Description

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

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.

This document was generated using information provided in "Payment Card Industry Data Security Standard Version 3.2", that can be found at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf.

Scan

<table>
<thead>
<tr>
<th>URL</th>
<th>testphp.vulnweb.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan date</td>
<td>19/06/2019, 09:36:16</td>
</tr>
<tr>
<td>Duration</td>
<td>15 minutes, 24 seconds</td>
</tr>
<tr>
<td>Profile</td>
<td>Full Web and Network Scan</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.

- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. (Requirement 1.2.1)
  **No alerts in this category**

- Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. (Requirement 1.3.4)
  **Total number of alerts in this category: 2**

- Do not disclose private IP addresses and routing information to unauthorized parties (Requirement 1.3.7)
  **Total number of alerts in this category: 3**

- Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network (Requirement 2.1)
  **Total number of alerts in this category: 30**

- Enable only necessary and secure services, protocols, daemons, etc (Requirement 2.2.2)
  **No alerts in this category**

- Configure system security parameters (Requirement 2.2.4)
  **Total number of alerts in this category: 31**

- Remove all unnecessary functionality (Requirement 2.2.5)
  **No alerts in this category**

- Encrypt all non-console administrative access using strong cryptography (Requirement 2.3)
  **No alerts in this category**

- Encrypt transmission of cardholder data across open, public networks (Requirement 4)
  **Total number of alerts in this category: 3**
- Use strong cryptography and security protocols (Requirement 4.1)
  No alerts in this category

- Protect all systems against malware and regularly update anti-virus software or programs (Requirement 5)
  No alerts in this category

- Develop and maintain secure systems and applications (Requirement 6)
  Total number of alerts in this category: 78

- Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches (Requirement 6.2)
  No alerts in this category

- Separate development/test environments from production environments, and enforce the separation with access controls (Requirement 6.4.1)
  Total number of alerts in this category: 8

- Removal of test data and accounts before production systems become active (Requirement 6.4.4)
  Total number of alerts in this category: 9

- Injection flaws (Requirement 6.5.1)
  Total number of alerts in this category: 22

- Buffer overflows (Requirement 6.5.2)
  Total number of alerts in this category: 1

- Insecure cryptographic storage (Requirement 6.5.3)
  No alerts in this category

- Insecure communications (Requirement 6.5.4)
  Total number of alerts in this category: 3

- Improper error handling (Requirement 6.5.5)
  Total number of alerts in this category: 22

- Cross-site scripting (XSS) (Requirement 6.5.7)
  Total number of alerts in this category: 16

- Improper Access Control (Requirement 6.5.8)
  Total number of alerts in this category: 16

- Cross Site Request Forgery (CSRF) (Requirement 6.5.9)
  Total number of alerts in this category: 17

- Broken authentication and session management (Requirement 6.5.10)
  No alerts in this category

- Limit repeated access attempts by locking out the user ID after not more than six attempts (Requirement 8.1.6)
  Total number of alerts in this category: 1

- Using strong cryptography, render all authentication credentials unreadable during transmission and storage (Requirement 8.2.1)
  Total number of alerts in this category: 3
Compliance According to Categories: A Detailed Report

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

(Requirement 1.2.1) Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, thus preventing unfiltered access between untrusted and trusted environments. This prevents malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within the entity's network out to an untrusted server).

Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.

No alerts in this category.

(Requirement 1.3.4) Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

All traffic outbound from the cardholder data environment should be evaluated to ensure that it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications (for example by restricting source/destination addresses/ports, and/or blocking of content).

Total number of alerts in this category: 2

Alerts in this category

Server Side Request Forgery

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.

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://hitM0546cxidr.bxss.me/

---

Server side request forgery

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://hitM0546cxidr.bxss.me/

---

(Requirement 1.3.7) Do not disclose private IP addresses and routing information to unauthorized parties

Restricting the disclosure of internal or private IP addresses is essential to prevent a hacker "learning" the IP addresses of the internal network, and using that information to access the network.

Methods used to meet the intent of this requirement may vary depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.
Total number of alerts in this category: 3

**Alerts in this category**

**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.

| 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/ipaddresses.txt  
| 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-200  
| Affected item | /secured/phpinfo.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.

| 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 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.
(Requirement 2.1) Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network

Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack.

Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.

Total number of alerts in this category: 30

Alerts in this category

<table>
<thead>
<tr>
<th>nginx SPDY heap buffer overflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 &quot;spdy&quot; option of the &quot;listen&quot; directive is used in a configuration file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.1</td>
</tr>
<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: Partial</td>
</tr>
<tr>
<td>Integrity Impact: Partial</td>
</tr>
<tr>
<td>Availability Impact: Partial</td>
</tr>
<tr>
<td>Exploitability: Proof of Concept</td>
</tr>
<tr>
<td>Remediation Level: Official Fix</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>CVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2014-0133</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-122</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server</td>
</tr>
</tbody>
</table>

| Affected parameter |

PHP allow_url_fopen enabled (AcuSensor)

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 | |

**Weak password**

This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

| 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 |
| 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 | |

**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%
```

---

**CVSS2**

- Base Score: 4.3
- Access Vector: Network_accessible
- Access Complexity: Medium
- 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

**CWE**

CWE-20

**Affected item**

/hpp/params.php

**Affected parameter**

p

**Variants**

CWS%07%0E000x%9C=%8D1N%C3%40%10E%DF%AE%8D%BDI%08)%D3%40%1D%A0%A2%05%09%11%89Hi%"%05D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X;IS%8C%FE%CC%9B%F9%FFAA%CB7jq%AF

---

**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.
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 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>
</tbody>
</table>

CWE  
CWE-538

Affected item  
/CVS/

Affected parameter
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.

CWE-538

Affected item /Flash/

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

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-538

Affected item /.idea/

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
### 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.

| 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/  
| 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  
| CWE | CWE-538  
| Affected item | /images/  
| Affected parameter |  

### 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.
| 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**

/_mmServerScripts/

**Affected parameter**

**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.

| 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**

/Mod_Rewrite_Shop/images/

**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.

### 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/
- **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.

### 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

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: /Templates/

Affected parameter

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.

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: /wvstests/

Affected parameter
### 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.

| 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/ |

### .htaccess file readable

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 |

| 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/scripts/ |

| Affected parameter | /wvstests/pmwiki_2_1_19/
### Insecure crossdomain.xml file

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.
**PHP allow_url_fopen enabled**

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.

**PHP errors enabled**

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
/ssured/phpinfo.php

Affected parameter

**PHP errors enabled (AcuSensor)**

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
### PHP open_basedir is not set

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

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.

**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
<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/secured/phpinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

### Cookie(s) without HttpOnly flag set

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.

**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

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>Web Server</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

### Cookie(s) without Secure flag set

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.

**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

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>Web Server</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

### 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.
A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.
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 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.

**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

(Requirement 2.2.2) **Enable only necessary and secure services, protocols, daemons, etc**

Ensures that only the necessary services and protocols are enabled as required for the function of the system.

No alerts in this category.

(Requirement 2.2.4) **Configure system security parameters**

Configure system security parameters to prevent misuse.
Total number of alerts in this category: 31

**Alerts in this category**
- 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>
</table>

| CVE | CVE-2014-0133 |
| CWE | CWE-122 |

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

**PHP allow_url_fopen enabled (AcuSensor)**

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  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</td>
<td></td>
</tr>
</tbody>
</table>

| CWE | CWE-16 |
| Affected item | Web Server |
| Affected parameter | |

**Weak password**

This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.
| 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  |

| 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 |

**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:

