availability Impact: None  
|                           | Exploitability: Not_defined  
|                           | Remediation Level: Not_defined  
|                           | Report Confidence: Not_defined  
|                           | Availability Requirement: Not_defined  
|                           | Collateral Damage Potential: Not_defined  
|                           | Confidentiality Requirement: Not_defined  
|                           | Integrity Requirement: Not_defined  
|                           | Target Distribution: Not_defined |

| CVSS3                      | Base Score: 5.3  
|                           | Attack Vector: Network  
|                           | Attack Complexity: Low  
|                           | Privileges Required: None  
|                           | User Interaction: None  
|                           | Scope: Unchanged  
|                           | Confidentiality Impact: Low  
|                           | Integrity Impact: None  
|                           | Availability Impact: None |
| CWE                       | CWE-200             |
| Affected item             | /secured/newuser.php |
| Affected parameter        | signup               |
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Base Score: 5.3</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Target Distribution: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

CWE

CWE-200

Affected item

/secure/newuser.php

Affected parameter

uaddress
**CVSS2**

Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined  

**CVSS3**

Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None  

**CWE**

CWE-200  

**Affected item**
/secured/newuser.php  

**Affected parameter**
ucc  

**Application error message**

This alert requires manual confirmation  

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.  

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE  | CWE-200 |
| Affected item | /secured/newuser.php |
| Affected parameter | uemail |

### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE  | CWE-200 |
| Affected item | /secured/newuser.php |
| Affected parameter | uuname |
| Variants | `12345\"\";||*\%00\%0d\%0a<\%00>\%bf%27\%8\%9i` |
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CWE: CWE-200

Affected item: /showimage.php

Affected parameter: file

Variants: acu4562%EF%BC%9Cs1%EF%B9%A5s2%CA%BA3%CA%B9uca4562

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**CVSS2**

<table>
<thead>
<tr>
<th>Base Score</th>
<th>5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score</th>
<th>5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Low</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

**CWE**

| CWE-200 |

**Affected item**

| /userinfo.php |

**Affected parameter**

| script#text |

**Variants**

| 12345"\");||%00{%0d%0a<%00>%bf%278f|

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score</th>
<th>5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>
**Base Score: 5.3**
**Attack Vector: Network**
**Attack Complexity: Low**
**Privileges Required: None**
**User Interaction: None**
**Scope: Unchanged**
**Confidentiality Impact: Low**
**Integrity Impact: None**
**Availability Impact: None**

**CWE**
CWE-200

**Affected item**
/userinfo.php

**Affected parameter**
uaddress

**Variants**
12345"\"];]]%00{%0d%0a<%00>%bf%27%00%0a

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

---

**Base Score: 5.0**
**Access Vector: Network accessible**
**Access Complexity: Low**
**Authentication: None**
**Confidentiality Impact: Partial**
**Integrity Impact: None**
**Availability Impact: None**

**Exploitability: Not defined**
**Remediation Level: Not defined**
**Report Confidence: Not defined**
**Availability Requirement: Not defined**
**Collateral Damage Potential: Not defined**
**Confidentiality Requirement: Not defined**
**Integrity Requirement: Not defined**
**Target Distribution: Not defined**

---

**Base Score: 5.3**
**Attack Vector: Network**
**Attack Complexity: Low**
**Privileges Required: None**
**User Interaction: None**
**Scope: Unchanged**
**Confidentiality Impact: Low**
**Integrity Impact: None**
**Availability Impact: None**

---

**CWE**
CWE-200

**Affected item**
/userinfo.php

**Affected parameter**
ucc

**Variants**
12345"\"];]]%00{%0d%0a<%00>%bf%27%00%0a

---
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Score:</strong> 5.0</td>
<td><strong>Base Score:</strong> 5.3</td>
</tr>
<tr>
<td><strong>Access Vector:</strong> Network_accessible</td>
<td><strong>Attack Vector:</strong> Network</td>
</tr>
<tr>
<td><strong>Access Complexity:</strong> Low</td>
<td><strong>Attack Complexity:</strong> Low</td>
</tr>
<tr>
<td><strong>Authentication:</strong> None</td>
<td><strong>Privileges Required:</strong> None</td>
</tr>
<tr>
<td><strong>Confidentiality Impact:</strong> Partial</td>
<td><strong>User Interaction:</strong> None</td>
</tr>
<tr>
<td><strong>Integrity Impact:</strong> None</td>
<td><strong>Scope:</strong> Unchanged</td>
</tr>
<tr>
<td><strong>Availability Impact:</strong> None</td>
<td><strong>Confidentiality Impact:</strong> Low</td>
</tr>
<tr>
<td><strong>Exploitability:</strong> Not_defined</td>
<td><strong>Integrity Impact:</strong> None</td>
</tr>
<tr>
<td><strong>Remediation Level:</strong> Not_defined</td>
<td><strong>Availability Impact:</strong> None</td>
</tr>
<tr>
<td><strong>Report Confidence:</strong> Not_defined</td>
<td><strong>Availability Requirement:</strong> Not_defined</td>
</tr>
<tr>
<td><strong>Availability Requirement:</strong> Not_defined</td>
<td><strong>Collateral Damage Potential:</strong> Not_defined</td>
</tr>
<tr>
<td><strong>Collateral Damage Potential:</strong> Not_defined</td>
<td><strong>Confidentiality Requirement:</strong> Not_defined</td>
</tr>
<tr>
<td><strong>Confidentiality Requirement:</strong> Not_defined</td>
<td><strong>Integrity Requirement:</strong> Not_defined</td>
</tr>
<tr>
<td><strong>Target Distribution:</strong> Not_defined</td>
<td><strong>Target Distribution:</strong> Not_defined</td>
</tr>
</tbody>
</table>

**CWE**

CWE-200

**Affected item**

/userinfo.php

**Affected parameter**

uemail

**Variants**

12345"\"");||\%00\%0d\%0a<\%00>\%bf%27\%0d\%0a

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /userinfo.php |
| Affected parameter | uname |
| Variants | 12345"\"');]]%00{%0d%0a<%00>%bf%27öä |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the ‘Attack details’ section for more information about the affected page.
<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>uphone</td>
</tr>
<tr>
<td>Variants</td>
<td><code>12345&quot;\&quot;;\\*\%00\%0d\%0a&lt;\%00&gt;\%bf%27\%0a\%0a</code></td>
</tr>
</tbody>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>urname</td>
</tr>
<tr>
<td>Variants</td>
<td><code>12345&quot;\&quot;;\\*\%00\%0d\%0a&lt;\%00&gt;\%bf%27\%0a\%0a</code></td>
</tr>
</tbody>
</table>
A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score</th>
<th>5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

### CWE

| CWE | CWE-538 |

**Affected item**

/`index.bak`

**Affected parameter**

---

**Credit card number disclosed (verified)**

This alert may be a false positive, manual confirmation is required.

The response contains one or more credit card numbers. The credit card numbers were validated using the Luhn algorithm to make sure they are real credit card numbers.
### CVSS2

- **Base Score:** 4.3
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE-200**

#### Affected item

/userinfo.php

#### Affected parameter

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not defined  
|       | Remediation Level: Not defined  
|       | Report Confidence: Not defined  
|       | Availability Requirement: Not defined  
|       | Collateral Damage Potential: Not defined  
|       | Confidentiality Requirement: Not defined  
|       | Integrity Requirement: Not defined  
|       | Target Distribution: Not defined |
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE   | CWE-538  
| Affected item | /_mmServerScripts/  
| Affected parameter | |

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/admin/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

### CVSS2
- **Base Score:** 5.0
  - **Access Vector:** Network\_accessible
  - **Access Complexity:** Low
  - **Authentication:** None
  - **Confidentiality Impact:** Partial
  - **Integrity Impact:** None
  - **Availability Impact:** None
  - **Exploitability:** Not\_defined
  - **Remediation Level:** Not\_defined
  - **Report Confidence:** Not\_defined
  - **Availability Requirement:** Not\_defined
  - **Collateral Damage Potential:** Not\_defined
  - **Confidentiality Requirement:** Not\_defined
  - **Integrity Requirement:** Not\_defined
  - **Target Distribution:** Not\_defined

### CVSS3
- **Base Score:** 7.5
  - **Attack Vector:** Network
  - **Attack Complexity:** Low
  - **Privileges Required:** None
  - **User Interaction:** None
  - **Scope:** Unchanged
  - **Confidentiality Impact:** High
  - **Integrity Impact:** None
  - **Availability Impact:** None

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Connections/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>
**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

| CVSS2 | Base Score: 5.0
| Access Vector: Network_accessible
| Access Complexity: Low
| Authentication: None
| Confidentiality Impact: Partial
| Integrity Impact: None
| Availability Impact: None
| Exploitability: Not_defined
| Remediation Level: Not_defined
| Report Confidence: Not_defined
| Availability Requirement: Not_defined
| Collateral Damage Potential: Not_defined
| Confidentiality Requirement: Not_defined
| Integrity Requirement: Not_defined
| Target Distribution: Not_defined |

| CVSS3 | Base Score: 7.5
| Attack Vector: Network
| Attack Complexity: Low
| Privileges Required: None
| User Interaction: None
| Scope: Unchanged
| Confidentiality Impact: High
| Integrity Impact: None
| Availability Impact: None |

CWE

CWE-538

Affected item /CVS/

Affected parameter
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-538 |
| Affected item | /Mod_Rewrite_Shop/images/ |
| Affected parameter | |

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**CVSS2**

- Base Score: 5.0
- Access Vector: NetworkAccessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: NotDefined
- Remediation Level: NotDefined
- Report Confidence: NotDefined
- Availability Requirement: NotDefined
- Collateral Damage Potential: NotDefined
- Confidentiality Requirement: NotDefined
- Integrity Requirement: NotDefined
- Target Distribution: NotDefined

**CVSS3**

- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Base Score: 7.5</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Exploitability: Not defined</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Remediation Level: Not defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not defined</td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td>Target Distribution: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

**CWE**
- CWE-538

**Affected item**
- `/wvstests/

**Affected parameter**

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

CVSS2

| Base Score: 5.0 |
| Access Vector: Network_accessible |
| Access Complexity: Low |
| Authentication: None |
| Confidentiality Impact: Partial |
| Integrity Impact: None |
| Availability Impact: None |
| Exploitability: Not_defined |
| Remediation Level: Not_defined |
| Report Confidence: Not_defined |
| Availability Requirement: Not_defined |
| Collateral Damage Potential: Not_defined |
| Confidentiality Requirement: Not_defined |
| Integrity Requirement: Not_defined |
| Target Distribution: Not_defined |

CVSS3

| Base Score: 7.5 |
| Attack Vector: Network |
| Attack Complexity: Low |
| Privileges Required: None |
| User Interaction: None |
| Scope: Unchanged |
| Confidentiality Impact: High |
| Integrity Impact: None |
| Availability Impact: None |

Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**CVSS2**

Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

**CVSS3**

Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None

**CWE**

CWE-200

Affected item /AJAX/infoartist.php

Affected parameter

---

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**CVSS2**

Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined
Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

| CWE            | CWE-200          |

| Affected item  | /Connections/DB_Connection.php |

| Affected parameter

---

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS2</th>
</tr>
</thead>
</table>
| Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |

**CWE**  
CWE-200  
Affected item /pictures/path-disclosure-unix.html  
Affected parameter

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | /secured/database_connect.php  
| Affected parameter |  

JetBrains .idea project directory

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CWE | CWE-538  
| Affected item | Web Server  
| Affected parameter |  

PHP errors enabled (verified)

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found that the PHP `display_errors` directive is enabled.
**CVSS2**

Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

**CVSS3**

Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None

**CWE**

CWE-16  
Affected item

/secured/phpinfo.php  
Affected parameter

**PHPinfo page (verified)**

PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.
**PHPinfo page found**

This script is using `phpinfo()` function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

**Source code disclosure**

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.
### CVSS2
Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not defined  
Remediation Level: Not defined  
Report Confidence: Not defined  
Availability Requirement: Not defined  
Collateral Damage Potential: Not defined  
Confidentiality Requirement: Not defined  
Integrity Requirement: Not defined  
Target Distribution: Not defined

### CVSS3
Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None

### CWE
CWE-538

**Affected item**  
/index.bak

**Affected parameter**

---

**Source code disclosure**

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.
CVSS3

Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

CWE

CWE-538

Affected item
/pictures/wp-config.bak

Affected parameter

---

**WS_FTP log file found (verified)**

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CWE

CWE-538

Affected item
/pictures/WS_FTP.LOG

Affected parameter

---

**MySQL username disclosure**

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.
CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CWE

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-538</td>
</tr>
</tbody>
</table>

Affected item

/Connections/DB_Connection.php

Affected parameter

MySQL username disclosure

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CWE

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-538</td>
</tr>
</tbody>
</table>

Affected item

/Connections/DB_Connection.php

Affected parameter

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

**CVSS3**

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

**CWE**

- **CWE-200**

**Affected item**

/admin/

**Affected parameter**

**Possible sensitive directories**

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

**CWE-200**

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/CVS/</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

### Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

**CWE-200**

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/hpp/test.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

### Possible virtual host found

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.
This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Score</strong>: 5.0</td>
<td></td>
</tr>
<tr>
<td><strong>Access Vector</strong>: Network accessible</td>
<td></td>
</tr>
<tr>
<td><strong>Access Complexity</strong>: Low</td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong>: None</td>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality Impact</strong>: Partial</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity Impact</strong>: None</td>
<td></td>
</tr>
<tr>
<td><strong>Availability Impact</strong>: None</td>
<td></td>
</tr>
<tr>
<td><strong>Exploitability</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Remediation Level</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Report Confidence</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Availability Requirement</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Collateral Damage Potential</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality Requirement</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity Requirement</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Target Distribution</strong>: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Score</strong>: 7.5</td>
<td></td>
</tr>
<tr>
<td><strong>Attack Vector</strong>: Network</td>
<td></td>
</tr>
<tr>
<td><strong>Attack Complexity</strong>: Low</td>
<td></td>
</tr>
<tr>
<td><strong>Privileges Required</strong>: None</td>
<td></td>
</tr>
<tr>
<td><strong>User Interaction</strong>: None</td>
<td></td>
</tr>
<tr>
<td><strong>Scope</strong>: Unchanged</td>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality Impact</strong>: High</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity Impact</strong>: None</td>
<td></td>
</tr>
<tr>
<td><strong>Availability Impact</strong>: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CWE</strong>: CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

**Affected item**: Web Server

**Affected parameter**:

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Score</strong>: 0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Access Vector</strong>: Network accessible</td>
<td></td>
</tr>
<tr>
<td><strong>Access Complexity</strong>: Low</td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong>: None</td>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality Impact</strong>: None</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity Impact</strong>: None</td>
<td></td>
</tr>
<tr>
<td><strong>Availability Impact</strong>: None</td>
<td></td>
</tr>
<tr>
<td><strong>Exploitability</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Remediation Level</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Report Confidence</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Availability Requirement</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Collateral Damage Potential</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality Requirement</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity Requirement</strong>: Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Target Distribution</strong>: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>
| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-200  
|     | Affected item | Web Server  
|     | Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-200  
|     | Affected item | /404.php  
|     | Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE   | CWE-200  
| Affected item | /cart.php  
| Affected parameter |

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE   | CWE-200  
| Affected item | /categories.php  
| Affected parameter |

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network\_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not\_defined
- **Remediation Level:** Not\_defined
- **Report Confidence:** Not\_defined
- **Availability Requirement:** Not\_defined
- **Collateral Damage Potential:** Not\_defined
- **Confidentiality Requirement:** Not\_defined
- **Integrity Requirement:** Not\_defined
- **Target Distribution:** Not\_defined

### CVSS3
- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-200**

#### Affected item
/disclaimer.php

#### Affected parameter

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network\_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not\_defined
- **Remediation Level:** Not\_defined
- **Report Confidence:** Not\_defined
- **Availability Requirement:** Not\_defined
- **Collateral Damage Potential:** Not\_defined
- **Confidentiality Requirement:** Not\_defined
- **Integrity Requirement:** Not\_defined
- **Target Distribution:** Not\_defined
### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE  | CWE-200 |
| Affected item | /guestbook.php |
| Affected parameter | |

### CVSS2

| Base Score: 0.0  
| Access Vector: Network_accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: None  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

### CVSS3

| Base Score: 0.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: None  
| Integrity Impact: None  
| Availability Impact: None |
| CWE  | CWE-200 |
| Affected item | /index.bak |
| Affected parameter | |
### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-200

#### Affected item
- `/index.php`

#### Affected parameter

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like `myname@mydomain.com` and then record any addresses found.

---

### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-200 |

#### Affected item

/`listproducts.php`

#### Affected parameter

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

---

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

---

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-200 |

#### Affected item

/`login.php`

#### Affected parameter

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS3 | Base Score: 0.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-200</td>
</tr>
<tr>
<td>Affected item</td>
<td>/product.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| --- | --- |
| CVSS3 | Base Score: 0.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /search.php |
| Affected parameter | |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
<th>CWE</th>
<th>Email address found</th>
</tr>
</thead>
</table>
| Base Score: 0.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined | Base Score: 0.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None | CWE-200 | One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found. |
| Affected item | /signup.php | Affected parameter | |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS3
- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-200

### Affected item
- `/Templates/main_dynamic_template.dwt.php`

### Affected parameter

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like `myname@mydomain.com` and then record any addresses found.

---

### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

---

### CVSS3
- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-200

### Affected item
- `/userinfo.php`

### Affected parameter

---

### Microsoft Office possible sensitive information

This document has been converted to HTML using Microsoft Office. It seems that Office has included sensitive information during the conversion.
| CVSS2  | Base Score: 5.0  
|        | Access Vector: Network_accessible  
|        | Access Complexity: Low  
|        | Authentication: None  
|        | Confidentiality Impact: Partial  
|        | Integrity Impact: None  
|        | Availability Impact: None  
|        | Exploitability: Not_defined  
|        | Remediation Level: Not_defined  
|        | Report Confidence: Not_defined  
|        | Availability Requirement: Not_defined  
|        | Collateral Damage Potential: Not_defined  
|        | Confidentiality Requirement: Not_defined  
|        | Integrity Requirement: Not_defined  
|        | Target Distribution: Not_defined  |
| CVSS3  | Base Score: 7.5  
|        | Attack Vector: Network  
|        | Attack Complexity: Low  
|        | Privileges Required: None  
|        | User Interaction: None  
|        | Scope: Unchanged  
|        | Confidentiality Impact: High  
|        | Integrity Impact: None  
|        | Availability Impact: None  |
| CWE    | CWE-200  
| Affected item | /secured/office.htm  
| Affected parameter |  

**Password type input with auto-complete enabled**

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

| CVSS2  | Base Score: 0.0  
|        | Access Vector: Network_accessible  
|        | Access Complexity: Low  
|        | Authentication: None  
|        | Confidentiality Impact: None  
|        | Integrity Impact: None  
|        | Availability Impact: None  
|        | Exploitability: Not_defined  
|        | Remediation Level: Not_defined  
|        | Report Confidence: Not_defined  
|        | Availability Requirement: Not_defined  
|        | Collateral Damage Potential: Not_defined  
|        | Confidentiality Requirement: Not_defined  
|        | Integrity Requirement: Not_defined  
|        | Target Distribution: Not_defined  |
**Password type input with auto-complete enabled**

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

**Possible internal IP address disclosure**

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-200**

**Affected item**
- /404.php

**Affected parameter**
- 

### Possible internal IP address disclosure

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.
This alert may be a false positive, manual confirmation is required.

### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-200**

**Affected item**
- /pictures/path-disclosure-unix.html

**Affected parameter**

---

**Possible server path disclosure (Unix)**

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined
### CVSS3
- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-200

**Affected item**
- `/secured/phpinfo.php`

**Affected parameter**

### Possible username or password disclosure

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-200

**Affected item**
- `/pictures/credentials.txt`

**Affected parameter**

### (12.4.3) Administrator and operator logs

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

Total number of alerts in this category: 92
Macromedia Dreamweaver remote database scripts (verified)

Macromedia Dreamweaver has created a directory (_mmServerScripts or _mmDBScripts) that contains scripts for testing database connectivity. One of these scripts (mmhttpdb.php or mmhttpdb.asp) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: High  
|       | Remediation Level: Official_fix  
|       | Report Confidence: Confirmed  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

CVE  
CVE-2004-1893

CWE  
CWE-16

Affected item  
Web Server

Affected parameter

Possible database backup

Manual confirmation is required for this alert.

It looks like this file contains a database backup/dump. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

CWE  
CWE-538

Affected item  /admin/create.sql
Affected parameter

.htaccess file readable (verified)

This directory contains an .htaccess file that is readable. This may indicate a server misconfiguration. .htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CWE

CWE-16

Affected item /Mod_Rewrite_Shop/

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2       | Base Score: 5.0  
|            | Access Vector: Network_accessible  
|            | Access Complexity: Low  
|            | Authentication: None  
|            | Confidentiality Impact: Partial  
|            | Integrity Impact: None  
|            | Availability Impact: None  
|            | Exploitability: Not_defined  
|            | Remediation Level: Not_defined  
|            | Report Confidence: Not_defined  
|            | Availability Requirement: Not_defined  
|            | Collateral Damage Potential: Not_defined  
|            | Confidentiality Requirement: Not_defined  
|            | Integrity Requirement: Not_defined  
|            | Target Distribution: Not_defined |

| CVSS3       | Base Score: 5.3  
|            | Attack Vector: Network  
|            | Attack Complexity: Low  
|            | Privileges Required: None  
|            | User Interaction: None  
|            | Scope: Unchanged  
|            | Confidentiality Impact: Low  
|            | Integrity Impact: None  
|            | Availability Impact: None  

| CWE         | CWE-200  
|            |  
| Affected item | /cart.php  
| Affected parameter | login  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2      | Base Score: 5.0  
|           | Access Vector: Network accessible  
|           | Access Complexity: Low  
|           | Authentication: None  
|           | Confidentiality Impact: Partial  
|           | Integrity Impact: None  
|           | Availability Impact: None  
|           | Exploitability: Not_defined  
|           | Remediation Level: Not_defined  
|           | Report Confidence: Not_defined  
|           | Availability Requirement: Not_defined  
|           | Collateral Damage Potential: Not_defined  
|           | Confidentiality Requirement: Not_defined  
|           | Integrity Requirement: Not_defined  
|           | Target Distribution: Not_defined |
| CVSS3      | Base Score: 5.3  
|           | Attack Vector: Network  
|           | Attack Complexity: Low  
|           | Privileges Required: None  
|           | User Interaction: None  
|           | Scope: Unchanged  
|           | Confidentiality Impact: Low  
|           | Integrity Impact: None  
|           | Availability Impact: None  

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/cart.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>Referer</td>
</tr>
</tbody>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.  

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-200  
|     |     

| Affected item | /cart.php  
| Affected parameter | User-Agent  

### Application error message

#### CVSS2

Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined  

| Affected item | /cart.php  
| Affected parameter | X-Forwarded-For  

### Application error message

#### CVSS3

Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None  

| CWE | CWE-200  
|     |     

| Affected item | /cart.php  
| Affected parameter | X-Forwarded-For  

### Application error message
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2       | Base Score: 5.0                  |
|            | Access Vector: Network_accessible |
|            | Access Complexity: Low           |
|            | Authentication: None             |
|            | Confidentiality Impact: Partial   |
|            | Integrity Impact: None           |
|            | Availability Impact: None        |
|            | Exploitability: Not_defined      |
|            | Remediation Level: Not_defined    |
|            | Report Confidence: Not_defined    |
|            | Availability Requirement: Not_defined |
|            | Collateral Damage Potential: Not_defined |
|            | Confidentiality Requirement: Not_defined |
|            | Integrity Requirement: Not_defined |
|            | Target Distribution: Not_defined  |

| CVSS3       | Base Score: 5.3                  |
|            | Attack Vector: Network           |
|            | Attack Complexity: Low           |
|            | Privileges Required: None        |
|            | User Interaction: None           |
|            | Scope: Unchanged                 |
|            | Confidentiality Impact: Low      |
|            | Integrity Impact: None           |
|            | Availability Impact: None        |

| CWE         | CWE-200                         |
|            | Affected item                    | /listproducts.php |
|            | Affected parameter               | artist            |
|            | Variants                         | 12345"\"|]]*%00[%0d%0a<%00>%bf%27δ□□|

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

---

**CVSS3**

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

---

**CWE**

- **CWE-200**

---

**Affected item**

- `/listproducts.php`

---

**Affected parameter**

- `login`

---

**Application error message**

---

**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

---

**CVSS3**

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

---

**CWE**

- **CWE-200**

---

**Affected item**

- `/listproducts.php`

---

**Affected parameter**

- `Referer`
Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2          | Base Score: 5.0  |
|               | Access Vector: Network_accessible |
|               | Access Complexity: Low |
|               | Authentication: None |
|               | Confidentiality Impact: Partial |
|               | Integrity Impact: None |
|               | Availability Impact: None |
|               | Exploitability: Not_defined |
|               | Remediation Level: Not_defined |
|               | Report Confidence: Not_defined |
|               | Availability Requirement: Not_defined |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined |
|               | Target Distribution: Not_defined |

| CVSS3          | Base Score: 5.3  |
|               | Attack Vector: Network |
|               | Attack Complexity: Low |
|               | Privileges Required: None |
|               | User Interaction: None |
|               | Scope: Unchanged |
|               | Confidentiality Impact: Low |
|               | Integrity Impact: None |
|               | Availability Impact: None |

CWE            | CWE-200  |

Affected item   | /listproducts.php  |
Affected parameter | User-Agent  |

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /listproducts.php |
| Affected parameter | X-Forwarded-For |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item
/product.php

Affected parameter
pic

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item
/secured/newuser.php

Affected parameter
login
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS3</td>
<td>Base Score: 5.3</td>
<td>Attack Vector: Network</td>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
<td>Confidentiality Impact: Low</td>
<td>Integrity Impact: None</td>
<td>Availability Impact: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CWE</td>
<td>CWE-200</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Affected item</td>
<td>/secured/newuser.php</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Affected parameter</td>
<td>signup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE
CWE-200

Affected item:
/secured/newuser.php

Affected parameter: uaddress

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined
**CVSS3**

- Base Score: 5.3
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: Low
- Integrity Impact: None
- Availability Impact: None

**CWE**

- CWE-200

**Affected item**

- /secured/newuser.php

**Affected parameter**

- ucc

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

---

**CVSS2**

- Base Score: 5.0
- Access Vector: Network_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

---

**CVSS3**

- Base Score: 5.3
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: Low
- Integrity Impact: None
- Availability Impact: None

**CWE**

- CWE-200

**Affected item**

- /secured/newuser.php

**Affected parameter**

- uemail
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|-------|----------------|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /secured/newuser.php |
| Affected parameter | uuname |
| Variants | 12345"\";\"]*%00{%0d%0a<%00>%bf%27\|\| |

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-200

**Affected item**
/showimage.php

**Affected parameter**
file

**Variants**
acu4562%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca4562

### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### CVSS3

| Base Score: 5.3 |
| Attack Vector: Network |
| Attack Complexity: Low |
| Privileges Required: None |
| User Interaction: None |
| Scope: Unchanged |
| Confidentiality Impact: Low |
| Integrity Impact: None |
| Availability Impact: None |

### CWE

| CWE-200 |

### Affected item

| /userinfo.php |

### Affected parameter

| script#text |

### Variants

| 12345"\");][%00(%0d%0a<%00>%bf%27%00| |

### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

### CVSS2

| Base Score: 5.0 |
| Access Vector: Network_accessible |
| Access Complexity: Low |
| Authentication: None |
| Confidentiality Impact: Partial |
| Integrity Impact: None |
| Availability Impact: None |
| Exploitability: Not_defined |
| Remediation Level: Not_defined |
| Report Confidence: Not_defined |
| Availability Requirement: Not_defined |
| Collateral Damage Potential: Not_defined |
| Confidentiality Requirement: Not_defined |
| Integrity Requirement: Not_defined |
| Target Distribution: Not_defined |

### CVSS3

| Base Score: 5.3 |
| Attack Vector: Network |
| Attack Complexity: Low |
| Privileges Required: None |
| User Interaction: None |
| Scope: Unchanged |
| Confidentiality Impact: Low |
| Integrity Impact: None |
| Availability Impact: None |

### CWE

| CWE-200 |

### Affected item

| /userinfo.php |

### Affected parameter

| uaddress |

### Variants

| 12345"\");][%00(%0d%0a<%00>%bf%27%00| |
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined  |
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None  |
| CWE | CWE-200 |
| Affected item | /userinfo.php |
| Affected parameter | ucc |
| Variants | 12345"\";]]}%00{%0d%0a<%00>%bf%27\"i |

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

### Affected item

- **/userinfo.php**

### Affected parameter

- **uemail**

### Variants

- `12345"\";\00\0%00%0d%0a<%00>%bf%27\8\5j`

### Application error message

**This alert requires manual confirmation**

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
</table>

**Affected item** /userinfo.php

**Affected parameter** uname

**Variants** 12345\"\"");\*%00{%0d%0a<%00>%bf%27ð¡

**Backup files**

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.
CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CWE
CWE-538

Affected item
/index.bak

Affected parameter

Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CWE
CWE-538

Affected item
/index.zip

Affected parameter

Credit card number disclosed (verified)

This alert may be a false positive, manual confirmation is required.

The response contains one or more credit card numbers. The credit card numbers were validated using the Luhn algorithm to make sure they are real credit card numbers.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

<table>
<thead>
<tr>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
</tr>
<tr>
<td>Affected parameter</td>
</tr>
</tbody>
</table>
| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-538 |
| Affected item | /_mmServerScripts/ |
| Affected parameter | |

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
## Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Base Score: 7.5</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

## CWE

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/admin/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

## Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Connections/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>
CVSS2
Base Score: 5.0
Access Vector: Network accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not defined
Remediation Level: Not defined
Report Confidence: Not defined
Availability Requirement: Not defined
Collateral Damage Potential: Not defined
Confidentiality Requirement: Not defined
Integrity Requirement: Not defined
Target Distribution: Not defined

CVSS3
Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

CWE
CWE-538

Affected item
/CVS/

Affected parameter

Directory listing (verified)
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Flash/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

#### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not defined</td>
</tr>
<tr>
<td>Remediation Level: Not defined</td>
</tr>
<tr>
<td>Report Confidence: Not defined</td>
</tr>
<tr>
<td>Availability Requirement: Not defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not defined</td>
</tr>
<tr>
<td>Target Distribution: Not defined</td>
</tr>
</tbody>
</table>

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/images/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE  | CWE-538  
|      | Affected item  
|      | /Mod_Rewrite_Shop/images/  
|      | Affected parameter |

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE | CWE-538  
| Affected item | /wvstests/  
| Affected parameter | 

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

### Error message on page

This alert requires manual confirmation.

