acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

13 December, 2016

OWASP TOP 10 2013

~ compliance report ~

Generated by Acunetix WVS Reporter (v10.5 Build 20160520)

OWASP TOP 10 2013

compliance report

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 2013 Project document, that can be found at http://www.owasp.org.

Scan

URL	**http://testphp.vulnweb.com:80/**
Scan date	12/13/2016 6:36:48 PM
Duration	1 hours, 19 minutes
Profile	Default

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: 75
- Broken Authentication and Session Management (A2)
  No alerts in this category
- Cross Site Scripting (XSS) (A3)
  Total number of alerts in this category: 38
- Insecure Direct Object Reference (A4)
  Total number of alerts in this category: 2
- Security Misconfiguration (A5)
  Total number of alerts in this category: 35
- Sensitive Data Exposure (A6)
  Total number of alerts in this category: 101
- Missing Function Level Access Control (A7)
  Total number of alerts in this category: 1
- Cross Site Request Forgery (CSRF) (A8)
  Total number of alerts in this category: 6
- Using Components with Known Vulnerabilities (A9)
  Total number of alerts in this category: 35
- UnvalidatedRedirects and Forwards (A10)

Total number of alerts in this category: 1

Compliance According to Categories: A Detailed Report

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

(A1) Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to 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: 75

Alerts in this category

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CVSS3	Base Score: 10 - Attack 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	**/**
Affected parameter	login
Variants	1

Affected item	**/AJAX/infoartist.php**
Affected parameter	id
Variants	1

Affected item	**/AJAX/infocateg.php**
Affected parameter	id
Variants	1

Affected item	**/AJAX/infotitle.php**
Affected parameter	id
Variants	1

Affected item	**/artists.php**
Affected parameter	artist
Variants	1
Affected item	**/artists.php**
Affected parameter	login

Variants	1

Affected item	**/cart.php**
Affected parameter	addcart
Variants	2
Affected item	**/cart.php**
Affected parameter	login
Variants	1

Affected item	**/guestbook.php**
Affected parameter	login
Variants	1

Affected item	**/listproducts.php**
Affected parameter	artist
Variants	1
Affected item	**/listproducts.php**
Affected parameter	cat
Variants	2
Affected item	**/listproducts.php**
Affected parameter	login
Variants	1

Affected item	**/Mod_Rewrite_Shop/buy.php**
Affected parameter	id
Variants	1

Affected item	**/Mod_Rewrite_Shop/details.php**
Affected parameter	id
Variants	1

Affected item	**/Mod_Rewrite_Shop/rate.php**
Affected parameter	id
Variants	1

Affected item	**/product.php**
Affected parameter	login
Variants	1
Affected item	**/product.php**
Affected parameter	pic
Variants	1

Affected item	**/search.php**
Affected parameter	login
Variants	1
Affected item	**/search.php**
Affected parameter	searchFor
Variants	2
Affected item	**/search.php**
Affected parameter	test
Variants	2

Affected item	**/secured/newuser.php**
Affected parameter	uuname
Variants	1

Affected item	**/sendcommand.php**
Affected parameter	cart_id
Variants	1

Affected item	**/userinfo.php**
Affected parameter	login
Variants	1
Affected item	**/userinfo.php**
Affected parameter	uaddress
Variants	2
Affected item	**/userinfo.php**
Affected parameter	ucc
Variants	2
Affected item	**/userinfo.php**
Affected parameter	uname
Variants	1
Affected item	**/userinfo.php**
Affected parameter	uphone
Variants	1
Affected item	**/userinfo.php**
Affected parameter	urname
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16
CVE	CVE-2004-1893

Affected item	**/**
Affected parameter	
Variants	1

SQL injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CVSS3	Base Score: 10 - Attack 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	/
Affected parameter	login
Variants	1

Affected item	**/cart.php**
Affected parameter	addcart
Variants	2
Affected item	**/cart.php**
Affected parameter	login
Variants	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CVSS3	Base Score: 10 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Changed - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
CWE	CWE-89

Affected item	**/AJAX/infoartist.php**
Affected parameter	id
Variants	1

Affected item	**/AJAX/infocateg.php**
Affected parameter	id
Variants	1

Affected item	**/AJAX/infotitle.php**
Affected parameter	id
Variants	1

Affected item	**/artists.php**
Affected parameter	artist
Variants	1

Affected item	**/artists.php**
Affected parameter	login
Variants	1

Affected item	**/guestbook.php**
Affected parameter	login
Variants	1

Affected item	**/listproducts.php**
Affected parameter	artist
Variants	1
Affected item	**/listproducts.php**
Affected parameter	cat
Variants	2
Affected item	**/listproducts.php**
Affected parameter	login
Variants	1

Affected item	**/Mod_Rewrite_Shop/buy.php**
Affected parameter	id
Variants	1

Affected item	**/Mod_Rewrite_Shop/details.php**
Affected parameter	id
Variants	1

Affected item	**/Mod_Rewrite_Shop/rate.php**
Affected parameter	id
Variants	1

Affected item	**/product.php**
Affected parameter	login
Variants	1
Affected item	**/product.php**
Affected parameter	pic
Variants	1

