True Positives

Vulnerability Scan Report

Scan Powered by invicti

SUBSCRIBED

Basic Information

Report Delivered	2025-07-11
Requested By	Jane Doe
Company Name	Acme Bank
Report Type	Subscribed Vulnerability
Report Format	Standard

True Impact Threat Level: 4

There is more than one high vulnerability that has been discovered by the scanner. Although each of these vulnerabilities may not be individually critical, they may be part of a chain of events that could be used to compromise the target.

Critical	High	Medium	Low	Informational
42	53	15	11	8

Scan Detail

Target	https://demo.testfire.net/
Scan Type	Full Scan
Start Time	Jul 10, 2025 at 5:45:30 AM GMT
Duration	1 hour, 15 min
Requests	17444
Average response time	1ms
Maximum response time	3600ms
Application Build	v.23.6.0
Crawl Mode	Standard

Severity / Vulnerabilities / Instances

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

Critical Severity

	Instances
SQL Injection	42

High Severity

	Instances
Blind Authentication over HTTP	10
Cross-site Scripting (DOM based)	10
Cross-site Scripting (XSS based)	10
Directory traversal	10
Local File Inclusion	10
Possible database backup	3

Medium Severity

	Instances
Directory Listings	4
Cross Frame Options not Implemented	3
HTTP Parameter pollution	3
Insecure crossdomain.xml policy	1

Low Severity

	Instances
Cookies Not Marked as HttpOnly	1
Cookies with missing, inconsistent or contradictory properties	1
Cookies with missing, inconsistent or contradictory properties	1
Session Cookie Not Marked as Secure	1
Session Token Sent in URL	1
Clickjacking: X-Frame-Options header missing	1
Content Security Policy (CSP) Not Implemented	1
Generic Email Address Disclosure	1
Permissions Policy header not implemented	1
X-Content-Type-Options (MIME) Not Implemented	1

Informational

	Instances
Content Security Policy (CSP) Not Implemented	1
Cross-origin resource sharing (CORS) Not Implemented	1
Hidden form input named csrftoken found	1
Session Token Sent in URL	1

Impacts

Severity Filter: Critical High Medium Low Informational

SEVERITY	IMPACT
Critical	SQL Injection
High	[Possible] Backup Source Code Detected
High	Basic authentication over HTTP
High	Cross-site Scripting
High	Cross-site Scripting (DOM based)
High	Directory traversal
High	Local File Inclusion
High	Possible database backup
High	Vulnerable package dependencies [high]
Medium	Directory listings
Medium	HTTP Header Injection
Medium	HTTP parameter pollution
Medium	Insecure crossdomain.xml policy
Medium	Insecure HTTP Usage
Medium	jetbrains .idea project directory
Medium	Open Redirection
Medium	Open Redirection
Medium	Password transmitted over HTTP
Medium	PHP errors enabled
Medium	PHP session.use_only_cookies is Disabled
Medium	PHPinfo pages
Medium	SSL/TLS Not Implemented
Medium	Vulnerable package dependencies [medium]
Low	[Possible] Internal IP Address Disclosure
Low	Cookies Not Marked as HttpOnly
Low	Cookies with missing, inconsistent or contradictory properties
Low	PHP allow_url_fopen is Enabled
Low	PHP allow_url_include is Enabled
Low	PHP display_errors is Enabled
Low	PHP open_basedir is Not Configured
Low	Possible sensitive files
Low	Possible username or password disclosure
Low	Programming Error Messages
Low	Session Checksum (PHP)
Low	Version Control Found
Informational	[Possible] Internal Path Disclosure (*nix)
Informational	[Possible] Internal Path Disclosure (Windows)
Informational	[Possible] MD_PWT Log File Detected
Informational	Content Security Policy (CSP) Not Implemented
Informational	Generic Email Address Disclosure
Informational	Permissions Policy header not implemented
Informational	X-Content-Type-Options (MIME) 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

If exploited, an SQL injection vulnerability could allow an unauthenticated attacker to bypass authentication and authentication 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 then has the ability to escalate an attack even further.