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: NetworkAccessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: NotDefined  
|       | Remediation Level: NotDefined  
|       | Report Confidence: NotDefined  
|       | Availability Requirement: NotDefined  
|       | Collateral Damage Potential: NotDefined  
|       | Confidentiality Requirement: NotDefined  
|       | Integrity Requirement: NotDefined  
|       | Target Distribution: NotDefined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE | CWE-200 |

| Affected item | /AJAX/infoartist.php |

| Affected parameter | |
| CVSS3                  | Base Score: 5.3  
|                       | Attack Vector: Network  
|                       | Attack Complexity: Low  
|                       | Privileges Required: None  
|                       | User Interaction: None  
|                       | Scope: Unchanged  
|                       | Confidentiality Impact: Low  
|                       | Integrity Impact: None  
|                       | Availability Impact: None  
| CWE                   | CWE-200  
| Affected item        | /AJAX/infocateg.php  
| Affected parameter   |  

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2                  | Base Score: 5.0  
|                       | Access Vector: Network_accessible  
|                       | Access Complexity: Low  
|                       | Authentication: None  
|                       | Confidentiality Impact: Partial  
|                       | Integrity Impact: None  
|                       | Availability Impact: None  
|                       | Exploitability: Not_defined  
|                       | Remediation Level: Not_defined  
|                       | Report Confidence: Not_defined  
|                       | Availability Requirement: Not_defined  
|                       | Collateral Damage Potential: Not_defined  
|                       | Confidentiality Requirement: Not_defined  
|                       | Integrity Requirement: Not_defined  
|                       | Target Distribution: Not_defined  

| CVSS3                  | Base Score: 5.3  
|                       | Attack Vector: Network  
|                       | Attack Complexity: Low  
|                       | Privileges Required: None  
|                       | User Interaction: None  
|                       | Scope: Unchanged  
|                       | Confidentiality Impact: Low  
|                       | Integrity Impact: None  
|                       | Availability Impact: None  
| CWE                   | CWE-200  
| Affected item        | /AJAX/infotitle.php  
| Affected parameter   |  

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2  | Base Score: 5.0  
|        | Access Vector: Network accessible  
|        | Access Complexity: Low  
|        | Authentication: None  
|        | Confidentiality Impact: Partial  
|        | Integrity Impact: None  
|        | Availability Impact: None  
|        | Exploitability: Not defined  
|        | Remediation Level: Not defined  
|        | Report Confidence: Not defined  
|        | Availability Requirement: Not defined  
|        | Collateral Damage Potential: Not defined  
|        | Confidentiality Requirement: Not defined  
|        | Integrity Requirement: Not defined  
|        | Target Distribution: Not defined |

| CVSS3  | Base Score: 5.3  
|        | Attack Vector: Network  
|        | Attack Complexity: Low  
|        | Privileges Required: None  
|        | User Interaction: None  
|        | Scope: Unchanged  
|        | Confidentiality Impact: Low  
|        | Integrity Impact: None  
|        | Availability Impact: None  

| CWE    | CWE-200  

| Affected item  | /Connections/DB_Connection.php  
| Affected parameter  | 

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
</table>
| Base Score: 5.0  
Access Vector: Network\_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not\_defined  
Remediation Level: Not\_defined  
Report Confidence: Not\_defined  
Availability Requirement: Not\_defined  
Collateral Damage Potential: Not\_defined  
Confidentiality Requirement: Not\_defined  
Integrity Requirement: Not\_defined  
Target Distribution: Not\_defined | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |

CWE-200

Affected item  
/pictures/path-disclosure-unix.html

Affected parameter

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE
CWE-200

Affected item
/secured/database_connect.php

JetBrains .idea project directory

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CWE
CWE-538

Affected item
Web Server

PHP errors enabled (verified)

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found that the PHP display_errors directive is enabled.
## CVSS2
Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

## CVSS3
Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None

## CWE
CWE-16

**Affected item**  
/secured/phpinfo.php

**Affected parameter**

---

### PHPinfo page (verified)

PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.
This script is using `phpinfo()` function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.
| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-538 |
| Affected item | /index.bak |
| Affected parameter | |

**Source code disclosure**

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.
### CVSS3

<table>
<thead>
<tr>
<th>Base Score</th>
<th>7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-538 |

### Affected item

/pictures/wp-config.bak

### Affected parameter

**WS_FTP log file found (verified)**

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score</th>
<th>5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

### CWE

| CWE-538 |

### Affected item

/pictures/WS_FTP.LOG

### Affected parameter

**MySQL username disclosure**

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.
CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CWE

| CWE-538 |

Affected item

/Connections/DB_Connection.php

Affected parameter

MySQL username disclosure

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-200**

**Affected item**
- `/admin/

**Affected parameter**

#### Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE  | CWE-200 |

**Affected item** | /CVS/ |

**Possible sensitive files**

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE  | CWE-200 |

**Affected item** | /hpp/test.php |

**Possible virtual host found**

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.
This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE  | CWE-200 |

| Affected item | Web Server |

| Affected parameter |

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-200</th>
</tr>
</thead>
</table>

**Affected item**

Web Server

**Affected parameter**

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-200</th>
</tr>
</thead>
</table>

**Affected item**

/404.php

**Affected parameter**

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-200**

### Affected item
- `/artists.php`

### Affected parameter

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS3             | Base Score: 0.0  
|                  | Attack Vector: Network  
|                  | Attack Complexity: Low  
|                  | Privileges Required: None  
|                  | User Interaction: None  
|                  | Scope: Unchanged  
|                  | Confidentiality Impact: None  
|                  | Integrity Impact: None  
|                  | Availability Impact: None  
| CWE              | CWE-200  
| Affected item    | /cart.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2             | Base Score: 0.0  
|                  | Access Vector: Network accessible  
|                  | Access Complexity: Low  
|                  | Authentication: None  
|                  | Confidentiality Impact: None  
|                  | Integrity Impact: None  
|                  | Availability Impact: None  
|                  | Exploitability: Not_defined  
|                  | Remediation Level: Not_defined  
|                  | Report Confidence: Not_defined  
|                  | Availability Requirement: Not_defined  
|                  | Collateral Damage Potential: Not_defined  
|                  | Confidentiality Requirement: Not_defined  
|                  | Integrity Requirement: Not_defined  
|                  | Target Distribution: Not_defined  
| CVSS3             | Base Score: 0.0  
|                  | Attack Vector: Network  
|                  | Attack Complexity: Low  
|                  | Privileges Required: None  
|                  | User Interaction: None  
|                  | Scope: Unchanged  
|                  | Confidentiality Impact: None  
|                  | Integrity Impact: None  
|                  | Availability Impact: None  
| CWE              | CWE-200  
| Affected item    | /categories.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS2
- **Base Score**: 0.0
- **Access Vector**: NetworkAccessible
- **Access Complexity**: Low
- **Authentication**: None
- **Confidentiality Impact**: None
- **Integrity Impact**: None
- **Availability Impact**: None
- **Exploitability**: NotDefined
- **Remediation Level**: NotDefined
- **Report Confidence**: NotDefined
- **Availability Requirement**: NotDefined
- **Collateral Damage Potential**: NotDefined
- **Confidentiality Requirement**: NotDefined
- **Integrity Requirement**: NotDefined
- **Target Distribution**: NotDefined

### CVSS3
- **Base Score**: 0.0
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Unchanged
- **Confidentiality Impact**: None
- **Integrity Impact**: None
- **Availability Impact**: None

### CWE
- **CWE**: CWE-200
- **Affected item**: /disclaimer.php
- **Affected parameter**: 

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### CVSS2
- **Base Score**: 0.0
- **Access Vector**: NetworkAccessible
- **Access Complexity**: Low
- **Authentication**: None
- **Confidentiality Impact**: None
- **Integrity Impact**: None
- **Availability Impact**: None
- **Exploitability**: NotDefined
- **Remediation Level**: NotDefined
- **Report Confidence**: NotDefined
- **Availability Requirement**: NotDefined
- **Collateral Damage Potential**: NotDefined
- **Confidentiality Requirement**: NotDefined
- **Integrity Requirement**: NotDefined
- **Target Distribution**: NotDefined
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-200

### Affected item
- `/index.php`

### Affected parameter

#### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like `myname@mydomain.com` and then record any addresses found.

### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE  | CWE-200  
| Affected item | /listproducts.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE  | CWE-200  
| Affected item | /login.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

**Affected item** `/logout.php`

**Affected parameter**

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like `myname@mydomain.com` and then record any addresses found.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-200 |

### Affected item

| /product.php |

### Affected parameter

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

---

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-200 |

### Affected item

| /search.php |

### Affected parameter

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
<th>CWE</th>
<th>Affected item</th>
<th>Affected parameter</th>
</tr>
</thead>
</table>
| Base Score: 0.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined | Base Score: 0.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None | CWE-200 | /signup.php | |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
## Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### CVSS2

| Base Score: 0.0 |
| Attack Vector: Network accessible |
| Access Complexity: Low |
| Authentication: None |
| Confidentiality Impact: None |
| Integrity Impact: None |
| Availability Impact: None |
| Exploitability: Not_defined |
| Remediation Level: Not_defined |
| Report Confidence: Not_defined |
| Availability Requirement: Not_defined |
| Collateral Damage Potential: Not_defined |
| Confidentiality Requirement: Not_defined |
| Integrity Requirement: Not_defined |
| Target Distribution: Not_defined |

### CVSS3

| Base Score: 0.0 |
| Attack Vector: Network |
| Attack Complexity: Low |
| Privileges Required: None |
| User Interaction: None |
| Scope: Unchanged |
| Confidentiality Impact: None |
| Integrity Impact: None |
| Availability Impact: None |

### CWE

| CWE-200 |

**Affected item**

/Templates/main_dynamic_template.dwt.php

**Affected parameter**

### Microsoft Office possible sensitive information

This document has been converted to HTML using Microsoft Office. It seems that Office has included sensitive information during the conversion.
| CVSS2          | Base Score: 5.0  
|               | Access Vector: NetworkAccessible  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: NotDefined  
|               | Remediation Level: NotDefined  
|               | Report Confidence: NotDefined  
|               | Availability Requirement: NotDefined  
|               | Collateral Damage Potential: NotDefined  
|               | Confidentiality Requirement: NotDefined  
|               | Integrity Requirement: NotDefined  
|               | Target Distribution: NotDefined |

| CVSS3          | Base Score: 7.5  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: High  
|               | Integrity Impact: None  
|               | Availability Impact: None  

| CWE            | CWE-200  
|               | Affected item /secured/office.htm  
|               | Affected parameter |

**Password type input with auto-complete enabled**

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

| CVSS2          | Base Score: 0.0  
|               | Access Vector: NetworkAccessible  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: None  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: NotDefined  
|               | Remediation Level: NotDefined  
|               | Report Confidence: NotDefined  
|               | Availability Requirement: NotDefined  
|               | Collateral Damage Potential: NotDefined  
|               | Confidentiality Requirement: NotDefined  
|               | Integrity Requirement: NotDefined  
|               | Target Distribution: NotDefined |
### CVSS3
- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-200

**Affected item:** Web Server

**Affected parameter:** form1

---

**Password type input with auto-complete enabled**

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Score:</strong></td>
<td>0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Access Vector:</strong></td>
<td>Network_accessible</td>
<td></td>
</tr>
<tr>
<td><strong>Access Complexity:</strong></td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td><strong>Authentication:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality Impact:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity Impact:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Availability Impact:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Exploitability:</strong></td>
<td>Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Remediation Level:</strong></td>
<td>Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Report Confidence:</strong></td>
<td>Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Availability Requirement:</strong></td>
<td>Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Collateral Damage Potential:</strong></td>
<td>Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality Requirement:</strong></td>
<td>Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity Requirement:</strong></td>
<td>Not_defined</td>
<td></td>
</tr>
<tr>
<td><strong>Target Distribution:</strong></td>
<td>Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Score:</strong></td>
<td>7.5</td>
<td></td>
</tr>
<tr>
<td><strong>Attack Vector:</strong></td>
<td>Network</td>
<td></td>
</tr>
<tr>
<td><strong>Attack Complexity:</strong></td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td><strong>Privileges Required:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>User Interaction:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Scope:</strong></td>
<td>Unchanged</td>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality Impact:</strong></td>
<td>High</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity Impact:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Availability Impact:</strong></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**CWE**
- **CWE:** CWE-200

**Affected item:** Web Server

**Affected parameter:** loginform

---

**Possible internal IP address disclosure**

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item
/404.php

Affected parameter

Possible internal IP address disclosure

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  |

| CWE | CWE-200  |

| Affected item | /pictures/ipaddresses.txt  |

| Affected parameter |  |

**Possible internal IP address disclosure**

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  |

| CWE | CWE-200  |

| Affected item | /secured/phpinfo.php  |

| Affected parameter |  |

**Possible server path disclosure (Unix)**

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.
This alert may be a false positive, manual confirmation is required.

| CVSS2 | | Base Score: 5.0  
| | | Access Vector: Network_accessible  
| | | Access Complexity: Low  
| | | Authentication: None  
| | | Confidentiality Impact: Partial  
| | | Integrity Impact: None  
| | | Availability Impact: None  
| | | Exploitability: Not_defined  
| | | Remediation Level: Not_defined  
| | | Report Confidence: Not_defined  
| | | Availability Requirement: Not_defined  
| | | Collateral Damage Potential: Not_defined  
| | | Confidentiality Requirement: Not_defined  
| | | Integrity Requirement: Not_defined  
| | | Target Distribution: Not_defined  

| CVSS3 | | Base Score: 7.5  
| | | Attack Vector: Network  
| | | Attack Complexity: Low  
| | | Privileges Required: None  
| | | User Interaction: None  
| | | Scope: Unchanged  
| | | Confidentiality Impact: High  
| | | Integrity Impact: None  
| | | Availability Impact: None  

| CWE | | CWE-200  

**Affected item**
/pictures/path-disclosure-unix.html

**Affected parameter**

**Possible server path disclosure (Unix)**

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
**CVSS3**

Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

**CWE**

CWE-200

**Affected item**

/secured/phpinfo.php

**Affected parameter**


**Possible username or password disclosure**

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

**CVSS2**

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

**CVSS3**

Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

**CWE**

CWE-200

**Affected item**

/pictures/credentials.txt

**Affected parameter**


**Installation of software on operational systems**

Procedures shall be implemented to control the installation of software on operational systems.

Total number of alerts in this category: 29
**Macromedia Dreamweaver remote database scripts (verified)**

Macromedia Dreamweaver has created a directory (`_mmServerScripts` or `_mmDBScripts`) that contains scripts for testing database connectivity. One of these scripts (`mmhttpdb.php` or `mmhttpdb.asp`) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: High</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Official_fix</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Confirmed</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVE</th>
<th>CVE-2004-1893</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-16</td>
</tr>
</tbody>
</table>

**Affected item**  Web Server

**Affected parameter**

---

**nginx SPDY heap buffer overflow**

A heap-based buffer overflow in the SPDY implementation in nginx 1.3.15 before 1.4.7 and 1.5.x before 1.5.12 allows remote attackers to execute arbitrary code via a crafted request. The problem affects nginx compiled with the ngx_http_spdy_module module (which is not compiled by default) and without --with-debug configure option, if the "spdy" option of the "listen" directive is used in a configuration file.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.1</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: High</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Proof_of_concept</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Official_fix</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVE</th>
<th>CVE-2014-0133</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-122</td>
</tr>
</tbody>
</table>

**Affected item**  Web Server

**Affected parameter**
The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

| CVSS2          | Base Score: 0.0  
|                | Access Vector: Network_accessible  
|                | Access Complexity: Low  
|                | Authentication: None  
|                | Confidentiality Impact: None  
|                | Integrity Impact: None  
|                | Availability Impact: None  
|                | Exploitability: Not_defined  
|                | Remediation Level: Not_defined  
|                | Report Confidence: Not_defined  
|                | Availability Requirement: Not_defined  
|                | Collateral Damage Potential: Not_defined  
|                | Confidentiality Requirement: Not_defined  
|                | Integrity Requirement: Not_defined  
|                | Target Distribution: Not_defined  
| CWE            | CWE-16  
| Affected item  | Web Server  
| Affected parameter |  

This directory contains an .htaccess file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

| CVSS2          | Base Score: 5.0  
|                | Access Vector: Network_accessible  
|                | Access Complexity: Low  
|                | Authentication: None  
|                | Confidentiality Impact: Partial  
|                | Integrity Impact: None  
|                | Availability Impact: None  
|                | Exploitability: Not_defined  
|                | Remediation Level: Not_defined  
|                | Report Confidence: Not_defined  
|                | Availability Requirement: Not_defined  
|                | Collateral Damage Potential: Not_defined  
|                | Confidentiality Requirement: Not_defined  
|                | Integrity Requirement: Not_defined  
|                | Target Distribution: Not_defined  
| CWE            | CWE-16  
| Affected item  | /Mod_Rewrite_Shop/  
| Affected parameter |  

Cross domain data hijacking
This page is possibly vulnerable to Cross domain data hijacking. If an attacker can create/upload a malicious Flash (SWF) file or control the top part of any page he can perform an attack known as Cross domain data hijacking. The Content-Type of the response doesn't matter. If the file is embedded using an <object> tag, it will be executed as a Flash file as long as the content of the file looks like a valid Flash file.

Here is the attack scenario:

- An attacker creates a malicious Flash (SWF) file
- The attacker changes the file extension to JPG
- The attacker uploads the file to victim.com
- The attacker embeds the file on attacker.com using an tag with type "application/x-shockwave-flash"
- The victim visits attacker.com, loads the file as embedded with the tag
- The attacker can now send and receive arbitrary requests to victim.com using the victims session
- The attacker sends a request to victim.com and extracts the CSRF token from the response

There are many ways to perform this attack. The attacker doesn't need to upload a file. The only requirement is that an attacker can control the data on a location of the target domain. One way is to abuse a JSONP API. Usually, the attacker can control the output of a JSONP API endpoint by changing the callback parameter. However, if an attacker uses an entire Flash file as callback, we can use it just like we would use an uploaded file in this attack.

A payload could look like this:

```html
<object style="height:1px;width:1px;" data="http://victim.com/user/jsonp?callback=CWS%07%0E
```

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 4.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector:</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/hpp/params.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>p</td>
</tr>
<tr>
<td>Variants</td>
<td>CWS%07%0E000x%9C=%8D1N%C3%40%10E%DF%AE%8D%BDI%08)%D3%40%1D%A0%A2%05%09%11%89HiP%0D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X%1S%8C%FE%CC%9B%F9%FF%AA%CB7Jq%AF%7F%ED%F2.%F8%01&gt;%9E%18p%9c%9AI%B%AC%GZ%F%DC%BEM%EC%ABdkj%1E%AC%2C%9F%A5(%B1%EB%89T%C2J)%93%DBT7%24%9C%8FH%CBD6)%A3%0Bx%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F%E8%FA%98%20b%26%1C%9F5%20h%f1%D1g%0F%14%C1%0A%j%8D%8B0Q%A8L%9B6%D4L%BD%_A8w%7E%9D[ %17%F3/%DCm%EF%CB%EF%E6%8D:n-%FB%B3%C3%DD.%E3d1d%EC%C7%3F6%CD0%09</td>
</tr>
</tbody>
</table>

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

| CVSS2 | Base Score: 5.0  
| Access Vector: Network_accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CVSS3 | Base Score: 7.5  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: High  
| Integrity Impact: None  
| Availability Impact: None |

| CWE | CWE-538  
| Affected item | `.idea/`  
| Affected parameter |
CWE-538

Affected item: `/idea/scopes/`

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**CVSS2**
- Base Score: 5.0
- Access Vector: Network_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**
- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

CWE-538

Affected item: `/_mmServerScripts/`

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/admin/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Connections/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

#### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

#### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

**CVSS3**

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

**CWE**

- **CWE-538**

**Affected item**

/Flash/

**Affected parameter**

---

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Base Score: 7.5</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
</tbody>
</table>

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-538**

**Affected item**
/wwstests/pmwiki_2_1_19/

**Affected parameter**

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The browser security model normally prevents web content from one domain from accessing data from another domain. This is commonly known as the "same origin policy". URL policy files grant cross-domain permissions for reading data. They permit operations that are not permitted by default. The URL policy file is located, by default, in the root directory of the target server, with the name crossdomain.xml (for example, at www.example.com/crossdomain.xml).

When a domain is specified in crossdomain.xml file, the site declares that it is willing to allow the operators of any servers in that domain to obtain any document on the server where the policy file resides. The crossdomain.xml file deployed on this website opens the server to all domains (use of a single asterisk "***" as a pure wildcard is supported) like so:

```xml
<cross-domain-policy>
  <allow-access-from domain="*" />
</cross-domain-policy>
```

This practice is suitable for public servers, but should not be used for sites located behind a firewall because it could permit access to protected areas. It should not be used for sites that require authentication in the form of passwords or cookies. Sites that use the common practice of authentication based on cookies to access private or user-specific data should be especially careful when using cross-domain policy files.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 6.5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE | CWE-538
---|------------------
Affected item | /wvstests/pmwiki_2_1_19/scripts/
Affected parameter |  

CWE | CWE-284
---|------------------
Affected item | Web Server
Affected parameter |  

---
The PHP configuration directive `allow_url_fopen` is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling `allow_url_fopen` and bad input filtering.

`allow_url_fopen` is enabled by default.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Low</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

CWE

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/secured/phpinfo.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**PHP errors enabled (verified)**

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix AcuSensor found that the PHP `display_errors` directive is enabled.
### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not Defined
- **Remediation Level:** Not Defined
- **Report Confidence:** Not Defined
- **Availability Requirement:** Not Defined
- **Collateral Damage Potential:** Not Defined
- **Confidentiality Requirement:** Not Defined
- **Integrity Requirement:** Not Defined
- **Target Distribution:** Not Defined

### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-16**
- **Affected item:** Web Server
- **Affected parameter:**

#### PHP errors enabled (verified)

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found that the PHP `display_errors` directive is enabled.

### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not Defined
- **Remediation Level:** Not Defined
- **Report Confidence:** Not Defined
- **Availability Requirement:** Not Defined
- **Collateral Damage Potential:** Not Defined
- **Confidentiality Requirement:** Not Defined
- **Integrity Requirement:** Not Defined
- **Target Distribution:** Not Defined
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-16  
|     |  

**Affected item**  
/secured/phpinfo.php

**Affected parameter**  

---

**PHP open_basedir is not set (verified)**

The `open_basedir` configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, `fopen()` or `gzopen()`, the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. `open_basedir` is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the `open_basedir` restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

---

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-16  
|     |  

**Affected item**  
/secured/phpinfo.php

**Affected parameter**  

---

**PHP session.use_only_cookies disabled (verified)**
When `use_only_cookies` is disabled, PHP will pass the session ID via the URL. This makes the application more vulnerable to session hijacking attacks. Session hijacking is basically a form of identity theft wherein a hacker impersonates a legitimate user by stealing his session ID. When the session token is transmitted in a cookie, and the request is made on a secure channel (that is, it uses SSL), the token is secure.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-16</th>
</tr>
</thead>
</table>

**Affected item**
/secured/phpinfo.php

**Affected parameter**

Cookie(s) without HttpOnly flag set (verified)

This cookie does not have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-16</th>
</tr>
</thead>
</table>

**Affected item**
Web Server

**Affected parameter**

Cookie(s) without Secure flag set (verified)

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.
Hidden form input named price was found

A hidden form input named price was found. It's not recommended to hide sensitive information in hidden form fields.

Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a `Content-Security-Policy` header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```plaintext
Content-Security-Policy: default-src 'self'; script-src 'self' '
```
Content-Security-Policy:

default-src 'self';

script-src 'self' https://code.jquery.com;

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>Web Server</th>
</tr>
</thead>
</table>

(13.1.1)Security of network services

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

No alerts in this category.

(13.2.1)Information transfer policies and procedures

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

Total number of alerts in this category: 3

Alerts in this category

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** High
- **Remediation Level:** Workaround
- **Report Confidence:** Confirmed
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 9.1
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-310

**Affected item**
- `/login.php`

**Affected parameter**
- `loginform`

---

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
### Unencrypted connection (verified)

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.8</th>
<th>Access Vector: Network accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Complexity: Medium</td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 9.1</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

CWE | CWE-310
--- | ---
Affected item | /signup.php
Affected parameter | form1

### (13.2.3)Electronic messaging

Information involved in electronic messaging shall be appropriately protected.

Total number of alerts in this category: 3

**Alerts in this category**

**User credentials are sent in clear text**

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
## CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network\_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** High
- **Remediation Level:** Workaround
- **Report Confidence:** Confirmed
- **Availability Requirement:** Not\_defined
- **Collateral Damage Potential:** Not\_defined
- **Confidentiality Requirement:** Not\_defined
- **Integrity Requirement:** Not\_defined
- **Target Distribution:** Not\_defined

## CVSS3

- **Base Score:** 9.1
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

## CWE

- **CWE-310**

### Affected item

**/login.php**

### Affected parameter

loginform

---

**User credentials are sent in clear text**

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
**Unencrypted connection (verified)**

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 9.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-310

**Affected item**

/signup.php

**Affected parameter**

form1

---

(14.1.2) Securing application services on public networks

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

Total number of alerts in this category: 95

**Alerts in this category**

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

**Affected item**

**Web Server**

**Affected parameter**

`login`

**Variants**

`test%2Ftest' AND 3*2*1=6 AND '000QvXx'='000QvXx`

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
CVSS3
Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE
CWE-89

Affected item
/AJAX/infoartist.php

Affected parameter
id

Variants
if(now()=sysdate(),sleep(0),0)

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2
Base Score: 6.8
Access Vector: Network accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3
Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE
CWE-89

Affected item
/ AJAX/infocateg.php

Affected parameter
id

Variants
if(now()=sysdate(),sleep(0),0)

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

**Affected item**: /AJAX/infotitle.php

**Affected parameter**: id

**Variants**: `if(now()=sysdate(),sleep(0),0)`

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|     |     

| Affected item | /artists.php  
|               |     

| Affected parameter | artist  
|                   |     

| Variants | 1 AND 3*2*1=6 AND 909=909  
|          |     

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|     |     

| Affected item | /artists.php  
|               |     

| Affected parameter | login  
|                   |     

| Variants | test%2Ftest' AND 3*2*1=6 AND '0009eun'='0009eun  
|          |     

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score**: 6.8
- **Access Vector**: Network accessible
- **Access Complexity**: Medium
- **Authentication**: None
- **Confidentiality Impact**: Partial
- **Integrity Impact**: Partial
- **Availability Impact**: Partial
- **Exploitability**: Not defined
- **Remediation Level**: Not defined
- **Report Confidence**: Not defined
- **Availability Requirement**: Not defined
- **Collateral Damage Potential**: Not defined
- **Confidentiality Requirement**: Not defined
- **Integrity Requirement**: Not defined
- **Target Distribution**: Not defined

### CVSS3
- **Base Score**: 10.0
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Changed
- **Confidentiality Impact**: High
- **Integrity Impact**: High
- **Availability Impact**: None

### CWE
- **CWE-89**

**Affected item**  
`/cart.php`  
**Affected parameter**  
`addcart`  
**Variants**  
`if(now()=sysdate(),sleep(0),0)`

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
- **Base Score**: 6.8
- **Access Vector**: Network accessible
- **Access Complexity**: Medium
- **Authentication**: None
- **Confidentiality Impact**: Partial
- **Integrity Impact**: Partial
- **Availability Impact**: Partial
- **Exploitability**: Not defined
- **Remediation Level**: Not defined
- **Report Confidence**: Not defined
- **Availability Requirement**: Not defined
- **Collateral Damage Potential**: Not defined
- **Confidentiality Requirement**: Not defined
- **Integrity Requirement**: Not defined
- **Target Distribution**: Not defined
### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **/cart.php**

### Affected parameter

- **login**

### Variants

- `test%2Ftest' AND 3*2*1=6 AND '000rpl5'='000rpl5`

### Blind SQL Injection

**SQL injection (SQLi)** refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **/guestbook.php**

### Affected parameter

- **login**

### Variants

- `(select(0)from(select(sleep(0)))v)+"+(select(0)from(select(sleep(0)))v)+"+(select(0)from(select(sleep(0)))v)+"/(select(0)from(select(sleep(0)))v)+"/`
<table>
<thead>
<tr>
<th><strong>CVSS2</strong></th>
<th><strong>CVSS3</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Base Score: 10.0</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/listproducts.php

**Affected parameter**

artist

**Variants**

1 AND 3*2*1=6 AND 568=568

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **/listproducts.php**

### Affected parameter

- **cat**

### Variants

- 1 AND 3*2*1=6 AND 551=551

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **/listproducts.php**

### Affected parameter

- **login**

### Variants

- test%2Ftest' AND 3*2*1=6 AND '000Ccg'n='000Ccg

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |

| CWE | CWE-89 |

**Affected item**  /product.php

**Affected parameter**  login

**Variants**  test%2Ftest' AND 3*2*1=6 AND '000vXGJ'='000vXGJ

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
## CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

## CWE

CWE-89

### Affected item

/\product.php

### Affected parameter

pic

### Variants

1 AND 3*2*1=6 AND 494=494

## Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

## CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

## CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

## CWE

CWE-89

### Affected item

/\search.php

### Affected parameter

login

### Variants

test%2Ftest' AND 3*2*1=6 AND '000NAzi'='000NAzi

## Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
CVSS2

Base Score: 6.8
Access Vector: Network accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Affected item
/search.php

Affected parameter
searchFor

Variants
0'XOR(if(now)=sysdate(),sleep(0),0))XOR'Z

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2

Base Score: 6.8
Access Vector: Network accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined
**CVSS3**

- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

**CWE**

- CWE-89

**Affected item**

/secure/newuser.php

**Affected parameter**

uname

**Variants**

0'XOR(if(now=sysdate(),sleep(0),0))XOR'Z

---

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS2**

- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**

- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

**CWE**

- CWE-89

**Affected item**

/secure/newuser.php

**Affected parameter**

uname

**Variants**

0'XOR(if(now=sysdate(),sleep(0),0))XOR'Z

---

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE-89**

#### Affected item
/sendcommand.php

#### Affected parameter
cart_id

#### Variants
(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'*/

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/userinfo.php

**Affected parameter**

login

**Variants**

test%2Ftest' AND 3*2*1=6 AND '000GmMl'='000GmMl

---

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

---

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/userinfo.php

**Affected parameter**

pass

**Variants**

-1' OR 3*2*1=6 AND 000283=000283 --

---

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---
**CVSS2**

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

**CVSS3**

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

**CWE**

- **CWE-89**

**Affected item**

/userinfo.php

**Affected parameter**

uname

**Variants**

-1' OR 3*2*1=6 AND 00059=00059 --

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Affected item
/userinfo.php

Affected parameter
urname

Variants
0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z

Cross site scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2

Base Score: 6.4
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: Low
Availability Impact: None

CWE

CWE-79

Affected item
Web Server

Affected parameter

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
### CVSS2
- **Base Score:** 6.4  
- **Access Vector:** Network _accessible_  
- **Access Complexity:** Low  
- **Authentication:** None  
- **Confidentiality Impact:** Partial  
- **Integrity Impact:** Partial  
- **Availability Impact:** None  
- **Exploitability:** Not defined  
- **Remediation Level:** Not defined  
- **Report Confidence:** Not defined  
- **Availability Requirement:** Not defined  
- **Collateral Damage Potential:** Not defined  
- **Confidentiality Requirement:** Not defined  
- **Integrity Requirement:** Not defined  
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 5.3  
- **Attack Vector:** Network  
- **Attack Complexity:** Low  
- **Privileges Required:** None  
- **User Interaction:** None  
- **Scope:** Unchanged  
- **Confidentiality Impact:** None  
- **Integrity Impact:** Low  
- **Availability Impact:** None

### CWE
- **CWE:** CWE-79

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/AJAX/showxml.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>mycookie</td>
</tr>
<tr>
<td>Variants</td>
<td>3''()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;t2Bk(9174)&lt;/ScRiPt&gt;</td>
</tr>
</tbody>
</table>

**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
### CVSS3

- **Base Score:** 5.3  
- **Attack Vector:** Network  
- **Attack Complexity:** Low  
- **Privileges Required:** None  
- **User Interaction:** None  
- **Scope:** Unchanged  
- **Confidentiality Impact:** None  
- **Integrity Impact:** Low  
- **Availability Impact:** None  

### CWE  

- **CWE:** CWE-79  
- **Affected item:** /comment.php  
- **Affected parameter:** name  
- **Variants:** `<your name here>`"()&%<acx><ScRiPt >3R9A(9055)</ScRiPt>`  

#### Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

### CVSS2

- **Base Score:** 6.4  
- **Access Vector:** Network_accessible  
- **Access Complexity:** Low  
- **Authentication:** None  
- **Confidentiality Impact:** Partial  
- **Integrity Impact:** Partial  
- **Availability Impact:** None  
- **Exploitability:** Not_defined  
- **Remediation Level:** Not_defined  
- **Report Confidence:** Not_defined  
- **Availability Requirement:** Not_defined  
- **Collateral Damage Potential:** Not_defined  
- **Confidentiality Requirement:** Not_defined  
- **Integrity Requirement:** Not_defined  
- **Target Distribution:** Not_defined  

### CVSS3

- **Base Score:** 5.3  
- **Attack Vector:** Network  
- **Attack Complexity:** Low  
- **Privileges Required:** None  
- **User Interaction:** None  
- **Scope:** Unchanged  
- **Confidentiality Impact:** None  
- **Integrity Impact:** Low  
- **Availability Impact:** None  

### CWE  

- **CWE:** CWE-79  
- **Affected item:** /guestbook.php  
- **Affected parameter:** name  
- **Variants:** `test"()&%<acx><ScRiPt >ZhcH(9839)</ScRiPt>`  

#### Cross site scripting (verified)
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 6.4</th>
<th>Access Vector: Network_accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Complexity: Low</td>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

**CWE**

CWE-79

**Affected item**

/\guestbook.php

**Affected parameter**

text

**Variants**

555"()&%<acx><ScRiPt>ZhcH(9771)</ScRiPt>
Cross-site Scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-79 |

**Affected item**

`/hpp/`

**Affected parameter**

`pp`

**Variants**

`12"()&%<acx><ScRiPt >obqU(9099)</ScRiPt>`

---

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

---

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-79 |

**Affected item**

`/hpp/index.php`

**Affected parameter**

`pp`

**Variants**

`12"()&%<acx><ScRiPt >olPQ(9384)</ScRiPt>`

---

### Cross site scripting (verified)
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

CWE-79

**Affected item**

/hpp/params.php

**Affected parameter**

p

**Variants**

`1"'()&%<acx><ScrIpt Ou8l(9421)</ScrIpt>`

---

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
</table>
| Base Score: 6.4  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
</table>
| Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: Low  
Availability Impact: None |

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-79</td>
<td></td>
</tr>
</tbody>
</table>

**Affected item**  
/listproducts.php

**Affected parameter**  
cat

**Variants**  
1"()='&%<acx><ScRiPt >QSnL(9032)</ScRiPt>
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Cross site scripting (verified)

CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: Low
Availability Impact: None

CWE

CWE-79

Affected item /search.php
Affected parameter searchFor
Variants the"()&%<acx><ScRiPt >KMI8(9062)</ScRiPt>

CVSS2

Base Score: 6.4
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: Low
Availability Impact: None

CWE

CWE-79

Affected item /secured/newuser.php
Affected parameter uaddress
Variants 3137 Laguna Street"()&%<acx><ScRiPt >AiSa(9916)</ScRiPt>

Cross site scripting (verified)
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

<table>
<thead>
<tr>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/secured/newuser.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>ucc</td>
</tr>
</tbody>
</table>

**CWE**

| CWE-79 |

**Affected parameter**

| 4111111111111111'()&%<acx><ScRiPt >AiSa(9443)</ScRiPt> |

**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

<table>
<thead>
<tr>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/secured/newuser.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>ucc</td>
</tr>
</tbody>
</table>

**CWE**

| CWE-79 |

**Affected parameter**

| 4111111111111111'()&%<acx><ScRiPt >AiSa(9443)</ScRiPt> |
### Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

#### CWE

CWE-79

**Affected item**: `/secured/newuser.php`

**Affected parameter**: `uemail`

**Variants**: `sample@email.tst"()&%<acx><ScRiPt >AiSa(9827)</ScRiPt>`

#### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

#### CWE

CWE-79

**Affected item**: `/secured/newuser.php`

**Affected parameter**: `uphone`

**Variants**: `555-666-0606"()&%<acx><ScRiPt >AiSa(9032)</ScRiPt>`

**Cross site scripting (verified)**
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2
- Base Score: 6.4
- Access Vector: Network accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

CVSS3
- Base Score: 5.3
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: None
- Integrity Impact: Low
- Availability Impact: None

CWE
- CWE-79

Affected item
- /secured/newuser.php

Affected parameter
- uname

Variants
- fnfOzvSR"()&%<acx><ScRiPt >AiSa(9571)</ScRiPt>
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Cross site scripting

 tarde

Cross site scripting (verified)
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

### CVSS2
- **Base Score:** 6.4
- **Access Vector:** Network\_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not\_defined
- **Remediation Level:** Not\_defined
- **Report Confidence:** Not\_defined
- **Availability Requirement:** Not\_defined
- **Collateral Damage Potential:** Not\_defined
- **Confidentiality Requirement:** Not\_defined
- **Integrity Requirement:** Not\_defined
- **Target Distribution:** Not\_defined

### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE-79**

### Affected item
- `/userinfo.php`

### Affected parameter
- `uaddress`

### Variants
- `<script>alert("&amp;#1607;&amp;#1575;&amp;#1603;&amp;#1585; &amp;#1593;&amp;#1605;&amp;#1606;&amp;#1610; &amp;#1608;&amp;#1575;&amp;#1604;&amp;#1606;&amp;#1593;&amp;#1605; &amp;#1608;&amp;#1575;&amp;#1604;&amp;#1604;&amp;#1607; ")&gt;&lt;/script&gt;&lt;/ScRiPt&gt;AuWK(9974)`

---

**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

### CVSS2
- **Base Score:** 6.4
- **Access Vector:** Network\_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not\_defined
- **Remediation Level:** Not\_defined
- **Report Confidence:** Not\_defined
- **Availability Requirement:** Not\_defined
- **Collateral Damage Potential:** Not\_defined
- **Confidentiality Requirement:** Not\_defined
- **Integrity Requirement:** Not\_defined
- **Target Distribution:** Not\_defined
### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE:** CWE-79

### Affected item
- `/userinfo.php`

### Affected parameter
- `ucc`

### Variants
- `4111111111111111”()&%<acx><ScRiPt >AuWK(9288)</ScRiPt>`

### Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

### CVSS2
- **Base Score:** 6.4
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE:** CWE-79

### Affected item
- `/userinfo.php`

### Affected parameter
- `uemail`

### Variants
- `sample@email.tst”()&%<acx><ScRiPt >AuWK(9249)</ScRiPt>`

### Cross site scripting (verified)
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2          | Base Score: 6.4                          |
|               | Access Vector: Network_accessible        |
|               | Access Complexity: Low                  |
|               | Authentication: None                     |
|               | Confidentiality Impact: Partial          |
|               | Integrity Impact: Partial                |
|               | Availability Impact: None                |
|               | Exploitability: Not_defined              |
|               | Remediation Level: Not_defined           |
|               | Report Confidence: Not_defined           |
|               | Availability Requirement: Not_defined    |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined       |
|               | Target Distribution: Not_defined         |

| CVSS3          | Base Score: 5.3                          |
|               | Attack Vector: Network                  |
|               | Attack Complexity: Low                  |
|               | Privileges Required: None               |
|               | User Interaction: None                  |
|               | Scope: Unchanged                        |
|               | Confidentiality Impact: None            |
|               | Integrity Impact: Low                   |
|               | Availability Impact: None               |

| CWE          | CWE-79                                   |

| Affected item | /userinfo.php                           |
| Affected parameter | uphone                                 |
| Variants      | 555-666-0606""%&<acx><ScRiPt >AuWK(9520)</ScRiPt> |

Cross-site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2          | Base Score: 6.4                          |
|               | Access Vector: Network_accessible        |
|               | Access Complexity: Low                  |
|               | Authentication: None                     |
|               | Confidentiality Impact: Partial          |
|               | Integrity Impact: Partial                |
|               | Availability Impact: None                |
|               | Exploitability: Not_defined              |
|               | Remediation Level: Not_defined           |
|               | Report Confidence: Not_defined           |
|               | Availability Requirement: Not_defined    |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined       |
|               | Target Distribution: Not_defined         |
### Macromedia Dreamweaver remote database scripts (verified)

Macromedia Dreamweaver has created a directory (_mmServerScripts or _mmDBScripts) that contains scripts for testing database connectivity. One of these scripts (mmhttpdb.php or mmhttpdb.asp) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>Low</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-79</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>uname</td>
</tr>
<tr>
<td>Variants</td>
<td>sawsan&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;AuWK(9947)&lt;/ScRiPt&gt;</td>
</tr>
</tbody>
</table>

### Remote file inclusion XSS (verified)

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. The server opens arbitrary URLs and puts the content retrieved from the URL into the response without filtering.
## CVSS2
- **Base Score:** 6.4
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

## CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

## CWE
- **CWE:** CWE-79
- **Affected item:** /showimage.php
- **Affected parameter:** file
- **Variants:** Http://bxss.me/t/xss.html?%00

### Server side request forgery (verified)

SSRF as in Server Side Request Forgery is a vulnerability that allows an attacker to force server interfaces into sending packets initiated by the victim server to the local interface or to another server behind the firewall. Consult Web References for more information about this problem.

## CVSS2
- **Base Score:** 5.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined
### CVSS3

Base Score: 9.0  
Attack Vector: Network  
Attack Complexity: High  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: High

### CWE

CWE-918

**Affected item**  /showimage.php

**Affected parameter**  file

**Variants**  http://hitzgveqywwbb.bxss.me/

---

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

### CVSS2

Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

### CVSS3

Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

### CWE

CWE-89

**Affected item**  Web Server

**Affected parameter**  login

**Variants**  1ACUSTART”tsfKpACUEND

---

### SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
**CVSS2**

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

**CVSS3**

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

**CWE**

- **CWE-89**

**Affected item**

AJAX/infoartist.php

**Affected parameter**

id

**Variants**

1'

---

**SQL injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS2**

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
## CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE | CWE-89 |

### Affected item

| /AJAX/infocateg.php |

### Affected parameter

| id |

### Variants

| 1'' |

### SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

## CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

## CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE | CWE-89 |

### Affected item

| /AJAX/infotitle.php |

### Affected parameter

| id |

### Variants

| 1'' |

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

**Affected item:** /artists.php

**Affected parameter:** artist

**Variants:** 1ACUSTART™TYdWwACUEND

---

#### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  
| CWE   | CWE-89  
| Affected item | /artists.php  
| Affected parameter | login  
| Variants | 1ACUSTART**Ohp3MACUEND  

### CVSS2

| Base Score: 6.8  
| Access Vector: Network_accessible  
| Access Complexity: Medium  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: Partial  
| Availability Impact: Partial  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined  

### CVSS3

| Base Score: 10.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Changed  
| Confidentiality Impact: High  
| Integrity Impact: High  
| Availability Impact: None  
| CWE   | CWE-89  
| Affected item | /cart.php  
| Affected parameter | addcart  
| Variants | 1ACUSTART**8DJP8ACUEND  

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

#### Affected item
- **/cart.php**

#### Affected parameter
- **del**

#### Variants
- **1ACUSTART"\"OFXxiACUEND**

### SQL injection (verified)

**SQL injection (SQLi)** refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Affected item
- **/cart.php**

### Affected parameter
- **login**

### Variants
- 1ACUSTART”SQSQJoACUEND

---

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

---

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Affected item
- **/guestbook.php**

### Affected parameter
- **login**

### Variants
- 1ACUSTART”BQWkpACUEND

---

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  
| CWE | CWE-89  
| Affected item | /listproducts.php  
| Affected parameter | artist  
| Variants | 1ACUSTART""KVSljACUEND  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

### CWE
- CWE-89

### Affected item
- `/listproducts.php`

### Affected parameter
- `cat`

### Variants
- `1ACUSTART"oA8ddACUEND`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

### CVSS3

- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

### CWE
- CWE-89

### Affected item
- `/listproducts.php`

### Affected parameter
- `login`

### Variants
- `1ACUSTART"38PotACUEND`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

#### Affected item

/Mod_Rewrite_Shop/BuyProduct-3/

#### Affected parameter

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

### Affected item

/Mod_Rewrite_Shop/Details/color-printer/3/

### Affected parameter

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

### Affected item

/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

### Affected parameter

### SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

#### Affected item
/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

#### Affected parameter

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/product.php

**Affected parameter**

login

**Variants**

1ACUSTART"**DynjHACUEND

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/product.php

**Affected parameter**

pic

**Variants**

1ACUSTART"**BkMWvACUEND

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |

| CWE | CWE-89 |

**Affected item**  /search.php

**Affected parameter**  login

**Variants**  1ACUSTART”wSLFJACUEND

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS3 | Base Score: 10.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Changed  
| Confidentiality Impact: High  
| Integrity Impact: High  
| Availability Impact: None |

| CWE | CWE-89 |

| Affected item | /search.php |

| Affected parameter | searchFor |

| Variants | 1ACUSTART"jbBDSACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
| Access Vector: Network_accessible  
| Access Complexity: Medium  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: Partial  
| Availability Impact: Partial  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Changed  
| Confidentiality Impact: High  
| Integrity Impact: High  
| Availability Impact: None |

| CWE | CWE-89 |

| Affected item | /search.php |

| Affected parameter | test |

| Variants | 1ACUSTART"f3W3tACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

- **Base Score:** 6.8  
- **Access Vector:** NetworkAccessible  
- **Access Complexity:** Medium  
- **Authentication:** None  
- **Confidentiality Impact:** Partial  
- **Integrity Impact:** Partial  
- **Availability Impact:** Partial  
- **Exploitability:** NotDefined  
- **Remediation Level:** NotDefined  
- **Report Confidence:** NotDefined  
- **Availability Requirement:** NotDefined  
- **Collateral Damage Potential:** NotDefined  
- **Confidentiality Requirement:** NotDefined  
- **Integrity Requirement:** NotDefined  
- **Target Distribution:** NotDefined

### CVSS3

- **Base Score:** 10.0  
- **Attack Vector:** Network  
- **Attack Complexity:** Low  
- **Privileges Required:** None  
- **User Interaction:** None  
- **Scope:** Changed  
- **Confidentiality Impact:** High  
- **Integrity Impact:** High  
- **Availability Impact:** None

### CWE

- **CWE-89**

### Affected item

- `/secured/newuser.php`

### Affected parameter

- `uuname`

### Variants

- `1ACUSTART"Fxw80ACUEND`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **/sendcommand.php**

### Affected parameter

- **cart_id**

### Variants

- 1ACUSTART"'FWG7kACUEND

### SQL injection (verified)

**SQL injection (SQLi)** refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **/userinfo.php**

### Affected parameter

- **login**

### Variants

- 1ACUSTART"'E6rbyACUEND

### SQL injection

**SQL injection (SQLi)** refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |
| CWE  | CWE-89 |
| Affected item | /userinfo.php |
| Affected parameter | pass |
| Variants | 1" |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **/userinfo.php**

### Affected parameter

- **script#text**

### Variants

- `1ACUSTART""k15cFACUEND`

---

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **/userinfo.php**

### Affected parameter

- **script#text**

### Variants

- `'and(select 1 from(select count(*) ,concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(83),CHAR(81),CHAR(114),CHAR(113),CHAR(103),CHAR(106),CHAR(69),CHAR(84)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'`
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/userinfo.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>uaddress</td>
</tr>
<tr>
<td>Variants</td>
<td>1ACUSTART™4a8ycACUEND</td>
</tr>
</tbody>
</table>

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS3
Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE
CWE-89

Affected item
/userinfo.php

Affected parameter
uaddress

Variants
1ACUSTART"aSjczACUEND

SQL injection (verified)

Base Score: 6.8
Access Vector: Network_accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS2
Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE
CWE-89

Affected item
/userinfo.php

Affected parameter
uaddress

Variants
'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(115),CHAR(103),CHAR(76),CHAR(66),CHAR(112),CHAR(110),CHAR(51),CHAR(67)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
| Access Vector: Network_accessible  
| Access Complexity: Medium  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: Partial  
| Availability Impact: Partial  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Changed  
| Confidentiality Impact: High  
| Integrity Impact: High  
| Availability Impact: None |

| CWE | CWE-89 |
| Affected item | /userinfo.php |
| Affected parameter | ucc |
| Variants | 1ACUSTART"GD7BwACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
| Access Vector: Network_accessible  
| Access Complexity: Medium  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: Partial  
| Availability Impact: Partial  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |
### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Affected item
- **/userinfo.php**

### Affected parameter
- **ucc**

### Variants
- 1ACUSTART"92yp8ACUEND

---

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Affected item
- **/userinfo.php**

### Affected parameter
- **ucc**

### Variants
- `AND(SELECT 1 FROM(SELECT COUNT(*),CONCAT((SELECT CONCAT(CHAR(52),CHAR(67),CHAR(117),CHAR(112),CHAR(101),CHAR(80),CHAR(106),CHAR(80),CHAR(50),CHAR(101),CHAR(65)) FROM INFORMATION_SCHEMA.TABLES LIMIT 0,1),FLOOR RAND(0)*2))X FROM INFORMATION_SCHEMA.TABLES GROUP BY X)A)AND'`
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8
| | Access Vector: Network_accessible
| | Access Complexity: Medium
| | Authentication: None
| | Confidentiality Impact: Partial
| | Integrity Impact: Partial
| | Availability Impact: Partial
| | Exploitability: Not_defined
| | Remediation Level: Not_defined
| | Report Confidence: Not_defined
| | Availability Requirement: Not_defined
| | Collateral Damage Potential: Not_defined
| | Confidentiality Requirement: Not_defined
| | Integrity Requirement: Not_defined
| | Target Distribution: Not_defined

| CVSS3 | Base Score: 10.0
| | Attack Vector: Network
| | Attack Complexity: Low
| | Privileges Required: None
| | User Interaction: None
| | Scope: Changed
| | Confidentiality Impact: High
| | Integrity Impact: High
| | Availability Impact: None

CWE  
CWE-89

Affected item  
/userinfo.php

Affected parameter  
uemail

Variants  
1ACUSTART”GQ1gIACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8
| | Access Vector: Network_accessible
| | Access Complexity: Medium
| | Authentication: None
| | Confidentiality Impact: Partial
| | Integrity Impact: Partial
| | Availability Impact: Partial
| | Exploitability: Not_defined
| | Remediation Level: Not_defined
| | Report Confidence: Not_defined
| | Availability Requirement: Not_defined
| | Collateral Damage Potential: Not_defined
| | Confidentiality Requirement: Not_defined
| | Integrity Requirement: Not_defined
| | Target Distribution: Not_defined

362
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

### Affected item

/userinfo.php

### Affected parameter

eemail

### Variants

'1ACUSTART''IGowmACUEND

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

```sql
and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(55),CHAR(102),CHAR(116),CHAR(85),CHAR(85),CHAR(77),CHAR(100),CHAR(80)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'
```

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

### Affected item

/userinfo.php

### Affected parameter

eemail

### Variants

'1ACUSTART''IGowmACUEND

### SQL injection

SQL injection (verified) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessable  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|     |  
| Affected item | /userinfo.php  
| Affected parameter | uname  
| Variants | 1''

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessable  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CWE | CWE-89  
|     |  
| Affected item | /userinfo.php  
| Affected parameter | uname  
| Variants | 1''
**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/userinfo.php

**Affected parameter**

uphone

**Variants**

1ACUSTART”e11WxACUEND

---

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

---

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

---

**CWE**

CWE-89

**Affected item**

/userinfo.php

**Affected parameter**

uphone

**Variants**

1ACUSTART”52CZqACUEND

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

365
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |
| CWE   | CWE-89  
|       | Affected item /userinfo.php  
|       | Affected parameter uphone  
|       | Variants `and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(74),CHAR(101),CHAR(105),CHAR(113),CHAR(67),CHAR(76),CHAR(80),CHAR(101)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and`  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS3**
- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

**CWE**
- CWE-89

**Affected item**
- /userinfo.php

**Affected parameter**
- uname

**Variants**
- 1ACUSTART”PDJIPACUEND

**CVSS2**
- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**
- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

**CWE**
- CWE-89

**Affected item**
- /userinfo.php

**Affected parameter**
- uname

**Variants**
- 1ACUSTART”2kmCQACUEND

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_DEFINED
- **Integrity Requirement:** Not_DEFINED
- **Target Distribution:** Not_DEFINED

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89
- **Affected item:** `/userinfo.php`
- **Affected parameter:** `urname`

### Variants
- `'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(111),CHAR(57),CHAR(108),CHAR(51),CHAR(99),CHAR(79),CHAR(101),CHAR(70)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'`

### Cross site scripting (content-sniffing)

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

### CVSS2
- **Base Score:** 6.4
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_DEFINED
- **Integrity Requirement:** Not_DEFINED
- **Target Distribution:** Not_DEFINED
(14.1.3) Protecting application services transactions

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Total number of alerts in this category: 3

Alerts in this category

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
### User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

#### CVSS2

| Base Score | 5.0 |
| Access Vector | Network accessible |
| Access Complexity | Low |
| Authentication | None |
| Confidentiality Impact | Partial |
| Integrity Impact | None |
| Availability Impact | None |
| Exploitability | High |
| Remediation Level | Workaround |
| Report Confidence | Confirmed |
| Availability Requirement | Not_defined |
| Collateral Damage Potential | Not_defined |
| Confidentiality Requirement | Not_defined |
| Integrity Requirement | Not_defined |
| Target Distribution | Not_defined |

#### CVSS3

| Base Score | 9.1 |
| Attack Vector | Network |
| Attack Complexity | Low |
| Privileges Required | None |
| User Interaction | None |
| Scope | Unchanged |
| Confidentiality Impact | High |
| Integrity Impact | High |
| Availability Impact | None |

#### CWE

CWE-310

### Unencrypted connection (verified)

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.
| CVSS2 | Base Score: 5.8  
Access Vector: Network accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 9.1  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE | CWE-310 |
| Affected item | Web Server |
| Affected parameter | |

(14.2.1)Secure development policy

Rules for the development of software and systems shall be established and applied to developments within the organization.

Total number of alerts in this category: 98

Alerts in this category

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
</table>
| Base Score: 6.8  
Access Vector: Network accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |

**CWE**

**CWE-89**

**Affected item**

Web Server

**Affected parameter**

login

**Variants**

test%2Ftest' AND 3*2*1=6 AND '000QvXx'='000QvXx

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

#### Affected item

/AJAX/infoartist.php

#### Affected parameter

id

#### Variants

if(now()=sysdate(),sleep(0),0)

---

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

#### Affected item

/AJAX/infocateg.php

#### Affected parameter

id

#### Variants

if(now()=sysdate(),sleep(0),0)

---

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| **CVSS2** | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| **CVSS3** | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| **CWE** | CWE-89 |
| **Affected item** | /AJAX/infotitle.php |
| **Affected parameter** | id |
| **Variants** | if(now()=sysdate(),sleep(0),0) |

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| **CVSS2** | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

#### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/artists.php

**Affected parameter**

artist

**Variants**

1 AND 3*2*1=6 AND 909=909

---

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/artists.php

**Affected parameter**

login

**Variants**

test%2Ftest' AND 3*2*1=6 AND '0009eun'='0009eun
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/cart.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>addcart</td>
</tr>
<tr>
<td>Variants</td>
<td>if(now()=sysdate(),sleep(0),0)</td>
</tr>
</tbody>
</table>

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
Access Vector: Network accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| --- | --- |
| CVSS3 | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE | CWE-89 |
| Affected item | /listproducts.php |
| Affected parameter | artist |
| Variants | 1 AND 3*2*1=6 AND 568=568 |

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
**CVSS3**

Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

---

**CWE**

CWE-89

**Affected item**  
/listproducts.php

**Affected parameter**  
cat

**Variants**  
1 AND 3*2*1=6 AND 551=551

---

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

**CVSS2**

Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Remotely Exploitable: No  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

---

**CVSS3**

Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

---

**CWE**

CWE-89

**Affected item**  
/listproducts.php

**Affected parameter**  
login

**Variants**  
test%2Ftest' AND 3*2*1=6 AND '000Ccgn'='000Ccgn

---

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

**Affected item:** `/product.php`

**Affected parameter:** login

**Variants:** `test%2Ftest' AND 3*2*1=6 AND '000vXGJ'='000vXGJ`

---

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS3**
- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

CWE
- CWE-89

**Affected item**
- /product.php

**Affected parameter**
- pic

**Variants**
- 1 AND 3*2*1=6 AND 494=494

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS2**
- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**
- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

CWE
- CWE-89

**Affected item**
- /search.php

**Affected parameter**
- login

**Variants**
- test%2Ftest' AND 3*2*1=6 AND '000NAzi'='000NAzi

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector:</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Changed</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

**CWE**

| CWE-89 |

**Affected item**

/search.php

**Affected parameter**

searchFor

**Variants**

0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.
### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  
| CWE | CWE-89  
| Affected item | /search.php  
| Affected parameter | test  
| Variants | (select(0)from(select(sleep(0)))v)**+(select(0)from(select(sleep(0)))v)+"**+(select(0)from(select(sleep(0)))v)+"*/  

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  
| CWE | CWE-89  
| Affected item | /secured/newuser.php  
| Affected parameter | uuname  
| Variants | 0'XOR(if(now())=sysdate(),sleep(0),0))XOR'Z  

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

**Affected item**
/sendcommand.php

**Affected parameter**
cart_id

**Variants**