Affected item	**/search.php**
Affected parameter	login
Variants	1
Affected item	**/search.php**
Affected parameter	searchFor
Variants	2
Affected item	**/search.php**
Affected parameter	test
Variants	2

Affected item	**/secured/newuser.php**
Affected parameter	uuname
Variants	1

Affected item	**/sendcommand.php**
Affected parameter	cart_id
Variants	2

Affected item	**/userinfo.php**
Affected parameter	login
Variants	1
Affected item	**/userinfo.php**
Affected parameter	pass

Variants	1
Affected item	**/userinfo.php**
Affected parameter	uaddress
Variants	2
Affected item	**/userinfo.php**
Affected parameter	ucc
Variants	2
Affected item	**/userinfo.php**
Affected parameter	uemail
Variants	2
Affected item	**/userinfo.php**
Affected parameter	uname
Variants	1
Affected item	**/userinfo.php**
Affected parameter	uphone
Variants	2
Affected item	**/userinfo.php**
Affected parameter	urname
Variants	2

(A2) Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

No alerts in this category.

(A3) Cross Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. 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: 38

Alerts in this category

Cross site scripting

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.

CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
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	2

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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.

CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
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	
Variants	1

Affected item	**/AJAX/showxml.php**
Affected parameter	mycookie
Variants	1

Affected item	**/comment.php**
Affected parameter	name
Variants	1

Affected item	**/guestbook.php**
Affected parameter	name
Variants	2

Affected item	**/guestbook.php**
Affected parameter	text
Variants	2

Affected item	**/hpp/**
Affected parameter	pp
Variants	1

Affected item	**/hpp/index.php**
Affected parameter	pp
Variants	1

Affected item	**/hpp/params.php**

Affected parameter	p
Variants	2

Affected item	**/hpp/params.php**
Affected parameter	pp
Variants	2

Affected item	**/listproducts.php**
Affected parameter	artist
Variants	1

Affected item	**/listproducts.php**
Affected parameter	cat
Variants	2

Affected item	**/search.php**
Affected parameter	searchFor
Variants	2

Affected item	**/secured/newuser.php**
Affected parameter	uaddress
Variants	1

Affected item	**/secured/newuser.php**
Affected parameter	ucc
Variants	1

Affected item	**/secured/newuser.php**
Affected parameter	uemail
Variants	1

Affected item	**/secured/newuser.php**
Affected parameter	uphone
Variants	1

Affected item	**/secured/newuser.php**
Affected parameter	urname
Variants	1

Affected item	**/secured/newuser.php**
Affected parameter	uuname
Variants	1

Affected item	**/userinfo.php**
Affected parameter	uaddress
Variants	2

Affected item	**/userinfo.php**
Affected parameter	ucc
Variants	2

Affected item	**/userinfo.php**
Affected parameter	uemail
Variants	2

Affected item	**/userinfo.php**
Affected parameter	uphone
Variants	2

Affected item	**/userinfo.php**
Affected parameter	urname
Variants	2

Cross site scripting (content-sniffing)

This type of XSS can only be triggered on (and affects) content sniffing browsers.
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.

CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
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	2

(A4) Insecure Direct Object Reference

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

Total number of alerts in this category: 2

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 execute commands outside of the web server's root directory.

CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
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	2

(A5) Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

Total number of alerts in this category: 35

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.

CVSS	Base Score: 5.1 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-122
CVE	CVE-2014-0133

Affected item	**Web Server**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**Web Server**
Affected parameter	
Variants	1

.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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/Mod_Rewrite_Shop**
Affected parameter	
Variants	1

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%3D%8D1N%C3%40%10E%DF%AE%8D%BDI%08%29%D3%40%1D%A0%A2%05%09%11%89HiP%22%05D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X%3B%21S%8C%FE%CC%9B%F9%FF%AA%CB7Jq%AF%7F%ED%F2%2E%F8%01%3E%9E%18p%C9c%9Al%8B%ACzG%F2%DC%BEM%EC%ABdkj%1E%AC%2C%9F%A5%28%B1%EB%89T%C2Jj%29%93%22%DBT7%24%9C%8FH%CBD6%29%A3%0Bx%29%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F4b%E8%FA%98%20b%5F%26%1C%9F5%20h%F1%D1g%0F%14%C1%0A%5Ds%8D%8B0Q%A8L%3C%9B6%D4L%BD%5F%A8w%7E%9D%5B%17%F3%2F%5B%DCm%7B%EF%CB%EF%E6%8D%3An%2D%FB%B3%C3%DD%2E%E3d1d%EC%C7%3F6%CD0%09" type="application/x-shockwave-flash" allowscriptaccess="always"
flashvars="c=alert&u=http://victim.com/secret_file.txt"></object>

CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-20

Affected item	**/hpp/params.php**
Affected parameter	p
Variants	2

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected item	**/.idea**
Affected parameter	
Variants	1

