

OWASP TOP 10 2017

Compliance Report

14 June 2019

Description

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas - and also provides guidance on where to go from here.

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.

A portion of this report is taken from OWASP's Top Ten 2017 Project document, that can be found at <http://www.owasp.org>.

Scan

URL	http://testphp.vulnweb.com/
Scan date	
Duration	
Profile	

Compliance at a Glance

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

[- Injection\(A1\)](#)

Total number of alerts in this category: 21

[- Broken Authentication\(A2\)](#)

Total number of alerts in this category: 2

[- Sensitive Data Exposure\(A3\)](#)

Total number of alerts in this category: 82

[- XML External Entity \(XXE\)\(A4\)](#)

No alerts in this category

[- Broken Access Control\(A5\)](#)

Total number of alerts in this category: 4

[- Security Misconfiguration\(A6\)](#)

Total number of alerts in this category: 31

[- Cross Site Scripting \(XSS\)\(A7\)](#)

Total number of alerts in this category: 21

[- Insecure Deserialization\(A8\)](#)

No alerts in this category

[- Using Components with Known Vulnerabilities\(A9\)](#)

Total number of alerts in this category: 30

[- Insufficient Logging and Monitoring\(A10\)](#)

No alerts in this category

Compliance According to Categories: A Detailed Report

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

(A1)Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

Total number of alerts in this category: 21

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.

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

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	Web Server
Affected parameter	login
Variants	1ACU\$TART"a0tvIACUEND

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/infocateg.php
Affected parameter	id

Variants	1ACUSTART""VWRwQACUEND
----------	------------------------

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""gGBR9ACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
-------	---

CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	/artists.php
Affected parameter	artist
Variants	1ACUSTART""G8aT2ACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	/cart.php
Affected parameter	login
Variants	1ACUSTART""N2YrdACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	/listproducts.php
Affected parameter	artist
Variants	1ACU\$TART""\$9PpFACUEND

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""w553HACUEND
----------	------------------------

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""xHX49ACUEND

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

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

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

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Affected parameter	

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	/product.php
Affected parameter	login
Variants	1ACU\$TART""itwRBACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
-------	---

CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	/product.php
Affected parameter	pic
Variants	1ACUSTART""LB20dACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	/search.php
Affected parameter	searchFor
Variants	1ACUSTART""jBvuDACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	/search.php
Affected parameter	test
Variants	1ACU\$TART"oxFM8ACUEND

SQL injection (verified)

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	/secured/newuser.php
Affected parameter	uname

Variants	1ACUSTART""IfN0LACUEND
----------	------------------------

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""kgkYFACUEND

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	uname
Variants	1ACU\$TART"xBpKWACUEND

HTTP parameter pollution

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 9.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-88
Affected item	/hpp/index.php
Affected parameter	pp
Variants	12&n988283=v982849

(A2)Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

Total number of alerts in this category: 2

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	

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_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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
CWE	CWE-307
Affected item	/userinfo.php
Affected parameter	

(A3) Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

Total number of alerts in this category: 82

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.

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

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.

CVSS2	Base Score: 5.1 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Proof_of_concept Remediation Level: Official_fix Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVE	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.

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	

Application error message

This alert requires manual confirmation

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

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

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

Application error message

This alert requires manual confirmation

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

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

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

CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	/listproducts.php
Affected parameter	cat
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	uname
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	/showimage.php
Affected parameter	file
Variants	acu6191%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca6191

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	

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 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%89HiP"%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%BEM%EC%ABdkj%1E%AC%2C%9F%A5(%B1%EB%89T%C2Jj)%93"%DBT7%24%9C%8FH%CB6)%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%0A]s%8D%8B0Q%A8L<%9B6%D4L%BD_%A8w%7E%9D[%17%F3/[%DCm{%EF%CB%EF%E6%8D:n-%FB%B3%C3%DD.%E3d1d%EC%C7%3F6%CD0%09

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	

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	

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	/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.

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

CWE	CWE-538
Affected item	/.idea/
Affected parameter	

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.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-538
Affected item	/Mod_Rewrite_Shop/images/
Affected parameter	

Directory listing

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.