```
(select(0)from(select(sleep(0)))v)//+(select(0)from(select(sleep(0)))v)+"//+
(select(0)from(select(sleep(0)))v)+"/
```

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

<table>
<thead>
<tr>
<th>CWE-89</th>
</tr>
</thead>
</table>

Affected item /userinfo.php

Affected parameter login

Variants test%2Ftest' AND 3*2*1=6 AND '000GmMl'='000GmMl

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

<table>
<thead>
<tr>
<th>CWE-89</th>
</tr>
</thead>
</table>

Affected item /userinfo.php

Affected parameter pass

Variants -1' OR 3*2*1=6 AND 000283=000283 --
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network-accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |
| CWE   | CW-89  
|       | Affected item /userinfo.php  
|       | Affected parameter uname  
|       | Variants -1' OR 3*2*1=6 AND 00059=00059 --  

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.
### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **userinfo.php**

### Affected parameter

- **urname**

### Variants

- `0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z`

### Cross site scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

### CVSS2

- **Base Score:** 6.4
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE

- **CWE:** CWE-79

### Affected item

- **Web Server**

### Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
### CVSS2
- **Base Score:** 6.4
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE:** CWE-79

**Affected item**
- `/AJAX/showxml.php`

**Affected parameter**
- `mycookie`

**Variants**
- `3"()&%<acx><ScRiPt >t2Bk(9174)</ScRiPt>`

---

**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Cross-site Scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Cross site scripting (verified)

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: Low
Availability Impact: None

CWE
CWE-79

Affected item
/comment.php

Affected parameter
name

Variants
<your name here>"()&%<acx><ScRiPt >3R9A(9055)</ScRiPt>

Cross site scripting (verified)

Base Score: 6.4
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CWE
CWE-79

Affected item
guestbook.php

Affected parameter
name

Variants
test"()&%<acx><ScRiPt >ZhcH(9839)</ScRiPt>
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
</table>
| **Base Score:** 6.4  
**Access Vector:** Network_accessible  
**Access Complexity:** Low  
**Authentication:** None  
**Confidentiality Impact:** Partial  
**Integrity Impact:** Partial  
**Availability Impact:** None  
**Exploitability:** Not_defined  
**Remediation Level:** Not_defined  
**Report Confidence:** Not_defined  
**Availability Requirement:** Not_defined  
**Collateral Damage Potential:** Not_defined  
**Confidentiality Requirement:** Not_defined  
**Integrity Requirement:** Not_defined  
**Target Distribution:** Not_defined |

<table>
<thead>
<tr>
<th>CVSS3</th>
</tr>
</thead>
</table>
| **Base Score:** 5.3  
**Attack Vector:** Network  
**Attack Complexity:** Low  
**Privileges Required:** None  
**User Interaction:** None  
**Scope:** Unchanged  
**Confidentiality Impact:** None  
**Integrity Impact:** Low  
**Availability Impact:** None |

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CWE-79</strong></td>
</tr>
</tbody>
</table>

**Affected item** /guestbook.php

**Affected parameter** text

**Variants** 555"()&%<acx><ScRiPt >ZhcH(9771)</ScRiPt>
### Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None |
| CWE | CWE-79 |
| Affected item | /hpp/ |
| Affected parameter | pp |
| Variants | 12"()&%<acx><ScRiPt >obqU(9099)</ScRiPt> |

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediaion Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None |
| CWE | CWE-79 |
| Affected item | /hpp/index.php |
| Affected parameter | pp |
| Variants | 12"()&%<acx><ScRiPt >olPQ(9384)</ScRiPt> |

### Cross site scripting (verified)
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None |

| CWE   | CWE-79 |

| Affected item | /hpp/params.php |
| Affected parameter | p |
| Variants | 1"'()&%<acx><ScRiPt Ou8l(9421)</ScRiPt> |

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
### Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None  

| CWE | CWE-79  

| Affected item | /hpp/params.php  

| Affected parameter | pp  

| Variants | 12"()&%<acx><ScRiPt >isgP(9729)</ScRiPt>  

### Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: NotDefined  
|       | Integrity Requirement: NotDefined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None  

| CWE | CWE-79  

| Affected item | /listproducts.php  

| Affected parameter | artist  

| Variants | 1"()&%<acx><ScRiPt >IBxb(9649)</ScRiPt>  

### Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2 | Base Score: 6.4  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|

| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: Low  
Availability Impact: None |
|---|---|

CWE  
CWE-79

Affected item  
/listproducts.php

Affected parameter  
cat

Variants  
1"()&%<acx><ScrIpt >QSnL(9032)</ScrIpt>
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None |

| CWE | CWE-79 |

**Affected item**  
/secured/newuser.php  
**Affected parameter**  
ucc  
**Variants**  
4111111111111111"()'&%<acx><ScRiPt >AiSa(9443)</ScRiPt>  

**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
### Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-79</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/secured/newuser.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>uemail</td>
</tr>
<tr>
<td>Variants</td>
<td><a href="mailto:sample@email.tst">sample@email.tst</a>&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;AiSa(9827)&lt;/ScRiPt&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-79</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/secured/newuser.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>uphone</td>
</tr>
<tr>
<td>Variants</td>
<td>555-666-0606&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;AiSa(9032)&lt;/ScRiPt&gt;</td>
</tr>
</tbody>
</table>
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None  
| CWE   | CWE-79  
| Affected item | /secured/newuser.php  
| Affected parameter | urname  
| Variants | fnfOzvSR"()&%<acx>&<ScRiPt >AiSa(9571)</ScRiPt>  

**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

398
### Cross site scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None  
| CWE | CWE-79  
| Affected item | /secured/newuser.php  
| Affected parameter | uuname  
| Variants | fnfOzvSR"()%&<acx><ScRiPt >AiSa(9368)</ScRiPt>  

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None  
| CWE | CWE-79  
| Affected item | /userinfo.php  
| Affected parameter | script#text  
| Variants | alert(document.domain);9943();}]9285  

### Cross site scripting (verified)
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2       | Base Score: 6.4  
|             | Access Vector: Network_accessible  
|             | Access Complexity: Low  
|             | Authentication: None  
|             | Confidentiality Impact: Partial  
|             | Integrity Impact: Partial  
|             | Availability Impact: None  
|             | Exploitability: Not_defined  
|             | Remediation Level: Not_defined  
|             | Report Confidence: Not_defined  
|             | Availability Requirement: Not_defined  
|             | Collateral Damage Potential: Not_defined  
|             | Confidentiality Requirement: Not_defined  
|             | Integrity Requirement: Not_defined  
|             | Target Distribution: Not_defined  

| CVSS3       | Base Score: 5.3  
|             | Attack Vector: Network  
|             | Attack Complexity: Low  
|             | Privileges Required: None  
|             | User Interaction: None  
|             | Scope: Unchanged  
|             | Confidentiality Impact: None  
|             | Integrity Impact: Low  
|             | Availability Impact: None  

| CWE         | CWE-79  

| Affected item | /userinfo.php  
| Affected parameter | uaddress  

| Variants | `&lt;script&gt;alert("&amp;#1607;&amp;#1575;&amp;#1603;&amp;#1585;&amp;#1593;&amp;#1605;&amp;#1606;&amp;#1610;&amp;#1608;&amp;#1575;&amp;#1604;&amp;#1606;&amp;#1593;&amp;#1605;&amp;#1608;&amp;#1575;&amp;#1604;&amp;#1604;&amp;#1607;">"&amp;gt;&lt;/script&gt;&lt;ScRiPt &gt;AuWK(9974) &lt;/ScRiPt&gt;`  

**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

| CVSS2       | Base Score: 6.4  
|             | Access Vector: Network_accessible  
|             | Access Complexity: Low  
|             | Authentication: None  
|             | Confidentiality Impact: Partial  
|             | Integrity Impact: Partial  
|             | Availability Impact: None  
|             | Exploitability: Not_defined  
|             | Remediation Level: Not_defined  
|             | Report Confidence: Not_defined  
|             | Availability Requirement: Not_defined  
|             | Collateral Damage Potential: Not_defined  
|             | Confidentiality Requirement: Not_defined  
|             | Integrity Requirement: Not_defined  
|             | Target Distribution: Not_defined  

400
Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-79

Affected item /userinfo.php

Affected parameter ucc

Variants 4111111111111111’()&%<acx><ScRiPt >AuWK(9288)</ScRiPt>

Cross site scripting (verified)

CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-79

Affected item /userinfo.php

Affected parameter uemail

Variants sample@email.tst’()&%<acx><ScRiPt >AuWK(9249)</ScRiPt>
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.4</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
</tr>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-79</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
</tr>
</thead>
<tbody>
<tr>
<td>/userinfo.php</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>uphone</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
</tr>
</thead>
<tbody>
<tr>
<td>555-666-0606&quot;&quot;&quot;&quot;&quot;&quot;%&lt;acx&gt;&lt;ScRiPt &gt;AuWK(9520)&lt;/ScRiPt&gt;</td>
</tr>
</tbody>
</table>

**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.4</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
### CVSS3

| CVSS3 | Base Score: 5.3  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: None  
| Integrity Impact: Low  
| Availability Impact: None |

### CWE

| CWE | CWE-79 |

### Affected item

| Affected item | /userinfo.php |

### Affected parameter

| Affected parameter | urname |

### Variants

| Variants | sawsan"()&%<acx><ScRiPt >AuWK(9947)</ScRiPt> |

### File inclusion

This script is possibly vulnerable to file inclusion attacks.

It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.

### CVSS2

| CVSS2 | Base Score: 7.5  
| Access Vector: Network_accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: Partial  
| Availability Impact: Partial  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

### CWE

| CWE | CWE-20 |

### Affected item

| Affected item | /showimage.php |

### Affected parameter

| Affected parameter | file |

### Variants

| Variants | showimage.php |

### Macromedia Dreamweaver remote database scripts (verified)

Macromedia Dreamweaver has created a directory (_mmServerScripts or _mmDBScripts) that contains scripts for testing database connectivity. One of these scripts (mmhttpdb.php or mmhttpdb.asp) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.
**nginx SPDY heap buffer overflow**

A heap-based buffer overflow in the SPDY implementation in nginx 1.3.15 before 1.4.7 and 1.5.x before 1.5.12 allows remote attackers to execute arbitrary code via a crafted request. The problem affects nginx compiled with the `ngx_http_spdy_module` module (which is not compiled by default) and without `--with-debug` configure option, if the "spdy" option of the "listen" directive is used in a configuration file.

---

**Remote file inclusion XSS (verified)**

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. The server opens arbitrary URLs and puts the content retrieved from the URL into the response without filtering.
| CVSS2 | Base Score: 6.4  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: Low  
Availability Impact: None |
| CWE | CWE-79 |
| Affected item | /showimage.php |
| Affected parameter | file |
| Variants | Http://bxss.me/t/xss.html?%00 |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

<table>
<thead>
<tr>
<th>Affected item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>login</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
</tr>
</thead>
<tbody>
<tr>
<td>1ACUSTART''tsfKpACUEND</td>
</tr>
</tbody>
</table>

### SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

<table>
<thead>
<tr>
<th>Affected item</th>
</tr>
</thead>
<tbody>
<tr>
<td>/AJAX/infoartist.php</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
</tr>
</thead>
<tbody>
<tr>
<td>1&quot;</td>
</tr>
</tbody>
</table>
### CVSS2

- **Base Score:** 6.8  
- **Access Vector:** Network accessible  
- **Access Complexity:** Medium  
- **Authentication:** None  
- **Confidentiality Impact:** Partial  
- **Integrity Impact:** Partial  
- **Availability Impact:** Partial  
- **Exploitability:** Not_defined  
- **Remediation Level:** Not_defined  
- **Report Confidence:** Not_defined  
- **Availability Requirement:** Not_defined  
- **Collateral Damage Potential:** Not_defined  
- **Confidentiality Requirement:** Not_defined  
- **Integrity Requirement:** Not_defined  
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0  
- **Attack Vector:** Network  
- **Attack Complexity:** Low  
- **Privileges Required:** None  
- **User Interaction:** None  
- **Scope:** Changed  
- **Confidentiality Impact:** High  
- **Integrity Impact:** High  
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89
- **Affected item:** /AJAX/infocateg.php
- **Affected parameter:** id
- **Variants:** 1"'

### SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8  
- **Access Vector:** Network accessible  
- **Access Complexity:** Medium  
- **Authentication:** None  
- **Confidentiality Impact:** Partial  
- **Integrity Impact:** Partial  
- **Availability Impact:** Partial  
- **Exploitability:** Not_defined  
- **Remediation Level:** Not_defined  
- **Report Confidence:** Not_defined  
- **Availability Requirement:** Not_defined  
- **Collateral Damage Potential:** Not_defined  
- **Confidentiality Requirement:** Not_defined  
- **Integrity Requirement:** Not_defined  
- **Target Distribution:** Not_defined
**CVSS 3**

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

**CWE**

- **CWE-89**

**Affected item**

- **/AJAX/infotitle.php**

**Affected parameter**

- **id**

**Variants**

- `1''`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

**CVSS 2**

- **Base Score:** 6.8
- **Access Vector:** Networkaccessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

**CVSS 3**

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

**CWE**

- **CWE-89**

**Affected item**

- **/artists.php**

**Affected parameter**

- **artist**

**Variants**

- `1ACUSTART'''TYdWwACUEND`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2          | Base Score: 6.8  |
|               | Access Vector: Network_accessible  |
|               | Access Complexity: Medium  |
|               | Authentication: None  |
|               | Confidentiality Impact: Partial  |
|               | Integrity Impact: Partial  |
|               | Availability Impact: Partial  |
|               | Exploitability: Not_defined  |
|               | Remediation Level: Not_defined  |
|               | Report Confidence: Not_defined  |
|               | Availability Requirement: Not_defined  |
|               | Collateral Damage Potential: Not_defined  |
|               | Confidentiality Requirement: Not_defined  |
|               | Integrity Requirement: Not_defined  |
|               | Target Distribution: Not_defined  |

| CVSS3          | Base Score: 10.0  |
|               | Attack Vector: Network  |
|               | Attack Complexity: Low  |
|               | Privileges Required: None  |
|               | User Interaction: None  |
|               | Scope: Changed  |
|               | Confidentiality Impact: High  |
|               | Integrity Impact: High  |
|               | Availability Impact: None  |

| CWE           | CWE-89  |
|               |  |

**Affected item**
/artists.php

**Affected parameter**
login

**Variants**
1ACUSTART''Ohp3MACUEND

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |

| CWE   | CWE-89 |

| Affected item | /cart.php |
| Affected parameter | addcart |
| Variants | 1ACUSTART"**8DJP8ACUEND |

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |

| CWE   | CWE-89 |

| Affected item | /cart.php |
| Affected parameter | del |
| Variants | 1ACUSTART"**OFXxiACUEND |

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| ------ | --------------------------------------------- |
| CVSS3 | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE    | CWE-89 |
| Affected item | /cart.php |
| Affected parameter | login |
| Variants | 1ACUSTART™SQSJoACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| ------ | --------------------------------------------- |
### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

#### Affected item
- /guestbook.php

#### Affected parameter
- login

#### Variants
- `1ACUSTART''BQWkpACUEND`

---

#### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

#### Affected item
- /listproducts.php

#### Affected parameter
- artist

#### Variants
- `1ACUSTART''KVSljACUEND`

---

#### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |
| CWE   | CWE-89 |
| Affected item | /listproducts.php |
| Affected parameter | cat |
| Variants | 1ACUSTART"oA8ddACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/Mod_Rewrite_Shop/Details/color-printer/3/

**Affected parameter**

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

---

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>
**SQL injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**CVSS2**

- Base Score: 6.8
- Access Vector: Network accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**

- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**CVSS3**

- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None
| CVSS2          | Base Score: 6.8  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Medium  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: Partial  
|               | Availability Impact: Partial  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  |
| CVSS3         | Base Score: 10.0  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Changed  
|               | Confidentiality Impact: High  
|               | Integrity Impact: High  
|               | Availability Impact: None  |
| CWE           | CWE-89  
| Affected item | /product.php  
| Affected parameter | login  
| Variants     | 1ACUSTART''DynjHACUEND  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Changed</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

`/product.php`

**Affected parameter**

`pic`

**Variants**

1ACUSTART"BkMWvACUEND

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessable</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Changed</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

`/search.php`

**Affected parameter**

`login`

**Variants**

1ACUSTART"wSLFJACUEND

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |
| CWE   | CWE-89 |
| Affected item | /search.php |
| Affected parameter | searchFor |
| Variants | 1ACUSTART"jbBDSACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS3 | Base Score: 10.0  
| | Attack Vector: Network  
| | Attack Complexity: Low  
| | Privileges Required: None  
| | User Interaction: None  
| | Scope: Changed  
| | Confidentiality Impact: High  
| | Integrity Impact: High  
| | Availability Impact: None  
| CWE | CWE-89  
| Affected item | /search.php  
| Affected parameter | test  
| Variants | 1ACUSTART"f3W3tACUEND  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
| | Access Vector: Network_accessible  
| | Access Complexity: Medium  
| | Authentication: None  
| | Confidentiality Impact: Partial  
| | Integrity Impact: Partial  
| | Availability Impact: Partial  
| | Exploitability: Not_defined  
| | Remediation Level: Not_defined  
| | Report Confidence: Not_defined  
| | Availability Requirement: Not_defined  
| | Collateral Damage Potential: Not_defined  
| | Confidentiality Requirement: Not_defined  
| | Integrity Requirement: Not_defined  
| | Target Distribution: Not_defined  
| CVSS3 | Base Score: 10.0  
| | Attack Vector: Network  
| | Attack Complexity: Low  
| | Privileges Required: None  
| | User Interaction: None  
| | Scope: Changed  
| | Confidentiality Impact: High  
| | Integrity Impact: High  
| | Availability Impact: None  
| CWE | CWE-89  
| Affected item | /secured/newuser.php  
| Affected parameter | uname  
| Variants | 1ACUSTART"Fxw80ACUEND  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** NetworkAccessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** NotDefined
- **Remediation Level:** NotDefined
- **Report Confidence:** NotDefined
- **Availability Requirement:** NotDefined
- **Collateral Damage Potential:** NotDefined
- **Confidentiality Requirement:** NotDefined
- **Integrity Requirement:** NotDefined
- **Target Distribution:** NotDefined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE-89**

#### Affected item
- `/sendcommand.php`

#### Affected parameter
- `cart_id`

#### Variants
- `1ACUSTART'"FWG7kACUEND`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Affected item /userinfo.php

Affected parameter login

Variants 1ACUSTART"E6rbyACUEND

CVSS2

Base Score: 6.8
Access Vector: Network_accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Affected item /userinfo.php

Affected parameter pass

Variants 1"
| CVSS2 | Base Score: 6.8  
| Access Vector: Network accessible  
| Access Complexity: Medium  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: Partial  
| Availability Impact: Partial  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Changed  
| Confidentiality Impact: High  
| Integrity Impact: High  
| Availability Impact: None |

| CWE | CWE-89 |

| Affected item | /userinfo.php |
| Affected parameter | script#text |
| Variants | 1ACUSTART”‘k15cFACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS3 | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None  |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-89</td>
</tr>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Variants</td>
<td>'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(83),CHAR(81),CHAR(114),CHAR(113),CHAR(103),CHAR(106),CHAR(69),CHAR(84)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'</td>
</tr>
</tbody>
</table>

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined  |
|---|---|
| CVSS3 | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None  |
| CWE | CWE-89  |
| Affected item | /userinfo.php  |
| Affected parameter | uaddress  |
| Variants | 1ACUSTART"4a8ycACUEND  |

**SQL injection (verified)**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |

| CWE   | CWE-89 |
|       |       |

| Affected item | /userinfo.php |
|               |             |

| Affected parameter | uaddress |
|                    |         |

| Variants | 1ACUSTART"aSjczACUEND |
|          |                 |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 10.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Changed  
| Confidentiality Impact: High  
| Integrity Impact: High  
| Availability Impact: None |

**CWE**  
CWE-89

**Affected item**  
/userinfo.php

**Affected parameter**  
uaddress

**Variants**  
`'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(115),CHAR(103),CHAR(76),CHAR(66),CHAR(112),CHAR(110),CHAR(51),CHAR(67)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'`

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
| Access Vector: Network_accessible  
| Access Complexity: Medium  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: Partial  
| Availability Impact: Partial  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Changed  
| Confidentiality Impact: High  
| Integrity Impact: High  
| Availability Impact: None |

**CWE**  
CWE-89

**Affected item**  
/userinfo.php

**Affected parameter**  
ucc

**Variants**  
1ACUSTART™GD7BwACUEND

**SQL injection (verified)**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 10.0</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Changed</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: High</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
<td></td>
</tr>
<tr>
<td>Affected parameter</td>
<td>ucc</td>
<td></td>
</tr>
<tr>
<td>Variants</td>
<td>1ACUSTART™92yp8ACUEND</td>
<td></td>
</tr>
</tbody>
</table>

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
**CVSS3**

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

**CWE**

- **CWE-89**

**Affected item**

- `/userinfo.php`

**Affected parameter**

- `ucc`

**Variants**

- `and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(112),CHAR(101),CHAR(80),CHAR(106),CHAR(80),CHAR(50),CHAR(101),CHAR(65)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and`

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

**CVSS2**

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

---

**CVSS3**

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

**CWE**

- **CWE-89**

**Affected item**

- `/userinfo.php`

**Affected parameter**

- `uemail`

**Variants**

- `1ACUSTART"GQ1giACUEND`

**SQL injection (verified)**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  

| Affected item | /userinfo.php  
| Affected parameter | uemail  

| Variants | 1ACUSTART"IGowmACUEND  

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

429
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  
| CWE   | CWE-89  
| Affected item | /userinfo.php  
| Affected parameter | uemail  
| Variants | 'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(55),CHAR(102),CHAR(116),CHAR(85),CHAR(85),CHAR(77),CHAR(100),CHAR(80)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'  

**SQL injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  
| CWE   | CWE-89  
| Affected item | /userinfo.php  
| Affected parameter | uname  
| Variants | 1''  

**SQL injection (verified)**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE  | CWE-89  
|      |  

| Affected item | /userinfo.php  
|               |  

| Affected parameter | uphone  
|                    |  

| Variants | 1ACUSTART"e11WxACUEND  
|          |  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

431
### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|-----|-------  

**Affected item**  
/userinfo.php

**Affected parameter**  
uphone

**Variants**  
'ACUSTART''52CZqACUEND

---

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

---

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|-----|-------  

**Affected item**  
/userinfo.php

**Affected parameter**  
uphone

**Variants**  
'and(select 1 from(select count(*),concat((select CHAR(52),CHAR(67),CHAR(117),CHAR(74),CHAR(101),CHAR(105),CHAR(113),CHAR(67),CHAR(76),CHAR(80),CHAR(101)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

| CVSS2 | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| CVSS3 | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE | CWE-89 |
| Affected item | /userinfo.php |
| Affected parameter | urname |
| Variants | 1ACUSTART''PDJfPACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

| CVSS2 | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
### CVSS3
Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None  

### CWE
CWE-89

### Affected item
/userinfo.php

### Affected parameter
urname

### Variants
1ACUSTART**2kmCQACUEND

---

#### SQL injection (verified)

**SQL injection (SQLi)** refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
Base Score: 6.8  
Access Vector: Network\_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not\_defined  
Remediation Level: Not\_defined  
Report Confidence: Not\_defined  
Availability Requirement: Not\_defined  
Collateral Damage Potential: Not\_defined  
Confidentiality Requirement: Not\_defined  
Integrity Requirement: Not\_defined  
Target Distribution: Not\_defined

### CVSS3
Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

### CWE
CWE-89

### Affected item
/userinfo.php

### Affected parameter
urname

### Variants
'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(111),CHAR(57),CHAR(108),CHAR(51),CHAR(99),CHAR(79),CHAR(101),CHAR(70)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'

---

#### Cross site scripting (content-sniffing)

434
This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None |

| CWE | CWE-79 |

| Affected item | /showimage.php |
| Affected parameter | file |
| Variants | ./pictures/1.jpg""&%<acx><ScRiPt>yTNC(9475)</ScRiPt> |

HTTP parameter pollution

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.
### CVSS2
Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: Partial  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

### CVSS3
Base Score: 9.1  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

### CWE
CWE-88

**Affected item**  
/hpp/

**Affected parameter**  
pp

**Variants**  
12&n994137=v968503

### HTTP parameter pollution
This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.

### CVSS2
Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: Partial  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined
| CVSS3 | Base Score: 9.1  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-88</th>
</tr>
</thead>
</table>

**Affected item**  
/hpp/index.php  

**Affected parameter**  
pp  

**Variants**  
12&n910804=v977330

**14.3.1 Protection of test data**

Test data shall be selected carefully, protected and controlled.

Total number of alerts in this category: 7

**Alerts in this category**

**Backup files**

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
</table>

**Affected item**  
/index.bak  

**Affected parameter**

**Backup files**

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.
| CVSS2          | Base Score: 5.0  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

| CWE          | CWE-538  

**Affected item** /index.zip  

**Affected parameter**  

---  

**JetBrains .idea project directory**  

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

---  

| CVSS2          | Base Score: 5.0  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

| CWE          | CWE-538  

**Affected item** Web Server  

**Affected parameter**  

---  

**PHPinfo page (verified)**  

PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.
| **CVSS2** | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| **CVSS3** | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| **CWE** | CWE-200 |
| **Affected item** | /secured/phpinfo.php |
| **Affected parameter** | |

**PHPinfo page found**

This script is using phpinfo() function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.
### CVSS3
- **Base Score**: 7.5
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Unchanged
- **Confidentiality Impact**: High
- **Integrity Impact**: None
- **Availability Impact**: None

### CWE
- **CWE-200**

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/secured/phpinfo.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

### WS_FTP log file found (verified)

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

### CVSS2
- **Base Score**: 5.0
- **Access Vector**: Network_accessible
- **Access Complexity**: Low
- **Authentication**: None
- **Confidentiality Impact**: Partial
- **Integrity Impact**: None
- **Availability Impact**: None
- **Exploitability**: Not_defined
- **Remediation Level**: Not_defined
- **Report Confidence**: Not_defined
- **Availability Requirement**: Not_defined
- **Collateral Damage Potential**: Not_defined
- **Confidentiality Requirement**: Not_defined
- **Integrity Requirement**: Not_defined
- **Target Distribution**: Not_defined

### CWE
- **CWE-538**

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/pictures/WS_FTP.LOG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

### Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.
### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/hpp/test.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>
### CVSS2

- **Base Score:** 6.8  
- **Access Vector:** Network accessible  
- **Access Complexity:** Medium  
- **Authentication:** None  
- **Confidentiality Impact:** Partial  
- **Integrity Impact:** Partial  
- **Availability Impact:** Partial  
- **Exploitability:** Not_defined  
- **Remediation Level:** Not_defined  
- **Report Confidence:** Not_defined  
- **Availability Requirement:** Not_defined  
- **Collateral Damage Potential:** Not_defined  
- **Confidentiality Requirement:** Not_defined  
- **Integrity Requirement:** Not_defined  
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0  
- **Attack Vector:** Network  
- **Attack Complexity:** Low  
- **Privileges Required:** None  
- **User Interaction:** None  
- **Scope:** Changed  
- **Confidentiality Impact:** High  
- **Integrity Impact:** High  
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89
- **Affected item:** Web Server
- **Affected parameter:** login
- **Variants:** test%2Ftest' AND 3*2*1=6 AND '000QvXx'='000QvXx

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE-89**

### Affected item

/\AJAX/infotitle.php

### Affected parameter

id

### Variants

if(now()=sysdate(),sleep(0),0)

---

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

### CWE

CWE-89

### Affected item

/artists.php

### Affected parameter

artist

### Variants

1 AND 3*2*1=6 AND 909=909

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
<th>Access Vector: Network_accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Complexity: Medium</td>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

### CWE

CWE-89

### Affected item

/artists.php

### Affected parameter

login

### Variants

test%2Ftest' AND 3*2*1=6 AND '0009eun'='0009eun

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
<table>
<thead>
<tr>
<th>Component</th>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>6.8</td>
<td>10.0</td>
</tr>
<tr>
<td>Access Vector</td>
<td>Network accessible</td>
<td>Network</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>Partial</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>Partial</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
<td>Not_defined</td>
</tr>
<tr>
<td>CWE</td>
<td>CWE-89</td>
<td></td>
</tr>
<tr>
<td>Affected item</td>
<td>/cart.php</td>
<td></td>
</tr>
<tr>
<td>Affected parameter</td>
<td>addcart</td>
<td></td>
</tr>
<tr>
<td>Variants</td>
<td>if(now()=sysdate(),sleep(0),0)</td>
<td></td>
</tr>
</tbody>
</table>

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |

**CWE**  
CWE-89

**Affected item**  
/cart.php

**Affected parameter**  
login

**Variants**  
test%2Ftest' AND 3*2*1=6 AND '000rpl5'='000rpl5

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |

**CWE**  
CWE-89

**Affected item**  
guestbook.php

**Affected parameter**  
login

**Variants**  
(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'*/(select(0)from(select(sleep(0)))v)+*/

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: NetworkAccessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: NotDefined  
|       | Remediation Level: NotDefined  
|       | Report Confidence: NotDefined  
|       | Availability Requirement: NotDefined  
|       | Collateral Damage Potential: NotDefined  
|       | Confidentiality Requirement: NotDefined  
|       | Integrity Requirement: NotDefined  
|       | Target Distribution: NotDefined |
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |
| CWE   | CWE-89 |
| Affected item | /listproducts.php |
| Affected parameter | artist |
| Variants | 1 AND 3*2*1=6 AND 568=568 |

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: NetworkAccessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: NotDefined  
|       | Remediation Level: NotDefined  
|       | Report Confidence: NotDefined  
|       | Availability Requirement: NotDefined  
|       | Collateral Damage Potential: NotDefined  
|       | Confidentiality Requirement: NotDefined  
|       | Integrity Requirement: NotDefined  
|       | Target Distribution: NotDefined |
## CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

## CWE

- **CWE:** CWE-89

## Affected item

- **/listproducts.php**

## Affected parameter

- **cat**

## Variants

- `1 AND 3*2*1=6 AND 551=551`

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

## CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

---

## CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

## CWE

- **CWE:** CWE-89

## Affected item

- **/listproducts.php**

## Affected parameter

- **login**

## Variants

- `test%2Ftest' AND 3*2*1=6 AND '000Ccgn'='000Ccgn`

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
**CVSS2**

- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

**CVSS3**

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

**CWE**

- **CWE-89**

**Affected item**

/product.php

**Affected parameter**

login

**Variants**

test%2Ftest' AND 3*2*1=6 AND '000vXGJ'='000vXGJ

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-89</th>
</tr>
</thead>
</table>

### Affected item

<table>
<thead>
<tr>
<th>/product.php</th>
</tr>
</thead>
</table>

### Affected parameter

<table>
<thead>
<tr>
<th>pic</th>
</tr>
</thead>
</table>

### Variants

<table>
<thead>
<tr>
<th>1 AND 3<em>2</em>1=6 AND 494=494</th>
</tr>
</thead>
</table>

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-89</th>
</tr>
</thead>
</table>

### Affected item

<table>
<thead>
<tr>
<th>/search.php</th>
</tr>
</thead>
</table>

### Affected parameter

<table>
<thead>
<tr>
<th>login</th>
</tr>
</thead>
</table>

### Variants

<table>
<thead>
<tr>
<th>test%2Ftest' AND 3<em>2</em>1=6 AND '000NAzi'='000NAzi</th>
</tr>
</thead>
</table>

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
Access Vector: Network accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE | CWE-89 |
| Affected item | /search.php |
| Affected parameter | searchFor |
| Variants | `0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z` |

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

- CWE-89

Affected item: `/search.php`

Affected parameter: `test`

Variants: `(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'*/(select(0)from(select(sleep(0)))v)/*`/`

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

- CWE-89

Affected item: `/secured/newuser.php`

Affected parameter: `uname`

Variants: `0''XOR(if(now()=sysdate(),sleep(0),0))XOR'Z`

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.
| CVSS2          | Base Score: 6.8  
|               | Access Vector: Network accessible  
|               | Access Complexity: Medium  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: Partial  
|               | Availability Impact: Partial  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  |
| CVSS3          | Base Score: 10.0  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Changed  
|               | Confidentiality Impact: High  
|               | Integrity Impact: High  
|               | Availability Impact: None  |
| CWE            | CWE-89            |
| Affected item  | /sendcommand.php  |
| Affected parameter | cart_id          |
| Variants       | (select(0)from(select(sleep(0)))v)""+(select(0)from(select(sleep(0)))v)+""+(select(0)from(select(sleep(0)))v)+""/ |

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- /userinfo.php

### Affected parameter

- login

### Variants

- `test%2Ftest' AND 3*2*1=6 AND '000GmMl'='000GmMl`

---

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

---

### CWE

- **CWE:** CWE-89

### Affected item

- /userinfo.php

### Affected parameter

- pass

### Variants

- `-1' OR 3*2*1=6 AND 000283=000283 --`

---

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
**CVSS2**

- **Base Score:** 6.8  
- **Access Vector:** Network accessible  
- **Access Complexity:** Medium  
- **Authentication:** None  
- **Confidentiality Impact:** Partial  
- **Integrity Impact:** Partial  
- **Availability Impact:** Partial  
- **Exploitability:** Not_defined  
- **Remediation Level:** Not_defined  
- **Report Confidence:** Not_defined  
- **Availability Requirement:** Not_defined  
- **Collateral Damage Potential:** Not_defined  
- **Confidentiality Requirement:** Not_defined  
- **Integrity Requirement:** Not_defined  
- **Target Distribution:** Not_defined

**CVSS3**

- **Base Score:** 10.0  
- **Attack Vector:** Network  
- **Attack Complexity:** Low  
- **Privileges Required:** None  
- **User Interaction:** None  
- **Scope:** Changed  
- **Confidentiality Impact:** High  
- **Integrity Impact:** High  
- **Availability Impact:** None

**CWE**

- **CWE-89**

**Affected item**  
`/userinfo.php`

**Affected parameter**  
`uname`

**Variants**  
`-1' OR 3*2*1=6 AND 00059=00059 --`

---

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Macromedia Dreamweaver remote database scripts (verified)

Macromedia Dreamweaver has created a directory (_mmServerScripts or _mmDBScripts) that contains scripts for testing database connectivity. One of these scripts (mmhttpdb.php or mmhttpdb.asp) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.

Possible database backup

Manual confirmation is required for this alert.

It looks like this file contains a database backup/dump. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.
### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not defined</td>
</tr>
<tr>
<td>Remediation Level: Not defined</td>
</tr>
<tr>
<td>Report Confidence: Not defined</td>
</tr>
<tr>
<td>Availability Requirement: Not defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not defined</td>
</tr>
<tr>
<td>Target Distribution: Not defined</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE: CWE-538</th>
</tr>
</thead>
</table>

**Affected item**

/admin/create.sql

**Affected parameter**

<table>
<thead>
<tr>
<th>SQL injection (verified)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.</td>
</tr>
</tbody>
</table>

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not defined</td>
</tr>
<tr>
<td>Remediation Level: Not defined</td>
</tr>
<tr>
<td>Report Confidence: Not defined</td>
</tr>
<tr>
<td>Availability Requirement: Not defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not defined</td>
</tr>
<tr>
<td>Target Distribution: Not defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE: CWE-89</th>
</tr>
</thead>
</table>

**Affected item**

Web Server

**Affected parameter**

login

**Variants**

1ACUSTART"tsfKpACUEND
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | | Base Score: 6.8  
| | | Access Vector: Network_accessible  
| | | Access Complexity: Medium  
| | | Authentication: None  
| | | Confidentiality Impact: Partial  
| | | Integrity Impact: Partial  
| | | Availability Impact: Partial  
| | | Exploitability: Not_defined  
| | | Remediation Level: Not_defined  
| | | Report Confidence: Not_defined  
| | | Availability Requirement: Not_defined  
| | | Collateral Damage Potential: Not_defined  
| | | Confidentiality Requirement: Not_defined  
| | | Integrity Requirement: Not_defined  
| | | Target Distribution: Not_defined  

| CVSS3 | | Base Score: 10.0  
| | | Attack Vector: Network  
| | | Attack Complexity: Low  
| | | Privileges Required: None  
| | | User Interaction: None  
| | | Scope: Changed  
| | | Confidentiality Impact: High  
| | | Integrity Impact: High  
| | | Availability Impact: None  

| CWE | | CWE-89  

| Affected item | | /AJAX/infoartist.php  
| Affected parameter | | id  
| Variants | | 1"  

**SQL injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

| CWE-89 |

**Affected item**

| /AJAX/infocateg.php |

**Affected parameter**

| id |

**Variants**

| 1'" |

---

**SQL injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

| CWE-89 |

**Affected item**

| /AJAX/infotitle.php |

**Affected parameter**

| id |

**Variants**

| 1'" |

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
CVSS2

Base Score: 6.8
Access Vector: Network_accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Affected item
/artists.php

Affected parameter
artist

Variants
1ACUSTART™TYdWwACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2

Base Score: 6.8
Access Vector: Network_accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined
### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|     |     

| Affected item | /artists.php  
|               |     

| Affected parameter | login  
|                    |     

| Variants | 1ACUSTART"'Ohp3MACUEND  
|          |     

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|     |     

| Affected item | /cart.php  
|               |     

| Affected parameter | addcart  
|                    |     

| Variants | 1ACUSTART"8DJP8ACUEND  
|          |     

---
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Base Score: 10.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-89</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/cart.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>del</td>
</tr>
<tr>
<td>Variants</td>
<td>1ACUSTART''OFXxiACUEND</td>
</tr>
</tbody>
</table>

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

### CWE

CWE-89

### Affected item

/cart.php

### Affected parameter

login

### Variants

1ACUSTART''SQSJoACUEND

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

Base Score: 6.8  
Access Vector: Network accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not defined  
Remediation Level: Not defined  
Report Confidence: Not defined  
Availability Requirement: Not defined  
Collateral Damage Potential: Not defined  
Confidentiality Requirement: Not defined  
Integrity Requirement: Not defined  
Target Distribution: Not defined

### CVSS3

Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

### CWE

CWE-89

### Affected item

/guestbook.php

### Affected parameter

login

### Variants

1ACUSTART''BQWkpACUEND

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |
| CWE  | CWE-89 |
| Affected item | /listproducts.php |
| Affected parameter | artist |
| Variants | 1ACUSTART'"KVSjACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS3

- **Base Score**: 10.0
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Changed
- **Confidentiality Impact**: High
- **Integrity Impact**: High
- **Availability Impact**: None

### CWE

- **CWE**: CWE-89

### Affected item

- **/listproducts.php**

### Affected parameter

- **cat**

### Variants

- 1ACUSTART"oA8ddACUEND

### CVSS2

- **Base Score**: 6.8
- **Access Vector**: Network_accessible
- **Access Complexity**: Medium
- **Authentication**: None
- **Confidentiality Impact**: Partial
- **Integrity Impact**: Partial
- **Availability Impact**: Partial
- **Exploitability**: Not_defined
- **Remediation Level**: Not_defined
- **Report Confidence**: Not_defined
- **Availability Requirement**: Not_defined
- **Collateral Damage Potential**: Not_defined
- **Confidentiality Requirement**: Not_defined
- **Integrity Requirement**: Not_defined
- **Target Distribution**: Not_defined

### CVSS3

- **Base Score**: 10.0
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Changed
- **Confidentiality Impact**: High
- **Integrity Impact**: High
- **Availability Impact**: None

### CWE

- **CWE**: CWE-89

### Affected item

- **/listproducts.php**

### Affected parameter

- **login**

### Variants

- 1ACUSTART"38PotACUEND

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2          | Base Score: 6.8  
|               | Access Vector: Network accessible  
|               | Access Complexity: Medium  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: Partial  
|               | Availability Impact: Partial  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

| CVSS3          | Base Score: 10.0  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Changed  
|               | Confidentiality Impact: High  
|               | Integrity Impact: High  
|               | Availability Impact: None  

| CWE           | CWE-89  

**Affected item**
/Mod_Rewrite_Shop/BuyProduct-3/

**Affected parameter**

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Base Score: 10.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Target Distribution: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
</tbody>
</table>

CWE     CWE-89
Affected item /Mod_Rewrite_Shop/Details/color-printer/3/
Affected parameter

SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

**Base Score:** 6.8  
**Access Vector:** Network accessible  
**Access Complexity:** Medium  
**Authentication:** None  
**Confidentiality Impact:** Partial  
**Integrity Impact:** Partial  
**Availability Impact:** Partial  
**Exploitability:** Not_defined  
**Remediation Level:** Not_defined  
**Report Confidence:** Not_defined  
**Availability Requirement:** Not_defined  
**Collateral Damage Potential:** Not_defined  
**Confidentiality Requirement:** Not_defined  
**Integrity Requirement:** Not_defined  
**Target Distribution:** Not_defined

### CVSS3

**Base Score:** 10.0  
**Attack Vector:** Network  
**Attack Complexity:** Low  
**Privileges Required:** None  
**User Interaction:** None  
**Scope:** Changed  
**Confidentiality Impact:** High  
**Integrity Impact:** High  
**Availability Impact:** None

### CWE

**CWE-89**

**Affected item**  
/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

**Affected parameter**

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

**Base Score:** 6.8  
**Access Vector:** Network accessible  
**Access Complexity:** Medium  
**Authentication:** None  
**Confidentiality Impact:** Partial  
**Integrity Impact:** Partial  
**Availability Impact:** Partial  
**Exploitability:** Not_defined  
**Remediation Level:** Not_defined  
**Report Confidence:** Not_defined  
**Availability Requirement:** Not_defined  
**Collateral Damage Potential:** Not_DEFINED  
**Confidentiality Requirement:** Not_DEFINED  
**Integrity Requirement:** Not_DEFINED  
**Target Distribution:** Not_DEFINED

---

469
| CVSS3 | Base Score: 10.0  
   Attack Vector: Network  
   Attack Complexity: Low  
   Privileges Required: None  
   User Interaction: None  
   Scope: Changed  
   Confidentiality Impact: High  
   Integrity Impact: High  
   Availability Impact: None |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
</tr>
<tr>
<td>Affected item</td>
</tr>
<tr>
<td>Affected parameter</td>
</tr>
<tr>
<td>Variants</td>
</tr>
</tbody>
</table>

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
   Access Vector: Network\_accessible  
   Access Complexity: Medium  
   Authentication: None  
   Confidentiality Impact: Partial  
   Integrity Impact: Partial  
   Availability Impact: Partial  
   Exploitability: Not\_defined  
   Remediation Level: Not\_defined  
   Report Confidence: Not\_defined  
   Availability Requirement: Not\_defined  
   Collateral Damage Potential: Not\_defined  
   Confidentiality Requirement: Not\_defined  
   Integrity Requirement: Not\_defined  
   Target Distribution: Not\_defined |
|-------|
| CVSS3 | Base Score: 10.0  
   Attack Vector: Network  
   Attack Complexity: Low  
   Privileges Required: None  
   User Interaction: None  
   Scope: Changed  
   Confidentiality Impact: High  
   Integrity Impact: High  
   Availability Impact: None |
| CWE   | CWE-89 |
| Affected item | /product.php |
| Affected parameter | pic |
| Variants | 1\texttt{ACUSTART}''\texttt{BkMWvACUEND} |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Affected item
- `/search.php`

### Affected parameter
- `login`

### Variants
- `1ACUSTART”wSLFJACUEND`

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **/search.php**

### Affected parameter

- **searchFor**

### Variants

- 1ACUSTART"jbBDSACUEND

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network-accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **/search.php**

### Affected parameter

- **test**

### Variants

- 1ACUSTART"f3W3tACUEND

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  

| Affected item | /secured/newuser.php  

| Affected parameter | uuname  

| Variants | 1ACUSTART"Fxw80ACUEND  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3
- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

### CWE
- CWE-89

### Affected item
- `/sendcommand.php`

### Affected parameter
- `cart_id`

### Variants
- `1ACUSTART''FWG7kACUEND`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
- Base Score: 6.8
- Access Vector: Network accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not defined
- Remediation Level: Not defined
- Report Confidence: Not defined
- Availability Requirement: Not defined
- Collateral Damage Potential: Not defined
- Confidentiality Requirement: Not defined
- Integrity Requirement: Not defined
- Target Distribution: Not defined

### CVSS3
- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

### CWE
- CWE-89

### Affected item
- `/userinfo.php`

### Affected parameter
- `login`

### Variants
- `1ACUSTART''E6rbyACUEND`

---

**SQL injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network_accessable
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE-89**
- **Affected item:** /userinfo.php
- **Affected parameter:** pass
- **Variants:** 1''

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS3 | Base Score: 10.0  
|-------|------------------  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|-----|-------  

**Affected item**
/userinfo.php

**Affected parameter**
script#text

**Variants**
1ACUSTART''k15cFACUEND

---

| CVSS2 | Base Score: 6.8  
|-------|------------------  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|-------|------------------  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|-----|-------  

**Affected item**
/userinfo.php

**Affected parameter**
script#text

**Variants**
\'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(83),CHAR(81),CHAR(114),CHAR(113),CHAR(103),CHAR(106),CHAR(69),CHAR(84)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 10.0</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Changed</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>uaddress</td>
</tr>
<tr>
<td>Variants</td>
<td>1ACUSTART&quot;’4a8ycACUEND</td>
</tr>
</tbody>
</table>

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
### CVSS3
<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE
**CWE-89**

### Affected item
/userinfo.php

### Affected parameter
uaddress

### Variants
1ACUSTART"aSjczACUEND

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3
<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE
**CWE-89**

### Affected item
/userinfo.php

### Affected parameter
uaddress

### Variants
'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(115),CHAR(103),CHAR(76),CHAR(66),CHAR(112),CHAR(110),CHAR(51),CHAR(67)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'

### SQL injection (verified)
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS2**
- Base Score: 6.8
- Access Vector: Network_accessable
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**
- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

**CWE**
- CWE-89

**Affected item**
- /userinfo.php

**Affected parameter**
- ucc

**Variants**
- 1ACUSTART™GD7BwACUEND

**SQL injection (verified)**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS2**
- Base Score: 6.8
- Access Vector: Network_accessable
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-89

Affected item

/userinfo.php

Affected parameter

ucc

Variants

1ACUSTART"92yp8ACUEND

SQL injection (verified)

Base Score: 6.8
Access Vector: Network accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS2

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-89

Affected item

/userinfo.php

Affected parameter

ucc

Variants

'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(112),CHAR(101),CHAR(80),CHAR(106),CHAR(80),CHAR(50),CHAR(101),CHAR(65)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Base Score: 10.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

CWE

CWE-89

Affected item

/userinfo.php

Affected parameter

uemail

Variants

1ACUSTART"GQ1gIACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
### CVSS3
<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE
| CWE-89 |

### Affected item
| /userinfo.php |

### Affected parameter
| uemail |

### Variants
| 1ACUSTART"IGowmACUEND |

---

#### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

### CVSS2
<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3
<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE
| CWE-89 |

### Affected item
| /userinfo.php |

### Affected parameter
| uemail |

### Variants
| 'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(55),CHAR(102),CHAR(116),CHAR(85),CHAR(85),CHAR(77),CHAR(100),CHAR(80)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and' |
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|        | Access Vector: Network accessible  
|        | Access Complexity: Medium  
|        | Authentication: None  
|        | Confidentiality Impact: Partial  
|        | Integrity Impact: Partial  
|        | Availability Impact: Partial  
|        | Exploitability: Not_defined  
|        | Remediation Level: Not_defined  
|        | Report Confidence: Not_defined  
|        | Availability Requirement: Not_defined  
|        | Collateral Damage Potential: Not_defined  
|        | Confidentiality Requirement: Not_defined  
|        | Integrity Requirement: Not_defined  
|        | Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
|        | Attack Vector: Network  
|        | Attack Complexity: Low  
|        | Privileges Required: None  
|        | User Interaction: None  
|        | Scope: Changed  
|        | Confidentiality Impact: High  
|        | Integrity Impact: High  
|        | Availability Impact: None |

| CWE | CWE-89 |

| Affected item | /userinfo.php |

| Affected parameter | uname |

| Variants | 1'' |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|        | Access Vector: Network accessible  
|        | Access Complexity: Medium  
|        | Authentication: None  
|        | Confidentiality Impact: Partial  
|        | Integrity Impact: Partial  
|        | Availability Impact: Partial  
|        | Exploitability: Not_defined  
|        | Remediation Level: Not_defined  
|        | Report Confidence: Not_defined  
|        | Availability Requirement: Not_defined  
|        | Collateral Damage Potential: Not_defined  
|        | Confidentiality Requirement: Not_defined  
|        | Integrity Requirement: Not_defined  
|        | Target Distribution: Not_defined |
CVSS3
Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE
CWE-89

Affected item
/userinfo.php

Affected parameter
uphone

Variants
1ACUSTART"e11WxACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2
Base Score: 6.8
Access Vector: Network accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3
Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE
CWE-89

Affected item
/userinfo.php

Affected parameter
uphone

Variants
1ACUSTART"52CZqACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE-89**

**Affected item**
- `/userinfo.php`

**Affected parameter**
- `uphone`

**Variants**
- `and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(74),CHAR(101),CHAR(105),CHAR(113),CHAR(67),CHAR(76),CHAR(80),CHAR(101)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'`

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/userinfo.php

**Affected parameter**

urname

**Variants**

1ACUSTART**PDJIPACUEND

---

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/userinfo.php

**Affected parameter**

urname

**Variants**

1ACUSTART**2kmCQACUEND

---

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89
- **Affected item:** /userinfo.php
- **Affected parameter:** urname
- **Variants:**
  ```sql
  'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(111),CHAR(57),CHAR(108),CHAR(51),CHAR(99),CHAR(79),CHAR(101),CHAR(70)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'
  ```

This directory contains an `.htaccess` file that is readable. This may indicate a server misconfiguration. .htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CWE

- **CWE:** CWE-16
- **Affected item:** /Mod_Rewrite_Shop/
Affected parameter

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | Web Server  
| Affected parameter | /["].php  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
## CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

## CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

## CWE

CWE-200

**Affected item**  
Web Server

**Affected parameter**  
`[*]<s>/<s>/<n>/`

## Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS3                                      | Base Score: 5.3  
|                                           | Attack Vector: Network  
|                                           | Attack Complexity: Low  
|                                           | Privileges Required: None  
|                                           | User Interaction: None  
|                                           | Scope: Unchanged  
|                                           | Confidentiality Impact: Low  
|                                           | Integrity Impact: None  
|                                           | Availability Impact: None |
| CWE                                        | CWE-200         |
| Affected item                             | /cart.php       |
| Affected parameter                        | login           |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2                                      | Base Score: 5.0  
|                                           | Access Vector: Network_accessible  
|                                           | Access Complexity: Low  
|                                           | Authentication: None  
|                                           | Confidentiality Impact: Partial  
|                                           | Integrity Impact: None  
|                                           | Availability Impact: None  
|                                           | Exploitability: Not_defined  
|                                           | Remediation Level: Not_defined  
|                                           | Report Confidence: Not_defined  
|                                           | Availability Requirement: Not_defined  
|                                           | Collateral Damage Potential: Not_defined  
|                                           | Confidentiality Requirement: Not_defined  
|                                           | Integrity Requirement: Not_defined  
|                                           | Target Distribution: Not_defined |
| CVSS3                                      | Base Score: 5.3  
|                                           | Attack Vector: Network  
|                                           | Attack Complexity: Low  
|                                           | Privileges Required: None  
|                                           | User Interaction: None  
|                                           | Scope: Unchanged  
|                                           | Confidentiality Impact: Low  
|                                           | Integrity Impact: None  
|                                           | Availability Impact: None |
| CWE                                        | CWE-200         |
| Affected item                             | /cart.php       |
| Affected parameter                        | Referer         |

**Application error message**
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2          | Base Score: 5.0  |
|               | Access Vector: Network_accessible |
|               | Access Complexity: Low |
|               | Authentication: None |
|               | Confidentiality Impact: Partial |
|               | Integrity Impact: None |
|               | Availability Impact: None |
|               | Exploitability: Not_defined |
|               | Remediation Level: Not_defined |
|               | Report Confidence: Not_defined |
|               | Availability Requirement: Not_defined |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined |
|               | Target Distribution: Not_defined |

| CVSS3          | Base Score: 5.3  |
|               | Attack Vector: Network |
|               | Attack Complexity: Low |
|               | Privileges Required: None |
|               | User Interaction: None |
|               | Scope: Unchanged |
|               | Confidentiality Impact: Low |
|               | Integrity Impact: None |
|               | Availability Impact: None |

| CWE            | CWE-200 |

| Affected item  | /cart.php |
| Affected parameter | User-Agent |

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

**CVSS3**

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

**CWE**

- **CWE-200**

**Affected item**

/\cart.php

**Affected parameter**

X-Forwarded-For

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

---

**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined
### CVSS3

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>5.3</td>
</tr>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Low</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

### Affected item

/listproducts.php

### Affected parameter

artist

### Variants