Affected item	**/.idea/scopes**
Affected parameter	
Variants	1

Affected item	**/_mmServerScripts**
Affected parameter	
Variants	1

Affected item	**/admin**
Affected parameter	
Variants	1

Affected item	**/Connections**
Affected parameter	
Variants	1

Affected item	**/CVS**
Affected parameter	
Variants	1

Affected item	**/Flash**
Affected parameter	
Variants	1

Affected item	**/images**
Affected parameter	
Variants	1

Affected item	**/Mod_Rewrite_Shop/images**
Affected parameter	
Variants	1

Affected item	**/pictures**
Affected parameter	
Variants	1

Affected item	**/Templates**
Affected parameter	
Variants	1

Affected item	**/wvstests**
Affected parameter	
Variants	1

Affected item	**/wvstests/pmwiki_2_1_19**
Affected parameter	
Variants	1

Affected item	**/wvstests/pmwiki_2_1_19/scripts**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
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	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
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	
Variants	1

PHP errors enabled

The display_errors directive determines whether error messages should be sent to the browser. These messages frequently contain sensitive information about your web application environment, and should never be presented to untrusted sources.

display_errors is on by default.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/secured/phpinfo.php**
Affected parameter	
Variants	1

Affected item	**Web Server**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
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	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/secured/phpinfo.php**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/**
Affected parameter	
Variants	1

Hidden form input named price was found

A hidden form input named price was found. It's not recommended to hide sensitive information in hidden form fields.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/product.php (68db51598a6b1e726aa518e093bbd4ff)**
Affected parameter	
Variants	1

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/medias/css/main.css**
Affected parameter	
Variants	1

Affected item	**/medias/js/common_functions.js**
Affected parameter	
Variants	1

Affected item	**/Mod_Rewrite_Shop/Details/color-printer/3**
Affected parameter	
Variants	1

Affected item	**/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1**
Affected parameter	
Variants	1

Affected item	**/Mod_Rewrite_Shop/Details/web-camera-a4tech/2**
Affected parameter	
Variants	1

Affected item	**/privacy.php**
Affected parameter	
Variants	1

Affected item	**/secured/office_files/filelist.xml**
Affected parameter	
Variants	1

Affected item	**/Templates/logout.php**
Affected parameter	
Variants	1

(A6) Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

Total number of alerts in this category: 101

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16
CVE	CVE-2004-1893

Affected item	*/*
Affected parameter	
Variants	1

nginx SPDY heap buffer overflow

A heap-based buffer overflow in the SPDY implementation in nginx 1.3.15 before 1.4.7 and 1.5.x before 1.5.12 allows remote attackers to execute arbitrary code via a crafted request. The problem affects nginx compiled with the ngx_http_spdy_module module (which is not compiled by default) and without --with-debug configure option, if the "spdy" option of the "listen" directive is used in a configuration file.

CVSS	Base Score: 5.1 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-122
CVE	CVE-2014-0133

Affected item	**Web Server**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**Web Server**
Affected parameter	
Variants	1

Script source code disclosure

It is possible to read the source code of this script by using script filename as a parameter. It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected item	**/showimage.php**
Affected parameter	file
Variants	1

.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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/Mod_Rewrite_Shop**
Affected parameter	
Variants	2

Application error message

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/listproducts.php**
Affected parameter	artist
Variants	1
Affected item	**/listproducts.php**
Affected parameter	cat
Variants	2

Affected item	**/secured/newuser.php**
Affected parameter	uuname
Variants	1

Affected item	**/showimage.php**
Affected parameter	file
Variants	2

Affected item	**/userinfo.php**
Affected parameter	uaddress
Variants	2
Affected item	**/userinfo.php**
Affected parameter	ucc
Variants	2
Affected item	**/userinfo.php**
Affected parameter	uemail
Variants	2
Affected item	**/userinfo.php**
Affected parameter	uphone
Variants	2
Affected item	**/userinfo.php**
Affected parameter	urname
Variants	2

Backup files

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

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected item	**/index.bak**
Affected parameter	
Variants	1

Affected item	**/index.zip**
Affected parameter	
Variants	1

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%3D%8D1N%C3%40%10E%DF%AE%8D%BDI%08%29%D3%40%1D%A0%A2%05%09%11%89HiP%22%05D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X%3B%21S%8C%FE%CC%9B%F9%FF%AA%CB7Jq%AF%7F%ED%F2%2E%F8%01%3E%9E%18p%C9c%9AI%8B%ACzG%F2%DC%BEM%EC%ABdkj%1E%AC%2C%9F%A5%28%B1%EB%89T%C2Jj%29%93%22%DBT7%24%9C%8FH%CBD6%29%A3%0Bx%29%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F4b%E8%FA%98%20b%5F%26%1C%9F5%20h%F1%D1g%0F%14%C1%0A%5Ds%8D%8B0Q%A8L%3C%9B6%D4L%BD%5F%A8w%7E%9D%5B%17%F3%2F%5B%DCm%7B%EF%CB%EF%E6%8D%3An%2D%FB%B3%C3%DD%2E%E3d1d%EC%C7%3F6%CD0%09" type="application/x-shockwave-flash" allowscriptaccess="always"
flashvars="c=alert&u=http://victim.com/secret_file.txt"></object>

CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-20

Affected item	**/hpp/params.php**
Affected parameter	p
Variants	2

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected item	**/.idea**
Affected parameter	
Variants	2