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

CWE	CWE-538
Affected item	/wvstests/
Affected parameter	

Directory listing

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

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-538
Affected item	/wvstests/pmwiki_2_1_19/
Affected parameter	

Directory listing

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	

Error message on page

This alert requires manual confirmation

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

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

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

Error message on page

This alert requires manual confirmation

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

Acunetix found an error or warning message that may disclose sensitive information. The message may also

contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

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

Error message on page

This alert requires manual confirmation

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

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

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

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

Error message on page

This alert requires manual confirmation

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

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

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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	/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-200
Affected item	/pictures/path-disclosure-unix.html
Affected parameter	

Error message on page

This alert requires manual confirmation

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

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

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report 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:

```
<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	CWE-284
Affected item	Web Server
Affected parameter	

JetBrains .idea project directory

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

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Affected item	Web Server
Affected parameter	

PHP 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.

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 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	/secured/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
Affected parameter	

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	CWE-200
Affected item	/secured/phpinfo.php
Affected parameter	

PHPinfo page found

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

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

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
CWE	CWE-16
Affected item	/secured/phpinfo.php
Affected parameter	

Source code disclosure

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

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

Source code disclosure

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

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

WS_FTP log file found

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

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

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
CWE	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.

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	

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
CWE	CWE-16
Affected item	Web Server
Affected parameter	

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.

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	/product.php
Affected parameter	

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_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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
CWE	CWE-307
Affected item	/userinfo.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	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-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	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-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.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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	

Possible virtual host found

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.

This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

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

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:

```
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	

Email address found

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

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

Email address found

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

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	/404.php
Affected parameter	

Email address found

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

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

Affected parameter	
--------------------	--

Email address found

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

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

Email address found

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

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

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

Email address found

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

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

Email address found

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

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	/guestbook.php
Affected parameter	

Email address found

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

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

Affected parameter	
--------------------	--

Email address found

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

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

Email address found

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

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

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

Email address found

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

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

Email address found

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

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

Email address found

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

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

Affected parameter	
--------------------	--

Email address found

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

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

Email address found

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

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

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

Email address found

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

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

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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	

Possible internal IP address disclosure

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

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

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

Possible server path disclosure (Unix)

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

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

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

Possible server path disclosure (Unix)

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

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

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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
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/database_connect.php
Affected parameter	

(A4)XML External Entity (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

No alerts in this category.

(A5)Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

Total number of alerts in this category: 4

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.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-22
Affected item	/showimage.php
Affected parameter	file
Variants	1ACUSTARTFILE/../../xxx\..\..\ACUENDFILE

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.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-22
Affected item	/showimage.php
Affected parameter	file
Variants	1ACUSTARTFILE/../../../../xxx\..\.\ACUENDFILE

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.

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
CWE	CWE-693
Affected item	Web Server
Affected parameter	

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_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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
CWE	CWE-307
Affected item	/userinfo.php
Affected parameter	

(A6)Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.

Total number of alerts in this category: 31

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.

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

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.

CVSS2	Base Score: 5.1 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Proof_of_concept Remediation Level: Official_fix Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVE	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.

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:

```
<object style="height:1px;width:1px;" data="http://victim.com/user/jsonp?callback=CWS%07%0E000x%9C=%8D1N%C3%40%10E%DF%AE%8D%BDI%08)%D3%40%1D%A0%A2%05%09%11%89HiP"%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%BEM%EC%ABdkj%1E%AC%2C%9F%A5(%B1%EB%89T%C2jj)%93"%DBT7%24%9C%8FH% 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%0A]s%8D%8B0Q%A8L<%9B6%D4L%BD_%A8w%7E%9D[%17%F3/[%DCm{%EF%CB%EF%E6%8D:n-%FB%B3%C3%DD.%E3d1d%EC%C7%3F6%CD0%09
```

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%89HiP"%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%BEM%EC%ABdkj%1E%AC%2C%9F%A5(%B1%EB%89T%C2jj)%93"%DBT7%24%9C%8FH% 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%0A]s%8D%8B0Q%A8L<%9B6%D4L%BD_%A8w%7E%9D[%17%F3/[%DCm{%EF%CB%EF%E6%8D:n-%FB%B3%C3%DD.%E3d1d%EC%C7%3F6%CD0%09

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	

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	

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	/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.

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

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.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-538
Affected item	/Mod_Rewrite_Shop/images/
Affected parameter	

Directory listing

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.