```
12345"\");||%00{%0d%0a<%00>%%b%27\0\0\0i
```

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

---

### CVSS2

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>5.0</td>
</tr>
<tr>
<td>Access Vector</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

---

### CVSS3

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>5.3</td>
</tr>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Low</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

### Affected item

/listproducts.php

### Affected parameter

cat

### Variants

```
12345"\");||%00{%0d%0a<%00>%%b%27\0\0\0i
```
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**CVSS2**
- Base Score: 5.0
- Access Vector: Network_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**
- Base Score: 5.3
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: Low
- Integrity Impact: None
- Availability Impact: None

**CWE**
- CWE-200

**Affected item**
- /listproducts.php

**Affected parameter**
- login
| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|------|------------|---|---|---|---|---|---|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |

CWE  
CWE-200

Affected item  
/listproducts.php

Affected parameter  
Referer

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS3 | Base Score: 5.3  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: Low  
| Integrity Impact: None  
| Availability Impact: None |
|---|---|
| CWE | CWE-200 |
| Affected item | /listproducts.php |
| Affected parameter | User-Agent |

| CVSS2 | Base Score: 5.0  
| Access Vector: Network_accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 5.3  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: Low  
| Integrity Impact: None  
| Availability Impact: None |
|---|---|
| CWE | CWE-200 |
| Affected item | /listproducts.php |
| Affected parameter | X-Forwarded-For |
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2          | Base Score: 5.0  
|                | Access Vector: Network_accessible  
|                | Access Complexity: Low  
|                | Authentication: None  
|                | Confidentiality Impact: Partial  
|                | Integrity Impact: None  
|                | Availability Impact: None  
|                | Exploitability: Not_defined  
|                | Remediation Level: Not_defined  
|                | Report Confidence: Not_defined  
|                | Availability Requirement: Not_defined  
|                | Collateral Damage Potential: Not_defined  
|                | Confidentiality Requirement: Not_defined  
|                | Integrity Requirement: Not_defined  
|                | Target Distribution: Not_defined  
| CVSS3          | Base Score: 5.3  
|                | Attack Vector: Network  
|                | Attack Complexity: Low  
|                | Privileges Required: None  
|                | User Interaction: None  
|                | Scope: Unchanged  
|                | Confidentiality Impact: Low  
|                | Integrity Impact: None  
|                | Availability Impact: None  
| CWE            | CWE-200  
| Affected item  | /product.php  
| Affected parameter | pic  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

---

**CVSS 2**

- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

---

**CVSS 3**

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

---

**CWE**

- **CWE-200**

**Affected item**

/secured/newuser.php

**Affected parameter**

login
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | /secured/newuser.php  
| Affected parameter | signup  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | /secured/newuser.php  
| Affected parameter | uaddress  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**CVSS2**
- Base Score: 5.0
- Access Vector: Network\_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not\_defined
- Remediation Level: Not\_defined
- Report Confidence: Not\_defined
- Availability Requirement: Not\_defined
- Collateral Damage Potential: Not\_defined
- Confidentiality Requirement: Not\_defined
- Integrity Requirement: Not\_defined
- Target Distribution: Not\_defined

**CVSS3**
- Base Score: 5.3
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: Low
- Integrity Impact: None
- Availability Impact: None

**CWE**
- CWE-200

**Affected item**
/\textit{secured/newuser.php}

**Affected parameter**
ucc

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

### Affected item

/secured/newuser.php

### Affected parameter

uemail

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Low</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

CWE:  CWE-200

Affected item: /userinfo.php

Affected parameter: script#text

Variants: 12345"\\);]]%00(%0d%0a<%00>%bf%27\8%b%8%8

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

CWE
CWE-200

Affected item /userinfo.php

Affected parameter uaddress

Variants 12345"\":\%00\%0d\%0a<\%00\%bf%27\%00%0d%0a
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | /userinfo.php  
| Affected parameter | ucc  
| Variants | 12345"\");i}*%00{%0d%0a<%=bf%27\\"\\"\n
### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | /userinfo.php  
| Affected parameter | uemail  
| Variants | 12345"\");i}*%00{%0d%0a<%=bf%27\\"\\"\n
505
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Base Score: 5.3</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

CWE

CWE-200

Affected item

/userinfo.php

Affected parameter

uname

Variants

12345"\",i[|]*%00(%0d%0a<%00>%bf%27\83 1
| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /userinfo.php |
| Affected parameter | uphone |
| Variants | 12345"%\*:\]%00{%0d%0a%00>%%bf%27%00 |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
## CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/userinfo.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>urname</td>
</tr>
</tbody>
</table>
| Variants | 12345"\";\"%00{%0d%0a<%00>\%bf%27\"\"

### Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

## CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network_accessable
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/index.bak</th>
</tr>
</thead>
</table>

### Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.
| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not defined  
Remediation Level: Not defined  
Report Confidence: Not defined  
Availability Requirement: Not defined  
Collateral Damage Potential: Not defined  
Confidentiality Requirement: Not defined  
Integrity Requirement: Not defined  
Target Distribution: Not defined |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-538</td>
</tr>
<tr>
<td>Affected item</td>
<td>/index.zip</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**Credit card number disclosed (verified)**

This alert may be a false positive, manual confirmation is required.

The response contains one or more credit card numbers. The credit card numbers were validated using the Luhn algorithm to make sure they are real credit card numbers.

| CVSS2 | Base Score: 4.3  
Access Vector: Network accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not defined  
Remediation Level: Not defined  
Report Confidence: Not defined  
Availability Requirement: Not defined  
Collateral Damage Potential: Not defined  
Confidentiality Requirement: Not defined  
Integrity Requirement: Not defined  
Target Distribution: Not defined |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-200</td>
</tr>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**Directory listing (verified)**
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>5.0</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>7.5</td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/idea/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>5.0</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>
CVSS3
Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

CWE
CWE-538

Affected item
/.idea/scopes/

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

CVSS2
Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3
Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

CWE
CWE-538

Affected item
/_mmServerScripts/

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**CVSS2**

Base Score: 5.0  
Access Vector: Network\_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not\_defined  
Remediation Level: Not\_defined  
Report Confidence: Not\_defined  
Availability Requirement: Not\_defined  
Collateral Damage Potential: Not\_defined  
Confidentiality Requirement: Not\_defined  
Integrity Requirement: Not\_defined  
Target Distribution: Not\_defined

**CVSS3**

Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**CWE**  
CWE-538

**Affected item**  
/Connections/

**Affected parameter**
Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
<table>
<thead>
<tr>
<th><strong>CVSS2</strong></th>
<th><strong>CVSS3</strong></th>
</tr>
</thead>
</table>
| Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| **CWE** | **Affected item** |
| CWE-538 | /pictures/ |

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th><strong>CVSS2</strong></th>
</tr>
</thead>
</table>
| Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
| CVSS2          | Base Score: 5.0  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  |
| CVSS3          | Base Score: 7.5  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: High  
|               | Integrity Impact: None  
|               | Availability Impact: None  |
| CWE            | CWE-538  
| Affected item  | /wvstests/pmwiki_2_1_19/  
| Affected parameter |  

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

### CWE

| CWE-538 |

### Affected item

/wvstests/pmwiki_2_1_19/scripts/

### Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-200 |

### Affected item

/AJAX/infoartist.php

### Error message on page
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE - CWE-200

Affected item: /AJAX/infocateg.php

Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### CVSS2

- **Base Score**: 5.0
- **Access Vector**: Network accessible
- **Access Complexity**: Low
- **Authentication**: None
- **Confidentiality Impact**: Partial
- **Integrity Impact**: None
- **Availability Impact**: None
- **Exploitability**: Not_defined
- **Remediation Level**: Not_defined
- **Report Confidence**: Not_defined
- **Availability Requirement**: Not_defined
- **Collateral Damage Potential**: Not_defined
- **Confidentiality Requirement**: Not_defined
- **Integrity Requirement**: Not_defined
- **Target Distribution**: Not_defined

### CVSS3

- **Base Score**: 5.3
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Unchanged
- **Confidentiality Impact**: Low
- **Integrity Impact**: None
- **Availability Impact**: None

### CWE

- **CWE**: CWE-200

### Affected item

/AJAX/infotitle.php

### Affected parameter

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /Connections/DB_Connection.php |
| Affected parameter | |

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /pictures/path-disclosure-unix.html |
| Affected parameter | |
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Access Vector: Network_accessible</td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Confidentiality Impact: Partial</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Exploitability: Not_defined</td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Availability Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td>Attack Vector: Network</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td>Integrity Impact: None</td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE | CWE-200

Affected item | /secured/database_connect.php

Affected parameter

JetBrains .idea project directory

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.
**CVSS2**

- **Base Score:** 5.0  
- **Access Vector:** Network accessible  
- **Access Complexity:** Low  
- **Authentication:** None  
- **Confidentiality Impact:** Partial  
- **Integrity Impact:** None  
- **Availability Impact:** None  
- **Exploitation:** Not_defined  
- **Remediation Level:** Not_defined  
- **Report Confidence:** Not_defined  
- **Availability Requirement:** Not_defined  
- **Collateral Damage Potential:** Not_defined  
- **Confidentiality Requirement:** Not_defined  
- **Integrity Requirement:** Not_defined  
- **Target Distribution:** Not_defined

---

**CWE**

- **CWE-538**

---

**Affected item**

- **Web Server**

---

**Affected parameter**

---

**PHP errors enabled (verified)**

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found that the PHP `display_errors` directive is enabled.

---

**CVSS2**

- **Base Score:** 5.0  
- **Access Vector:** Network accessible  
- **Access Complexity:** Low  
- **Authentication:** None  
- **Confidentiality Impact:** Partial  
- **Integrity Impact:** None  
- **Availability Impact:** None  
- **Exploitation:** Not_defined  
- **Remediation Level:** Not_defined  
- **Report Confidence:** Not_defined  
- **Availability Requirement:** Not_defined  
- **Collateral Damage Potential:** Not_defined  
- **Confidentiality Requirement:** Not_defined  
- **Integrity Requirement:** Not_defined  
- **Target Distribution:** Not_defined

---

**CVSS3**

- **Base Score:** 5.3  
- **Attack Vector:** Network  
- **Attack Complexity:** Low  
- **Privileges Required:** None  
- **User Interaction:** None  
- **Scope:** Unchanged  
- **Confidentiality Impact:** Low  
- **Integrity Impact:** None  
- **Availability Impact:** None

---

**CWE**

- **CWE-16**

---

**Affected item**

- `/secured/phpinfo.php`

---

**Affected parameter**

---
PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

**CVSS2**
- Base Score: 5.0
- Access Vector: Network_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**
- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

**CWE**
- CWE-200

**Affected item**
/secured/phpinfo.php

**Affected parameter**

---

This script is using phpinfo() function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

**CVSS2**
- Base Score: 5.0
- Access Vector: Network_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined
### Source code disclosure

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE | CWE-200 |

**Affected item**  
/secured/phpinfo.php

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE | CWE-538 |

**Affected item**  
/index.bak

| Source code disclosure |

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.
CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-538

Affected item

/pictures/wp-config.bak

Affected parameter

WS_FTP log file found (verified)

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

MySQL username disclosure
For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: NetworkAccessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: NotDefined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Connections/DB_Connection.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

MySQL username disclosure

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: NetworkAccessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: NotDefined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: NotDefined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/secured/database_connect.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

Possible sensitive directories
A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|-------|--------------------------------------------------|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE   | CWE-200 |
| Affected item | /admin/ |

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |

529
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

CWE-200

**Affected item**

/CVS/

**Affected parameter**

---

### Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

CWE-200

**Affected item**

/hpp/test.php

**Affected parameter**

---

### Possible virtual host found

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.
This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

| CWE            | CWE-200          |

<table>
<thead>
<tr>
<th>Affected item</th>
<th>Web Server</th>
</tr>
</thead>
</table>

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-200  
| Affected item | Web Server  
| Affected parameter |  

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-200  
| Affected item | /404.php  
| Affected parameter |  

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS2
- **Base Score**: 0.0
- **Access Vector**: Network accessible
- **Access Complexity**: Low
- **Authentication**: None
- **Confidentiality Impact**: None
- **Integrity Impact**: None
- **Availability Impact**: None
- **Exploitability**: Not_defined
- **Remediation Level**: Not_defined
- **Report Confidence**: Not_defined
- **Availability Requirement**: Not_defined
- **Collateral Damage Potential**: Not_defined
- **Confidentiality Requirement**: Not_defined
- **Integrity Requirement**: Not_defined
- **Target Distribution**: Not_defined

### CVSS3
- **Base Score**: 0.0
- **Attack Vector**: Network
- **Attack Complexity**: Low
- **Privileges Required**: None
- **User Interaction**: None
- **Scope**: Unchanged
- **Confidentiality Impact**: None
- **Integrity Impact**: None
- **Availability Impact**: None

### CWE
- **CWE-200**

**Affected item**
- `/artists.php`

**Affected parameter**

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-200  
| Affected item | /cart.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-200  
| Affected item | /categories.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS2       | Base Score: 0.0  
|            | Access Vector: Network_accessible  
|            | Access Complexity: Low  
|            | Authentication: None  
|            | Confidentiality Impact: None  
|            | Integrity Impact: None  
|            | Availability Impact: None  
|            | Exploitability: Not_defined  
|            | Remediation Level: Not_defined  
|            | Report Confidence: Not_defined  
|            | Availability Requirement: Not_defined  
|            | Collateral Damage Potential: Not_defined  
|            | Confidentiality Requirement: Not_defined  
|            | Integrity Requirement: Not_defined  
|            | Target Distribution: Not_defined  
| CVSS3       | Base Score: 0.0  
|            | Attack Vector: Network  
|            | Attack Complexity: Low  
|            | Privileges Required: None  
|            | User Interaction: None  
|            | Scope: Unchanged  
|            | Confidentiality Impact: None  
|            | Integrity Impact: None  
|            | Availability Impact: None  
| CWE         | CWE-200  
| Affected item | /disclaimer.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS3 | Base Score: 0.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: None  
| Integrity Impact: None  
| Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /guestbook.php |
| Affected parameter |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
| Access Vector: Network_accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: None  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |
| CVSS3 | Base Score: 0.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: None  
| Integrity Impact: None  
| Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /index.bak |
| Affected parameter |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

### CWE

CWE-200

### Affected item

/listproducts.php

### Affected parameter

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
<th>Access Vector: Network_accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

### CWE

CWE-200

### Affected item

/login.php

### Affected parameter

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS2 | Base Score: 0.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 0.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /logout.php |
| Affected parameter | |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: None  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE  | CWE-200  
| Affected item | /product.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE  | CWE-200  
| Affected item | /search.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
## CVSS2

- **Base Score:** 0.0
- **Access Vector:** Networkaccessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

## CVSS3

- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

## CWE

- **CWE:** CWE-200

### Affected item

- **/signup.php**

### Affected parameter

#### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like `myname@mydomain.com` and then record any addresses found.

## CVSS2

- **Base Score:** 0.0
- **Access Vector:** Networkaccessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined
<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
<td></td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/Templates/main_dynamic_template.dwt.php</th>
</tr>
</thead>
</table>

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
<td></td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/userinfo.php</th>
</tr>
</thead>
</table>

**Microsoft Office possible sensitive information**

This document has been converted to HTML using Microsoft Office. It seems that Office has included sensitive information during the conversion.
When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Possible internal IP address disclosure

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
| CVSS2               | Base Score: 5.0  
|                   | Access Vector: Network_accessible  
|                   | Access Complexity: Low  
|                   | Authentication: None  
|                   | Confidentiality Impact: Partial  
|                   | Integrity Impact: None  
|                   | Availability Impact: None  
|                   | Exploitability: Not_defined  
|                   | Remediation Level: Not_defined  
|                   | Report Confidence: Not_defined  
|                   | Availability Requirement: Not_defined  
|                   | Collateral Damage Potential: Not_defined  
|                   | Confidentiality Requirement: Not_defined  
|                   | Integrity Requirement: Not_defined  
|                   | Target Distribution: Not_defined  

| CVSS3               | Base Score: 7.5  
|                   | Attack Vector: Network  
|                   | Attack Complexity: Low  
|                   | Privileges Required: None  
|                   | User Interaction: None  
|                   | Scope: Unchanged  
|                   | Confidentiality Impact: High  
|                   | Integrity Impact: None  
|                   | Availability Impact: None  

| CWE               | CWE-200  
| Affected item     | /404.php  
| Affected parameter |  

**Possible internal IP address disclosure**

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

### Affected item

- `/pictures/ipaddresses.txt`

### Possible internal IP address disclosure

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

### Affected item

- `/secured/phpinfo.php`

### Possible server path disclosure (Unix)

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.
This alert may be a false positive, manual confirmation is required.

| CVSS2          | Base Score: 5.0  |
|               | Access Vector: Network_accessible |
|               | Access Complexity: Low |
|               | Authentication: None |
|               | Confidentiality Impact: Partial |
|               | Integrity Impact: None |
|               | Availability Impact: None |
|               | Exploitability: Not_defined |
|               | Remediation Level: Not_defined |
|               | Report Confidence: Not_defined |
|               | Availability Requirement: Not_defined |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined |
|               | Target Distribution: Not_defined |

| CVSS3          | Base Score: 7.5  |
|               | Attack Vector: Network |
|               | Attack Complexity: Low |
|               | Privileges Required: None |
|               | User Interaction: None |
|               | Scope: Unchanged |
|               | Confidentiality Impact: High |
|               | Integrity Impact: None |
|               | Availability Impact: None |

CWE: CWE-200

**Affected item**
/pictures/path-disclosure-unix.html

**Affected parameter**

---

**Possible server path disclosure (Unix)**

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

| CVSS2          | Base Score: 5.0  |
|               | Access Vector: Network_accessible |
|               | Access Complexity: Low |
|               | Authentication: None |
|               | Confidentiality Impact: Partial |
|               | Integrity Impact: None |
|               | Availability Impact: None |
|               | Exploitability: Not_defined |
|               | Remediation Level: Not_defined |
|               | Report Confidence: Not_defined |
|               | Availability Requirement: Not_defined |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined |
|               | Target Distribution: Not_defined |
**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-200

Affected item

/secured/phpinfo.php

**Possible username or password disclosure**

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-200

**Affected item**

/pictures/credentials.txt

**Affected parameter**

(18.1.4) Privacy and protection of personally identifiable information

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

Total number of alerts in this category: 159
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|----------------|------------------------------------------------|
| CVSS3 | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE | CWE-89 |
| Affected item | Web Server |
| Affected parameter | login |
| Variants | test%2Ftest' AND 3*2*1=6 AND '000QvXx'='000QvXx |

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
| Access Vector: Network_accessible  
| Access Complexity: Medium  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: Partial  
| Availability Impact: Partial  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Changed  
| Confidentiality Impact: High  
| Integrity Impact: High  
| Availability Impact: None |

| CWE | CWE-89 |

| Affected item | /AJAX/infoartist.php |

| Affected parameter | id |

| Variants | if(now()=sysdate(),sleep(0),0) |

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
| Access Vector: Network_accessible  
| Access Complexity: Medium  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: Partial  
| Availability Impact: Partial  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS3

- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

CWE

- CWE-89

Affected item

/AJAX/infocateg.php

Affected parameter

id

Variants

if(now()=sysdate(),sleep(0),0)

CVSS2

- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

CVSS3

- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

CWE

- CWE-89

Affected item

/AJAX/infotitle.php

Affected parameter

id

Variants

if(now()=sysdate(),sleep(0),0)

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
CVSS2

Base Score: 6.8
Access Vector: Network accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not defined
Remediation Level: Not defined
Report Confidence: Not defined
Availability Requirement: Not defined
Collateral Damage Potential: Not defined
Confidentiality Requirement: Not defined
Integrity Requirement: Not defined
Target Distribution: Not defined

CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Affected item /artists.php
Affected parameter artist
Variants 1 AND 3*2*1=6 AND 909=909

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-89

Affected item /artists.php

Affected parameter login

Variants test%2Ftest' AND 3*2*1=6 AND '0009eun'='0009eun

CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-89

Affected item /cart.php

Affected parameter addcart

Variants if(now())=sysdate(),sleep(0),0)
| CVSS2 | Base Score: 6.8  
Access Vector: Network\_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not\_defined  
Remediation Level: Not\_defined  
Report Confidence: Not\_defined  
Availability Requirement: Not\_defined  
Collateral Damage Potential: Not\_defined  
Confidentiality Requirement: Not\_defined  
Integrity Requirement: Not\_defined  
Target Distribution: Not\_defined |
| --- | --- |
| CVSS3 | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE | CWE-89 |
| Affected item | /cart.php |
| Affected parameter | login |
| Variants | test\%2Ftest' AND 3*2*1=6 AND '000rpl5'='000rpl5 |

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Affected item
/guestbook.php

Affected parameter
login

Variants
(select(0)from(select(sleep(0)))v)/**+(select(0)from(select(sleep(0)))v)+""+
(select(0)from(select(sleep(0)))v)+""/

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2

Base Score: 6.8
Access Vector: Network_accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Affected item
/listproducts.php

Affected parameter
artist

Variants
1 AND 3*2*1=6 AND 568=568

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

**Affected item:** `/listproducts.php`

**Affected parameter:** `cat`

**Variants:** `1 AND 3*2*1=6 AND 551=551`

### Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/listproducts.php

**Affected parameter**

login

**Variants**

test%2Ftest' AND 3*2*1=6 AND '000Ccg'='000Ccg

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

**Affected item**

/product.php

**Affected parameter**

login

**Variants**

test%2Ftest' AND 3*2*1=6 AND '000vXGJ'='000vXGJ
| CVSS2 | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE | CWE-89 |
| Affected item | /product.php |
| Affected parameter | pic |
| Variants | 1 AND 3*2*1=6 AND 494=494 |

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-89

Affected item
/search.php

Affected parameter
login

Variants
test%2Ftest' AND 3*2*1=6 AND '000NAzi'='000NAzi

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE-89**
- **Affected item:** `/search.php`
- **Affected parameter:** test
- **Variants:** `(select(0)from(select(sleep(0)))v)+"+(select(0)from(select(sleep(0)))v)+"+(select(0)from(select(sleep(0)))v)+"/`
| CVSS3                      | Base Score: 10.0  
|                           | Attack Vector: Network  
|                           | Attack Complexity: Low  
|                           | Privileges Required: None  
|                           | User Interaction: None  
|                           | Scope: Changed  
|                           | Confidentiality Impact: High  
|                           | Integrity Impact: High  
|                           | Availability Impact: None  |
| CWE                       | CWE-89  |
| Affected item             | /secured/newuser.php  |
| Affected parameter        | uname  |
| Variants                  | 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z  |

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2                      | Base Score: 6.8  
|                           | Access Vector: Network_accessible  
|                           | Access Complexity: Medium  
|                           | Authentication: None  
|                           | Confidentiality Impact: Partial  
|                           | Integrity Impact: Partial  
|                           | Availability Impact: Partial  
|                           | Exploitability: Not_defined  
|                           | Remediation Level: Not_defined  
|                           | Report Confidence: Not_defined  
|                           | Availability Requirement: Not_defined  
|                           | Collateral Damage Potential: Not_defined  
|                           | Confidentiality Requirement: Not_defined  
|                           | Integrity Requirement: Not_defined  
|                           | Target Distribution: Not_defined  |

| CVSS3                      | Base Score: 10.0  
|                           | Attack Vector: Network  
|                           | Attack Complexity: Low  
|                           | Privileges Required: None  
|                           | User Interaction: None  
|                           | Scope: Changed  
|                           | Confidentiality Impact: High  
|                           | Integrity Impact: High  
|                           | Availability Impact: None  |
| CWE                       | CWE-89  |
| Affected item             | /sendcommand.php  |
| Affected parameter        | cart_id  |
| Variants                  | (select(0)from(select(sleep(0)))v)+"+(select(0)from(select(sleep(0)))v)+"+(select(0)from(select(sleep(0)))v)+"/  |

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
| Access Vector: Network_accessible  
| Access Complexity: Medium  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: Partial  
| Availability Impact: Partial  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |
| CVSS3 | Base Score: 10.0  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Changed  
| Confidentiality Impact: High  
| Integrity Impact: High  
| Availability Impact: None |
| CWE | CWE-89 |
| Affected item | /userinfo.php |
| Affected parameter | login |
| Variants | test%2Ftest' AND 3*2*1=6 AND '000GmMl'='000GmMl |

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-89

Affected item

/userinfo.php

Affected parameter

pass

Variants

-1' OR 3*2*1=6 AND 000283=000283 --

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_DEFINED</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-89

Affected item

/userinfo.php

Affected parameter

uname

Variants

-1' OR 3*2*1=6 AND 00059=00059 --

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8
|       | Access Vector: Network_accessible
|       | Access Complexity: Medium
|       | Authentication: None
|       | Confidentiality Impact: Partial
|       | Integrity Impact: Partial
|       | Availability Impact: Partial
|       | Exploitability: Not_defined
|       | Remediation Level: Not_defined
|       | Report Confidence: Not_defined
|       | Availability Requirement: Not_defined
|       | Collateral Damage Potential: Not_defined
|       | Confidentiality Requirement: Not_defined
|       | Integrity Requirement: Not_defined
|       | Target Distribution: Not_defined

| CVSS3 | Base Score: 10.0
|       | Attack Vector: Network
|       | Attack Complexity: Low
|       | Privileges Required: None
|       | User Interaction: None
|       | Scope: Changed
|       | Confidentiality Impact: High
|       | Integrity Impact: High
|       | Availability Impact: None

| CWE | CWE-89

**Affected item**: /userinfo.php

**Affected parameter**: uname

**Variants**: 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z

**Macromedia Dreamweaver remote database scripts (verified)**

Macromedia Dreamweaver has created a directory (_mmServerScripts or _mmDBScripts) that contains scripts for testing database connectivity. One of these scripts (mmhttpdb.php or mmhttpdb.asp) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.

| CVSS2 | Base Score: 5.0
|       | Access Vector: Network_accessible
|       | Access Complexity: Low
|       | Authentication: None
|       | Confidentiality Impact: Partial
|       | Integrity Impact: None
|       | Availability Impact: None
|       | Exploitability: High
|       | Remediation Level: Official_fix
|       | Report Confidence: Confirmed
|       | Availability Requirement: Not_defined
|       | Collateral Damage Potential: Not_defined
|       | Confidentiality Requirement: Not_defined
|       | Integrity Requirement: Not_defined
|       | Target Distribution: Not_defined

| CVE | CVE-2004-1893

| CWE | CWE-16

**Affected item**: Web Server

**Affected parameter**
Possible database backup

Manual confirmation is required for this alert.

It looks like this file contains a database backup/dump. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not defined</td>
<td></td>
</tr>
</tbody>
</table>

CWE

CWE-538

Affected item
/admin/create.sql

Affected parameter

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 10.0</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Changed</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: High</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>
### CWE-89

**Affected item**: Web Server

**Affected parameter**: login

**Variants**: 1ACUSTART"tsfKpACUEND

---

#### SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th><strong>CVSS2</strong></th>
<th><strong>CVSS3</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Score</strong>: 6.8</td>
<td><strong>Base Score</strong>: 10.0</td>
</tr>
<tr>
<td><strong>Access Vector</strong>: Network accessible</td>
<td><strong>Attack Vector</strong>: Network</td>
</tr>
<tr>
<td><strong>Access Complexity</strong>: Medium</td>
<td><strong>Attack Complexity</strong>: Low</td>
</tr>
<tr>
<td><strong>Authentication</strong>: None</td>
<td><strong>Privileges Required</strong>: None</td>
</tr>
<tr>
<td><strong>Confidentiality Impact</strong>: Partial</td>
<td><strong>User Interaction</strong>: None</td>
</tr>
<tr>
<td><strong>Integrity Impact</strong>: Partial</td>
<td><strong>Scope</strong>: Changed</td>
</tr>
<tr>
<td><strong>Availability Impact</strong>: Partial</td>
<td><strong>Confidentiality Impact</strong>: High</td>
</tr>
<tr>
<td><strong>Exploitability</strong>: Not_defined</td>
<td><strong>Integrity Impact</strong>: High</td>
</tr>
<tr>
<td><strong>Remediation Level</strong>: Not_defined</td>
<td><strong>Availability Impact</strong>: None</td>
</tr>
<tr>
<td><strong>Report Confidence</strong>: Not_defined</td>
<td><strong>Target Distribution</strong>: Not_defined</td>
</tr>
</tbody>
</table>

---

**CWE** | CWE-89

**Affected item**: /AJAX/infoartist.php

**Affected parameter**: id

**Variants**: 1"

---

#### SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |

| CWE | CWE-89 |

| Affected item | /AJAX/infocateg.php |

| Affected parameter | id |

| Variants | 1" |

**SQL injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
|CVSS3| Base Score: 10.0  
|     | Attack Vector: Network  
|     | Attack Complexity: Low  
|     | Privileges Required: None  
|     | User Interaction: None  
|     | Scope: Changed  
|     | Confidentiality Impact: High  
|     | Integrity Impact: High  
|     | Availability Impact: None  

|CWE| CWE-89  

|Affected item| /AJAX/infotitle.php  

|Affected parameter| id  

|Variants| 1''  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

|CVSS2| Base Score: 6.8  
|     | Access Vector: Network_accessible  
|     | Access Complexity: Medium  
|     | Authentication: None  
|     | Confidentiality Impact: Partial  
|     | Integrity Impact: Partial  
|     | Availability Impact: Partial  
|     | Exploitability: Not_defined  
|     | Remediation Level: Not_defined  
|     | Report Confidence: Not_defined  
|     | Availability Requirement: Not_defined  
|     | Collateral Damage Potential: Not_defined  
|     | Confidentiality Requirement: Not_defined  
|     | Integrity Requirement: Not_defined  
|     | Target Distribution: Not_defined  

|CVSS3| Base Score: 10.0  
|     | Attack Vector: Network  
|     | Attack Complexity: Low  
|     | Privileges Required: None  
|     | User Interaction: None  