Affected item	**/.idea/scopes**
Affected parameter	
Variants	2

Affected item	**/_mmServerScripts**
Affected parameter	
Variants	2

Affected item	**/admin**
Affected parameter	
Variants	2

Affected item	**/Connections**
Affected parameter	
Variants	2

Affected item	**/CVS**
Affected parameter	
Variants	2

Affected item	**/Flash**
Affected parameter	
Variants	2

Affected item	**/images**
Affected parameter	
Variants	2

Affected item	**/Mod_Rewrite_Shop/images**
Affected parameter	
Variants	2

Affected item	**/pictures**
Affected parameter	
Variants	2

Affected item	**/Templates**
Affected parameter	
Variants	2

Affected item	**/wvstests**
Affected parameter	
Variants	2

Affected item	**/wvstests/pmwiki_2_1_19**
Affected parameter	
Variants	2

Affected item	**/wvstests/pmwiki_2_1_19/scripts**
Affected parameter	
Variants	2

Error message on page

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/AJAX/infoartist.php**
Affected parameter	
Variants	1

Affected item	**/AJAX/infocateg.php**
Affected parameter	
Variants	1

Affected item	**/AJAX/infotitle.php**
Affected parameter	
Variants	1

Affected item	**/Connections/DB_Connection.php**
Affected parameter	
Variants	1

Affected item	**/pictures/path-disclosure-unix.html**
Affected parameter	
Variants	1

Affected item	**/secured/database_connect.php**

Affected parameter	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
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	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected item	/
Affected parameter	

Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
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	
Variants	1

PHP errors enabled

The display_errors directive determines whether error messages should be sent to the browser. These messages frequently contain sensitive information about your web application environment, and should never be presented to untrusted sources.

display_errors is on by default.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/secured/phpinfo.php**
Affected parameter	
Variants	2

Affected item	**Web Server**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
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	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/secured/phpinfo.php**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/secured/phpinfo.php**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/secured/phpinfo.php**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected item	**/index.bak**
Affected parameter	
Variants	1

Affected item	**/pictures/wp-config.bak**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected item	**/pictures//WS_FTP.LOG**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial

CWE	CWE-693

Affected item	**Web Server**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/**
Affected parameter	
Variants	1

Hidden form input named price was found

A hidden form input named price was found. It's not recommended to hide sensitive information in hidden form fields.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/product.php (68db51598a6b1e726aa518e093bbd4ff)**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected item	**/Connections/DB_Connection.php**
Affected parameter	
Variants	1

Affected item	**/secured/database_connect.php**

Affected parameter	
Variants	1

Possible sensitive directories

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

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/admin**
Affected parameter	
Variants	1

Affected item	**/CVS**
Affected parameter	
Variants	1

Affected item	**/secured**
Affected parameter	
Variants	1

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/medias/css/main.css**
Affected parameter	
Variants	1

Affected item	**/medias/js/common_functions.js**
Affected parameter	
Variants	1

Affected item	**/Mod_Rewrite_Shop/Details/color-printer/3**
Affected parameter	

Variants	1

Affected item	**/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1**
Affected parameter	
Variants	1

Affected item	**/Mod_Rewrite_Shop/Details/web-camera-a4tech/2**
Affected parameter	
Variants	1

Affected item	**/privacy.php**
Affected parameter	
Variants	1

Affected item	**/secured/office_files/filelist.xml**
Affected parameter	
Variants	1

Affected item	**/Templates/logout.php**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/**
Affected parameter	
Variants	1

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.

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

CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/secured/office.htm**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/login.php**
Affected parameter	
Variants	2

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None

	- User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/404.php**
Affected parameter	
Variants	1

Affected item	**/pictures/ipaddresses.txt**
Affected parameter	
Variants	1

Affected item	**/secured/phpinfo.php**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/pictures/path-disclosure-unix.html**
Affected parameter	
Variants	1

Affected item	**/secured/phpinfo.php**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**/Connections/DB_Connection.php**
Affected parameter	
Variants	1

Affected item	**/pictures/credentials.txt**
Affected parameter	
Variants	1

Affected item	**/secured/database_connect.php**
Affected parameter	
Variants	1

(A7) Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

Total number of alerts in this category: 1

Alerts in this category

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.

CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-693

Affected item	**Web Server**
Affected parameter	
Variants	1

(A8) Cross Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Total number of alerts in this category: 6

Alerts in this category

HTML form without CSRF protection

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 4.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: Required - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None
CWE	CWE-352

Affected item	**/**
Affected parameter	Unnamed Form
Variants	1

Affected item	**/comment.php (7aae61e4ef757b75f29861b71d32976e)**
Affected parameter	fComment
Variants	1

Affected item	**/hpp (fbc1d56ba0737d3fa577aa5a19c9fd49)**
Affected parameter	Unnamed Form
Variants	1

Affected item	**/signup.php**
Affected parameter	form1
Variants	1

Affected item	**/userinfo.php (9d1db3f4d16732c9716e14a3e959fa2d)**
Affected parameter	form1
Variants	1

Possible CSRF (Cross-site request forgery)

Manual confirmation is required for this alert.
This script is possibly vulnerable to cross-site request forgery. Cross Site Reference Forgery (CSRF/XSRF) is a class of attack that affects web based applications with a predictable structure for invocation. An attacker tricks the user into performing an action of the attackers choosing by directing the victim's actions on the target application with a link or other content.
The attack works by including a link or script in a page that accesses a site to which the user is known (or is supposed) to have authenticated. Here is an example:
<img src="http://bank.example/withdraw?from=victim&amount=1000000&to=attacker">
If the bank keeps authentication information in a cookie, and if the cookie hasn't expired, then victim's browser's attempt to load the image will submit the withdrawal form with his cookie.