```
<object style="height:1px;width:1px;" data="http://victim.com/user/jsonp?callback=CWS%07%0f"
```
| CVSS2 | Base Score: 4.3  
|       | Access Vector: Network accessible  
|       | 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  
| CWE  | CWE-20  
| Affected item | /hpp/params.php  
| Affected parameter | p  
| Variants | CWS%07%0E000x%9C=%8D1N%C3%40%10E%DF%AE%8D%BDl%08)%D3%40%1D%A0%A2%05%09%11%89H%F%05D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X;!S%8C%FE%CC%9B%F9%FF%AA%CB7jq%AF%7F%ED%F2.%F8%01>%9E%18p%C9c%9AI%8B%ACzG%F2%DC%EM%EC%ABdk%1E%AC%2C%9f%A5(%B1%EB%89T%C2j)%93%DBT7%24%9C%8F%CBD6)%A3%0Bx)%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F4b%E8%FA%98%20b.%26%1C%9F5%20h%F1%D1g%0F%14%C1%0Aj%8D%8B0Q%A8L%9B6%D4L%BD.%A8w%7E%9D%7F3/%Dcm{%EF%CB%EF%E6%8Dn-%FB%B3%C3%DD.%E3d1d%EC%C7%3F6%CD0%09  

**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.

| 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 | /admin/  
| 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.

<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

Affected item  
/Connections/

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.

<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>
### 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.

<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></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**  
/CVS/

**Affected parameter**

---

**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.

<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>Availability Requirement: Not_defined</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not_defined</td>
</tr>
<tr>
<td>Integrity Requirement: 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/

Affected parameter

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.

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/scopes/

Affected parameter

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.
<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>
<tr>
<td>CVSS3</td>
<td></td>
</tr>
<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>
<tr>
<td>CWE</td>
<td></td>
</tr>
<tr>
<td>CWE-538</td>
<td></td>
</tr>
</tbody>
</table>

**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.

<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>
<tr>
<td>CVSS3</td>
<td></td>
</tr>
<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>
<tr>
<td>CWE</td>
<td></td>
</tr>
<tr>
<td>CWE-538</td>
<td></td>
</tr>
</tbody>
</table>

**Affected item**

/\_mmServerScripts/

**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.

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

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

**CWE**

CWE-538

**Affected item**

/Mod_Rewrite_Shop/images/

**Affected parameter**
### 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.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CVE-538</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/pictures/</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 | /Templates/ |
| Affected parameter | |

### 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.

<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>
**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.

| 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 | |

| 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 | |
**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/scripts/

**Affected parameter**

.htaccess file readable

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**

Insecure crossdomain.xml file

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.

| 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: 6.5  
Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None  
Scope: Unchanged  
Confidentiality Impact: Low  
Integrity Impact: Low  
Availability Impact: None |

**CWE**

<table>
<thead>
<tr>
<th>CWE-284</th>
</tr>
</thead>
</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

## 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-16

## Affected item

- **/secured/phpinfo.php**

## Affected parameter

**PHP errors enabled**

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.
### PHP errors enabled (AcuSensor)

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.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessable</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: 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-16**

### PHP open_basedir is not set

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.

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessable</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: 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-16

**Affected item**

/secured/phpinfo.php

**Affected parameter**

- PHP session.use_only_cookies disabled

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.

**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: CWE-16

**Affected item**

/secured/phpinfo.php

**Affected parameter**

- Clickjacking: X-Frame-Options header missing

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
### CWE-693

**Affected item**: Web Server

**Affected parameter**: Cookie(s) without HttpOnly flag set

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.

### CWE-16

**Affected item**: Web Server

**Affected parameter**: Cookie(s) without Secure flag set

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.
# CVSS2

<table>
<thead>
<tr>
<th>Base Score</th>
<th>0.0</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>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>

# CWE

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

## 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.

<table>
<thead>
<tr>
<th>Base Score</th>
<th>0.0</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>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>

## Login page password-guessing attack

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.
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 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:

```
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>
<th></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 |  |
| CWE | CWE-16  |
| Affected item | Web Server  |
| Affected parameter |  |

**(Requirement 2.2.5) Remove all unnecessary functionality**

Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

No alerts in this category.

**(Requirement 2.3) Encrypt all non-console administrative access using strong cryptography.**

If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator’s IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data.

Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information.

To be considered "strong cryptography", industry-recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use. (Refer to "strong cryptography" in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms, and industry standards and best practices such as NIST SP 800-52 and SP 800-57, OWASP, etc.)

No alerts in this category.

**(Requirement 4) Encrypt transmission of cardholder data across open, public networks**

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

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  
|       | Exploitation: 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 | Web Server  

| Affected parameter |  

---

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  
|       | Exploitation: 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 |  

---
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 | /signup.php |
| Affected parameter | |

(Requirement 4.1) Use strong cryptography and security protocols

Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

No alerts in this category.

(Requirement 5) Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"-including viruses, worms, and Trojans- enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

No alerts in this category.

(Requirement 6) Develop and maintain secure systems and applications
Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Total number of alerts in this category: 78

### Alerts in this category

#### Macromedia Dreamweaver remote database scripts

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>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>High</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Official_fix</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>

**CVE**

CVE-2004-1893

**CWE**

CWE-16

**Affected item**

**Web Server**

**Affected parameter**

#### Weak password

This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 7.5</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>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: 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>
</tr>
</thead>
<tbody>
<tr>
<td>/userinfo.php</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.