|     | Scope: Changed  
|     | Confidentiality Impact: High  
|     | Integrity Impact: High  
|     | Availability Impact: None  

|CWE| CWE-89  

|Affected item| /artists.php  

|Affected parameter| artist  

|Variants| 1ACUSTART''TYdWwACUEND  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Networkaccessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Affected item
- **/artists.php**

### Affected parameter
- **login**

### Variants
- **1ACUSTART''Ohp3MACUEND**

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE-89**

### Affected item

- `/cart.php`

### Affected parameter

- `addcart`

### Variants

- `1ACUSTART"8DJP8ACUEND`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE-89**

### Affected item

- `/cart.php`

### Affected parameter

- `del`

### Variants

- `1ACUSTART"OFXxiACUEND`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- `/cart.php`

### Affected parameter

- `login`

### Variants

- `1ACUSTART''SQSJoACUEND`

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS3 | Base Score: 10.0  
     | Attack Vector: Network  
     | Attack Complexity: Low  
     | Privileges Required: None  
     | User Interaction: None  
     | Scope: Changed  
     | Confidentiality Impact: High  
     | Integrity Impact: High  
     | Availability Impact: None |
|-------|----------------------|
| CWE   | CWE-89               |
| Affected item | /guestbook.php |
| Affected parameter | login |
| Variants | 1ACUSTART™"BQWkpACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
     | Access Vector: Network accessible  
     | Access Complexity: Medium  
     | Authentication: None  
     | Confidentiality Impact: Partial  
     | Integrity Impact: Partial  
     | Availability Impact: Partial  
     | Exploitability: Not defined  
     | Remediation Level: Not defined  
     | Report Confidence: Not defined  
     | Availability Requirement: Not defined  
     | Collateral Damage Potential: Not defined  
     | Confidentiality Requirement: Not defined  
     | Integrity Requirement: Not defined  
     | Target Distribution: Not defined |
|-------|----------------------|

| CVSS3 | Base Score: 10.0  
     | Attack Vector: Network  
     | Attack Complexity: Low  
     | Privileges Required: None  
     | User Interaction: None  
     | Scope: Changed  
     | Confidentiality Impact: High  
     | Integrity Impact: High  
     | Availability Impact: None |
|-------|----------------------|
| CWE   | CWE-89               |
| Affected item | /listproducts.php |
| Affected parameter | artist |
| Variants | 1ACUSTART™"KVSljACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE-89**
- **Affected item:** /listproducts.php
- **Affected parameter:** cat
- **Variants:** 1ACUSTART"'oA8ddACUEND

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

### CWE

CWE-89

### Affected item

/listproducts.php

### Affected parameter

login

### Variants

1ACUSTART"38PotACUEND

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

### CVSS3

Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

### CWE

CWE-89

### Affected item

/Mod_Rewrite_Shop/BuyProduct-3/

### Affected parameter

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |
| CWE | CWE-89  
| Affected item | /Mod_Rewrite_Shop/Details/color-printer/3/  
| Affected parameter |  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|     |  

**Affected item**
/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/  

**Affected parameter**

### SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
|     |  

**Affected item**
/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/  

**Affected parameter**

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |

**CWE**  
CWE-89  

**Affected item**  
/product.php  

**Affected parameter**  
login  

**Variants**  
1ACUSTART""DynjHACUEND  

---  

**SQL injection (verified)**  

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Affected item
- **/product.php**

### Affected parameter
- **pic**

### Variants
- 1ACUSTART"'BkMWvACUEND

---

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Affected item
- **/search.php**

### Affected parameter
- **login**

### Variants
- 1ACUSTART"'wSLFJACUEND

---

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
CVSS2

Base Score: 6.8
Access Vector: Network_accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Affected item /search.php
Affected parameter searchFor
Variants 1ACUSTART"jbBDSACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
**CVSS3**

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

**CWE**

CWE-89

**Affected item**

/search.php

**Affected parameter**

test

**Variants**

1ACUSTART"f3W3tACUEND

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**CVSS2**

Base Score: 6.8
Access Vector: Network_accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

---

**CVSS3**

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

**CWE**

CWE-89

**Affected item**

/secured/newuser.php

**Affected parameter**

uname

**Variants**

1ACUSTART"Fxw80ACUEND

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS2 | Base Score: 6.8  
|       | Access Vector: NetworkAccessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: NotDefined  
|       | Remediation Level: NotDefined  
|       | Report Confidence: NotDefined  
|       | Availability Requirement: NotDefined  
|       | Collateral Damage Potential: NotDefined  
|       | Confidentiality Requirement: NotDefined  
|       | Integrity Requirement: NotDefined  
|       | Target Distribution: NotDefined  |
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |
| CWE  | CWE-89  
| Affected item | /sendcommand.php  
| Affected parameter | cart_id  
| Variants | 1ACUSTART""FWG7kACUEND  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Changed</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>CWE</td>
<td>CWE-89</td>
</tr>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>login</td>
</tr>
<tr>
<td>Variants</td>
<td>1ACUSTART&quot;E6rbyACUEND</td>
</tr>
</tbody>
</table>

SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Affected item
/userinfo.php

### Affected parameter
script#text

### Variants
1ACUSTART"'k15cFACUEND

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **userinfo.php**

### Affected parameter

- **script#text**

### Variants

- `'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(83),CHAR(81),CHAR(114),CHAR(113),CHAR(103),CHAR(106),CHAR(69),CHAR(84)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **userinfo.php**

### Affected parameter

- **uaddress**

### Variants

- `1ACUSTART"4a8ycACUEND`

---

**SQL injection (verified)**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  

| Affected item | /userinfo.php  
| Affected parameter | uaddress  
| Variants | 1ACUSTART"aSjczACUEND  

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  

| Affected item | /userinfo.php  
| Affected parameter | uaddress  
| Variants | 1ACUSTART"aSjczACUEND  

SQL injection (verified)
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |
| CWE  | CWE-89  |
| Affected item | /userinfo.php  |
| Affected parameter | uaddress  |
| Variants | 'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(115),CHAR(103),CHAR(76),CHAR(66),CHAR(112),CHAR(110),CHAR(51),CHAR(67)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'  |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |
| CWE  | CWE-89  |
| Affected item | /userinfo.php  |
| Affected parameter | ucc  |
| Variants | 1ACUSTART™GD7BwACUEND  |

**SQL injection (verified)**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None |

| CWE | CWE-89 |

| Affected item | /userinfo.php |
| Affected parameter | ucc |
| Variants | 1ACUSTART™92yp8ACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
### CVSS3
<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE
| CWE-89 |

### Affected item
| /userinfo.php |

### Affected parameter
| ucc |

### Variants
| 'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(112),CHAR(101),CHAR(80),CHAR(106),CHAR(80),CHAR(50),CHAR(101),CHAR(65)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and' |

---

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

---

### CVSS2
| Base Score: 6.8 |
| Access Vector: Network_accessible |
| Access Complexity: Medium |
| Authentication: None |
| Confidentiality Impact: Partial |
| Integrity Impact: Partial |
| Availability Impact: Partial |
| Exploitability: Not_defined |
| Remediation Level: Not_defined |
| Report Confidence: Not_defined |
| Availability Requirement: Not_defined |
| Collateral Damage Potential: Not_defined |
| Confidentiality Requirement: Not_defined |
| Integrity Requirement: Not_defined |
| Target Distribution: Not_defined |

---

### CVSS3
| Base Score: 10.0 |
| Attack Vector: Network |
| Attack Complexity: Low |
| Privileges Required: None |
| User Interaction: None |
| Scope: Changed |
| Confidentiality Impact: High |
| Integrity Impact: High |
| Availability Impact: None |

### CWE
| CWE-89 |

### Affected item
| /userinfo.php |

### Affected parameter
| uemail |

### Variants
| '1ACUSTART''GQ1gIACUEND |

---

### SQL injection (verified)
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE | CWE-89 |
| Affected item | /userinfo.php |
| Affected parameter | uemail |
| Variants | 1ACUSTART™IGowmACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  
| CWE | CWE-89  
| Affected item | `/userinfo.php`  
| Affected parameter | `uemail`  
| Variants | `'and((select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(55),CHAR(102),CHAR(116),CHAR(85),CHAR(85),CHAR(77),CHAR(100),CHAR(80)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'`  

### SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  
| CWE | CWE-89  
| Affected item | `/userinfo.php`  
| Affected parameter | `uname`  
| Variants | `'`  

### SQL injection (verified)
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/userinfo.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>uphone</td>
</tr>
<tr>
<td>Variants</td>
<td>1ACUSTART&quot;e11WxACUEND</td>
</tr>
</tbody>
</table>

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **userinfo.php**

### Affected parameter

- **uphone**

### Variants

- `1ACUSTART"52CZqACUEND`

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

### CVSS2

- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE:** CWE-89

### Affected item

- **userinfo.php**

### Affected parameter

- **uphone**

### Variants

- `'and(select 1 from(select count(*) , concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(74),CHAR(101),CHAR(105),CHAR(113),CHR(67),CHR(76),CHR(80),CHR(101))) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'`
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  

| Affected item | /userinfo.php  

| Affected parameter | surname  

| Variants | 1ACUSTART"PDJfPACUEND  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

593
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-89

Affected item /userinfo.php

Affected parameter uname

Variants 1ACUSTART™2kmCQACUEND

CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediaion Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

CWE-89

Affected item /userinfo.php

Affected parameter uname

Variants 'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(111),CHAR(57),CHAR(108),CHAR(51),CHAR(99),CHAR(79),CHAR(101),CHAR(70))) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'

.htaccess file readable (verified)
This directory contains an `.htaccess` file that is readable. This may indicate a server misconfiguration. `.htaccess` files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td><code>/Mod_Rewrite_Shop/</code></td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item Web Server

Affected parameter /[*].php

Application error message

CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item Web Server

Affected parameter /[*]/<s/>/<s/>/<n>/
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|-------|----------------|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE   | CWE-200 |
| Affected item | /cart.php |
| Affected parameter | login |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
</table>
| Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/cart.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>Referer</td>
</tr>
</tbody>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application’s internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Affected item | /cart.php  
| Affected parameter | User-Agent  

### CVSS2

| Base Score: 5.0  
| Access Vector: Network_accessible  
| Access Complexity: Low  
| Authentication: None  
| Confidentiality Impact: Partial  
| Integrity Impact: None  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined  

### CVSS3

| Base Score: 5.3  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: None  
| Scope: Unchanged  
| Confidentiality Impact: Low  
| Integrity Impact: None  
| Availability Impact: None  

| CWE | CWE-200  
| Affected item | /cart.php  
| Affected parameter | X-Forwarded-For  

### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application’s internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

![CVSS2](image1)

**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

![CVSS3](image2)

**CVSS3**

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

**CWE**

- **CWE-200**

**Affected item**

/\listproducts.php

**Affected parameter**

artist

**Variants**

12345"\";]]*%00[%0d%0a<%00>%bf%27δ□□]

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE | CWE-200 |

| Affected item | /listproducts.php |
| Affected parameter | cat |
| Variants | 12345"\";||*00|%0d%0a<00>\bf%27\000i |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item
/listproducts.php

Affected parameter
login

CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item
/listproducts.php

Affected parameter
Referer

Application error message
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/listproducts.php</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>User-Agent</td>
</tr>
</tbody>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /listproducts.php |
| Affected parameter | X-Forwarded-For |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  |
| CWE   | CWE-200  |
| Affected item | /product.php  |
| Affected parameter | pic  |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  |
| CWE   | CWE-200  |
| Affected item | /secured/newuser.php  |
| Affected parameter | login  |

**Application error message**
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE   | CWE-200  
| Affected item | /secured/newuser.php  
| Affected parameter | signup  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

**CVSS3**

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

**CWE**

- **CWE-200**

**Affected item**

/secure/newuser.php

**Affected parameter**

uaddress

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/secured/newuser.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>ucc</td>
</tr>
</tbody>
</table>

### Application error message

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/secured/newuser.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>uemail</td>
</tr>
</tbody>
</table>
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-200  

| Affected item | /secured/newuser.php  
| Affected parameter | uuname  
| Variants | 12345"\";]j]*%00[\%0d%0a<%00>%bf%27\x0a\x00|
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-200
- **Affected item:** /showimage.php
- **Affected parameter:** file
- **Variants:** acu4562%EF%BC%9Cs1%EF%B9%A5s2%CA%A5s3%CA%B9uca4562

#### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined
### CVE-200

#### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

---

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

#### CWE

CWE-200

#### Affected item

/userinfo.php

#### Affected parameter

script#text

#### Variants

12345"\"");]]%00(%0d%0a<%00>%0a%f%27%0d%0a}

---

#### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
<th>Access Vector: Network_accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Complexity: Low</td>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

---

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

#### CWE

CWE-200

#### Affected item

/userinfo.php

#### Affected parameter

uaddress

#### Variants

12345"\"");]]%00(%0d%0a<%00>%0a%f%27%0d%0a}
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|-------|---------------------------------------------------------------|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE   | CWE-200 |
| Affected item | /userinfo.php |
| Affected parameter | ucc |
| Variants | 12345"\";li*%00(%0d%0a<%00>%bf%27%b%b%20|

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
**CVSS2**

- Base Score: 5.0
- Access Vector: Network accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**

- Base Score: 5.3
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: Low
- Integrity Impact: None
- Availability Impact: None

**CWE**

- CWE-200

**Affected item**

/userinfo.php

**Affected parameter**

uemail

**Variants**

12345"\";]]%00{%0d%0a<%00>%bf%27'ð¡

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

**CVSS2**

- Base Score: 5.0
- Access Vector: Network accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE   | CWE-200  
| Affected item | /userinfo.php  
| Affected parameter | uname  
| Variants | 12345"\");\*%00{%0d%0a<%00>%bf%27\[\]i  

### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE   | CWE-200  
| Affected item | /userinfo.php  
| Affected parameter | uphone  
| Variants | 12345"\");\*%00{%0d%0a<%00>%bf%27\[\]i  

614
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not defined  
|       | Remediation Level: Not defined  
|       | Report Confidence: Not defined  
|       | Availability Requirement: Not defined  
|       | Collateral Damage Potential: Not defined  
|       | Confidentiality Requirement: Not defined  
|       | Integrity Requirement: Not defined  
|       | Target Distribution: Not defined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |

CWE  
CWE-200

Affected item  
/userinfo.php

Affected parameter  
urname

Variants  
12345""\n;]]%00(%0d%0a<%00>%bf%27ò®i

Backup files  
A possible backup file was found on your web-server. These files are usually created by developers to backup their work.
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not defined  
|       | Remediation Level: Not defined  
|       | Report Confidence: Not defined  
|       | Availability Requirement: Not defined  
|       | Collateral Damage Potential: Not defined  
|       | Confidentiality Requirement: Not defined  
|       | Integrity Requirement: Not defined  
|       | Target Distribution: Not defined  

| CWE | CWE-538  
|     |  

| Affected item | /index.bak  
|               |  

### Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not defined  
|       | Remediation Level: Not defined  
|       | Report Confidence: Not defined  
|       | Availability Requirement: Not defined  
|       | Collateral Damage Potential: Not defined  
|       | Confidentiality Requirement: Not defined  
|       | Integrity Requirement: Not defined  
|       | Target Distribution: Not defined  

| CWE | CWE-538  
|     |  

| Affected item | /index.zip  
|               |  

### Credit card number disclosed (verified)

This alert may be a false positive, manual confirmation is required.

The response contains one or more credit card numbers. The credit card numbers were validated using the Luhn algorithm to make sure they are real credit card numbers.
| CVSS2 | Base Score: 4.3  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-200  
|     | Affected item /userinfo.php  
|     | Affected parameter  

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/.idea/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**CVSS2**

- Base Score: 5.0
- Access Vector: Network accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**

- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/.idea/scopes/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-538**

**Affected item**
- `/_mmServerScripts/

**Affected parameter**

---

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

**CVSS2**
- Base Score: 5.0
- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**
- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

**CWE**
- CWE-538

**Affected item**
- /admin/

**Affected parameter**

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### Directory Listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

| CVSS2       | Base Score: 5.0  
|            | Access Vector: Network_accessible  
|            | Access Complexity: Low  
|            | Authentication: None  
|            | Confidentiality Impact: Partial  
|            | Integrity Impact: None  
|            | Availability Impact: None  
|            | Exploitability: Not_defined  
|            | Remediation Level: Not_defined  
|            | Report Confidence: Not_defined  
|            | Availability Requirement: Not_defined  
|            | Collateral Damage Potential: Not_defined  
|            | Confidentiality Requirement: Not_defined  
|            | Integrity Requirement: Not_defined  
|            | Target Distribution: Not_defined  
| CVSS3       | Base Score: 7.5  
|            | Attack Vector: Network  
|            | Attack Complexity: Low  
|            | Privileges Required: None  
|            | User Interaction: None  
|            | Scope: Unchanged  
|            | Confidentiality Impact: High  
|            | Integrity Impact: None  
|            | Availability Impact: None  
| CWE         | CWE-538  
| Affected item | /CVS/  
| Affected parameter |  

---

**CWE-538**

Affected item: `/CVS/`

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/Flash/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

#### CVSS2

| Base Score: 5.0
| Access Vector: Network accessible
| Access Complexity: Low
| Authentication: None
| Confidentiality Impact: Partial
| Integrity Impact: None
| Availability Impact: None
| Exploitability: Not_defined
| Remediation Level: Not_defined
| Report Confidence: Not_defined
| Availability Requirement: Not_defined
| Collateral Damage Potential: Not_defined
| Confidentiality Requirement: Not_defined
| Integrity Requirement: Not_defined
| Target Distribution: Not_defined

#### CVSS3

| Base Score: 7.5
| Attack Vector: Network
| Attack Complexity: Low
| Privileges Required: None
| User Interaction: None
| Scope: Unchanged
| Confidentiality Impact: High
| Integrity Impact: None
| Availability Impact: None

### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE-538**

#### Affected item

- `/pictures/`

#### Affected parameter

---

### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

---

### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE-538**

#### Affected item

- `/Templates/`

#### Affected parameter

---

### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 7.5</td>
</tr>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-538</td>
</tr>
</tbody>
</table>

**Affected item** /wvstests/

**Affected parameter**

**Directory listing (verified)**

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

| CVSS2   | Base Score: 5.0  
|         | Access Vector: Network_accessible  
|         | Access Complexity: Low  
|         | Authentication: None  
|         | Confidentiality Impact: Partial  
|         | Integrity Impact: None  
|         | Availability Impact: None  
|         | Exploitability: Not_defined  
|         | Remediation Level: Not_defined  
|         | Report Confidence: Not_defined  
|         | Availability Requirement: Not_defined  
|         | Collateral Damage Potential: Not_defined  
|         | Confidentiality Requirement: Not_defined  
|         | Integrity Requirement: Not_defined  
|         | Target Distribution: Not_defined  
| CWE     | CWE-538  
| Affected item | /wvstests/pmwiki_2_1_19/  
| Affected parameter |  

### Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the
Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

CWE-200

### Affected item

/AJAX/infoartist.php

### Affected parameter

#### Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

**CWE**

CWE-200

**Affected item**

/AJAX/infocateg.php

**Affected parameter**

---

### Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
<th>Access Vector: Network_accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Complexity: Low</td>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

**CWE**

CWE-200

**Affected item**

/AJAX/infotitle.php

**Affected parameter**

---

### Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert requires manual confirmation.

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

| CWE         | CWE-200 |

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/Connections/DB_Connection.php</th>
</tr>
</thead>
</table>

Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-200
- **Affected item:** /pictures/path-disclosure-unix.html
- **Affected parameter:**

---

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
JetBrains .idea project directory

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

PHP errors enabled (verified)

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found that the PHP `display_errors` directive is enabled.
**CVSS2**

- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

**CVSS3**

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

**CWE**

- **CWE-16**

**Affected item**

/secure/phpinfo.php

**Affected parameter**

**PHPinfo page (verified)**

PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.
| CVSS3          | Base Score: 7.5  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: High  
|               | Integrity Impact: None  
|               | Availability Impact: None  |

| CWE           | CWE-200 |

| Affected item | /secured/phpinfo.php |

**PHPinfo page found**

This script is using phpinfo() function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

| CVSS2          | Base Score: 5.0  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: None  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  |

| CVSS3          | Base Score: 7.5  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: High  
|               | Integrity Impact: None  
|               | Availability Impact: None  |

| CWE           | CWE-200 |

| Affected item | /secured/phpinfo.php |

| Affected parameter |  |

**Source code disclosure**

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.
| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-538 |
| Affected item | /index.bak |
| Affected parameter | |

**Source code disclosure**

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
WS_FTP log file found (verified)

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

MySQL username disclosure

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.
**MySQL username disclosure**

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

**Possible sensitive directories**

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Affected item
/admin/

Affected parameter

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
| CVSS3 | Base Score: 7.5  
  | Attack Vector: Network  
  | Attack Complexity: Low  
  | Privileges Required: None  
  | User Interaction: None  
  | Scope: Unchanged  
  | Confidentiality Impact: High  
  | Integrity Impact: None  
  | Availability Impact: None |

| CWE | CWE-200 |

| Affected item | /CVS/ |

| Affected parameter |  |

### Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

| CVSS2 | Base Score: 5.0  
  | Access Vector: Network accessible  
  | Access Complexity: Low  
  | Authentication: None  
  | Confidentiality Impact: Partial  
  | Integrity Impact: None  
  | Availability Impact: None  
  | Exploitability: Not_defined  
  | Remediation Level: Not_defined  
  | Report Confidence: Not_defined  
  | Availability Requirement: Not_defined  
  | Collateral Damage Potential: Not_defined  
  | Confidentiality Requirement: Not_defined  
  | Integrity Requirement: Not_defined  
  | Target Distribution: Not_defined |

| CVSS3 | Base Score: 7.5  
  | Attack Vector: Network  
  | Attack Complexity: Low  
  | Privileges Required: None  
  | User Interaction: None  
  | Scope: Unchanged  
  | Confidentiality Impact: High  
  | Integrity Impact: None  
  | Availability Impact: None |

| CWE | CWE-200 |

| Affected item | /hpp/test.php |

| Affected parameter |  |

### Possible virtual host found

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.
This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE   | CWE-200 |

| Affected item | Web Server |

| Affected parameter |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE  | CWE-200  
| Affected item | Web Server  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE  | CWE-200  
| Affected item | /404.php  
| Affected parameter |  

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS2

- **Base Score:** 0.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

**Affected item:** `/artists.php`

**Affected parameter:**

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

---

### CVSS2

- **Base Score:** 0.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network\_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not\_defined  
|       | Remediation Level: Not\_defined  
|       | Report Confidence: Not\_defined  
|       | Availability Requirement: Not\_defined  
|       | Collateral Damage Potential: Not\_defined  
|       | Confidentiality Requirement: Not\_defined  
|       | Integrity Requirement: Not\_defined  
|       | Target Distribution: Not\_defined  |

| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  |

| CWE | CWE-200 |
|     |     |

**Affected item**
/disclaimer.php

**Affected parameter**

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### CVSS3

- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

#### Affected item

- `/guestbook.php`

#### Affected parameter


### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### CVSS2

- **Base Score:** 0.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

#### Affected item

- `/index.bak`

#### Affected parameter


### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

---

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

#### CWE

| CWE-200 |

<table>
<thead>
<tr>
<th>Affected item</th>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>/listproducts.php</td>
<td></td>
</tr>
</tbody>
</table>

---

#### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

---

#### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
<th>Access Vector: Network_accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Complexity: Low</td>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

---

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

#### CWE

| CWE-200 |

<table>
<thead>
<tr>
<th>Affected item</th>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>/login.php</td>
<td></td>
</tr>
</tbody>
</table>

---

#### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | CWE-200 |

**Affected item**  
`/logout.php`

**Affected parameter**

---

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like `myname@mydomain.com` and then record any addresses found.
### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

#### CWE

CWE-200

#### Affected item

/product.php

#### Affected parameter

---

### Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

#### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

#### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

#### CWE

CWE-200

#### Affected item

/search.php

#### Affected parameter

---
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
| CVSS3   | Base Score: 0.0  
|         | Attack Vector: Network  
|         | Attack Complexity: Low  
|         | Privileges Required: None  
|         | User Interaction: None  
|         | Scope: Unchanged  
|         | Confidentiality Impact: None  
|         | Integrity Impact: None  
|         | Availability Impact: None  |
| CWE     | CWE-200  |
| Affected item | /Templates/main_dynamic_template.dwt.php |
| Affected parameter | |

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| CVSS2   | Base Score: 0.0  
|         | Access Vector: Network_accessible  
|         | Access Complexity: Low  
|         | Authentication: None  
|         | Confidentiality Impact: None  
|         | Integrity Impact: None  
|         | Availability Impact: None  
|         | Exploitability: Not_defined  
|         | Remediation Level: Not_defined  
|         | Report Confidence: Not_defined  
|         | Availability Requirement: Not_defined  
|         | Collateral Damage Potential: Not_defined  
|         | Confidentiality Requirement: Not_defined  
|         | Integrity Requirement: Not_defined  
|         | Target Distribution: Not_defined  |
| CVSS3   | Base Score: 0.0  
|         | Attack Vector: Network  
|         | Attack Complexity: Low  
|         | Privileges Required: None  
|         | User Interaction: None  
|         | Scope: Unchanged  
|         | Confidentiality Impact: None  
|         | Integrity Impact: None  
|         | Availability Impact: None  |
| CWE     | CWE-200  |
| Affected item | /userinfo.php |
| Affected parameter | |

**Microsoft Office possible sensitive information**

This document has been converted to HTML using Microsoft Office. It seems that Office has included sensitive information during the conversion.
### CVSS2

| Base Score: 5.0 | Access Vector: Network accessible |
| Access Complexity: Low |
| Authentication: None |
| Confidentiality Impact: Partial |
| Integrity Impact: None |
| Availability Impact: None |
| Exploitability: Not_defined |
| Remediation Level: Not_defined |
| Report Confidence: Not_defined |
| Availability Requirement: Not_defined |
| Collateral Damage Potential: Not_defined |
| Confidentiality Requirement: Not_defined |
| Integrity Requirement: Not_defined |
| Target Distribution: Not_defined |

### CVSS3

| Base Score: 7.5 | Attack Vector: Network |
| Attack Complexity: Low |
| Privileges Required: None |
| User Interaction: None |
| Scope: Unchanged |
| Confidentiality Impact: High |
| Integrity Impact: None |
| Availability Impact: None |

### CWE

CWE-200

Affected item: /secured/office.htm

Affected parameter: Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
Possible internal IP address disclosure

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.
### CVSS3

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>7.5</td>
</tr>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

### CWE

CWE-200

### Affected item

/pictures/ipaddresses.txt

### Possible internal IP address disclosure

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

### CVSS2

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>5.0</td>
</tr>
<tr>
<td>Access Vector</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

### Possible server path disclosure (Unix)

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.
This alert may be a false positive, manual confirmation is required.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 7.5</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

**Affected item**

/pictures/path-disclosure-unix.html

**Affected parameter**

**Possible server path disclosure (Unix)**

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>
**Possible username or password disclosure**

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

---

**CVSS3**  
Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None

**CWE**  
CWE-200

**Affected item**  
/secured/phpinfo.php

---

**CVSS2**  
Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

---

**CVSS3**  
Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None

**CWE**  
CWE-200

**Affected item**  
/pictures/credentials.txt

---

**18.1.5) Regulation of cryptographic controls**

Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

Total number of alerts in this category: 1
Unencrypted connection (verified)

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CWE-310</td>
</tr>
<tr>
<td>Base Score: 5.8</td>
<td>Base Score: 9.1</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td>Confidentiality Impact: High</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: High</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Affected item**

Web Server

**Affected parameter**
Affected Items: A Detailed Report

This section provides full details of the types of vulnerabilities found according to individual affected items.

Web Server

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

| CVSS2          | Base Score: 6.8  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Medium  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: Partial  
|               | Availability Impact: Partial  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

| CVSS3          | Base Score: 10.0  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Changed  
|               | Confidentiality Impact: High  
|               | Integrity Impact: High  
|               | Availability Impact: None  

CWE          | CWE-89  

Parameter | login  

Variants | test%2Ftest' AND 3*2*1=6 AND '000QvXx'='000QvXx  

/AJAX/infoartist.php

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| CVSS2     | Base Score: 6.8  
Access Vector: Network accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not defined  
Remediation Level: Not defined  
Report Confidence: Not defined  
Availability Requirement: Not defined  
Collateral Damage Potential: Not defined  
Confidentiality Requirement: Not defined  
Integrity Requirement: Not defined  
Target Distribution: Not defined |
| CVSS3     | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE       | CWE-89 |
| Parameters | id |
| Variants  | if(now())=sysdate(),sleep(0),0) |

**AJAX/infocateg.php**

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

*This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4*
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4
CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

| CWE-89 |

Parameter

| login |

Variants

| test%2Ftest' AND 3*2*1=6 AND '0009eun'='0009eun |

/cart.php

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

| CWE-89 |

Parameter

| addcart |

Variants

| if(now())=sysdate(),sleep(0),0 |

Blind SQL Injection
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>6.8</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>10.0</td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Changed</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-89</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>login</td>
<td></td>
</tr>
</tbody>
</table>

Variants

test%2Ftest' AND 3*2*1=6 AND '000rpI5'='000rpI5

/guestbook.php

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>6.8</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>
### CVSS3

<table>
<thead>
<tr>
<th>Base Score</th>
<th>10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Changed</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

### CWE

**CWE**

CWE-89

### Parameter

**login**

### Variants