This vulnerability is also known by several other names including Session Riding and One-Click Attack.

Affected item	**/AJAX/infotitle.php**
Affected parameter	
Variants	1

(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: 35

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.

CVSS	Base Score: 5.1 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-122
CVE	CVE-2014-0133

Affected item	**Web Server**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None

CWE	CWE-16

Affected item	**Web Server**
Affected parameter	
Variants	1

.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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/Mod_Rewrite_Shop**
Affected parameter	
Variants	1

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%3D%8D1N%C3%40%10E%DF%AE%8D%BDI%08%29%D3%40%1D%A0%A2%05%09%11%89HiP%22%05D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X%3B%21S%8C%FE%CC%9B%F9%FF%AA%CB7Jq%AF%7F%ED%F2%2E%F8%01%3E%9E%18p%C9c%9AI%8B%ACzG%F2%DC%BEM%EC%ABdkj%1E%AC%2C%9F%A5%28%B1%EB%89T%C2Jj%29%93%22%DBT7%24%9C%8FH%CBD6%29%A3%0Bx%29%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F4b%E8%FA%98%20b%5F%26%1C%9F5%20h%F1%D1g%0F%14%C1%0A%5Ds%8D%8B0Q%A8L%3C%9B6%D4L%BD%5F%A8w%7E%9D%5B%17%F3%2F%5B%DCm%7B%EF%CB%EF%E6%8D%3An%2D%FB%B3%C3%DD%2E%E3d1d%EC%C7%3F6%CD0%09" type="application/x-shockwave-flash" allowscriptaccess="always"
flashvars="c=alert&u=http://victim.com/secret_file.txt"></object>

CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None

CWE	CWE-20

Affected item	**/hpp/params.php**
Affected parameter	p
Variants	2

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-538

Affected item	**/.idea**
Affected parameter	
Variants	1

Affected item	**/.idea/scopes**
Affected parameter	
Variants	1

Affected item	**/_mmServerScripts**
Affected parameter	
Variants	1

Affected item	**/admin**
Affected parameter	
Variants	1

Affected item	**/Connections**
Affected parameter	
Variants	1

Affected item	**/CVS**
Affected parameter	
Variants	1

Affected item	**/Flash**
Affected parameter	
Variants	1

Affected item	**/images**
Affected parameter	
Variants	1

Affected item	**/Mod_Rewrite_Shop/images**
Affected parameter	

Variants	1

Affected item	**/pictures**
Affected parameter	
Variants	1

Affected item	**/Templates**
Affected parameter	
Variants	1

Affected item	**/wvstests**
Affected parameter	
Variants	1

Affected item	**/wvstests/pmwiki_2_1_19**
Affected parameter	
Variants	1

Affected item	**/wvstests/pmwiki_2_1_19/scripts**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
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	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
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	
Variants	1

PHP errors enabled

The display_errors directive determines whether error messages should be sent to the browser. These messages frequently contain sensitive information about your web application environment, and should never be presented to untrusted sources.

display_errors is on by default.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/secured/phpinfo.php**
Affected parameter	
Variants	1

Affected item	**Web Server**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
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	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/secured/phpinfo.php**
Affected parameter	
Variants	1

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.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/**
Affected parameter	
Variants	1

Hidden form input named price was found

A hidden form input named price was found. It's not recommended to hide sensitive information in hidden form fields.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/product.php (68db51598a6b1e726aa518e093bbd4ff)**
Affected parameter	
Variants	1

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**/medias/css/main.css**
Affected parameter	
Variants	1

Affected item	**/medias/js/common_functions.js**
Affected parameter	
Variants	1

Affected item	**/Mod_Rewrite_Shop/Details/color-printer/3**
Affected parameter	
Variants	1

Affected item	**/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1**
Affected parameter	
Variants	1

Affected item	**/Mod_Rewrite_Shop/Details/web-camera-a4tech/2**
Affected parameter	
Variants	1

Affected item	**/privacy.php**
Affected parameter	
Variants	1

Affected item	**/secured/office_files/filelist.xml**
Affected parameter	
Variants	1

Affected item	**/Templates/logout.php**
Affected parameter	
Variants	1

(A10) UnvalidatedRedirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Total number of alerts in this category: 1

Alerts in this category

URL redirection

This script is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 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-601

Affected item	**/redir.php**
Affected parameter	r
Variants	1

Affected Items: A Detailed Report

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

/

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
login	1

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, A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

CVE CVE-2004-1893

Parameter	Variations
	1

SQL injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
login	1

HTML form without CSRF protection

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

This alert belongs to the following categories: A8

CVSS Base Score: 2.6

- Access Vector: Network
- Access Complexity: High
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-352

