Your Logo Here

Vulnerability Scan Report

Scan Power by invicti

SUBSCRIBER

Basic Information

Report Delivered:	2025-07-11
Requested By:	Jane Doe
Company Name:	Acme Bank
Report Type:	Subscriber Monthly
Report Format:	Standard

Critical

True Inspect Threat Level 4

One or more critical-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Scan Detail

Target	http://testphp.vulnweb.com/
Scan Type	Full Scan
Start Time	Jul 10, 2025 at 3:16:00 AM GMT
Scan Duration	16 minutes
Requests	77244
Average Response Time	55ms
Maximum Response Time	30000ms
Application Build	vnull
Authentication Profile	-

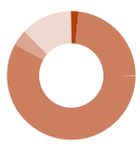
Critical	High	Medium	Low	Informational
42	53	15	11	8

Severity	Vulnerabilities	Instances
Critical	1	42
High	8	53
Medium	14	15
Low	11	11
Informational	8	8
Total	42	129

Critical Severity

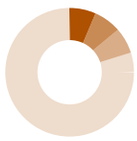
	Instances
SQL Injection	42

High Severity



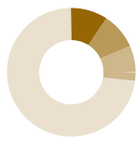
	Instances
Basic authentication over HTTP	1
Cross-site Scripting	43
Cross-site Scripting (DOM based)	2
Others	7

Medium Severity



	Instances
Directory listings	1
HTTP Header Injection	1
HTTP parameter pollution	1
Others	12

Low Severity



	Instances
Cookies Not Marked as HttpOnly	1
Cookies with missing, inconsistent or contradictory properties	1
PHP allow_url_fopen Is Enabled	1
Others	8

Informational

	Instances
Content Security Policy (CSP) Not Implemented	1
Generic Email Address Disclosure	1
.htaccess File Detected	1
Others	5

Impacts

Severity Filter: ☑ Critical ☑ High ☑ Medium ☑ Low ☑ Informational

SEVERITY	IMPACT	
Critical	42	SQL Injection
High	2	[Possible] Backup Source Code Detected
High	1	Basic authentication over HTTP
High	43	Cross-site Scripting
High	2	Cross-site Scripting (DOM based)
High	1	Directory traversal
High	1	Local File Inclusion
High	1	Possible database backup
High	2	Vulnerable package dependencies [high]
Medium	1	Directory listings
Medium	1	HTTP Header Injection
Medium	1	HTTP parameter pollution
Medium	1	Insecure crossdomain.xml policy
Medium	1	Insecure HTTP Usage
Medium	1	JetBrains .idea project directory
Medium	1	Open Redirection
Medium	1	Open Redirection
Medium	1	Password transmitted over HTTP
Medium	1	PHP errors enabled
Medium	1	PHP session.use_only_cookies Is Disabled
Medium	1	PHPinfo pages
Medium	1	SSL/TLS Not Implemented
Medium	2	Vulnerable package dependencies [medium]
Low	1	[Possible] Internal IP Address Disclosure
Low	1	Cookies Not Marked as HttpOnly
Low	1	Cookies with missing, inconsistent or contradictory properties
Low	1	PHP allow_url_fopen Is Enabled
Low	1	PHP allow_url_fopen Is Enabled
Low	1	PHP display_errors Is Enabled
Low	1	PHP open_basedir Is Not Configured
Low	1	Possible sensitive files
Low	1	Possible username or password disclosure
Low	1	Programming Error Messages
Low	1	Version Disclosure (PHP)
Informational	1	.htaccess File Detected
Informational	1	[Possible] Internal Path Disclosure (*nix)
Informational	1	[Possible] Internal Path Disclosure (Windows)
Informational	1	[Possible] WS_FTP Log File Detected

Informational	1	Content Security Policy (CSP) Not Implemented
Informational	1	Generic Email Address Disclosure
Informational	1	Permissions-Policy header not implemented
Informational	1	X-Content-Type-Options (XCTO) Not Implemented

SQL Injection

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

Impact

An attacker can use SQL injection to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

http://testphp.vulnweb.com/	ACUSENSOR	Verified
http://testphp.vulnweb.com/		
http://testphp.vulnweb.com/404.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/AJAX/infoartist.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/AJAX/infocateg.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/AJAX/infotitle.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/artists.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/cart.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/cart.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/categories.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/listproducts.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/listproducts.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html	ACUSENSOR	Verified

http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html	ACUSENSOR	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html	ACUSENSOR	Verified
http://testphp.vulnweb.com/product.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/search.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/search.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/secured/newuser.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/sendcommand.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/userinfo.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/userinfo.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/userinfo.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/userinfo.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/userinfo.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/userinfo.php	ACUSENSOR	Verified
http://testphp.vulnweb.com/userinfo.php	ACUSENSOR	Verified

Show Details

[Possible] Backup Source Code Detected

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

Impact

Backup files can contain script sources, configuration files or other sensitive information that may help an malicious user to prepare more advanced attacks.

http://testphp.vulnweb.com/index.bak	Confidence: 80%
http://testphp.vulnweb.com/index.zip	Confidence: 80%

Show Details

Basic authentication over HTTP

In the context of an HTTP transaction, basic access authentication is a method for an HTTP user agent to provide a user name and password when making a request.