http://testphp.vulnweb.com/	Fixed
http://testphp.vulnweb.com/	
http://testphp.vulnweb.com/AJAX/info.php	Fixed
http://testphp.vulnweb.com/AJAX/titles.php	Fixed
http://testphp.vulnweb.com/AJAX/styles.php	Fixed
http://testphp.vulnweb.com/AJAX/infoartist.php	Fixed
http://testphp.vulnweb.com/artists.php	Fixed
http://testphp.vulnweb.com/cart.php	Fixed
http://testphp.vulnweb.com/categories.php	Fixed
http://testphp.vulnweb.com/disclaimer.php	Fixed
http://testphp.vulnweb.com/guestbook.php	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.color-green/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.color-red/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.color-white/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.color-yellow/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-1000/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-1200/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-1400/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-1600/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-1800/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-2000/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-2200/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-2400/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-2600/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-2800/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-3000/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-3200/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-3400/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-3600/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-3800/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-4000/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-4200/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-4400/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-4600/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-4800/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-5000/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-5200/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-5400/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-5600/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-5800/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-6000/3/	Fixed
http://testphp.vulnweb.com/product.php	Fixed
http://testphp.vulnweb.com/search.php	Fixed
http://testphp.vulnweb.com/secured/newuser.php	Fixed
http://testphp.vulnweb.com/signup.php	Fixed
http://testphp.vulnweb.com/Templates/	Fixed
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.bak	Fixed
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.bak/Editable	Fixed
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.bak/Editable/Left	Fixed
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.bak/Editable/Right	Fixed
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.bak/Editable/Top	Fixed

Show Details

[Possible] Backup Source Code Detected

A possible backup file was found on your web server. These files may expose the source code of the application to attackers.

Impact

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

http://testphp.vulnweb.com/index.bak	Confirmed Fixed
http://testphp.vulnweb.com/index.zip	Confirmed Fixed

Show Details

Basic authentication over HTTP

A Basic authentication HTTP request was found. Basic authentication is a method for an HTTP user agent to provide a user name and password when making a request.

Due to Basic directives are protected using Basic Authentication over an HTTP connection. With Basic Authentication the user credentials are sent in cleartext and because HTTP is not secure, they are vulnerable to interception.

Impact

User credentials are sent in cleartext and are vulnerable to passive eavesdropping.

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

Show Details

Cross-site Scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts (in the form of JavaScript) in another user's browser. 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.

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 use this to execute code and take over the account, redirect users to phishing or other sites, or perform actions to modify the content of the page presented to the user.

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 use this to execute code and take over the account, redirect users to phishing or other sites, or perform actions to modify the content of the page presented to the user.

http://testphp.vulnweb.com/AJAX/infoartist.php	
http://testphp.vulnweb.com/AJAX/infoartist.php	
http://testphp.vulnweb.com/AJAX/infotitle.php	
http://testphp.vulnweb.com/AJAX/infotitle.php	Fixed
http://testphp.vulnweb.com/artists.php	Fixed
http://testphp.vulnweb.com/cart.php	Fixed
http://testphp.vulnweb.com/guestbook.php	Fixed
http://testphp.vulnweb.com/guestbook.php	Fixed
http://testphp.vulnweb.com/hpp/params.php	Fixed
http://testphp.vulnweb.com/hpp/params.php	Fixed
http://testphp.vulnweb.com/listproducts.php	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.color-green/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.color-red/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.color-white/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.color-yellow/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-1000/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-1200/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-1400/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-1600/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-1800/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-2000/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-2200/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-2400/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-2600/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-2800/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-3000/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-3200/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-3400/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-3600/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-3800/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-4000/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-4200/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-4400/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-4600/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-4800/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-5000/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-5200/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-5400/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-5600/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-5800/3/	Fixed
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details.width-6000/3/	Fixed
http://testphp.vulnweb.com/product.php	Fixed
http://testphp.vulnweb.com/search.php	Fixed
http://testphp.vulnweb.com/secured/newuser.php	Fixed
http://testphp.vulnweb.com/secured/newuser.php	Fixed
http://testphp.vulnweb.com/secured/newuser.php	Fixed
http://testphp.vulnweb.com/secured/newuser.php	Fixed
http://testphp.vulnweb.com/secured/newuser.php	Fixed
http://testphp.vulnweb.com/signup.php	Fixed
http://testphp.vulnweb.com/signup.php	Fixed
http://testphp.vulnweb.com/signup.php	Fixed
http://testphp.vulnweb.com/signup.php	Fixed
http://testphp.vulnweb.com/signup.php	Fixed
http://testphp.vulnweb.com/signup.php	Fixed

Show Details

Cross-site Scripting (DOM based)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts (in the form of JavaScript) in another user's browser. 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.