Parameter	Variations
Unnamed Form	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

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: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/.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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/.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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/_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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/404.php

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

Possible sensitive directories

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

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/AJAX/infoartist.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

Error message on page

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/AJAX/infocateg.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

Error message on page

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/AJAX/infotitle.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

Error message on page

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

Possible CSRF (Cross-site request forgery)

Manual confirmation is required for this alert.
This script is possibly vulnerable to cross-site request forgery. Cross Site Reference Forgery (CSRF/XSRF) is a class of attack that affects web based applications with a predictable structure for invocation. An attacker tricks the user into performing an action of the attackers choosing by directing the victim's actions on the target application with a link or other content.
The attack works by including a link or script in a page that accesses a site to which the user is known (or is supposed) to have authenticated. Here is an example:
<img src="http://bank.example/withdraw?from=victim&amount=1000000&to=attacker">
If the bank keeps authentication information in a cookie, and if the cookie hasn't expired, then victim's browser's attempt to load the image will submit the withdrawal form with his cookie.

This vulnerability is also known by several other names including Session Riding and One-Click Attack.

This alert belongs to the following categories: A8

Parameter	Variations
	1

/AJAX/showxml.php

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
mycookie	1

/artists.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
artist	1
login	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
artist	1
login	1

/cart.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
addcart	2
login	1

SQL injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
addcart	2
login	1

/comment.php

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
name	1

/comment.php (7aae61e4ef757b75f29861b71d32976e)

HTML form without CSRF protection

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

This alert belongs to the following categories: A8

CVSS Base Score: 2.6

- Access Vector: Network
- Access Complexity: High
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-352

Parameter	Variations
fComment	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/Connections/DB_Connection.php

Error message on page

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

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: A6

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

Possible sensitive directories

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

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/guestbook.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
login	1

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
name	2
text	2

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
login	1

/hpp (fbc1d56ba0737d3fa577aa5a19c9fd49)

HTML form without CSRF protection

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

This alert belongs to the following categories: A8

CVSS Base Score: 2.6

- Access Vector: Network
- Access Complexity: High
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-352

Parameter	Variations
Unnamed Form	1

/hpp/

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
pp	1

/hpp/index.php

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
pp	1

/hpp/params.php

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
p	2
pp	2

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%3D%8D1N%C3%40%10E%DF%AE%8D%BDI%08%29%D3%40%1D%A0%A2%05%09%11%89HiP%22%05D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X%3B%21S%8C%FE%CC%9B%F9%FF%AA%CB7Jq%AF%7F%ED%F2%2E%F8%01%3E%9E%18p%C9c%9Al%8B%ACzG%F2%DC%BEM%EC%ABdkj%1E%AC%2C%9F%A5%28%B1%EB%89T%C2Jj%29%93%22%DBT7%24%9C%8FH%CBD6%29%A3%0Bx%29%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F4b%E8%FA%98%20b%5F%26%1C%9F5%20h%F1%D1g%0F%14%C1%0A%5Ds%8D%8B0Q%A8L%3C%9B6%D4L%BD%5F%A8w%7E%9D%5B%17%F3%2F%5B%DCm%7B%EF%CB%EF%E6%8D%3An%2D%FB%B3%C3%DD%2E%E3d1d%EC%C7%3F6%CD0%09" type="application/x-shockwave-flash" allowscriptaccess="always"
flashvars="c=alert&u=http://victim.com/secret_file.txt"></object>

This alert belongs to the following categories: A5, A6, A9

CVSS Base Score: 4.4

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-20

Parameter	Variations
p	2

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/listproducts.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
artist	1
cat	2
login	1

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
artist	1
cat	2

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
artist	1
cat	2
login	1

Application error message

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
artist	1
cat	2

/login.php

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: A6

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	2

/medias/css/main.css

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

This alert belongs to the following categories: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

/medias/js/common_functions.js

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

This alert belongs to the following categories: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

/Mod_Rewrite_Shop/buy.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

/Mod_Rewrite_Shop/details.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

/Mod_Rewrite_Shop/Details/color-printer/3

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

This alert belongs to the following categories: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

This alert belongs to the following categories: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

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

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

This alert belongs to the following categories: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/Mod_Rewrite_Shop/rate.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
id	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/pictures//WS_FTP.LOG

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/pictures/path-disclosure-unix.html

Error message on page

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/privacy.php

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

This alert belongs to the following categories: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

/product.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
login	1
pic	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
login	1
pic	1

/product.php (68db51598a6b1e726aa518e093bbd4ff)

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: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

/redir.php

URL redirection

This script is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

This alert belongs to the following categories: A10

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-601

Parameter	Variations
r	1

/search.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
login	1
searchFor	2
test	2

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
searchFor	2

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
login	1
searchFor	2
test	2

/secured

Possible sensitive directories

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

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/secured/database_connect.php

Error message on page

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

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: A6

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/secured/newuser.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
uuname	1

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
uaddress	1
ucc	1
uemail	1
uphone	1
urname	1
uuname	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
uuname	1

Application error message

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
uuname	1

/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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/secured/office_files/filelist.xml

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

This alert belongs to the following categories: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

/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: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

PHP errors enabled

The display_errors directive determines whether error messages should be sent to the browser. These messages frequently contain sensitive information about your web application environment, and should never be presented to untrusted sources.

display_errors is on by default.