One or more directories are protected using Basic Authentication over an HTTP connection. With Basic Authentication the user credentials are sent as cleartext and because HTTPS is not used, they are vulnerable to packet sniffing.

Impact

User credentials are sent as cleartext and are vulnerable to packet sniffing.

http://testphp.vulnweb.com/	Verified

Show Details

Cross-site Scripting

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

Impact

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

Furthermore, JavaScript can read and make arbitrary modifications to the contents of a page being displayed to a user. Therefore, XSS in conjunction with some clever social engineering opens up a lot of possibilities for an attacker.

http://testphp.vulnweb.com/	
http://testphp.vulnweb.com/AJAX/infoartist.php	
http://testphp.vulnweb.com/AJAX/infocateg.php	
http://testphp.vulnweb.com/AJAX/infotitle.php	
http://testphp.vulnweb.com/AJAX/showxml.php	Verified
http://testphp.vulnweb.com/artists.php	Verified
http://testphp.vulnweb.com/cart.php	Verified
http://testphp.vulnweb.com/guestbook.php	Verified
http://testphp.vulnweb.com/guestbook.php	Verified
http://testphp.vulnweb.com/hpp/	Verified
http://testphp.vulnweb.com/hpp/params.php	Verified
http://testphp.vulnweb.com/hpp/params.php	Verified
http://testphp.vulnweb.com/listproducts.php	Verified
http://testphp.vulnweb.com/listproducts.php	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html	Verified
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html	Verified
http://testphp.vulnweb.com/product.php	Verified
http://testphp.vulnweb.com/search.php	Verified
http://testphp.vulnweb.com/search.php	Verified
http://testphp.vulnweb.com/secured/newuser.php	Verified
http://testphp.vulnweb.com/secured/newuser.php	Verified
http://testphp.vulnweb.com/secured/newuser.php	Verified
http://testphp.vulnweb.com/secured/newuser.php	Verified
http://testphp.vulnweb.com/secured/newuser.php	Verified
http://testphp.vulnweb.com/secured/newuser.php	Verified
http://testphp.vulnweb.com/sendcommand.php	Verified
http://testphp.vulnweb.com/userinfo.php	Verified
http://testphp.vulnweb.com/userinfo.php	Verified
http://testphp.vulnweb.com/userinfo.php	Verified
http://testphp.vulnweb.com/userinfo.php	Verified
http://testphp.vulnweb.com/userinfo.php	Verified
http://testphp.vulnweb.com/userinfo.php	Verified

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

Show Details

Cross-site Scripting (DOM based)

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.

While a traditional cross-site scripting vulnerability occurs on the server-side code, document object model based cross-site scripting is a type of vulnerability which affects the script code in the client's browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

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

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

Show Details

Directory traversal

This script is vulnerable to directory traversal attacks.

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

Impact

By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute commands, leading to a full compromise of the Web server.

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

Show Details

Local File Inclusion

This script is vulnerable to file inclusion attacks.

The script was found to reference and potentially retrieve files from user-specified locations. User input is not sufficiently validated or sanitized prior to being passed to the vulnerable script's include function.

Impact

It is possible for a remote attacker to include a file from local or remote resources and/or execute arbitrary script code with the privileges of the web-server.

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

Show Details

Possible database backup

Manual confirmation is required for this alert.

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

Impact

These file(s) may disclose sensitive information. This information can be used to launch further attacks.

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

Show Details

Vulnerable package dependencies [high]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

http://testphp.vulnweb.com/ ACUSENSOR Confidence: 100%

http://testphp.vulnweb.com/vendor/installed.json

Show Details

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

http://testphp.vulnweb.com/ Verified

Show Details

HTTP Header Injection

This script is vulnerable to CRLF injection attacks.

HTTP headers have the structure "Key: Value", where each line is separated by the CRLF combination. If the user input is injected into the value section without properly escaping/removing CRLF characters it is possible to alter the HTTP headers structure.
HTTP Response Splitting is a new application attack technique which enables various new attacks such as web cache poisoning, cross user defacement, hijacking pages with sensitive user information and cross-site scripting (XSS). The attacker sends a single HTTP request that forces the web server to form an output stream, which is then interpreted by the target as two HTTP responses instead of one response.

Impact

Is it possible for a remote attacker to inject custom HTTP headers. For example, an attacker can inject session cookies or HTML code. This may conduct to vulnerabilities like XSS (cross-site scripting) or session fixation.

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

Show Details

HTTP parameter pollution

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

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

Impact

The impact depends on the affected web application. An attacker could

- Override existing hardcoded HTTP parameters
- Modify the application behaviors
- Access and, potentially exploit, uncontrollable variables
- Bypass input validation checkpoints and WAFs rules

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

Show Details

Insecure crossdomain.xml policy

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="*" />
<allow-http-request-headers-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.