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

Directory listing

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

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

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-538
Affected item	/wvstests/pmwiki_2_1_19/
Affected parameter	

Directory listing

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	

.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:

```
<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	CWE-284
Affected item	Web Server
Affected parameter	

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.

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 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	/secured/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

Affected parameter

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
-------	---

CWE	CWE-16
Affected item	/secured/phpinfo.php
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.

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	

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
CWE	CWE-16
Affected item	Web Server
Affected parameter	

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.

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	/product.php
Affected parameter	

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_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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
CWE	CWE-307
Affected item	/userinfo.php
Affected parameter	

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:

```
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	

(A7)Cross Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Total number of alerts in this category: 21

Alerts in this category

Cross site scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/404.php
Affected parameter	

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/AJAX/showxml.php
Affected parameter	mycookie

Variants	3'''()&%<acx><ScRiPt >Dr2g(9728)</ScRiPt>
----------	---

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/comment.php
Affected parameter	name
Variants	<your name here>'''()&%<acx><ScRiPt >Fmkf(9116)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
-------	---

CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/guestbook.php
Affected parameter	name
Variants	anonymous user"()&%<acx><ScRiPt >f1ej(9263)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/guestbook.php
Affected parameter	text
Variants	555"()&%<acx><ScRiPt >f1ej(9412)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/hpp/index.php
Affected parameter	pp
Variants	12""()&%<acx><ScRiPt >cmk3(9252)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/hpp/params.php

Affected parameter	p
Variants	valid''()&%<acx><ScRiPt >MMS5(9673)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/hpp/params.php
Affected parameter	pp
Variants	12''()&%<acx><ScRiPt >MMS5(9309)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
-------	---

CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/listproducts.php
Affected parameter	artist
Variants	1'"()&%<acx><ScRiPt >Sire(9566)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/listproducts.php
Affected parameter	cat
Variants	1'"()&%<acx><ScRiPt >zyVC(9500)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/search.php
Affected parameter	searchFor
Variants	query"()&%<acx><ScRiPt >Tyhi(9324)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/secured/newuser.php

Affected parameter	uaddress
Variants	3137 Laguna Street'"()&%<acx><ScRiPt >dsFp(9150)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/secured/newuser.php
Affected parameter	ucc
Variants	4111111111111111'"()&%<acx><ScRiPt >dsFp(9320)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
-------	---

CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/secured/newuser.php
Affected parameter	uemail
Variants	sample@email.tst'')&%<acx><ScRiPt >dsFp(9654)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/secured/newuser.php
Affected parameter	uphone
Variants	555-666-0606'')&%<acx><ScRiPt >dsFp(9775)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/secured/newuser.php
Affected parameter	urname
Variants	UH0dllxh"()&%<acx><ScRiPt >dsFp(9061)</ScRiPt>

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/secured/newuser.php

Affected parameter	uname
Variants	UHOdIIXh'"())&%<acx><ScRiPt >dsFp(9067)</ScRiPt>

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.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/showimage.php
Affected parameter	file
Variants	Http://bxss.me/t/xss.html?%00

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.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/showimage.php
Affected parameter	file
Variants	Http://bxss.me/t/xss.html?%00

Cross site scripting (content-sniffing)

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None

CWE	CWE-79
Affected item	/showimage.php
Affected parameter	file
Variants	./pictures/1.jpg'"()&%<acx><ScRiPt >P8DS(9240)</ScRiPt>

Cross site scripting (content-sniffing)

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	/showimage.php
Affected parameter	file
Variants	./pictures/1.jpg'"()&%<acx><ScRiPt >Fi7k(9890)</ScRiPt>

(A8) Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

No alerts in this category.

(A9) Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses

and enable a range of possible attacks and impacts.

Total number of alerts in this category: 30

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.

CVSS2	Base Score: 5.1 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Proof_of_concept Remediation Level: Official_fix Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVE	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.