### 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-200 |

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

<table>
<thead>
<tr>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>artist</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
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** | /search.php |

| **Affected parameter** | test |

| **Variants** | THRzWXVGcGj2c3I= |

---

**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** | Accept-Language |

---

**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 | Client-IP  

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

<table>
<thead>
<tr>
<th>Affected item</th>
<th><code>/secured/newuser.php</code></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.

| 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><code>/secured/newuser.php</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td>Origin</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
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

| /secured/newuser.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.

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>
## 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

/secured/newuser.php

### Affected parameter

User-Agent

---

### 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

/secured/newuser.php

### Affected parameter

uuname

### 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**

/secured/newuser.php

**Affected parameter**

Via

---

**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 | 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 | /secured/newuser.php |
| Affected parameter | X-Forwarded-Host |

**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 |
| /showimage.php |
| file |
| acu8522%EF%BC%9Cs1%EF%B9%A5s2%CA%BA3%CA%B9uca8522 |

---

### 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 |
| /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  |

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

**Affected item** /index.zip

**Affected parameter**

---

**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.

| 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** /admin/

**Affected parameter**

---

**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.
### 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.

| 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 | /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-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.

### 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 parameter
/Flash/
<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**

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>/.idea/scopes/</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

**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.

| 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 | /images/  
| Affected parameter |  

### 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.

### 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

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-538

**Affected item**: `/Mod_Rewrite_Shop/images/`

**Affected parameter**: 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.
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

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>/wvstests/</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
| 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/scripts/` |
| 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/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
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 | `/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.

---

| 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.

### 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
- **/guestbook.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:** CWE-200

**Affected item**
- `/listproducts.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:** 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
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  

| 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**

---

**.htaccess file readable**

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.

| CWE            | CWE-16  

**Affected item** `/Mod_Rewrite_Shop/`  

**Affected parameter**
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.

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

**PHP errors enabled**

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.

<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-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/secured/phpinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>
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
| 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 |
| 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.
**WS_FTP log file found**

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.

### 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.

### 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**

/secured/database_connect.php

**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.
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.
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  
|       | Remediaiton Level: Not_defined  
|       | Report Confidence: Not_defined  
|       | 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

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  
|       | Remediaiton Level: Not_defined  
|       | Report 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:</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>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>Web Server</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>/404.php</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.

---

**CWE-200**

**Affected item**

- Web Server

<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>

---

**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  /cart.php  

| 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
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>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
<td>Base Score: 0.0</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: None</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: None</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>

Affected item: /categories.php

CWE: CWE-200

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>
<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>
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.

#### CWE

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

#### 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 |
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.
### 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>
</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 |

<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>/signup.php</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  
/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: 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    |  

**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.
### 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.
**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
### 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**  
`/pictures/path-disclosure-unix.html`

**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**  
`/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 | /Connections/DB_Connection.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 |
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.

<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></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            | /secured/database_connect.php |

Affected parameter       |                            |

(Requirement 6.2) Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches

There is a constant stream of attacks using widely published exploits, often called “zero day” (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. If the most recent patches are not implemented on critical systems as soon as possible, a malicious individual can use these exploits to attack or disable a system, or gain access to sensitive data.

Prioritizing patches for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months.

This requirement applies to applicable patches for all installed software, including payment applications (both those that are PA-DSS validated and those that are not).

No alerts in this category.

(Requirement 6.4.1) Separate development/test environments from production environments, and enforce the separation with access controls
Due to the constantly changing state of development and test environments, they tend to be less secure than the production environment. Without adequate separation between environments, it may be possible for the production environment, and cardholder data, to be compromised due to less-stringent security configurations and possible vulnerabilities in a test or development environment.

Total number of alerts in this category: 8

**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  
| 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 |  

**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**

| Affected item | CWE-538  
|               | Web Server  

**PHPinfo page**

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**

| Affected item | CWE-200  
|               | /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 | |

**WS_FTP log file found**

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 |
<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>/pictures/</td>
</tr>
<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.

<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>

CWE       | CWE-200     |

Affected item | /hpp/test.php |

Affected parameter | |
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

/Mod_Rewrite_Shop/.htaccess

(Requirement 6.4.4) Removal of test data and accounts before production systems become active

Test data and accounts should be removed before the system component becomes active (in production), since these items may give away information about the functioning of the application or system. Possession of such information could facilitate compromise of the system and related cardholder data.

Total number of alerts in this category: 9

Alerts in this category

Weak password

This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

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

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
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

---

**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.
**PHPinfo page**

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

**CWE**
CWE-538

Affected item: **Web Server**

**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 parameter: `/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**

---

**WS_FTP log file found**

**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.

**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 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 | /Mod_Rewrite_Shop/.htaccess |
| Affected parameter |   |
(Requirement 6.5.1) Injection flaws

Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.

Total number of alerts in this category: 22

Alerts in this category

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 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-20</td>
</tr>
<tr>
<td>Affected item</td>
<td>/showimage.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>file</td>
</tr>
<tr>
<td>Variants</td>
<td>showimage.php</td>
</tr>
</tbody>
</table>

Macromedia Dreamweaver remote database scripts

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-2004-1893

**Affected item**: Web Server

**Affected parameter**: SQL injection (verified)

**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>CVE</th>
<th>CVE-2004-1893</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-16</td>
</tr>
<tr>
<td><strong>Affected item</strong></td>
<td><strong>Web Server</strong></td>
</tr>
<tr>
<td><strong>Affected parameter</strong></td>
<td><strong>login</strong></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-16

**Affected item**: Web Server

**Affected parameter**: login

**Variants**: 1ACUSTART"g4WCKACUEND

**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>CVE</th>
<th>CVE-2004-1893</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-16</td>
</tr>
<tr>
<td><strong>Affected item</strong></td>
<td><strong>Web Server</strong></td>
</tr>
<tr>
<td><strong>Affected parameter</strong></td>
<td><strong>login</strong></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-89**

**Affected item**

- `/AJAX/infocateg.php`

**Affected parameter**

- `id`

**Variants**

- `1ACUSTART'"yoMxZACUEND`

---

**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**

- `/AJAX/infotitle.php`

**Affected parameter**

- `id`

**Variants**

- `1ACUSTART'"4tE4KACUEND`

---

**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.

| CVSS2 | Base Score: 6.8  
| CVSS3 | 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"z24toACUEND  

| CVSS2 | Base Score: 6.8  
| CVSS3 | 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  

CWE-89
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 |

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-89</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/guestbook.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td>login</td>
</tr>
<tr>
<td>Variants</td>
<td>1ACUSTART''NdFmvACUEND</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**  
/listproducts.php

**Affected parameter**  
cat

**Variants**  
1ACUSTART"aSMWKACUEND

### 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"ujujigACUEND

### 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 (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 (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/network-attached-storage-dlink/1/

**Affected parameter**

---

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.