This alert belongs to the following categories: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

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: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

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: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

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: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
	1

/sendcommand.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
cart_id	1

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
cart_id	2

/showimage.php

Cross site scripting

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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
file	2

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 execute commands outside of the web server's root directory.

This alert belongs to the following categories: A4

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-22

Parameter	Variations
file	2

Script source code disclosure

It is possible to read the source code of this script by using script filename as a parameter. It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations

file	1

Application error message

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
file	2

Cross site scripting (content-sniffing)

This type of XSS can only be triggered on (and affects) content sniffing browsers.
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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
file	2

/signup.php

HTML form without CSRF protection

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

This alert belongs to the following categories: A8

CVSS Base Score: 2.6

- Access Vector: Network
- Access Complexity: High
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-352

Parameter	Variations
form1	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/Templates/logout.php

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

This alert belongs to the following categories: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

/userinfo.php

Blind SQL Injection

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
login	1
uaddress	2
ucc	2
uname	1
uphone	1
urname	1

Cross site scripting (verified)

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

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. 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: A3

CVSS Base Score: 6.4

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-79

Parameter	Variations
uaddress	2
ucc	2
uemail	2
uphone	2
urname	2

SQL injection (verified)

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This alert belongs to the following categories: A1

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-89

Parameter	Variations
login	1
pass	1
uaddress	2
ucc	2
uemail	2
uname	1
uphone	2
urname	2

Application error message

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

This alert belongs to the following categories: A6

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-200

Parameter	Variations
uaddress	2
ucc	2
uemail	2
uphone	2
urname	2

/userinfo.php (9d1db3f4d16732c9716e14a3e959fa2d)

HTML form without CSRF protection

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

This alert belongs to the following categories: A8

CVSS Base Score: 2.6

- Access Vector: Network
- Access Complexity: High
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: Partial
- Availability Impact: None

CWE CWE-352

Parameter	Variations
form1	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

/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: A5, A6, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-538

Parameter	Variations
	1

Web Server

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: A5, A6, A9

CVSS Base Score: 5.1

- Access Vector: Network
- Access Complexity: High
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-122

CVE CVE-2014-0133

Parameter	Variations
	1

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: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

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: A5, A6, A9

CVSS Base Score: 5.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CWE CWE-284

Parameter	Variations
	1

PHP errors enabled

The display_errors directive determines whether error messages should be sent to the browser. These messages frequently contain sensitive information about your web application environment, and should never be presented to untrusted sources.

display_errors is on by default.

This alert belongs to the following categories: A5, A6, A9

CVSS Base Score: 0.0

- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: None

CWE CWE-16

Parameter	Variations
	1

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: A6, A7

CVSS Base Score: 6.8

- Access Vector: Network
- Access Complexity: Medium
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: Partial
- Availability Impact: Partial

CWE CWE-693

Parameter	Variations
	1

Scanned items (coverage report)

http://testphp.vulnweb.com/

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
Host	HTTP Header

http://testphp.vulnweb.com/style.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/images/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/images/logo.gif

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/login.php

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/userinfo.php

Vulnerabilities have been identified for this URL

17 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
pass	URL encoded POST
uname	URL encoded POST

Input scheme 2	
Input name	Input type
	URL encoded POST
uaddress	URL encoded POST
ucc	URL encoded POST
uemail	URL encoded POST
uphone	URL encoded POST
urname	URL encoded POST

Input scheme 3	
Input name	Input type
uname	URL encoded POST
update	URL encoded POST

Input scheme 4	
Input name	Input type
uaddress	URL encoded POST
ucc	URL encoded POST
uemail	URL encoded POST
uname	URL encoded POST

update	URL encoded POST
uphone	URL encoded POST
urname	URL encoded POST

http://testphp.vulnweb.com/cart.php

Vulnerabilities have been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
del	URL encoded GET

Input scheme 2	
Input name	Input type
del	URL encoded GET
addcart	URL encoded POST

Input scheme 3	
Input name	Input type
addcart	URL encoded POST
price	URL encoded POST

http://testphp.vulnweb.com/search.php

Vulnerabilities have been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
test	URL encoded GET
	URL encoded POST
searchFor	URL encoded POST

Input scheme 2	
Input name	Input type
test	URL encoded GET
searchFor	URL encoded POST

http://testphp.vulnweb.com/hpp/

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
pp	URL encoded GET

http://testphp.vulnweb.com/hpp/params.php

Vulnerabilities have been identified for this URL

6 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

Input scheme 2	
Input name	Input type

p	URL encoded GET
pp	URL encoded GET

Input scheme 3	
Input name	Input type
aaaa	URL encoded GET
p	URL encoded GET
pp	URL encoded GET

http://testphp.vulnweb.com/hpp/index.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
pp	URL encoded GET

http://testphp.vulnweb.com/hpp/test.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/index.php