Impact

Using an insecure cross-domain policy file could expose your site to various attacks.

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

Show Details

Insecure HTTP Usage

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

http://testphp.vulnweb.com/

Show Details

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.

Impact

These files may expose sensitive information that may help an malicious user to prepare more advanced attacks.

http://testphp.vulnweb.com/

Show Details

Open 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.

Impact

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

http://testphp.vulnweb.com/

Show Details

Open Redirection

This endpoint 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.

Impact

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

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

Show Details

Password transmitted over HTTP

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

http://testphp.vulnweb.com/

Show Details

PHP errors enabled

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

Acunetix AcuSensor found that the PHP `display_errors` directive is enabled.

Impact

Application error messages may disclose sensitive information which can be used to escalate attacks.

http://testphp.vulnweb.com/ ACUSENSOR Verified

Show Details

PHP session.use_only_cookies Is 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.

Impact

Application dependant - possible session hijacking.

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

Show Details

PHPinfo pages

One or more **phpinfo()** pages were found. The **phpinfo()** function exposes a large amount of information about the PHP configuration and that of its environment. This includes information about PHP compilation options and extensions, the PHP version, server information, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

Impact

The phpinfo() pages may expose sensitive information that may help an malicious user to prepare more advanced attacks.

http://testphp.vulnweb.com/ Confidence: 95%

Show Details

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

http://testphp.vulnweb.com/ Verified

Show Details

Vulnerable package dependencies [medium]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

http://testphp.vulnweb.com/ ACUSENSOR Confidence: 100%

http://testphp.vulnweb.com/vendor/installed.json

Show Details

[Possible] Internal IP Address Disclosure

One or more strings matching an internal IPv4 address were found. These IPv4 addresses may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

The significance of this finding should be confirmed manually.

Impact

Possible sensitive information disclosure.

http://testphp.vulnweb.com/

Show Details

Cookies Not Marked as HttpOnly

One or more cookies don't 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.

Impact

Cookies can be accessed by client-side scripts.

http://testphp.vulnweb.com/ Verified

Show Details

Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

http://testphp.vulnweb.com/ Verified

Show Details

PHP allow_url_fopen Is 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.

Impact

Application dependant - possible remote file inclusion.

http://testphp.vulnweb.com/ ACUSENSOR Verified

Show Details

PHP allow_url_fopen Is 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.

Impact

Application dependant - possible remote file inclusion.

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

Show Details

PHP display_errors Is Enabled

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

Acunetix found that the PHP `display_errors` directive is enabled.

Impact

Application error messages may disclose sensitive information which can be used to escalate attacks.

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

Show Details

PHP open_basedir Is Not Configured

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.

Impact

Application dependant - possible remote code inclusion.

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

Show Details

Possible sensitive files

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

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

http://testphp.vulnweb.com/

Show Details

Possible username or password disclosure

One or more credential pairs (username+password) were found. This information could be sensitive.

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

Impact

Possible sensitive information disclosure.

http://testphp.vulnweb.com/

Show Details

Programming Error Messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.
These messages may also contain the location of the file that produced an unhandled exception.
Consult the 'Attack details' section for more information about the affected page(s).

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

http://testphp.vulnweb.com/

Show Details

Version Disclosure (PHP)

The web server is sending the X-Powered-By: response headers, revealing the PHP version.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

http://testphp.vulnweb.com/

Show Details

.htaccess File Detected

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.

Impact

Possible sensitive information disclosure.

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

Show Details

[Possible] Internal Path Disclosure (*nix)

One or more fully qualified path names were found. 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.

Impact

Possible sensitive information disclosure.

http://testphp.vulnweb.com/

Show Details

[Possible] Internal Path Disclosure (Windows)

One or more fully qualified path names were been found. 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.

Impact

Possible sensitive information disclosure.

http://testphp.vulnweb.com/

Show Details

[Possible] WS_FTP Log File Detected

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.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

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

Show Details

Content Security Policy (CSP) Not Implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

http://testphp.vulnweb.com/

Show Details

Generic Email Address Disclosure

One or more email addresses have been found on this website. 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.

Impact

Email addresses posted on Web sites may attract spam.

http://testphp.vulnweb.com/

Show Details

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

http://testphp.vulnweb.com/

Show Details

X-Content-Type-Options (XCTO) Not Implemented

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing. This allows web browsers to perform MIME-Sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.

X-Content-Type-Options (XCTO) is an HTTP header that can be used to prevent MIME type sniffing, which can help to mitigate certain types of attacks, including Cross Site Scripting (XSS). It also enables Cross-Origin Read Blocking (CORB) for sensitive resources, helping protect against Cross-Site Script Inclusion (XSSI) and side channel attacks.

Impact

XCTO header can be used as an additional layer of defense to prevent various attacks, such as Cross-Site Scripting (XSS), Cross-Site Script Inclusion (XSSI), side channel attacks, and others.

http://testphp.vulnweb.com/

Show Details

Coverage

> http://testphp.vulnweb.com