<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 |

<table>
<thead>
<tr>
<th><strong>CWE</strong></th>
<th><strong>CWE-89</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Affected item</strong></td>
<td><code>/product.php</code></td>
</tr>
<tr>
<td><strong>Affected parameter</strong></td>
<td><code>login</code></td>
</tr>
<tr>
<td><strong>Variants</strong></td>
<td><code>1ACUSTART&quot;J4lrQACUEND</code></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""yaOoIACUEND

---

#### 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**  
/search.php

**Affected parameter**  
searchFor

**Variants**  
1ACUSTART""8QYc0ACUEND

---

#### 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
<table>
<thead>
<tr>
<th>CWE-89</th>
</tr>
</thead>
</table>

**Affected item**: /search.php

**Affected parameter**: test

**Variants**: 1ACUSTART'"jnFGwACUEND

#### 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

<table>
<thead>
<tr>
<th>CWE-89</th>
</tr>
</thead>
</table>

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

**Affected parameter**: uuname
**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**: pass

**Variants**: 1ACUSTART""wumiPACUEND
### 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

- `uname`

### Variants

- `1ACUSTART"69F6OACUEND`

### 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: CWE-88

### Affected item

- `/hpp/`

### Affected parameter

- `pp`

### Variants

- `12&n985927=v908480`

### (Requirement 6.5.2) Buffer overflows

Buffer overflows occur when an application does not have appropriate bounds checking on its buffer space. This can cause the information in the buffer to be pushed out of the buffer's memory space and into executable memory space. When this occurs, the attacker has the ability to insert malicious code at the end of the buffer and then push that malicious code into executable memory space by overflowing the buffer. The malicious code is then executed and often enables the attacker remote access to the application and/or infected system.
Alerts in this category

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:</td>
<td>5.1</td>
</tr>
<tr>
<td>Access Vector:</td>
<td>Network_accessable</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>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>Proof_of_concept</td>
</tr>
<tr>
<td>Remediation Level:</td>
<td>Official_fix</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>

CVE  CVE-2014-0133
CWE  CWE-122
Affected item  Web Server
Affected parameter

(Requirement 6.5.3) Insecure cryptographic storage

Applications that do not utilize strong cryptographic functions properly to store data are at increased risk of being compromised, and exposing authentication credentials and/or cardholder data. If an attacker is able to exploit weak cryptographic processes, they may be able to gain clear-text access to encrypted data.

No alerts in this category.

(Requirement 6.5.4) Insecure communications

Applications that do not utilize strong cryptographic functions properly to store data are at increased risk of being compromised, and exposing authentication credentials and/or cardholder data. If an attacker is able to exploit weak cryptographic processes, they may be able to gain clear-text access to encrypted data.

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:** Web Server
- **Affected parameter:** 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:** 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

Affected item: /signup.php

(Requirement 6.5.5) Improper error handling

Applications can unintentionally leak information about their configuration or internal workings, or expose privileged information through improper error handling methods. Attackers use this weakness to steal sensitive data or compromise the system altogether. If a malicious individual can create errors that the application does not handle properly, they can gain detailed system information, create denial-of-service interruptions, cause security to fail, or crash the server. For example, the message "incorrect password provided" tells an attacker the user ID provided was accurate and that they should focus their efforts only on the password. Use more generic error messages, like "data could not be verified."

Total number of alerts in this category: 22

Alerts in this category

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

### 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>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td><code>/listproducts.php</code></td>
</tr>
<tr>
<td>Affected parameter</td>
<td>cat</td>
</tr>
<tr>
<td>Variants</td>
<td>12345&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;);</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

---

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td><code>/search.php</code></td>
</tr>
<tr>
<td>Affected parameter</td>
<td>test</td>
</tr>
<tr>
<td>Variants</td>
<td>THRzWXVGcGj2c3I=</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.
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 Client-IP

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.

| CWE            | CWE-CWE-200 |
|               | /secured/newuser.php |
|               | 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**  
Origin

**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
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
/secured/newuser.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:** CWE-200

### Affected item
- `/secured/newuser.php`

### Affected parameter
- `uuname`

### Variants
- `12345"\"\";]]>*%00{%0d%0a<%00>%bf%27\¥\i`
### 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
- **Via**

---

### 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
- **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.
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

- `/showimage.php`

### Affected parameter

- `file`

### Variants

- `acu8522%EF%BC%9Cs1%EF%B9%A5s2%CA%BA%s3%CA%B9uca8522`

---

#### 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>
</tbody>
</table>

### Remediation Level: Not_defined

### Report Confidence: 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

- `/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:** 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:** 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**

#### 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:** 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: 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.

| 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...
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

- **/listproducts.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

<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>
</tr>
</thead>
<tbody>
<tr>
<td>5.0</td>
<td>Network_accessable</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>
</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:** CWE-200

### Affected item

- **/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...
(Requirement 6.5.7) Cross-site scripting (XSS)

XSS flaws occur whenever an application takes user-supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser, which can hijack user sessions, deface web sites, possibly introduce worms, etc.

Total number of alerts in this category: 16

Alerts in this category

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 (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)

**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

/guestbook.php

### Affected parameter

name

### Variants

anonymous user""()&%<acx><ScRiPt >VpLG(9726)</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.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 6.4</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: 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>Exploitability: None</td>
</tr>
<tr>
<td>Availability Requirement: Not defined</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td>Collateral Damage Potential: Not defined</td>
<td>Access Complexity: Low</td>
</tr>
<tr>
<td>Confidentiality Requirement: Not defined</td>
<td>Authentication: None</td>
</tr>
<tr>
<td>Integrity Requirement: Not defined</td>
<td>Availability Requirement: Not defined</td>
</tr>
<tr>
<td>Target Distribution: Not defined</td>
<td>Confidentiality Impact: Partial</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-79</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>valid&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;l0dD(9690)&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>Affected parameter</th>
<th>pp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variants</td>
<td>12&quot;&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;l0dD(9493)&lt;/ScRiPt&gt;</td>
</tr>
</tbody>
</table>

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

/listproducts.php

Affected parameter

artist

Variants

1""()&%<acx><ScRiPt >UdHe(9195)</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</th>
<th>6.4</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>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>

### 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>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                  | CWE-79 |

### Affected item

- /secured/newuser.php

### Affected parameter

- ucc

### Variants

- 4111111111111111"()&%<acx><Script >udoj(9874)</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.
### Remote file inclusion XSS

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.