```
(select(0)from(select(sleep(0)))v)"'+(select(0)from(select(sleep(0)))v)+'"+(
select(0)from(select(sleep(0)))v)+"/
```

#### /listproducts.php

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

### CVSS2

<table>
<thead>
<tr>
<th>Base Score</th>
<th>6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score</th>
<th>10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Changed</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

### CWE

**CWE-89**

### Parameter

**artist**

### Variants

```
1 AND 3*2*1=6 AND 568=568
```

**Blind SQL Injection**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>6.8</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>10.0</td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Changed</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>cat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variants</td>
<td>1 AND 3<em>2</em>1=6 AND 551=551</td>
</tr>
</tbody>
</table>

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>6.8</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

665
Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

---

**CVSS2**

- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

---

**CVSS3**

- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

---

**CWE**

- CWE-89

**Parameter**

- pic

**Variants**

- 1 AND 3*2*1=6 AND 494=494

---

/search.php

**Blind SQL Injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

---

**CVSS2**

- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined
CVSS3
Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE
CWE-89
Parameter
login
Variants
test%2Ftest' AND 3*2*1=6 AND '000NAzi'='000NAzi

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

CVSS2
Base Score: 6.8
Access Vector: Network_accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3
Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE
CWE-89
Parameter
searchFor
Variants
0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Base Score: 10.0</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

CWE

CWE-89

Parameter
test

Variants
(SELECT(0)FROM(SELECT(sleep(0)))V)+"+(SELECT(0)FROM(SELECT(sleep(0)))V)+"*/secured/newuser.php

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |
| CWE   | CWE-89  |
| Parameter | uname  |
| Variants | 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z  |

/sendcommand.php

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |
| CWE   | CWE-89  |
| Parameter | cart_id  |
| Variants | (select(0)from(select(sleep(0)))v)**+(select(0)from(select(sleep(0)))v)+""+(select(0)from(select(sleep(0)))v)+""/ |

/userinfo.php

Blind SQL Injection
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 10.0</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Changed</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: High</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

CWE

CWE-89

Parameter

login

Variants
test%2Ftest' AND 3*2*1=6 AND '000GmMl'='000GmMl

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>
CVSS3

Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

CWE

CWE-89

Parameter  
pass

Variants  
-1' OR 3*2*1=6 AND 000283=000283 --

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

CVSS2

Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined

CVSS3

Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None

CWE

CWE-89

Parameter  
uname

Variants  
-1' OR 3*2*1=6 AND 00059=00059 --

Blind SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Web Server

Cross site scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

| CVSS2          | Base Score: 6.4  
|                | Access Vector: Network_accessible  
|                | Access Complexity: Low  
|                | Authentication: None  
|                | Confidentiality Impact: Partial  
|                | Integrity Impact: Partial  
|                | Availability Impact: None  
|                | Exploitability: Not_defined  
|                | Remediation Level: Not_defined  
|                | Report Confidence: Not_defined  
|                | Availability Requirement: Not_defined  
|                | Collateral Damage Potential: Not_defined  
|                | Confidentiality Requirement: Not_defined  
|                | Integrity Requirement: Not_defined  
|                | Target Distribution: Not_defined  

| CVSS3          | Base Score: 5.3  
|                | Attack Vector: Network  
|                | Attack Complexity: Low  
|                | Privileges Required: None  
|                | User Interaction: None  
|                | Scope: Unchanged  
|                | Confidentiality Impact: None  
|                | Integrity Impact: Low  
|                | Availability Impact: None  

| CWE            | CWE-79  
| Parameter      | name  
| Variants       | <your name here>""(&amp;<acx>&lt;ScRiPt &gt;3R9A(9055)&lt;/ScRiPt>  

/guestbook.php

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1
**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

*This alert belongs to the following categories: 14.1.2, 14.2.1*
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None |
| CWE  | CWE-79 |
| Parameter | text |
| Variants | 555"()&%<acx><ScRiPt >ZhcH(9771)</ScRiPt> |

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None |
| CWE  | CWE-79 |
| Parameter | pp |
| Variants | 12"()&%<acx><ScRiPt >obqU(9099)</ScRiPt> |

Cross site scripting (verified)

/hpp/index.php
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

| CVSS2 | Base Score: 6.4  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: Low  
Availability Impact: None |
| CWE | CWE-79 |
| Parameter | pp |
| Variants | `12"()&%<acx><ScRiPt >olPQ(9384)</ScRiPt>` |

/hpp/params.php

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1
Cross-site Scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

CWE

CWE-79

Parameter

p

Variants 1"(()&%<acx><ScRiPt >Ou8l(9421)</ScRiPt>
| CVSS3          | Base Score: 5.3  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: None  
|               | Integrity Impact: Low  
|               | Availability Impact: None |
| CWE            | CWE-79           |
| Parameter     | pp              |
| Variants      | 12''(')&%<acx><ScRiPt >isgP(9729)</ScRiPt> |

/listproducts.php

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

| CVSS2          | Base Score: 6.4  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Low  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: Partial  
|               | Availability Impact: None  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined |
| CVSS3          | Base Score: 5.3  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Unchanged  
|               | Confidentiality Impact: None  
|               | Integrity Impact: Low  
|               | Availability Impact: None |
| CWE            | CWE-79           |
| Parameter     | artist          |
| Variants      | 1''(')&%<acx><ScRiPt >IBxb(9649)</ScRiPt> |

Cross site scripting (verified)
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector:</td>
</tr>
<tr>
<td></td>
<td>Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector:</td>
</tr>
<tr>
<td></td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-79</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>cat</td>
</tr>
<tr>
<td>Variants</td>
<td>1&quot;&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;QSnL(9032)&lt;/ScRiPt&gt;</td>
</tr>
</tbody>
</table>

/search.php

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1
Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

**CWE**

| CWE-79 | |

**Parameter**

| uaddress |

**Variants**

| 3137 Laguna Street"("&%<acx><ScRiPt >AiSa(9916)</ScRiPt> |

Cross site scripting (verified)

**CVSS2**

<table>
<thead>
<tr>
<th>Base Score: 6.4</th>
<th>Access Vector: Network_accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Complexity: Low</td>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS3**

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
<th>Attack Vector: Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Complexity: Low</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

**CWE**

| CWE-79 | |

**Parameter**

| ucc |

**Variants**

| 4111111111111111"("&%<acx><ScRiPt >AiSa(9443)</ScRiPt> |
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None  

| CWE | CWE-79  
| Parameter | uemail  
| Variants | sample@email.tst"()&%<acx><ScRiPt >AiSa(9827)</ScRiPt>  

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

684
<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-79</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>uphone</td>
</tr>
<tr>
<td>Variants</td>
<td>555-666-0606&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;AiSa(9032)&lt;/ScRiPt&gt;</td>
</tr>
</tbody>
</table>

**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

*This alert belongs to the following categories: 14.1.2, 14.2.1*

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-79</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>surname</td>
</tr>
<tr>
<td>Variants</td>
<td>fnfOzvSR&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;AiSa(9571)&lt;/ScRiPt&gt;</td>
</tr>
</tbody>
</table>

**Cross site scripting (verified)**
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

| CVSS2 | Base Score: 6.4  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| --- | --- |
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: None  
Integrity Impact: Low  
Availability Impact: None |
| CWE | CWE-79 |
| Parameter | uuname |
| Variants | fnfOzvSR"()&%<acx><ScRiPt >AiSa(9368)</ScRiPt> |

`/userinfo.php`

**Cross site scripting**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1
Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1
Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.4</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-79</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>uemail</td>
</tr>
<tr>
<td>Variants</td>
<td><a href="mailto:sample@email.tst">sample@email.tst</a>&quot;(/&amp;%&lt;acx&gt;&lt;ScRiPt &gt;AuWK(9249)&lt;/ScRiPt&gt;</td>
</tr>
</tbody>
</table>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.4</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None  
| CWE | CWE-79  
| Parameter | uphone  
| Variants | 555-666-0606""]()&%<acx><ScRiPt >AuWK(9520)</ScRiPt>  

**Cross site scripting (verified)**

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: 14.1.2, 14.2.1

| CVSS2 | Base Score: 6.4  
|       | Access Vector: Network accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None  
| CWE | CWE-79  
| Parameter | upname  
| Variants | sawsan""()&%<acx><ScRiPt >AuWK(9947)</ScRiPt>  

/showimage.php

**Directory traversal (verified)**
This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

This alert belongs to the following categories: 8.2.3, 9.4.5

### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE:** CWE-22

<table>
<thead>
<tr>
<th>Parameter</th>
<th>file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variants</td>
<td>../../../../../../../../../../../../../proc/version</td>
</tr>
</tbody>
</table>

### File inclusion

This script is possibly vulnerable to file inclusion attacks.

It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.

This alert belongs to the following categories: 9.4.5, 14.2.1
**Web Server**

**Macromedia Dreamweaver remote database scripts (verified)**

Macromedia Dreamweaver has created a directory (\_mmServerScripts or \_mmDBScripts) that contains scripts for testing database connectivity. One of these scripts (mmhttpdb.php or mmhttpdb.asp) can be accessed without user ID or password and contains numerous operations, such as listing Datasource Names or executing arbitrary SQL queries.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 14.1.2, 14.2.1, 18.1.3, 18.1.4*

---

**nginx SPDY heap buffer overflow**
A heap-based buffer overflow in the SPDY implementation in nginx 1.3.15 before 1.4.7 and 1.5.x before 1.5.12 allows remote attackers to execute arbitrary code via a crafted request. The problem affects nginx compiled with the ngx_http_spdy_module module (which is not compiled by default) and without --with-debug configure option, if the "spdy" option of the "listen" directive is used in a configuration file.

This alert belongs to the following categories: 12.5.1, 14.2.1

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-2014-0133</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CWE</td>
<td>CWE-122</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PHP allow_url_fopen enabled (verified)**

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

This alert belongs to the following categories: 12.5.1

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 0.0</th>
<th>Access Vector: Network_accessible</th>
<th>Access Complexity: Low</th>
<th>Authentication: None</th>
<th>Confidentiality Impact: None</th>
<th>Integrity Impact: None</th>
<th>Availability Impact: None</th>
<th>Exploitability: Not_defined</th>
<th>Remediation Level: Not_defined</th>
<th>Report Confidence: Not_defined</th>
<th>Availability Requirement: Not_defined</th>
<th>Collateral Damage Potential: Not_defined</th>
<th>Confidentiality Requirement: Not_defined</th>
<th>Integrity Requirement: Not_defined</th>
<th>Target Distribution: Not_defined</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Parameter

Variants
Possible database backup

Manual confirmation is required for this alert.

It looks like this file contains a database backup/dump. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>5.0</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

CWE

CWE-538

Parameter

Variants

/showimage.php

Remote file inclusion XSS (verified)

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. The server opens arbitrary URLs and puts the content retrieved from the URL into the response without filtering.

This alert belongs to the following categories: 14.1.2, 14.2.1
### CVSS2

- **Base Score:** 6.4
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE

- **CWE:** CWE-79

### Parameter

- **file**

### Variants

- **Http://bxss.me/t/xss.html?%00**

---

**Server side request forgery (verified)**

SSRF as in Server Side Request Forgery is a vulnerability that allows an attacker to force server interfaces into sending packets initiated by the victim server to the local interface or to another server behind the firewall. Consult Web References for more information about this problem.

*This alert belongs to the following categories: 14.1.2*

---

### CVSS2

- **Base Score:** 5.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined
| CVSS3 | Base Score: 9.0  
|       | Attack Vector: Network  
|       | Attack Complexity: High  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: High  |

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-918</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>file</th>
</tr>
</thead>
</table>

| Variants | http://hitzgveqywwbb.bxss.me/ |

**Web Server**

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

*This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4*

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  |

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>login</th>
</tr>
</thead>
</table>

| Variants | 1ACUSTART""tsfKpACUEND |

**/AJAX/infoartist.php**

**SQL injection**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>6.8</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>10.0</td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Changed</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-89

<table>
<thead>
<tr>
<th>Parameter</th>
<th>id</th>
</tr>
</thead>
</table>

| Variants         | 1'' |

/AJAX/infocateg.php

SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>6.8</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

697
**/AJAX/infotitle.php**

**SQL injection**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

*This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4*
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

| CVSS2          | Base Score: 6.8  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Medium  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: Partial  
|               | Availability Impact: Partial  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

| CVSS3          | Base Score: 10.0  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Changed  
|               | Confidentiality Impact: High  
|               | Integrity Impact: High  
|               | Availability Impact: None  

| CWE            | CWE-89  
| Parameter      | artist  
| Variants       | 1ACUSTART""TYdWwACUEND  

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

| CVSS2          | Base Score: 6.8  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Medium  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: Partial  
|               | Availability Impact: Partial  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

699
### SQL injection (verified)

**/cart.php**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a [web application's database server](https://example.com).

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Changed</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: High</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>login</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
<th>1ACUSTART””Ohp3MACUEND</th>
</tr>
</thead>
</table>

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>addcart</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
<th>1ACUSTART””8DJP8ACUEND</th>
</tr>
</thead>
</table>

### SQL injection (verified)
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 10.0</td>
</tr>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-89</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>del</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
</tr>
</thead>
<tbody>
<tr>
<td>1ACUSTART&quot;&quot;OFXxiACUEND</td>
</tr>
</tbody>
</table>

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
### guestbook.php

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

*This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4*

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Changed</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>login</td>
</tr>
<tr>
<td>Variants</td>
<td>1ACUSTART&quot;SQSJoACUEND</td>
</tr>
</tbody>
</table>

---

### listproducts.php

**SQL injection (verified)**

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Changed</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>login</td>
</tr>
<tr>
<td>Variants</td>
<td>1ACUSTART&quot;BQWkpACUEND</td>
</tr>
</tbody>
</table>
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
| Parameter | artist  
| Variants | 1ACUSTART""KVSljACUEND  

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

703
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

#### Parameter

| cat |

#### Variants

| 1ACUSTART"'oA8ddACUEND |

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

*This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4*

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

#### Parameter

| login |

#### Variants

| 1ACUSTART"'38PotACUEND |

**/Mod_Rewrite_Shop/BuyProduct-3/**

**SQL injection (verified)**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

---

**CVSS2**

- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**

- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

**CWE**

- CWE-89

**Parameter**

- /Mod_Rewrite_Shop/Details/color-printer/3/

**SQL injection (verified)**

---

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

---

**CVSS2**

- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

---

705
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Changed</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td></td>
</tr>
<tr>
<td>Variants</td>
<td></td>
</tr>
</tbody>
</table>

/product.php

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
</tr>
<tr>
<td>Access Vector: NetworkAccessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 10.0</td>
</tr>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-89</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>login</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
</tr>
</thead>
<tbody>
<tr>
<td>1ACUSTART&quot;wSLFJACUEND</td>
</tr>
</tbody>
</table>

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
</tr>
<tr>
<td>Access Vector: NetworkAccessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
CVSS3
Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE
CWE-89

Parameter
searchFor

Variants
1ACUSTART"jbBDSACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

CVSS2
Base Score: 6.8
Access Vector: Network_accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3
Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE
CWE-89

Parameter
test

Variants
1ACUSTART"f3W3tACUEND

/secured/newuser.php

SQL injection (verified)
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

**CVSS2**
- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**
- Base Score: 10.0
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: None

**CWE**
- CWE-89

**Parameter**
- uuname

**Variants**
- 1ACUSTART"'Fxw80ACUEND

/sendcommand.php

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

**CVSS2**
- Base Score: 6.8
- Access Vector: Network_accessible
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

711
CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Parameter
cart_id

Variants
1ACUSTART"FWG7kACUEND

/userinfo.php

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

CVSS2

Base Score: 6.8
Access Vector: Network_accessible
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 10.0
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Changed
Confidentiality Impact: High
Integrity Impact: High
Availability Impact: None

CWE

CWE-89

Parameter
login

Variants
1ACUSTART"E6rbyACUEND

SQL injection
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| CVSS2     | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| CVSS3     | Base Score: 10.0  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Changed  
Confidentiality Impact: High  
Integrity Impact: High  
Availability Impact: None |
| CWE       | CWE-89 |
| Parameter | pass |
| Variants  | 1'' |

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| CVSS2     | Base Score: 6.8  
Access Vector: Network_accessible  
Access Complexity: Medium  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: Partial  
Availability Impact: Partial  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE: CWE-89 |

### Parameter

| Script#text |

### Variants

| 1ACUSTART"'k15cFACUEND |

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

*This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4*

---

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE: CWE-89 |

### Parameter

| Script#text |

### Variants

| 'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(83),CHAR(81),CHAR(114),CHAR(113),CHAR(103),CHAR(106),CHAR(69),CHAR(84)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and' |

---

**SQL injection (verified)**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

| CVSS2          | Base Score: 6.8  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Medium  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: Partial  
|               | Availability Impact: Partial  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

| CVSS3          | Base Score: 10.0  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: None  
|               | Scope: Changed  
|               | Confidentiality Impact: High  
|               | Integrity Impact: High  
|               | Availability Impact: None  

| CWE            | CWE-89  

| Parameter      | uaddress  

| Variants       | 1ACUSTART"4a8ycACUEND  

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

| CVSS2          | Base Score: 6.8  
|               | Access Vector: Network_accessible  
|               | Access Complexity: Medium  
|               | Authentication: None  
|               | Confidentiality Impact: Partial  
|               | Integrity Impact: Partial  
|               | Availability Impact: Partial  
|               | Exploitability: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

715
| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
| Parameter | uaddress  
| Variants | '1ACUSTART''aSjczACUEND  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

*This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4*

| CVSS2 | Base Score: 6.8  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Medium  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: Partial  
|       | Availability Impact: Partial  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 10.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Changed  
|       | Confidentiality Impact: High  
|       | Integrity Impact: High  
|       | Availability Impact: None  

| CWE | CWE-89  
| Parameter | uaddress  
| Variants | 'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(115),CHAR(103),CHAR(76),CHAR(66),CHAR(112),CHAR(110),CHAR(51),CHAR(67)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'  

**SQL injection (verified)**
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 10.0</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Changed</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>ucc</td>
</tr>
<tr>
<td>Variants</td>
<td>1ACUSTART&quot;&quot;GD7BwACUEND</td>
</tr>
</tbody>
</table>

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
### CVSS3

<table>
<thead>
<tr>
<th>Base Score</th>
<th>10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Changed</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>CWE-89</th>
</tr>
</thead>
</table>

### Variants

`1ACUSTART"92yp8ACUEND`

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

**This alert belongs to the following categories:** 14.1.2, 14.2.1, 18.1.3, 18.1.4

---

### CVSS2

<table>
<thead>
<tr>
<th>Base Score</th>
<th>6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

---

### CVSS3

<table>
<thead>
<tr>
<th>Base Score</th>
<th>10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Changed</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>CWE-89</th>
</tr>
</thead>
</table>

### Variants

`'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(112),CHAR(101),CHAR(80),CHAR(106),CHAR(80),CHAR(50),CHAR(101),CHAR(65)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'`

### SQL injection (verified)
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 10.0</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Changed</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: High</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-89</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>uemail</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
<th>1ACUSTART&quot;&quot;GQ1gIACUEND</th>
</tr>
</thead>
</table>

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>
### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Parameter
- **uemail**

### Variants
- `1ACUSTART"IGowmACUEND`

---

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application’s database server.

*This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4*

---

### CVSS2
- **Base Score:** 6.8
- **Access Vector:** Network_accessible
- **Access Complexity:** Medium
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** Partial
- **Availability Impact:** Partial
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 10.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Changed
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE
- **CWE:** CWE-89

### Parameter
- **uemail**

### Variants
- `\'and(\select 1 from(select count(*)\n.concat((\select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(55),CHAR(102),CHAR(116),CHAR(85),CHAR(85),CHAR(77),CHAR(100),CHAR(80)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and`
SQL injection (SQLI) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>uname</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td>1&quot;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 10.0</td>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td>uname</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scope: Changed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-89</td>
<td>1&quot;</td>
</tr>
</tbody>
</table>

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>Access Vector: Network_accessable</td>
<td>uname</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td>1&quot;</td>
<td></td>
</tr>
</tbody>
</table>
SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4
This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

| CVSS2          | Base Score: 6.8  
|                | Access Vector: Network_accessible  
|                | Access Complexity: Medium  
|                | Authentication: None  
|                | Confidentiality Impact: Partial  
|                | Integrity Impact: Partial  
|                | Availability Impact: Partial  
|                | Exploitability: Not_defined  
|                | Remediation Level: Not_defined  
|                | Report Confidence: Not_defined  
|                | Availability Requirement: Not_defined  
|                | Collateral Damage Potential: Not_defined  
|                | Confidentiality Requirement: Not_defined  
|                | Integrity Requirement: Not_defined  
|                | Target Distribution: Not_defined  

| CVSS3          | Base Score: 10.0  
|                | Attack Vector: Network  
|                | Attack Complexity: Low  
|                | Privileges Required: None  
|                | User Interaction: None  
|                | Scope: Changed  
|                | Confidentiality Impact: High  
|                | Integrity Impact: High  
|                | Availability Impact: None  

| CWE            | CWE-89  
|                | Parameter: uphone  
|                | Variants: ‘and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(74),CHAR(101),CHAR(105),CHAR(113),CHAR(67),CHAR(76),CHAR(80),CHAR(101)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'  

**SQL injection (verified)**

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

| CVSS2          | Base Score: 6.8  
|                | Access Vector: Network_accessible  
|                | Access Complexity: Medium  
|                | Authentication: None  
|                | Confidentiality Impact: Partial  
|                | Integrity Impact: Partial  
|                | Availability Impact: Partial  
|                | Exploitability: Not_defined  
|                | Remediation Level: Not_defined  
|                | Report Confidence: Not_defined  
|                | Availability Requirement: Not_defined  
|                | Collateral Damage Potential: Not_defined  
|                | Confidentiality Requirement: Not_defined  
|                | Integrity Requirement: Not_defined  
|                | Target Distribution: Not_defined  

723
### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

This alert belongs to the following categories: 14.1.2, 14.2.1, 18.1.3, 18.1.4

---

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-89</th>
</tr>
</thead>
</table>

### Parameter

| uname |

### Variants

1ACUSTART"PDJfPACUEND

---

### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

| CWE-89 |

### Parameter

| uname |

### Variants

1ACUSTART"2kmCQACUEND

---

### SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
<table>
<thead>
<tr>
<th><strong>CVSS2</strong></th>
<th><strong>CVSS3</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.8</td>
<td>Base Score: 10.0</td>
</tr>
<tr>
<td>Access Vector: Network accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Medium</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td>Scope: Changed</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: High</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CWE</strong></th>
<th><strong>Parameter</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-89</td>
<td><strong>uname</strong></td>
</tr>
</tbody>
</table>

| **Variants** | 
|---------------|--------------------------------------------------|
| `'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(111),CHAR(57),CHAR(108),CHAR(51),CHAR(99),CHAR(79),CHAR(101),CHAR(70)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and' | 

/Mod_Rewrite_Shop/

.htaccess file readable (verified)

This directory contains an .htaccess file that is readable. This may indicate a server misconfiguration. .htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4
**Web Server**

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

| CVSS2       | Base Score: 5.0 |
|            | Access Vector: Network accessible |
|            | Access Complexity: Low |
|            | Authentication: None |
|            | Confidentiality Impact: Partial |
|            | Integrity Impact: None |
|            | Availability Impact: None |
|            | Exploitability: Not_defined |
|            | Remediation Level: Not_defined |
|            | Report Confidence: Not_defined |
|            | Availability Requirement: Not_defined |
|            | Collateral Damage Potential: Not_defined |
|            | Confidentiality Requirement: Not_defined |
|            | Integrity Requirement: Not_defined |
|            | Target Distribution: Not_defined |

| CVSS3       | Base Score: 5.3 |
|            | Attack Vector: Network |
|            | Attack Complexity: Low |
|            | Privileges Required: None |
|            | User Interaction: None |
|            | Scope: Unchanged |
|            | Confidentiality Impact: Low |
|            | Integrity Impact: None |
|            | Availability Impact: None |

| CWE         | CWE-200 |

Parameter

login

Variants

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
<th>CWE</th>
<th>Parameter</th>
<th>Variants</th>
</tr>
</thead>
</table>
| Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None | CWE-200 | Referer | |
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None |

| CWE   | CWE-200 |

| Parameter | User-Agent |

| Variants |

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector:</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Low</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

CWE          | CWE-200  |
Parameter    | artist   |
Variants     | 12345"\n\";i]"%00[\%0d%0a<\%00>%bf%27'\n\n"\n
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Parameter | login  
| Variants |  

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE | CWE-200  
| Parameter | Referer  
| Variants |  

733
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

| CVSS2 | Base Score: 5.0 |
|       | Access Vector: Network_accessible |
|       | Access Complexity: Low |
|       | Authentication: None |
|       | Confidentiality Impact: Partial |
|       | Integrity Impact: None |
|       | Availability Impact: None |
|       | Exploitability: Not_defined |
|       | Remediation Level: Not_defined |
|       | Report Confidence: Not_defined |
|       | Availability Requirement: Not_defined |
|       | Collateral Damage Potential: Not_defined |
|       | Confidentiality Requirement: Not_defined |
|       | Integrity Requirement: Not_defined |
|       | Target Distribution: Not_defined |

| CVSS3 | Base Score: 5.3 |
|       | Attack Vector: Network |
|       | Attack Complexity: Low |
|       | Privileges Required: None |
|       | User Interaction: None |
|       | Scope: Unchanged |
|       | Confidentiality Impact: Low |
|       | Integrity Impact: None |
|       | Availability Impact: None |

CWE

CWE-200

Parameter

User-Agent

Variants

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
# CVSS2

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>5.0</td>
</tr>
<tr>
<td>Access Vector</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

# CVSS3

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>5.3</td>
</tr>
<tr>
<td>Attack Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction</td>
<td>None</td>
</tr>
<tr>
<td>Scope</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Low</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

## CWE

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-200</td>
</tr>
</tbody>
</table>

## Parameter

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>X-Forwarded-For</td>
</tr>
</tbody>
</table>

## Variants

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
</table>

### /product.php

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variants</th>
</tr>
</thead>
<tbody>
<tr>
<td>/secured/newuser.php</td>
<td>pic</td>
</tr>
</tbody>
</table>

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-200</th>
</tr>
</thead>
</table>

### Parameter

<table>
<thead>
<tr>
<th>signup</th>
</tr>
</thead>
</table>

### Variants

### Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

### CVSS2

<table>
<thead>
<tr>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-200</th>
</tr>
</thead>
</table>

### Parameter

<table>
<thead>
<tr>
<th>uaddress</th>
</tr>
</thead>
</table>

### Variants
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.3</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ucc</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
<th></th>
</tr>
</thead>
</table>

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-200**

#### Parameter
- **uemail**

#### Variants

---

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE   | CWE-200  

| Parameter | script#text  

| Variants | 12345''\"
|          | ];]]%00{%0d%0a<%00>%bf%27\"\"i  

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

| CVSS2 |基线分值: 5.0  
| 欺骗向量: Network_accessible  
| 访问复杂性: Low  
| 认证: None  
| 机密性影响: Partial  
| 完整性影响: None  
| 可用性影响: None  
| 利用性: Not_defined  
| 救援级别: Not_defined  
| 报告信心: Not_defined  
| 可用性要求: Not_defined  
| 剩余损害潜力: Not_defined  
| 机密性要求: Not_defined  
| 完整性要求: Not_defined  
| 目标分布: Not_defined |

| CVSS3 | 基线分值: 5.3  
| 攻击向量: Network  
| 攻击复杂性: Low  
| 需要的权限: None  
| 用户交互: None  
| 范围: Unchanged  
| 机密性影响: Low  
| 完整性影响: None  
| 可用性影响: None  

| CWE | CWE-200 |

| Parameter | uaddress |

| Variants | 12345"\";\"i\"j\"*%00(%0d%0a<%00>\%bf%27\"ò\"i |

**Application error message**

此警报需要手动确认

应用程序错误或警告消息可能暴露有关应用程序内部工作情况的敏感信息给攻击者。

Acunetix找到一个可能泄露敏感信息的错误或警告消息。消息也可能包含产生未处理异常的文件的位置。有关受影响页面的更多信息，请参阅“攻击细节”部分。

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** Low
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE-200**
- **Parameter:** ucc
- **Variants:** 12345"\";\"%00%0d%0a<%00>%bf%27\"ð¡

**Application error message**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Base Score: 5.3</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
</tbody>
</table>

CWE

CWE-200

Parameter

uphone

Variants

12345"\"");i]"%00{%0d%0a<%00>%bf%27\"%i

Application error message

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200  
Parameter | surname |
| Variants | 12345"\");j]*%00%c0d%0a<%00>%%bf%27öäì |

/\index.bak

Backup files

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.1.4, 12.4.2, 12.4.3, 14.3.1, 18.1.3, 18.1.4

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CWE | CWE-538  
Parameter | |
| Variants | |
A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.1.4, 12.4.2, 12.4.3, 14.3.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network_accessable</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variants</th>
</tr>
</thead>
</table>

/index.zip

Credit card number disclosed (verified)

This alert may be a false positive, manual confirmation is required.

The response contains one or more credit card numbers. The credit card numbers were validated using the Luhn algorithm to make sure they are real credit card numbers.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 4.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network_accessable</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

/userinfo.php
This page is possibly vulnerable to Cross domain data hijacking. If an attacker can create/upload a malicious Flash (SWF) file or control the top part of any page he can perform an attack known as Cross domain data hijacking. The Content-Type of the response doesn't matter. If the file is embedded using an <object> tag, it will be executed as a Flash file as long as the content of the file looks like a valid Flash file.

Here is the attack scenario:

- An attacker creates a malicious Flash (SWF) file
- The attacker changes the file extension to JPG
- The attacker uploads the file to victim.com
- The attacker embeds the file on attacker.com using an tag with type "application/x-shockwave-flash"
- The victim visits attacker.com, loads the file as embedded with the tag
- The attacker can now send and receive arbitrary requests to victim.com using the victims session
- The attacker sends a request to victim.com and extracts the CSRF token from the response

There are many ways to perform this attack. The attacker doesn't need to upload a file. The only requirement is that an attacker can control the data on a location of the target domain. One way is to abuse a JSONP API. Usually, the attacker can control the output of a JSONP API endpoint by changing the callback parameter. However, if an attacker uses an entire Flash file as callback, we can use it just like we would use an uploaded file in this attack.

A payload could look like this:

```
<object style="height:1px;width:1px;" data="http://victim.com/userjsonp?callback=CWS%07%0E
```

This alert belongs to the following categories: 12.5.1
This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

This alert belongs to the following categories: 14.1.2, 14.2.1
### CVSS3

- **Base Score:** 5.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE

- **CWE:** CWE-79

### Parameter

- **file**

### Variants

- `.pictures/1.jpg``&%<acx><ScRiPt >yTNC(9475)</ScRiPt>`

### Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

*This alert belongs to the following categories:* 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-538

### Parameter

- **file**

### Variants

- `.idea/scopes/`
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4*

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

**CWE**

CWE-538

**Parameter**

Variants

_/mmServerScripts/_

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4*
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE      | CWE-538 |

Parameter

Variants

.CVSI/

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4

CVSS2

- Base Score: 5.0
- Access Vector: Network_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

CVSS3

- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

CWE

CWE-538

Parameter

Variants

/Mod_Rewrite_Shop/images/

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4

CVSS2

- Base Score: 5.0
- Access Vector: Network_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th><strong>CVSS2</strong></th>
<th><strong>CVSS3</strong></th>
<th><strong>CWE</strong></th>
<th><strong>Parameter</strong></th>
<th><strong>Variants</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Base Score: 7.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Scope: Unchanged</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td>Exploitability: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td>Remediation Level: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td>Report Confidence: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td>Availability Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

/wvstests/

Directory listing (verified)

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4

DIRECTORY LISTING

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4
The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4

| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessable  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-538 |
| Parameter | |
| Variants | |

/AJAX/infoartist.php

Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
| CVSS2 | Base Score: 5.0  
Access Vector: Network_accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 5.3  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Parameter |  |
| Variants |  |

/AJAX/infocateg.php

**Error message on page**

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*
| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessable  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  
| CWE  | CWE-200  
| Parameter |  
| Variants |  

/AJAX/infotitle.php  

Error message on page  

This alert requires manual confirmation  

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.  

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.  

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
| CVSS2 | Base Score: 5.0
Access Vector: Network_accessable
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 5.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: Low
Integrity Impact: None
Availability Impact: None |
| CWE | CWE-200 |
| Parameter | |
| Variants | |

/Connections/DB_Connection.php

Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Base Score: 5.3</td>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Complexity: Low</td>
<td>Attack Complexity: Low</td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Privileges Required: None</td>
<td>Privileges Required: None</td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td>User Interaction: None</td>
<td>User Interaction: None</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>Scope: Unchanged</td>
<td>Scope: Unchanged</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Confidentiality Impact: Low</td>
<td>Confidentiality Impact: Low</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Integrity Impact: None</td>
<td>Integrity Impact: None</td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Availability Impact: None</td>
<td>Availability Impact: None</td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CWE

Parameter

CWE-200

Variants

/pictures/path-disclosure-unix.html

Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>Base Score: 5.3</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: Low</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-200</td>
<td></td>
</tr>
</tbody>
</table>

/secured/database_connect.php

Error message on page

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
| CVSS2               | Base Score: 5.0  
|                    | Access Vector: Network_accessible  
|                    | Access Complexity: Low  
|                    | Authentication: None  
|                    | Confidentiality Impact: Partial  
|                    | Integrity Impact: None  
|                    | Availability Impact: None  
|                    | Exploitability: Not_defined  
|                    | Remediation Level: Not_defined  
|                    | Report Confidence: Not_defined  
|                    | Availability Requirement: Not_defined  
|                    | Collateral Damage Potential: Not_defined  
|                    | Confidentiality Requirement: Not_defined  
|                    | Integrity Requirement: Not_defined  
|                    | Target Distribution: Not_defined  
| CVSS3               | Base Score: 5.3  
|                    | Attack Vector: Network  
|                    | Attack Complexity: Low  
|                    | Privileges Required: None  
|                    | User Interaction: None  
|                    | Scope: Unchanged  
|                    | Confidentiality Impact: Low  
|                    | Integrity Impact: None  
|                    | Availability Impact: None  
| CWE               | CWE-200  
| Parameter         |  
| Variants          |  

/404.php

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3
<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 2.6</td>
<td>Base Score: 4.3</td>
</tr>
<tr>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Access Complexity: High</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
<td>User Interaction: Required</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-352</td>
<td>&lt;empty&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
<th></th>
</tr>
</thead>
</table>

/artists.php

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

*This alert belongs to the following categories: 9.2.3*
| CVSS2  | Base Score: 2.6  
|        | Access Vector: Network accessible  
|        | Access Complexity: High  
|        | Authentication: None  
|        | Confidentiality Impact: None  
|        | Integrity Impact: Partial  
|        | Availability Impact: None  
|        | Exploitability: Not_defined  
|        | Remediation Level: Not_defined  
|        | Report Confidence: Not_defined  
|        | Availability Requirement: Not_defined  
|        | Collateral Damage Potential: Not_defined  
|        | Confidentiality Requirement: Not_defined  
|        | Integrity Requirement: Not_defined  
|        | Target Distribution: Not_defined  

| CVSS3  | Base Score: 4.3  
|        | Attack Vector: Network  
|        | Attack Complexity: Low  
|        | Privileges Required: None  
|        | User Interaction: Required  
|        | Scope: Unchanged  
|        | Confidentiality Impact: None  
|        | Integrity Impact: Low  
|        | Availability Impact: None  

| CWE    | CWE-352  
|        | Parameter | <empty>  
|        | Variants |  

**/cart.php**

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

*This alert belongs to the following categories: 9.2.3*
CVSS2
Base Score: 2.6
Access Vector: Network_accessable
Access Complexity: High
Authentication: None
Confidentiality Impact: None
Integrity Impact: Partial
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3
Base Score: 4.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: Low
Availability Impact: None

CWE
CWE-352

Parameter
<empty>

Variants

/categories.php

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim’s browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3
<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>2.6</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>High</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>4.3</td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>Required</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Low</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-352</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>&lt;empty&gt;</td>
</tr>
<tr>
<td>Variants</td>
<td></td>
</tr>
</tbody>
</table>

### /comment.php

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

*This alert belongs to the following categories: 9.2.3*
CVSS2
Base Score: 2.6
Access Vector: Network_accessible
Access Complexity: High
Authentication: None
Confidentiality Impact: None
Integrity Impact: Partial
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3
Base Score: 4.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: Low
Availability Impact: None

CWE
CWE-352

Parameter
fComment

Variants

/disclaimer.php

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3
### CVSS2
- **Base Score:** 2.6
- **Access Vector:** Network accessible
- **Access Complexity:** High
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 4.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** Required
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE:** CWE-352
- **Parameter:** <empty>
- **Variants:**

**/guestbook.php**

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim’s browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

*This alert belongs to the following categories: 9.2.3*
**CVSS2**

- Base Score: 2.6
- Access Vector: Network_accessible
- Access Complexity: High
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: Partial
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

**CVSS3**

- Base Score: 4.3
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: Required
- Scope: Unchanged
- Confidentiality Impact: None
- Integrity Impact: Low
- Availability Impact: None

**CWE**

- CWE-352

**Parameter**

- <empty>

**Variants**

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

*This alert belongs to the following categories: 9.2.3*
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 4.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: Required</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

### CWE

<table>
<thead>
<tr>
<th>CWE-352</th>
</tr>
</thead>
</table>

### Parameter

| faddentry |

### Variants

/hpp/

### HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

*This alert belongs to the following categories: 9.2.3*
Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: High</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 4.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: Required</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-352</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>&lt;empty&gt;</td>
</tr>
<tr>
<td>Variants</td>
<td></td>
</tr>
</tbody>
</table>

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.
Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3

| CVSS2          | Base Score: 2.6  
|                | Access Vector: Network_accessible  
|                | Access Complexity: High  
|                | Authentication: None  
|                | Confidentiality Impact: None  
|                | Integrity Impact: Partial  
|                | Availability Impact: None  
|                | Exploitability: Not_defined  
|                | Remediation Level: Not_defined  
|                | Report Confidence: Not_defined  
|                | Availability Requirement: Not_defined  
|                | Collateral Damage Potential: Not_defined  
|                | Confidentiality Requirement: Not_defined  
|                | Integrity Requirement: Not_defined  
|                | Target Distribution: Not_defined  
| CVSS3          | Base Score: 4.3  
|                | Attack Vector: Network  
|                | Attack Complexity: Low  
|                | Privileges Required: None  
|                | User Interaction: Required  
|                | Scope: Unchanged  
|                | Confidentiality Impact: None  
|                | Integrity Impact: Low  
|                | Availability Impact: None  
| CWE            | CWE-352  
| Parameter      | <empty>  
| Variants       |  

/listproducts.php

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3
CVSS2

Base Score: 2.6
Access Vector: Network_accessible
Access Complexity: High
Authentication: None
Confidentiality Impact: None
Integrity Impact: Partial
Availability Impact: None
Exploitability: Not_defined
 Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 4.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: Low
Availability Impact: None

CWE

CWE-352

Parameter
<empty>

Variants

/login.php

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3
CVSS2

Base Score: 2.6
Access Vector: Network accessible
Access Complexity: High
Authentication: None
Confidentiality Impact: None
Integrity Impact: Partial
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 4.3
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Scope: Unchanged
Confidentiality Impact: None
Integrity Impact: Low
Availability Impact: None

CWE

CWE-352

Parameter
<empty>

Variants

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3

CVSS2

Base Score: 2.6
Access Vector: Network accessible
Access Complexity: High
Authentication: None
Confidentiality Impact: None
Integrity Impact: Partial
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined
Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim’s browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3
Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3

| CVSS2 | Base Score: 2.6  
| Access Vector: Network_accessible  
| Access Complexity: High  
| Authentication: None  
| Confidentiality Impact: None  
| Integrity Impact: Partial  
| Availability Impact: None  
| Exploitability: Not_defined  
| Remediation Level: Not_defined  
| Report Confidence: Not_defined  
| Availability Requirement: Not_defined  
| Collateral Damage Potential: Not_defined  
| Confidentiality Requirement: Not_defined  
| Integrity Requirement: Not_defined  
| Target Distribution: Not_defined |

| CVSS3 | Base Score: 4.3  
| Attack Vector: Network  
| Attack Complexity: Low  
| Privileges Required: None  
| User Interaction: Required  
| Scope: Unchanged  
| Confidentiality Impact: None  
| Integrity Impact: Low  
| Availability Impact: None |

CWE  
CWE-352  
Parameter  
<empty>  
Variants

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
This alert belongs to the following categories: 9.2.3

| CVSS2 | Base Score: 2.6  
|       | Access Vector: Network_accessible  
|       | Access Complexity: High  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  |

| CVSS3 | Base Score: 4.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: Required  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None  |

| CWE | CWE-352 |
| Parameter | f_addcart |
| Variants | |

/search.php

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3
### CVSS2
- **Base Score:** 2.6
- **Access Vector:** Network accessible
- **Access Complexity:** High
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 4.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** Required
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE:** CWE-352

### Parameter
- **<empty>**

### Variants

<table>
<thead>
<tr>
<th>/signup.php</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTML form without CSRF protection</strong></td>
</tr>
</tbody>
</table>

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

*This alert belongs to the following categories: 9.2.3*
| CVSS2 | Base Score: 2.6  
|       | Access Vector: Network_accessible  
|       | Access Complexity: High  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Partial  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  
| CVSS3 | Base Score: 4.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: Required  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: Low  
|       | Availability Impact: None  
| CWE | CWE-352  
| Parameter | <empty>  
| Variants |  

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

*This alert belongs to the following categories: 9.2.3*
### CVSS3
- **Base Score:** 4.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** Required
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE-352**

### Parameter
- **form1**

### Variants

**/Templates/main_dynamic_template.dwt.php**

**HTML form without CSRF protection**

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the ‘Attack details’ section for more information about the affected HTML form.

_This alert belongs to the following categories: 9.2.3_

### CVSS2
- **Base Score:** 2.6
- **Access Vector:** Network_accessible
- **Access Complexity:** High
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 4.3
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** Required
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** Low
- **Availability Impact:** None

### CWE
- **CWE-352**

### Parameter
- **<empty>**

### Variants
/userinfo.php

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

This alert belongs to the following categories: 9.2.3

| CVSS2         | Base Score: 2.6  
|               | Access Vector: Network_accessible  
|               | Access Complexity: High  
|               | Authentication: None  
|               | Confidentiality Impact: None  
|               | Integrity Impact: Partial  
|               | Availability Impact: None  
|               | Exploitation: Not_defined  
|               | Remediation Level: Not_defined  
|               | Report Confidence: Not_defined  
|               | Availability Requirement: Not_defined  
|               | Collateral Damage Potential: Not_defined  
|               | Confidentiality Requirement: Not_defined  
|               | Integrity Requirement: Not_defined  
|               | Target Distribution: Not_defined  

| CVSS3         | Base Score: 4.3  
|               | Attack Vector: Network  
|               | Attack Complexity: Low  
|               | Privileges Required: None  
|               | User Interaction: Required  
|               | Scope: Unchanged  
|               | Confidentiality Impact: None  
|               | Integrity Impact: Low  
|               | Availability Impact: None  

| CWE          | CWE-352  

| Parameter   | <empty>  

| Variants   |  

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
This alert belongs to the following categories: 9.2.3

| CVSS2          | Base Score: 2.6              |
|               | Access Vector: Network_accessible |
|               | Access Complexity: High      |
|               | Authentication: None         |
|               | Confidentiality Impact: None |
|               | Integrity Impact: Partial    |
|               | Availability Impact: None    |
|               | Exploitability: Not_defined  |
|               | Remediation Level: Not_defined|
|               | Report Confidence: Not_defined|
|               | Availability Requirement: Not_defined |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined |
|               | Target Distribution: Not_defined |

| CVSS3          | Base Score: 4.3              |
|               | Attack Vector: Network       |
|               | Attack Complexity: Low       |
|               | Privileges Required: None    |
|               | User Interaction: Required   |
|               | Scope: Unchanged             |
|               | Confidentiality Impact: None |
|               | Integrity Impact: Low        |
|               | Availability Impact: None    |

| CWE            | CWE-352                      |
| Parameter      | form1                        |
| Variants       | /hpp/                        |

**HTTP parameter pollution**

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.

This alert belongs to the following categories: 14.2.1

| CVSS2          | Base Score: 5.0              |
|               | Access Vector: NetworkAccessible |
|               | Access Complexity: Low       |
|               | Authentication: None         |
|               | Confidentiality Impact: None |
|               | Integrity Impact: Partial    |
|               | Availability Impact: None    |
|               | Exploitability: Not_defined  |
|               | Remediation Level: Not_defined|
|               | Report Confidence: Not_defined|
|               | Availability Requirement: Not_defined |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined |
|               | Target Distribution: Not_defined |
### /hpp/index.php

**HTTP parameter pollution**

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.

*This alert belongs to the following categories: 14.2.1*

---

### CVSS3

- **Base Score:** 9.1
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE-88**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>pp</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Variants</strong></td>
<td>12&amp;n94137=v968503</td>
</tr>
</tbody>
</table>

---

### CVSS2

- **Base Score:** 5.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** Partial
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

---

### CVSS3

- **Base Score:** 9.1
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** High
- **Availability Impact:** None

### CWE

- **CWE-88**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>pp</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Variants</strong></td>
<td>12&amp;n910804=v977330</td>
</tr>
</tbody>
</table>

---

### Web Server
The browser security model normally prevents web content from one domain from accessing data from another domain. This is commonly known as the "same origin policy". URL policy files grant cross-domain permissions for reading data. They permit operations that are not permitted by default. The URL policy file is located, by default, in the root directory of the target server, with the name crossdomain.xml (for example, at www.example.com/crossdomain.xml).

When a domain is specified in crossdomain.xml file, the site declares that it is willing to allow the operators of any servers in that domain to obtain any document on the server where the policy file resides. The crossdomain.xml file deployed on this website opens the server to all domains (use of a single asterisk "*" as a pure wildcard is supported) like so:

```
<cross-domain-policy>
<allow-access-from domain="*" />
</cross-domain-policy>
```

This practice is suitable for public servers, but should not be used for sites located behind a firewall because it could permit access to protected areas. It should not be used for sites that require authentication in the form of passwords or cookies. Sites that use the common practice of authentication based on cookies to access private or user-specific data should be especially careful when using cross-domain policy files.

*This alert belongs to the following categories: 12.5.1*

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector:</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 6.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Low</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>Low</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-284</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td></td>
</tr>
<tr>
<td>Variants</td>
<td></td>
</tr>
</tbody>
</table>

JetBrains .idea project directory
The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

This alert belongs to the following categories: 8.2.3, 9.4.1, 9.4.5, 12.1.4, 12.4.2, 12.4.3, 14.3.1, 18.1.3, 18.1.4

|---------------|---------------------------------------------------------------|

| CWE          | CWE-538 |

| Parameter | CWE-538 |

| Variant | /secured/phpinfo.php |

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

This alert belongs to the following categories: 12.5.1

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined</th>
</tr>
</thead>
</table>
Web Server

**PHP errors enabled (verified)**

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix AcuSensor found that the PHP `display_errors` directive is enabled.

*This alert belongs to the following categories: 12.5.1*
PHP errors enabled (verified)

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found that the PHP `display_errors` directive is enabled.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 12.5.1, 18.1.3, 18.1.4

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 5.3  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: Low  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE | Parameter: CWE-16  
| Variants |  

PHP open_basedir is not set (verified)

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

This alert belongs to the following categories: 12.5.1
**PHP session.use_only_cookies disabled (verified)**

When use_only_cookies is disabled, PHP will pass the session ID via the URL. This makes the application more vulnerable to session hijacking attacks. Session hijacking is basically a form of identity theft wherein a hacker impersonates a legitimate user by stealing his session ID. When the session token is transmitted in a cookie, and the request is made on a secure channel (that is, it uses SSL), the token is secure.

*This alert belongs to the following categories: 12.5.1*
PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.1.4, 12.4.2, 12.4.3, 14.3.1, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

| CWE                  | CWE-200 |

| Parameter            | |

| Variants             | |

PHPinfo page found

This script is using phpinfo() function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.1.4, 12.4.2, 12.4.3, 14.3.1, 18.1.3, 18.1.4
CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitation: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

CWE

CWE-200

Parameter

Variants

/index.bak

Source code disclosure

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

This alert belongs to the following categories: 8.2.3, 9.4.1, 9.4.5, 12.4.2, 12.4.3, 18.1.3, 18.1.4
CVSS3

Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

CWE

CWE-538

Parameter

Variants

/pictures/wp-config.bak

Source code disclosure

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

This alert belongs to the following categories: 8.2.3, 9.4.1, 9.4.5, 12.4.2, 12.4.3, 18.1.3, 18.1.4

CVSS2

Base Score: 5.0
Access Vector: Network_accessible
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Exploitability: Not_defined
Remediation Level: Not_defined
Report Confidence: Not_defined
Availability Requirement: Not_defined
Collateral Damage Potential: Not_defined
Confidentiality Requirement: Not_defined
Integrity Requirement: Not_defined
Target Distribution: Not_defined

CVSS3

Base Score: 7.5
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None
Availability Impact: None

CWE

CWE-538

Parameter

Variants

/login.php

User credentials are sent in clear text
User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

This alert belongs to the following categories: 13.2.1, 13.2.3, 14.1.3

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>5.0</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>High</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Workaround</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Confirmed</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>9.1</td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>High</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-310</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>loginform</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Variants</th>
</tr>
</thead>
</table>

/signup.php

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

This alert belongs to the following categories: 13.2.1, 13.2.3, 14.1.3

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>5.0</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>Partial</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>High</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Workaround</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Confirmed</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>
WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

This alert belongs to the following categories: 8.2.3, 9.4.1, 9.4.5, 12.1.4, 12.4.2, 12.4.3, 14.3.1, 18.1.3, 18.1.4

Web Server

Cookie(s) without HttpOnly flag set (verified)

This cookie does not have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

This alert belongs to the following categories: 12.5.1
Cookie(s) without Secure flag set (verified)

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

This alert belongs to the following categories: 12.5.1

Hidden form input named price was found

A hidden form input named price was found. It's not recommended to hide sensitive information in hidden form fields.

This alert belongs to the following categories: 12.5.1
For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

**This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Base Score: 0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS2**

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-538</th>
</tr>
</thead>
</table>

**Possible sensitive directories**

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

**This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

**CVSS2**
### CVSS3
- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

### CWE
- CWE-200

### Parameter

### Variants

---

/\CVS/

**Possible sensitive directories**

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

*This alert belongs to the following categories:* 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

---

### CVSS2
- Base Score: 5.0
- Access Vector: Network_accessible
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None
- Exploitability: Not_defined
- Remediation Level: Not_defined
- Report Confidence: Not_defined
- Availability Requirement: Not_defined
- Collateral Damage Potential: Not_defined
- Confidentiality Requirement: Not_defined
- Integrity Requirement: Not_defined
- Target Distribution: Not_defined

---

### CVSS3
- Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

### CWE
- CWE-200

### Parameter

### Variants

---

/\hpp/test.php

**Possible sensitive files**
A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.1.4, 12.4.2, 12.4.3, 14.3.1, 18.1.3, 18.1.4

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined  

| CVSS3 | Base Score: 7.5  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: High  
|       | Integrity Impact: None  
|       | Availability Impact: None  

| CWE  | CWE-200  

| Parameter |  
| Variants |  

**Web Server**

**Possible virtual host found**

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.

This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
### CVSS2
- **Base Score:** 5.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** Partial
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not defined
- **Remediation Level:** Not defined
- **Report Confidence:** Not defined
- **Availability Requirement:** Not defined
- **Collateral Damage Potential:** Not defined
- **Confidentiality Requirement:** Not defined
- **Integrity Requirement:** Not defined
- **Target Distribution:** Not defined

### CVSS3
- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **Parameter:** CWE-200
- **Variants**

#### Unencrypted connection (verified)

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

*This alert belongs to the following categories: 13.2.1, 13.2.3, 14.1.3, 18.1.5*
Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a `Content-Security-Policy` header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```plaintext
Content-Security-Policy:
  default-src 'self';
  script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

*This alert belongs to the following categories: 12.5.1*
Variants

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*

| CVSS2         | Base Score: 0.0
|              | Access Vector: Network_accessable
|              | Access Complexity: Low
|              | Authentication: None
|              | Confidentiality Impact: None
|              | Integrity Impact: None
|              | Availability Impact: None
|              | Exploitability: Not_defined
|              | Remediation Level: Not_defined
|              | Report Confidence: Not_defined
|              | Availability Requirement: Not_defined
|              | Collateral Damage Potential: Not_defined
|              | Confidentiality Requirement: Not_defined
|              | Integrity Requirement: Not_defined
|              | Target Distribution: Not_defined

| CVSS3         | Base Score: 0.0
|              | Attack Vector: Network
|              | Attack Complexity: Low
|              | Privileges Required: None
|              | User Interaction: None
|              | Scope: Unchanged
|              | Confidentiality Impact: None
|              | Integrity Impact: None
|              | Availability Impact: None

| CWE           | CWE-200

| Parameter     | Variants

/404.php

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>Parameter</th>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Access Vector</td>
<td>Network accessible</td>
<td>Network</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>None</td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>None</td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability</td>
<td>Not_defined</td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>Not_defined</td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>Not_defined</td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement</td>
<td>Not_defined</td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential</td>
<td>Not_defined</td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement</td>
<td>Not_defined</td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement</td>
<td>Not_defined</td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution</td>
<td>Not_defined</td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

CWE

Parameter

CWE-200

Variants

/disclaimer.php

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
| CVSS3 | Base Score: 0.0  
|       | Attack Vector: Network  
|       | Attack Complexity: Low  
|       | Privileges Required: None  
|       | User Interaction: None  
|       | Scope: Unchanged  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None |
| CWE  | CWE-200 |
| Parameter  | |
| Variants  | |

/guestbook.php

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

| CVSS2 | Base Score: 0.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: None  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: Not_defined  
|       | Remediation Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | Availability Requirement: Not_defined  
|       | Collateral Damage Potential: Not_defined  
|       | Confidentiality Requirement: Not_defined  
|       | Integrity Requirement: Not_defined  
|       | Target Distribution: Not_defined |
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

| CVSS2          | Base Score: 0.0 |
|               | Access Vector: Network_accessible |
|               | Access Complexity: Low |
|               | Authentication: None |
|               | Confidentiality Impact: None |
|               | Integrity Impact: None |
|               | Availability Impact: None |
|               | Exploitability: Not_defined |
|               | Remediation Level: Not_defined |
|               | Report Confidence: Not_defined |
|               | Availability Requirement: Not_defined |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined |
|               | Target Distribution: Not_defined |

| CVSS3          | Base Score: 0.0 |
|               | Attack Vector: Network |
|               | Attack Complexity: Low |
|               | Privileges Required: None |
|               | User Interaction: None |
|               | Scope: Unchanged |
|               | Confidentiality Impact: None |
|               | Integrity Impact: None |
|               | Availability Impact: None |

| CWE            | CWE-200 |

| Parameter      | |
| Variants       | |

/listproducts.php

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
</tr>
<tr>
<td>Access Vector: Network.Accessible</td>
</tr>
<tr>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Authentication: None</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
</tr>
<tr>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td>Privileges Required: None</td>
</tr>
<tr>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Variants</td>
</tr>
</tbody>
</table>

/search.php

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variants</th>
</tr>
</thead>
<tbody>
<tr>
<td>/signup.php</td>
<td></td>
</tr>
</tbody>
</table>

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
### CVSS3
- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-200**

### Parameter
- **Variants**

#### /Templates/main_dynamic_template.dwt.php

**Email address found**

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

### CVSS2
- **Base Score:** 0.0
- **Access Vector:** Network accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3
- **Base Score:** 0.0
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE
- **CWE-200**

### Parameter
- **Variants**

#### /userinfo.php
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>0.0</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network_accessible</td>
</tr>
<tr>
<td>Access Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Authentication:</td>
<td>None</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Exploitability:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Report Confidence:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Availability Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Collateral Damage Potential:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement:</td>
<td>Not_defined</td>
</tr>
<tr>
<td>Target Distribution:</td>
<td>Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>0.0</td>
</tr>
<tr>
<td>Attack Vector:</td>
<td>Network</td>
</tr>
<tr>
<td>Attack Complexity:</td>
<td>Low</td>
</tr>
<tr>
<td>Privileges Required:</td>
<td>None</td>
</tr>
<tr>
<td>User Interaction:</td>
<td>None</td>
</tr>
<tr>
<td>Scope:</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact:</td>
<td>None</td>
</tr>
<tr>
<td>Availability Impact:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter:</td>
<td>CWE-200</td>
</tr>
<tr>
<td>Variants:</td>
<td></td>
</tr>
</tbody>
</table>

/secured/office.htm

Microsoft Office possible sensitive information

This document has been converted to HTML using Microsoft Office. It seems that Office has included sensitive information during the conversion.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
|---|---|
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Parameter |  |
| Variants |  |

**Web Server**

**Password type input with auto-complete enabled**

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*
### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>form1</td>
<td></td>
</tr>
</tbody>
</table>

### Variants

- Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

*This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4*

### CVSS2

- **Base Score:** 0.0
- **Access Vector:** Network_accessible
- **Access Complexity:** Low
- **Authentication:** None
- **Confidentiality Impact:** None
- **Integrity Impact:** None
- **Availability Impact:** None
- **Exploitability:** Not_defined
- **Remediation Level:** Not_defined
- **Report Confidence:** Not_defined
- **Availability Requirement:** Not_defined
- **Collateral Damage Potential:** Not_defined
- **Confidentiality Requirement:** Not_defined
- **Integrity Requirement:** Not_defined
- **Target Distribution:** Not_defined

### CVSS3

- **Base Score:** 7.5
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **Scope:** Unchanged
- **Confidentiality Impact:** High
- **Integrity Impact:** None
- **Availability Impact:** None

### CWE

- **CWE:** CWE-200

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>loginform</td>
<td></td>
</tr>
</tbody>
</table>

### Variants

- /404.php

### Possible internal IP address disclosure
A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Vector: Network accessible</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Base Score: 7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: High</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: None</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

Parameter

Variants

/pictures/ipaddresses.txt

Possible internal IP address disclosure

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
| CVSS2 | Base Score: 5.0  
| | Access Vector: Network_accessible  
| | Access Complexity: Low  
| | Authentication: None  
| | Confidentiality Impact: Partial  
| | Integrity Impact: None  
| | Availability Impact: None  
| | Exploitability: Not_defined  
| | Remediation Level: Not_defined  
| | Report Confidence: Not_defined  
| | Availability Requirement: Not_defined  
| | Collateral Damage Potential: Not_defined  
| | Confidentiality Requirement: Not_defined  
| | Integrity Requirement: Not_defined  
| | Target Distribution: Not_defined  
| CVSS3 | Base Score: 7.5  
| | Attack Vector: Network  
| | Attack Complexity: Low  
| | Privileges Required: None  
| | User Interaction: None  
| | Scope: Unchanged  
| | Confidentiality Impact: High  
| | Integrity Impact: None  
| | Availability Impact: None  
| CWE | CWE-200  
| Parameter | /secured/phpinfo.php  
| | Possible internal IP address disclosure  
| | A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.  
| | This alert may be a false positive, manual confirmation is required.  
| | This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4  
| CVSS2 | Base Score: 5.0  
| | Access Vector: Network_accessible  
| | Access Complexity: Low  
| | Authentication: None  
| | Confidentiality Impact: Partial  
| | Integrity Impact: None  
| | Availability Impact: None  
| | Exploitability: Not_defined  
| | Remediation Level: Not_defined  
| | Report Confidence: Not_defined  
| | Availability Requirement: Not_defined  
| | Collateral Damage Potential: Not_defined  
| | Confidentiality Requirement: Not_defined  
| | Integrity Requirement: Not_defined  
| | Target Distribution: Not_defined  
<p>|</p>
<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Parameter</th>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 7.5</td>
<td>/pictures/path-disclosure-unix.html</td>
<td>CWE-200</td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td>Possible server path disclosure (Unix)</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td>One or more fully qualified path names</td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td>were found on this page. From this</td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td>information the attacker may learn</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td>the file system structure from the</td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>web server. This information can be</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>used to conduct further attacks.</td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td>This alert may be a false positive,</td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td>manual confirmation is required.</td>
<td></td>
</tr>
</tbody>
</table>

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Parameter</th>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
<td>/secured/phpinfo.php</td>
<td>CWE-200</td>
</tr>
<tr>
<td>Access Vector: Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Complexity: Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitability: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Level: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Confidence: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Requirement: Not_defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Distribution: Not_defined</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS3</th>
<th>Parameter</th>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 7.5</td>
<td>/secured/phpinfo.php</td>
<td>CWE-200</td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileges Required: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Interaction: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scope: Unchanged</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality Impact: High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Impact: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Impact: None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Possible server path disclosure (Unix)

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4

| CVSS2          | Base Score: 5.0  |
|               | Access Vector: Network_accessible |
|               | Access Complexity: Low |
|               | Authentication: None |
|               | Confidentiality Impact: Partial |
|               | Integrity Impact: None |
|               | Availability Impact: None |
|               | Exploitability: Not_defined |
|               | Remediation Level: Not_defined |
|               | Report Confidence: Not_defined |
|               | Availability Requirement: Not_defined |
|               | Collateral Damage Potential: Not_defined |
|               | Confidentiality Requirement: Not_defined |
|               | Integrity Requirement: Not_defined |
|               | Target Distribution: Not_defined |

| CVSS3          | Base Score: 7.5  |
|               | Attack Vector: Network |
|               | Attack Complexity: Low |
|               | Privileges Required: None |
|               | User Interaction: None |
|               | Scope: Unchanged |
|               | Confidentiality Impact: High |
|               | Integrity Impact: None |
|               | Availability Impact: None |

CWE          | CWE-200 |

Parameter

Variants

/pictures/credentials.txt

Possible username or password disclosure

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

This alert belongs to the following categories: 8.2.3, 9.4.1, 12.4.2, 12.4.3, 18.1.3, 18.1.4
| CVSS2 | Base Score: 5.0  
Access Vector: Network accessible  
Access Complexity: Low  
Authentication: None  
Confidentiality Impact: Partial  
Integrity Impact: None  
Availability Impact: None  
Exploitability: Not_defined  
Remediation Level: Not_defined  
Report Confidence: Not_defined  
Availability Requirement: Not_defined  
Collateral Damage Potential: Not_defined  
Confidentiality Requirement: Not_defined  
Integrity Requirement: Not_defined  
Target Distribution: Not_defined |
| CVSS3 | Base Score: 7.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: High  
Integrity Impact: None  
Availability Impact: None |
| CWE | CWE-200 |
| Parameter | |
| Variants | |
Scanned items (coverage report)

http://testphp.vulnweb.com/
http://testphp.vulnweb.com/.idea/
http://testphp.vulnweb.com/_mmServerScripts/
http://testphp.vulnweb.com/404.php
http://testphp.vulnweb.com/admin/
http://testphp.vulnweb.com/admin/create.sql
http://testphp.vulnweb.com/AJAX/infoartist.php
http://testphp.vulnweb.com/cart.php
http://testphp.vulnweb.com/categories.php
http://testphp.vulnweb.com/comment.php
http://testphp.vulnweb.com/Connections/
http://testphp.vulnweb.com/Connections/DB_Connection.php
http://testphp.vulnweb.com/CVS/
http://testphp.vulnweb.com/Flash/
http://testphp.vulnweb.com/guestbook.php
http://testphp.vulnweb.com/hpp/
http://testphp.vulnweb.com/images/
http://testphp.vulnweb.com/index.bak
http://testphp.vulnweb.com/index.zip
http://testphp.vulnweb.com/listproducts.php
http://testphp.vulnweb.com/login.php
http://testphp.vulnweb.com/logout.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/
http://testphp.vulnweb.com/pictures/
http://testphp.vulnweb.com/pictures/credentials.txt
http://testphp.vulnweb.com/pictures/ipaddresses.txt
http://testphp.vulnweb.com/pictures/wp-config.bak
http://testphp.vulnweb.com/search.php
http://testphp.vulnweb.com/secured/newuser.php
http://testphp.vulnweb.com/secured/office.htm
http://testphp.vulnweb.com/sendcommand.php
http://testphp.vulnweb.com/showimage.php
http://testphp.vulnweb.com/signup.php
http://testphp.vulnweb.com/Templates/
http://testphp.vulnweb.com/wvstests/