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/artists.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
artist	URL encoded GET

http://testphp.vulnweb.com/privacy.php

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/guestbook.php

Vulnerabilities have been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
name	URL encoded POST
text	URL encoded POST

Input scheme 2	
Input name	Input type
	URL encoded POST
name	URL encoded POST
text	URL encoded POST

http://testphp.vulnweb.com/categories.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Flash/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Flash/add.swf

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Flash/add.fla

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/AJAX/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/AJAX/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/AJAX/styles.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/AJAX/titles.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/AJAX/artists.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/AJAX/categories.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/AJAX/showxml.php

Vulnerabilities have been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
text/xml	Custom POST
xml.node#text	XML
xml.node#text	XML
xml.node:name	XML
xml.node:name	XML

http://testphp.vulnweb.com/AJAX/infoartist.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type

id	URL encoded GET

http://testphp.vulnweb.com/AJAX/infocateg.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

http://testphp.vulnweb.com/AJAX/infotitle.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded POST

http://testphp.vulnweb.com/AJAX/htaccess.conf

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/disclaimer.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

http://testphp.vulnweb.com/Mod_Rewrite_Shop/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

http://testphp.vulnweb.com/signup.php

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/sendcommand.php

Vulnerabilities have been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded POST
cart_id	URL encoded POST

Input scheme 2	
Input name	Input type
cart_id	URL encoded POST

http://testphp.vulnweb.com/listproducts.php

Vulnerabilities have been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
cat	URL encoded GET

Input scheme 2	
Input name	Input type
artist	URL encoded GET

Input scheme 3	
Input name	Input type
artist	URL encoded GET
cat	URL encoded GET

http://testphp.vulnweb.com/product.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
pic	URL encoded GET

http://testphp.vulnweb.com/showimage.php

Vulnerabilities have been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
file	URL encoded GET
size	URL encoded GET

Input scheme 2	
Input name	Input type
file	URL encoded GET

http://testphp.vulnweb.com/redir.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
r	URL encoded GET

http://testphp.vulnweb.com/Templates/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Templates/logout.php

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com:80/crossdomain.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/secured/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/secured/newuser.php

Vulnerabilities have been identified for this URL

10 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded POST
uaddress	URL encoded POST
ucc	URL encoded POST
uemail	URL encoded POST
upass	URL encoded POST
upass2	URL encoded POST
uphone	URL encoded POST
urname	URL encoded POST
uuname	URL encoded POST

Input scheme 2	
Input name	Input type
signup	URL encoded POST

http://testphp.vulnweb.com/secured/style.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/secured/database_connect.php

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/secured/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/secured/office.htm

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/secured/phpinfo.php

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

http://testphp.vulnweb.com/secured/office_files

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/secured/office_files/filelist.xml

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/comment.php

Vulnerabilities have been identified for this URL

17 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
aid	URL encoded GET

Input scheme 2	
Input name	Input type
	URL encoded POST
comment	URL encoded POST
name	URL encoded POST
phpaction	URL encoded POST

Input scheme 3	
Input name	Input type
pid	URL encoded GET

Input scheme 4	
Input name	Input type
aid	URL encoded GET
pid	URL encoded GET

Input scheme 5	
Input name	Input type
aid	URL encoded GET
pid	URL encoded GET
name	URL encoded POST

Input scheme 6	
Input name	Input type
aid	URL encoded GET
pid	URL encoded GET
comment	URL encoded POST
name	URL encoded POST
phpaction	URL encoded POST
Submit	URL encoded POST

http://testphp.vulnweb.com/.idea/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/.idea/.name

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/.idea/acuart.iml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/.idea/encodings.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/.idea/misc.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/.idea/modules.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/.idea/scopes/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/.idea/scopes/scope_settings.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/.idea/vcs.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/.idea/workspace.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/_mmServerScripts/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
Type	URL encoded POST

http://testphp.vulnweb.com/_mmServerScripts/mysql.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/404.php

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/adm1nPan3l/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/adm1nPan3l/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/admin/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/admin/create.sql

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/bxss/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/bxss/adminPan3l/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/bxss/adminPan3l/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/bxss/adminPan3l/style.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/bxss/cleanDatabase.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/bxss/database_connect.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/bxss/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/bxss/test.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/bxss/vuln.php

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

http://testphp.vulnweb.com/clearguestbook.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/clientaccesspolicy.xml

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Connections/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/Connections/DB_Connection.php

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/CVS/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/CVS/Entries

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/CVS/Entries.Log

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/CVS/Repository

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/CVS/Root

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/database_connect.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/index.bak

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/1.jpg.tn

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/2.jpg.tn

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/3.jpg.tn

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/4.jpg.tn

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/5.jpg.tn

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/6.jpg.tn

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/7.jpg.tn

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/8.jpg.tn

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/credentials.txt

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/ipaddresses.txt

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/path-disclosure-unix.html

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/path-disclosure-win.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/wp-config.bak

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/pictures/WS_FTP.LOG

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/wvstests/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/version.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/medias

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/medias/img

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/medias/css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/medias/css/main.css

Vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/medias/js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

http://testphp.vulnweb.com/medias/js/common_functions.js

Vulnerabilities have been identified for this URL

No input(s) found for this URL