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Score:</strong> 6.4</td>
<td><strong>Access Vector:</strong> Network_accessible</td>
<td><strong>Access Complexity:</strong> Low</td>
<td><strong>Authentication:</strong> None</td>
<td><strong>Confidentiality Impact:</strong> Partial</td>
<td><strong>Integrity Impact:</strong> Partial</td>
<td><strong>Availability Impact:</strong> None</td>
</tr>
<tr>
<td><strong>Exploitability:</strong> Not_defined</td>
<td><strong>Remediation Level:</strong> Not_defined</td>
<td><strong>Report Confidence:</strong> Not_defined</td>
<td><strong>Availability Requirement:</strong> Not_defined</td>
<td><strong>Collateral Damage Potential:</strong> Not_defined</td>
<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></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>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Score:</strong> 5.3</td>
<td><strong>Attack Vector:</strong> Network</td>
<td><strong>Attack Complexity:</strong> Low</td>
<td><strong>Privileges Required:</strong> None</td>
<td><strong>User Interaction:</strong> None</td>
<td><strong>Scope:</strong> Unchanged</td>
<td><strong>Confidentiality Impact:</strong> None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Integrity Impact:</strong> Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Availability Impact:</strong> None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CWE-79</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Affected item**
/showimage.php

**Affected parameter**
file

**Variants**
Http://bxss.me/t/xss.html?%00
### 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

---

**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.
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  

(Requirement 6.5.8) Improper Access Control

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Consistently enforce access control in presentation layer and business logic for all URLs. Frequently, the only way an application protects sensitive functionality is by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

An attacker may be able to enumerate and navigate the directory structure of a website (directory traversal) thus gaining access to unauthorized information as well as gaining further insight into the workings of the site for later exploitation.
If user interfaces permit access to unauthorized functions, this access could result in unauthorized individuals gaining access to privileged credentials or cardholder data. Only authorized users should be permitted to access direct object references to sensitive resources. Limiting access to data resources will help prevent cardholder data from being presented to unauthorized resources.

Total number of alerts in this category: 16

**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>
</tbody>
</table>

**CWE**

CWE-22

**Affected item**
/showimage.php

**Affected parameter**
file

**Variants**
1ACUSTARTFILE/../xxx/..\..\..\ACUENDFILE
### 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.
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**

- /Connections/

**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.

**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**

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**

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

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>
<th>CWE</th>
<th>Affected item</th>
<th>Affected parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>.idea/</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**
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

**Affected item**

/\images/\n
**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.

<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-538

<table>
<thead>
<tr>
<th>Affected item</th>
<th>/_mmServerScripts/</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

### 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

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

### 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.

### 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/  
| Affected parameter |  

**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.

| 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**

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

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 | `/wvstests/pmwiki_2_1_19/` |
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/scripts/ |

| Affected parameter |

(Requirement 6.5.9) Cross Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then enables the attacker to perform any state-changing operations the victim is authorized to perform (such as updating account details, making purchases, or even authenticating to the application).

Total number of alerts in this category: 17

**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.
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.

**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

---

**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 /artists.php
- Affected parameter
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.
## CWE-352

**Affected item**: /categories.php

**Affected parameter**: HTML form without CSRF protection

### 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

<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**: /comment.php

**Affected parameter**: HTML form without CSRF protection

### 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:** /disclaimer.php
- **Affected parameter:**

---

**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
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

---

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-352</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/guestbook.php</td>
</tr>
<tr>
<td>Affected parameter</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

---

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-352</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/hpp/</td>
</tr>
<tr>
<td>Affected parameter</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-352**

**Affected item**

/\index.php

**Affected parameter**

---

### 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**  
/listproducts.php

**Affected parameter**

---

### 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**

---

### 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.
### 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 | /logout.php  
| Affected parameter |
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>CWE</th>
<th>CWE-352</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/product.php</td>
</tr>
<tr>
<td>Affected parameter</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

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-352</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/search.php</td>
</tr>
<tr>
<td>Affected parameter</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.
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.
(Requirement 6.5.10) Broken authentication and session management

Secure authentication and session management prevents unauthorized individuals from compromising legitimate account credentials, keys, or session tokens that would otherwise enable the intruder to assume the identity of an authorized user.

No alerts in this category.

(Requirement 8.1.6) Limit repeated access attempts by locking out the user ID after not more than six attempts

Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account.

Total number of alerts in this category: 1

Alerts in this category

Login page password-guessing attack

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

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: None
- Integrity Impact: None
- Availability Impact: Low
(Requirement 8.2.1) Using strong cryptography, render all authentication credentials unreadable during transmission and storage

Many network devices and applications transmit unencrypted, readable passwords across the network and/or store passwords without encryption.

A malicious individual can easily intercept unencrypted passwords during transmission using a "sniffer," or directly access unencrypted passwords in files where they are stored, and use this data to gain unauthorized access.

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.

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-307</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>/userinfo.php</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

<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: High</td>
</tr>
<tr>
<td>Remediation Level: Workaround</td>
</tr>
<tr>
<td>Report Confidence: Confirmed</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: 9.1</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: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE | CWE-310 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected item</td>
<td>Web Server</td>
</tr>
<tr>
<td>Affected parameter</td>
<td></td>
</tr>
</tbody>
</table>

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  
| Affected item | `/login.php`  
| 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: 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 | `/signup.php`  
| Affected parameter |   |
Affected Items: A Detailed Report

This section provides full details of the types of vulnerabilities found according to individual affected items.