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 use this to execute code and take over the account, redirect users to phishing or other sites, or perform actions to modify the content of the page presented to the user.

http://testphp.vulnweb.com/artists.php	Fixed
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.bak/Editable/Left	Fixed
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.bak/Editable/Right	Fixed
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.bak/Editable/Top	Fixed

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/Templates/.php	Fixed

Show Details

Local File Inclusion

This script is vulnerable to file inclusion attacks.

The script's parameter value is being passed to various files from user-specified locations. User input is not sufficiently validated or sanitized prior to being passed to the underlying script or function.

Impact

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

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

Show Details

Possible database backup

Manual confirmation is required for this alert.

One or more possible database backup were identified. A database backup contains a record of the tables structure and/or the data from a database and is usually in the form of a collection of data definition language (DDL) statements along with data-insertion statements. This information may be used to reconstruct the database schema or parts of it or simply to obtain a copy of all stored data. This information is highly undesirable and should not be found on a production system.

Impact

Database backups may disclose sensitive information. This information can be used to launch further attacks.

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

Show Details

Vulnerable package dependencies [high]

Due to the packages that are used in your web application we detected issues 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. Its recommended to investigate each vulnerable package individually.

http://testphp.vulnweb.com/secured/phpfunctions.php	Confirmed Fixed

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/	Fixed

Show Details

HTTP Header Injection

This script is vulnerable to HTTP Header Injection attacks.

HTTP Header Injection vulnerability in the parameter 'mail' was found (parameter is injected to the HTTP Location header). This vulnerability affects web application's processing of user-supplied HTTP Location headers. Most web clients use this type of HTTP header to perform a redirection. Depending on the web application, it may also be possible to modify the content of the response entirely by injecting additional headers and/or a new HTTP response body. This attacker attack vector is HTTP response splitting. HTTP response splitting is a technique that allows an attacker to inject a single or multiple HTTP response(s) into the response stream sent by a web server in response to a single HTTP request. This is possible because the web server often includes user-supplied input in HTTP headers without validating or sanitizing it first.

Impact

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

http://testphp.vulnweb.com/mail.php	Fixed

Show Details

HTTP parameter pollution

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HTTP affects crawlers 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 manipulate the logic of the application or modify application parameters in unintended ways.

Impact

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

- Override existing hardcoded HTTP parameters
- Modify application behaviors
- Access unauthorized resources and sensitive data
- Bypass input validation and application firewalls

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

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. Internet browsers may be instructed to circumvent this security model with cross-domain policy files, which unfortunately could be misused if not properly configured. In this case, a URL was found to be serving a cross-domain policy file that is overly permissive.

Impact

Cross-domain policy files can be used to allow access to data or functionality across domains that would be prevented by the browser's security model in the absence of such a policy. In the worst case, a misconfigured cross-domain policy file could potentially allow a malicious third-party site to perform cross-site scripting and cross-site request forgery attacks against your site, read sensitive data, or interact with your site in a privileged manner.

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

Show Details

Insecure HTTP Usage

Cookie was set over HTTP without the secure flag, and should be sent only over HTTPS.

Impact

In some circumstances, it could be used to lead to man-in-the-middle (MitM) attacks.

http://testphp.vulnweb.com/	Fixed

Show Details

jetBrains .idea project directory

The .idea folder contains all of JetBrains's project settings. It stores workspace settings, version control information, notes for the project team, such as tasks and locations of its component modules, compiler settings, etc. If you're behind a site source (or the site/source-tree contains information for connecting to the database and credentials), the .idea folder may contain sensitive information that should not be accessible to the public. Depending on the server configuration, it may also be possible to download the entire contents of the .idea folder. Downloading this folder may expose source code to your competitors.

Impact

There may be sources and/or information that may help an malicious user to prepare more advanced attacks.

http://testphp.vulnweb.com/	Fixed

Show Details

Open Redirection

This script is possibly vulnerable to URL redirection attacks.

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

Impact

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

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