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:

```
<object style="height:1px;width:1px;" data="http://victim.com/user/jsonp?callback=CWS%07%0f
```

CVSS2	<p>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</p>
CWE	CWE-20
Affected item	/hpp/params.php
Affected parameter	p
Variants	<p>CWS%07%0E000x%9C=%8D1N%C3%40%10E%DF%AE%8D%BDI%08)%D3%40%1D%A0%A2%05%09%11%89HiP"%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%BEM%EC%ABdkj%1E%AC%2C%9F%A5(%B1%EB%89T%C2jj)%93"%DBT7%24%9C%8FH%CB6)%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%0A]s%8D%8B0Q%A8L<%9B6%D4L%BD_%A8w%7E%9D[%17%F3/[%DCm{%EF%CB%EF%E6%8D:n-%FB%B3%C3%DD.%E3d1d%EC%C7%3F6%CD0%09</p>

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	<p>Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined</p>
CVSS3	<p>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</p>
CWE	CWE-538
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.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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	

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	/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.

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

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

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.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-538
Affected item	/Mod_Rewrite_Shop/images/
Affected parameter	

Directory listing

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.

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

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

Directory listing

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

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-538
Affected item	/wvstests/pmwiki_2_1_19/
Affected parameter	

Directory listing

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	

.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:

```
<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	CWE-284
Affected item	Web Server
Affected parameter	

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.

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 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	/secured/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
Affected parameter	

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
CWE	CWE-16
Affected item	/secured/phpinfo.php
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.

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	

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
CWE	CWE-16
Affected item	Web Server
Affected parameter	

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.

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	/product.php
Affected parameter	

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_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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
CWE	CWE-307
Affected item	/userinfo.php
Affected parameter	

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:

```
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	

(A10)Insufficient Logging and Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

No alerts in this category.

Affected Items: A Detailed Report

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

/404.php

Cross site scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: A7

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

/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: A7

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

/comment.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: A7

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
-----------	------------

/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: A7

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 (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: A7

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

/hpp/index.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: A7

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
-----------	------------

/hpp/params.php

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: A7

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 (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: A7

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: A7

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 (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: A7

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

/search.php

Cross site scripting (verified)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

This alert belongs to the following categories: A7

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

/secured/newuser.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: A7

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 (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: A7

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 (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: A7

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 (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: A7

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 (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: A7

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 (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: A7

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

/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: A5

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-22
Parameter	Variations

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: A5

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
-------	---

CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-22
Parameter	Variations

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: A1, A3, A6

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

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: A3, A6, A9

CVSS2	Base Score: 5.1 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Proof_of_concept Remediation Level: Official_fix Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVE	CVE-2014-0133
CWE	CWE-122
Parameter	Variations

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: A3, A6, A9

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
Parameter	Variations

/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: A7

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

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: A7

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
-----------	------------

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: A1

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/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: A1

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: A1

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
-----------	------------

/artists.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: A1

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: A1

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

/listproducts.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: A1

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: A1

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: A1

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

/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: A1

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

/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: A1

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

/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: A1

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
-----------	------------

/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

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: A1

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

/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: A1

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: A1

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

/search.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: A1

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: A1

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: A1

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

/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: A1

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: A1

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

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.

This alert belongs to the following categories: A2, A3, A6, A9

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
Parameter	Variations

/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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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/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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/index.bak

Backup files

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

This alert belongs to the following categories: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report 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
-----------	------------

/index.zip

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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report 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

/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:

```
<object style="height:1px;width:1px;" data="http://victim.com/user/jsonp?callback=CWS%07%0f
```

This alert belongs to the following categories: A3, A6, A9

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
Parameter	Variations

/showimage.php

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 alert belongs to the following categories: A7

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 (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 alert belongs to the following categories: A7

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

/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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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/

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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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
-----------	------------

/_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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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
-----------	------------

/Templates/

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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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/

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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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/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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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/infotitle.php

Error message on page

This alert requires manual confirmation

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

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

This alert belongs to the following categories: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/Connections/DB_Connection.php

Error message on page

This alert requires manual confirmation

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

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

This alert belongs to the following categories: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report 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
Parameter	Variations

/hpp/index.php

HTTP parameter pollution

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.