/AJAX/showxml.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: Requirement 6.5.7

<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>
</table>

/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: Requirement 6.5.7

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
</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: Requirement 6.5.7

| 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 | Variations |

| 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 | Variations |
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: Requirement 6.5.7

<table>
<thead>
<tr>
<th>Parameter</th>
<th>CVSS2</th>
<th>CVSS3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Base Score: 6.4</td>
<td>Base Score: 5.3</td>
</tr>
<tr>
<td></td>
<td>Access Vector: Network_accessible</td>
<td>Attack Vector: Network</td>
</tr>
<tr>
<td></td>
<td>Access Complexity: Low</td>
<td>Attack Complexity: Low</td>
</tr>
<tr>
<td></td>
<td>Authentication: None</td>
<td>Privileges Required: None</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact: Partial</td>
<td>User Interaction: None</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact: Partial</td>
<td>Scope: Unchanged</td>
</tr>
<tr>
<td></td>
<td>Availability Impact: None</td>
<td>Confidentiality Impact: None</td>
</tr>
<tr>
<td></td>
<td>Exploitability: Not_defined</td>
<td>Integrity Impact: Low</td>
</tr>
<tr>
<td></td>
<td>Remediation Level: Not_defined</td>
<td>Availability Impact: None</td>
</tr>
<tr>
<td></td>
<td>Report Confidence: Not_defined</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Availability Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Collateral Damage Potential: Not_defined</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrity Requirement: Not_defined</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Target Distribution: Not_defined</td>
<td></td>
</tr>
</tbody>
</table>

CWE

CWE-79

Parameter

Variations

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: Requirement 6.5.7

<table>
<thead>
<tr>
<th>Parameter</th>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Base Score: 6.4</td>
</tr>
<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>
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: Requirement 6.5.7
### 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**
- Variations

### /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: Requirement 6.5.7
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: Requirement 6.5.7

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>/search.php</td>
<td></td>
</tr>
</tbody>
</table>

**Cross site scripting (verified)**

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score:</td>
<td>6.4</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>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>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>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></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-79</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>/secured/newuser.php</td>
<td></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: Requirement 6.5.7
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: Requirement 6.5.7
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: Requirement 6.5.7

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.4</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>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>

CVSS3

<table>
<thead>
<tr>
<th>Base Score: 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Vector:</td>
</tr>
<tr>
<td>Attack Complexity:</td>
</tr>
<tr>
<td>Privileges Required:</td>
</tr>
<tr>
<td>User Interaction:</td>
</tr>
<tr>
<td>Scope:</td>
</tr>
<tr>
<td>Confidentiality Impact:</td>
</tr>
<tr>
<td>Integrity Impact:</td>
</tr>
<tr>
<td>Availability Impact:</td>
</tr>
</tbody>
</table>

CWE

CWE-79

Parameter

Variations

/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: Requirement 6.5.8

<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>
**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: Requirement 6.5.8*

---

**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: Requirement 6.5.1*
Web Server

Macromedia Dreamweaver remote database scripts

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: Requirement 6, Requirement 6.5.1

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: Requirement 2.1, Requirement 2.2.4, Requirement 6.5.2
### PHP allow_url_fopen enabled (AcuSensor)

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: Requirement 2.1, Requirement 2.2.4*

<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>CVE</th>
<th>CVE-2014-0133</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-122</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
</table>

### /showimage.php

**Remote file inclusion XSS**

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: Requirement 6.5.7*
### Remote file inclusion XSS

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: Requirement 6.5.7*
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: Requirement 1.3.4

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS2</td>
<td></td>
</tr>
<tr>
<td>Base Score: 5.8</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: 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>
<tr>
<td>CVSS3</td>
<td></td>
</tr>
<tr>
<td>Base Score: 9.0</td>
<td></td>
</tr>
<tr>
<td>Attack Vector: Network</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity: High</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: High</td>
<td></td>
</tr>
<tr>
<td>CWE</td>
<td>CWE-918</td>
</tr>
<tr>
<td>Parameter</td>
<td>Variations</td>
</tr>
</tbody>
</table>

Server side request forgery

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: Requirement 1.3.4

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS2</td>
<td></td>
</tr>
<tr>
<td>Base Score: 5.8</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: 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>
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: Requirement 6.5.1

/CASCADE/infocateg.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: Requirement 6.5.1
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

Parameter
Variations

AJAX/infotitle.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: Requirement 6.5.1
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: Requirement 6.5.1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</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 | Variations |
|-----------|------------|

/cart.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: Requirement 6.5.1
| 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  
| Parameter | Variations  

/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: Requirement 6.5.1*
### 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: **Requirement 6.5.1**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS2</td>
<td></td>
</tr>
<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       |                       |
| 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                |

### 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: **Requirement 6.5.1**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS2</td>
<td></td>
</tr>
<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: 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

Parameter

CWE-89

Variations

/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: Requirement 6.5.1

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

Parameter

CWE-89

Variations

/Mod_Rewrite_Shop/Details/color-printer/3/

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: Requirement 6.5.1
### 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:** CWE-89

### Variations

/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/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.

*This alert belongs to the following categories: Requirement 6.5.1*
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.

This alert belongs to the following categories: Requirement 6.5.1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
</table>
| /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/ | 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 |
| 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 | Variations |
| /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: Requirement 6.5.1
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
Parameter
Variations

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: Requirement 6.5.1
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: Requirement 6.5.1

| 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  

| Parameter | Variations  

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: Requirement 6.5.1

| 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  

| Parameter | Variations  

/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: Requirement 6.5.1*

<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>Variations</td>
</tr>
</tbody>
</table>

/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: Requirement 6.5.1*
## 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: Requirement 6.5.1*
This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

This alert belongs to the following categories: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.4.4

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 7.5</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: 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>Base Score: 7.5</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: 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>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Variations</td>
</tr>
</tbody>
</table>

/listproducts.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: Requirement 6, Requirement 6.5.5
### 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

#### Parameter Variations

**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:** Requirement 6, Requirement 6.5.5

---

### 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
/search.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: Requirement 6, Requirement 6.5.5

/secured/newuser.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: Requirement 6, Requirement 6.5.5

| 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      | Variations  

**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: Requirement 6, Requirement 6.5.5
### 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: Requirement 6, Requirement 6.5.5*
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: Requirement 6, Requirement 6.5.5

---

CWE

CWE-200

Parameter

Variations
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: Requirement 6, Requirement 6.5.5
| 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 | Variations |

**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: Requirement 6, Requirement 6.5.5*

| 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 | Variations |

**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...
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: Requirement 6, Requirement 6.5.5
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: Requirement 6, Requirement 6.5.5

/showimage.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: Requirement 6, Requirement 6.5.5

| 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 | Variations |

/\texttt{\textasciitilde\texttt{index.bak}}\texttt{\textasciitilde}

**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: Requirement 6, Requirement 6.4.1, Requirement 6.4.4

| 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 | Variations |
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: Requirement 6, Requirement 6.4.1, Requirement 6.4.4

<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>

CWE
CWE-538

Parameter
Variations

/hpp/params.php

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%07%
```

This alert belongs to the following categories: Requirement 2.1, Requirement 2.2.4
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: Requirement 6.5.7
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: Requirement 6.5.7

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network</td>
<td>Network accessible</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>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>

CWE

CWE-79

Parameter

Variations

/admin/

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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector: Network</td>
<td>Network accessible</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>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: 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 | Variations |

/Connections/

**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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8*

| 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 | Variations |

/CVS/

**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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8*
| 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     | Variations                                           |

**/Flash/**

**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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8*
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
</table>

/**/idea/

**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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8

**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

Variations

/**/idea/scopes/

**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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8
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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8*
/_mmServerScripts/

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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8

<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>

CWE

CWE-538

Parameter

Variations

/Mod_Rewrite_Shop/images/

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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8
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
Variations

/pictures/

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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8
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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>/Templates/</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Directory listing</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>/wvstests/</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Directory listing</strong></td>
<td></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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8

<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-538</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CWE</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Variations</strong></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  
| Parameter     | Variations  

/wvstests/pmwiki_2_1_19/

**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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8*
/wvstests/pmwiki_2_1_19/scripts/

**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: Requirement 2.1, Requirement 2.2.4, Requirement 6, Requirement 6.5.8*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS2</td>
<td></td>
</tr>
<tr>
<td>Base Score: 5.0</td>
<td></td>
</tr>
<tr>
<td>Access Vector: Network_accessable</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>
<tr>
<td>CVSS3</td>
<td></td>
</tr>
<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>
<tr>
<td>CWE</td>
<td></td>
</tr>
<tr>
<td>CWE-538</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Variations</td>
</tr>
</tbody>
</table>

/ 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: Requirement 6, Requirement 6.5.5*
| 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 | Variations |

/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: Requirement 6, Requirement 6.5.5
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>/AJAX/infotitle.php</td>
<td>Error message on page</td>
</tr>
<tr>
<td>/Connections/DB_Connection.php</td>
<td>Error message on page</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.

This alert belongs to the following categories: Requirement 6, Requirement 6.5.5
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: Requirement 6, Requirement 6.5.5

<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

Parameter
Variations

/guestbook.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: Requirement 6, Requirement 6.5.5
| **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 | Variations |

**/listproducts.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: Requirement 6, Requirement 6.5.5*
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

Variations

/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: Requirement 6, Requirement 6.5.5

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

Variations

/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: Requirement 6, Requirement 6.5.5

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Parameter</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>Parameter</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>

CWE | CWE-200

/Mod_Rewrite_Shop/

.htaccess file readable

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: Requirement 2.1, Requirement 2.2.4, Requirement 6

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Parameter</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>
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: Requirement 6.5.9

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

---

**Web Server**

**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: Requirement 6.5.9

| 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  

<table>
<thead>
<tr>
<th>CWE</th>
<th>CWE-352</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Variations</td>
</tr>
</tbody>
</table>

---

**/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: Requirement 6.5.9
/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: Requirement 6.5.9*
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

This alert belongs to the following categories: Requirement 6.5.9
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: Requirement 6.5.9

| 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 | Variations  

/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: Requirement 6.5.9
### 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
- **Variations**

/\**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: Requirement 6.5.9*
### CVSS3

<table>
<thead>
<tr>
<th>Base Score: 4.3</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: Required</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

<table>
<thead>
<tr>
<th>CWE-352</th>
</tr>
</thead>
</table>

### Parameter

<table>
<thead>
<tr>
<th>Variations</th>
</tr>
</thead>
</table>

---

**/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: Requirement 6.5.9*

---

**/hpp/**

**HTML form without CSRF protection**

This alert requires manual confirmation

---

### 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

<table>
<thead>
<tr>
<th>CWE-352</th>
</tr>
</thead>
</table>

### Parameter

<table>
<thead>
<tr>
<th>Variations</th>
</tr>
</thead>
</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: Requirement 6.5.9*

<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 |

| Parameter | Variations |

/index.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: Requirement 6.5.9*
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
Variations

/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: Requirement 6.5.9
**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>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-352</td>
<td></td>
</tr>
</tbody>
</table>

**/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: Requirement 6.5.9*

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-352</td>
<td></td>
</tr>
</tbody>
</table>

**/logout.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: Requirement 6.5.9

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

CWE: CWE-352

/\product.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: Requirement 6.5.9
### 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
- **Variations**

**/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: Requirement 6.5.9*
/signup.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: Requirement 6.5.9

/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: Requirement 6.5.9

<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>Variations</td>
</tr>
</tbody>
</table>

/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: Requirement 6.5.1
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: 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: 9.1</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: High</td>
</tr>
<tr>
<td>Availability Impact: None</td>
</tr>
</tbody>
</table>

CWE

<table>
<thead>
<tr>
<th>CWE-88</th>
</tr>
</thead>
</table>

Parameter

| Variations |

---

**Web Server**

**Insecure crossdomain.xml file**

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.

*This alert belongs to the following categories: Requirement 2.1, Requirement 2.2.4*
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: Requirement 6, Requirement 6.4.1, Requirement 6.4.4

/secured/phpinfo.php

PHP allow_url_fopen enabled
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: Requirement 2.1, Requirement 2.2.4

| 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  
|       | 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 |
| Parameter | Variations |

**PHP errors enabled**

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: Requirement 2.1, Requirement 2.2.4, Requirement 6

| 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
</table>
| **Web Server**

**PHP errors enabled (AcuSensor)**

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: Requirement 2.1, Requirement 2.2.4*

**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: 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
</table>
| **/secured/phpinfo.php**

**PHPinfo page**

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