This alert belongs to the following categories: A1

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 9.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-88

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:

```
<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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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	CWE-284
Parameter	Variations

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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report 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

/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: A3, A6, A9

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

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: A3, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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
Parameter	Variations

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: A3, A6, A9

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
Parameter	Variations

/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.

This alert belongs to the following categories: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

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: A3, A6, A9

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
Parameter	Variations

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: A3, A6, A9

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
Parameter	Variations

/index.bak

Source code disclosure

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

This alert belongs to the following categories: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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/

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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report 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

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: A3, A5

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
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: A3, A6, A9

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
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: A3, A6, A9

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
Parameter	Variations

/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: A3, A6, A9

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
Parameter	Variations

/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: A2, A3, A5, A6, A9

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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
CWE	CWE-307
Parameter	Variations

/Connections/DB_Connection.php

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: A3

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-538
Parameter	Variations

/secured/database_connect.php

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: A3

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-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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

Web Server

Possible virtual host found

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.

This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

This alert belongs to the following categories: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

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:

```
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: A3, A6, A9

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
Parameter	Variations

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: A3

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

/404.php

Email address found

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

This alert belongs to the following categories: A3

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

/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.

This alert belongs to the following categories: A3

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

/cart.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: A3

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

/categories.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: A3

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: A3

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

/guestbook.php

Email address found

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

This alert belongs to the following categories: A3

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

/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: A3

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

/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: A3

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: A3

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

/login.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: A3

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

/logout.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: A3

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: A3

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

/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: A3

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

/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: A3

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: A3

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

/secured/office.htm

Microsoft Office possible sensitive information

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

This alert belongs to the following categories: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

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: A3

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
Parameter	Variations

/404.php

Possible internal IP address disclosure

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

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

This alert belongs to the following categories: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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/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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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 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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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

/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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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: A3

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined 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/database_connect.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: A3

CVSS2	<p>Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined</p>
CVSS3	<p>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</p>
CWE	CWE-200
Parameter	Variations

Scanned items (coverage report)

<http://testphp.vulnweb.com/>
<http://testphp.vulnweb.com/404.php>
<http://testphp.vulnweb.com/admin/>
<http://testphp.vulnweb.com/AJAX/infoartist.php>
<http://testphp.vulnweb.com/AJAX/infocateg.php>
<http://testphp.vulnweb.com/AJAX/infotitle.php>
<http://testphp.vulnweb.com/AJAX/showxml.php>
<http://testphp.vulnweb.com/artists.php>
<http://testphp.vulnweb.com/cart.php>
<http://testphp.vulnweb.com/categories.php>
<http://testphp.vulnweb.com/comment.php>
<http://testphp.vulnweb.com/Connections/>
http://testphp.vulnweb.com/Connections/DB_Connection.php
<http://testphp.vulnweb.com/CVS/>
<http://testphp.vulnweb.com/disclaimer.php>
<http://testphp.vulnweb.com/Flash/>
<http://testphp.vulnweb.com/guestbook.php>
<http://testphp.vulnweb.com/hpp/index.php>
<http://testphp.vulnweb.com/hpp/params.php>
<http://testphp.vulnweb.com/hpp/test.php>
<http://testphp.vulnweb.com/.idea/>
<http://testphp.vulnweb.com/.idea/scopes/>
<http://testphp.vulnweb.com/images/>
<http://testphp.vulnweb.com/index.bak>
<http://testphp.vulnweb.com/index.php>
<http://testphp.vulnweb.com/index.zip>
<http://testphp.vulnweb.com/listproducts.php>
<http://testphp.vulnweb.com/login.php>
<http://testphp.vulnweb.com/logout.php>
http://testphp.vulnweb.com/_mmServerScripts/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess
http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/
<http://testphp.vulnweb.com/pictures/>
<http://testphp.vulnweb.com/pictures/credentials.txt>
<http://testphp.vulnweb.com/pictures/ipaddresses.txt>
<http://testphp.vulnweb.com/pictures/path-disclosure-unix.html>
<http://testphp.vulnweb.com/pictures/wp-config.bak>
<http://testphp.vulnweb.com/product.php>
<http://testphp.vulnweb.com/search.php>
http://testphp.vulnweb.com/secured/database_connect.php
<http://testphp.vulnweb.com/secured/newuser.php>
<http://testphp.vulnweb.com/secured/office.htm>
<http://testphp.vulnweb.com/secured/phpinfo.php>
<http://testphp.vulnweb.com/showimage.php>
<http://testphp.vulnweb.com/signup.php>
<http://testphp.vulnweb.com/Templates/>
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
<http://testphp.vulnweb.com/userinfo.php>
<http://testphp.vulnweb.com/wvstests/>
http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/
http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/