<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>

### Parameter

<table>
<thead>
<tr>
<th>Variations</th>
</tr>
</thead>
</table>

**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: Requirement 6, Requirement 6.4.1, Requirement 6.4.4
**PHP open_basedir is not set**

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: Requirement 2.1, Requirement 2.2.4*

| 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: 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  

**PHP session.use_only_cookies disabled**

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: Requirement 2.1, Requirement 2.2.4*
| 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 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-16</td>
</tr>
<tr>
<td>Parameter</td>
<td>Variations</td>
</tr>
<tr>
<td>/index.bak</td>
<td>Source code disclosure</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This alert belongs to the following categories: Requirement 6</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                                           |
| Parameter | Variations                                      |
| /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: Requirement 6

| 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 | Variations |

**Web Server**

**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: Requirement 4, Requirement 6.5.4, Requirement 8.2.1

| CVSS2 | Base Score: 5.0  
|       | Access Vector: Network_accessible  
|       | Access Complexity: Low  
|       | Authentication: None  
|       | Confidentiality Impact: Partial  
|       | Integrity Impact: None  
|       | Availability Impact: None  
|       | Exploitability: 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 |
/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: Requirement 4, Requirement 6.5.4, Requirement 8.2.1

CVSS2

| Base Score: 5.0       |
| Access Vector: Network_accessible |
| Access Complexity: Low       |
| Authentication: None         |
| Confidentiality Impact: Partial |
| Integrity Impact: None       |
| Availability Impact: None    |
| Exploitability: 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

Parameter

Variations

/sign up.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: Requirement 4, Requirement 6.5.4, Requirement 8.2.1
### 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>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>

### CVSS3

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</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>

### CWE

- **CWE-310**: Parameter Variations
  - WS_FTP log file found
    - 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: Requirement 6, Requirement 6.4.1, Requirement 6.4.4

### 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>

### CWE

- **CWE-538**: Parameter Variations
  - Web Server
    - Clickjacking: X-Frame-Options header missing
Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

*This alert belongs to the following categories: Requirement 2.2.4*

<table>
<thead>
<tr>
<th>CVSS2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score</td>
<td>4.3</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>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>

| CWE            | CWE-693          |

| Parameter | Variations |

**Cookie(s) without HttpOnly flag set**

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: Requirement 2.1, Requirement 2.2.4*

<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>

| CWE            | CWE-16           |

| Parameter | Variations |

**Cookie(s) without Secure flag set**

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: Requirement 2.1, Requirement 2.2.4

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
</table>

/product.php

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: Requirement 2.1, Requirement 2.2.4

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Variations</th>
</tr>
</thead>
</table>

/userinfo.php

Login page password-guessing attack

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

This alert belongs to the following categories: Requirement 2.1, Requirement 2.2.4, Requirement 8.1.6
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: Requirement 6
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.

This alert belongs to the following categories: Requirement 6

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 0.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessable</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

Parameter

Variations

/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: Requirement 6, Requirement 6.4.1, Requirement 6.4.4

<table>
<thead>
<tr>
<th>CVSS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score: 5.0</td>
</tr>
<tr>
<td>Access Vector: Network_accessable</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

- **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
- **Variations:**

---

**/Mod_Rewrite_Shop/.htaccess**

#### 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: Requirement 6, Requirement 6.4.1, Requirement 6.4.4

### 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
- **Variations:**

---

**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.
**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: Requirement 2.1, Requirement 2.2.4*
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: Requirement 6
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: Requirement 6

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 0.0</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: 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>Base Score: 0.0</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: 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>

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: Requirement 6

<table>
<thead>
<tr>
<th>CVSS2</th>
<th>Base Score: 0.0</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: 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>
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: Requirement 6
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| 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 | Variations |

**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: Requirement 6*
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: Requirement 6

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

/index.bak

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: Requirement 6

<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>

/index.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: Requirement 6

<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>CWE-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Variations</td>
</tr>
</tbody>
</table>
| 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 | Variations  
| /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: Requirement 6
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: Requirement 6
| 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 | Variations |

/product.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: Requirement 6
### /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: Requirement 6

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

**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

### /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.

This alert belongs to the following categories: Requirement 6

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

/ 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: Requirement 6

| 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 |
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: Requirement 6

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

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: Requirement 6
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: Requirement 1.3.7, Requirement 6*
**/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: Requirement 1.3.7, Requirement 6

| 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     | Variations

**/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: Requirement 1.3.7, Requirement 6
### 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**
- **Variations**

/pictures/path-disclosure-unix.html

**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: Requirement 6*
### /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.

*This alert belongs to the following categories: Requirement 6*

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

### /Connections/DB_Connection.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.

*This alert belongs to the following categories: Requirement 6*
| 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     | Variations  

/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: Requirement 6*
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: Requirement 6
Scanned items (coverage report)

176.28.50.16
http://testphp.vulnweb.com/
176.28.50.16:106/tcp
176.28.50.16:110/tcp
176.28.50.16:143/tcp
176.28.50.16:21/tcp
176.28.50.16:22/tcp
176.28.50.16:25/tcp
http://testphp.vulnweb.com/404.php
176.28.50.16:465/tcp
176.28.50.16:53/tcp
176.28.50.16:80/tcp
176.28.50.16:8443/tcp
176.28.50.16:8880/tcp
176.28.50.16:993/tcp
176.28.50.16:995/tcp
http://testphp.vulnweb.com/adm1nPan3l/
http://testphp.vulnweb.com/adm1nPan3l/index.php
http://testphp.vulnweb.com/admin/
http://testphp.vulnweb.com/admin/create.sql
http://testphp.vulnweb.com/AJAX/
http://testphp.vulnweb.com/AJAX/htaccess.conf
http://testphp.vulnweb.com/AJAX/infoartist.php
http://testphp.vulnweb.com/AJAX/infocateg.php
http://testphp.vulnweb.com/AJAX/styles.css
http://testphp.vulnweb.com/bxss/
http://testphp.vulnweb.com/bxss/adminPan3l/
http://testphp.vulnweb.com/bxss/adminPan3l/style.css
http://testphp.vulnweb.com/bxss/cleanDatabase.php
http://testphp.vulnweb.com/bxss/test.js
http://testphp.vulnweb.com/cart.php
http://testphp.vulnweb.com/categories.php
http://testphp.vulnweb.com/clientaccesspolicy.xml
http://testphp.vulnweb.com/comment.php
http://testphp.vulnweb.com/Connections/
http://testphp.vulnweb.com/Connections/DB_Connection.php
http://testphp.vulnweb.com/crossdomain.xml
http://testphp.vulnweb.com/CVS/
http://testphp.vulnweb.com/CVS/Entries
http://testphp.vulnweb.com/CVS/Repository
http://testphp.vulnweb.com/CVS/Root
http://testphp.vulnweb.com/Flash/
http://testphp.vulnweb.com/Flash/add.fla
http://testphp.vulnweb.com/Flash/add.swf
176.28.50.16:general/icmp
176.28.50.16:general/tcp
http://testphp.vulnweb.com/guestbook.php
http://testphp.vulnweb.com/hpp/