# Website Vulnerability Scanner Report

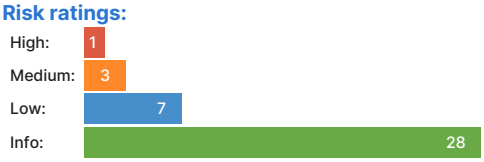
✔ http://testphp.vulnweb.com/

The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

## Summary

**Overall risk level:**
High

**Risk ratings:**




**Scan information:**

| | |
|---|---|
| Start time: | Sep 01, 2024 / 17:21:12 UTC+0530 |
| Finish time: | Sep 01, 2024 / 17:25:43 UTC+0530 |
| Scan duration: | 4 min, 31 sec |
| Tests performed: | 39/39 |
| Scan status: | Finished |

## Findings

### Vulnerabilities found for server-side software

UNCONFIRMED

| Risk Level | CVSS | CVE | Summary | Affected software |
|---|---|---|---|---|
| | 9.8 | CVE-2024-4577 | In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. | php 5.6.40 |
| | 7.5 | CVE-2017-8923 | The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string. | php 5.6.40 |
| | 7.5 | CVE-2017-9225 | An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds write in onigenc_unicode_get_case_fold_codes_by_str() occurs during regular expression compilation. Code point 0xFFFFFFFF is not properly handled in unicode_unfold_key(). A malformed regular expression could result in 4 bytes being written off the end of a stack buffer of expand_case_fold_string() during the call to onigenc_unicode_get_case_fold_codes_by_str(), a typical stack buffer overflow. | php 5.6.40 |
| | 7.5 | CVE-2019-9641 | An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF. | php 5.6.40 |
| | 6.8 | CVE-2015-9253 | An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility. | php 5.6.40 |

Details

**Risk description:**
The risk is that an attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

**Recommendation:**
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

**Classification:**
CWE : CWE-1026
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2021 : A6 - Vulnerable and Outdated Components

## Communication is not secure

CONFIRMED

| URL | Response URL | Evidence |
|---|---|---|
| http://testphp.vulnweb.com/ | http://testphp.vulnweb.com/ | Communication is made over unsecure, unencrypted HTTP. |

Details

**Risk description:**
The risk is that an attacker who manages to intercept the communication at the network level can read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

**Recommendation:**
We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

**Classification:**
CWE : CWE-311
OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure
OWASP Top 10 - 2021 : A4 - Insecure Design

## Directory listing is enabled

CONFIRMED

| URL |
|---|
| http://testphp.vulnweb.com/Flash |
| http://testphp.vulnweb.com/Mod_Rewrite_Shop/images |
| http://testphp.vulnweb.com/admin |
| http://testphp.vulnweb.com/images |

Details

**Risk description:**
The risk is that it's often the case that sensitive files are "hidden" among public files in that location and attackers can use this vulnerability to access them.

**Recommendation:**
We recommend reconfiguring the web server in order to deny directory listing. Furthermore, you should verify that there are no sensitive files at the mentioned URLs.

**References:**
http://projects.webappsec.org/w/page/13246922/Directory%20Indexing

**Classification:**
CWE : CWE-548
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A1 - Broken Access Control

**Screenshot:**

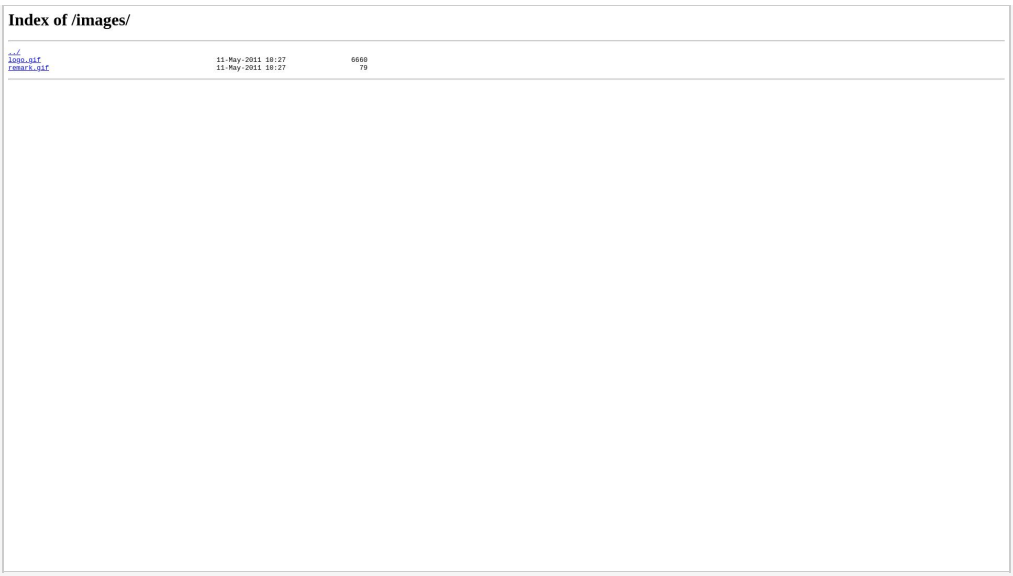



**Figure 1.** Directory Listing

## Insecure client access policy

CONFIRMED

| URL |
| --- |
| http://testphp.vulnweb.com/crossdomain.xml |

Details

**Risk description:**

In `crossdomain.xml` , the external websites which are permitted to read content from this website via Flash are specified in the XML tag `<allow-access-from>` . If the value of this tag is too permissive (ex. wildcard), it means that any Flash script from an external website could access content from this website, including confidential information of users.

If the allowed domains are too permissive (ex. wildcard) in `clientaccesspolicy.xml` , then any external website will be able to read content (including sensitive information) from this website.
Flash is not supported anymore and this poses a risk only if the user's clients use older browsers, making them vulnerable to their information being accessed by a malicious external Flash script.

**Recommendation:**

We recommend to carefully review the content of the policy file and permit access only for legitimate domains.

**References:**

http://blog.h3xstream.com/2015/04/crossdomainxml-beware-of-wildcards.html
https://msdn.microsoft.com/en-us/library/cc197955(v=vs.95).aspx

**Classification:**

CWE : CWE-16
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

**Screenshot:**


Figure 2.

## Missing security header: Content-Security-Policy

CONFIRMED

| URL | Evidence |
| --- | --- |
| http://testphp.vulnweb.com/ | Response does not include the HTTP Content-Security-Policy security header or meta tag<br>Request / Response |

Details

**Risk description:**
The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

**Recommendation:**
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

**References:**
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

**Classification:**
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Missing security header: X-Content-Type-Options

CONFIRMED

| URL | Evidence |
| --- | --- |
| http://testphp.vulnweb.com/ | Response headers do not include the X-Content-Type-Options HTTP security header<br>Request / Response |

Details

**Risk description:**
The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

**Recommendation:**
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

**References:**
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

**Classification:**
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Missing security header: Referrer-Policy

CONFIRMED

| URL | Evidence |
| --- | --- |
| http://testphp.vulnweb.com/ | Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.<br>Request / Response |

Details

**Risk description:**
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

**Recommendation:**
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

**References:**
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

**Classification:**
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Server software and technology found

UNCONFIRMED

| Software / Version | Category |
| --- | --- |
| Nginx 1.19.0 | Web servers, Reverse proxies |
| PHP 5.6.40 | Programming languages |
| Ubuntu | Operating systems |
| DreamWeaver | Editors |
| Adobe Flash | Programming languages |

Details

**Risk description:**
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

**Recommendation:**
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

**References:**
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

**Classification:**
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

**Screenshot:**

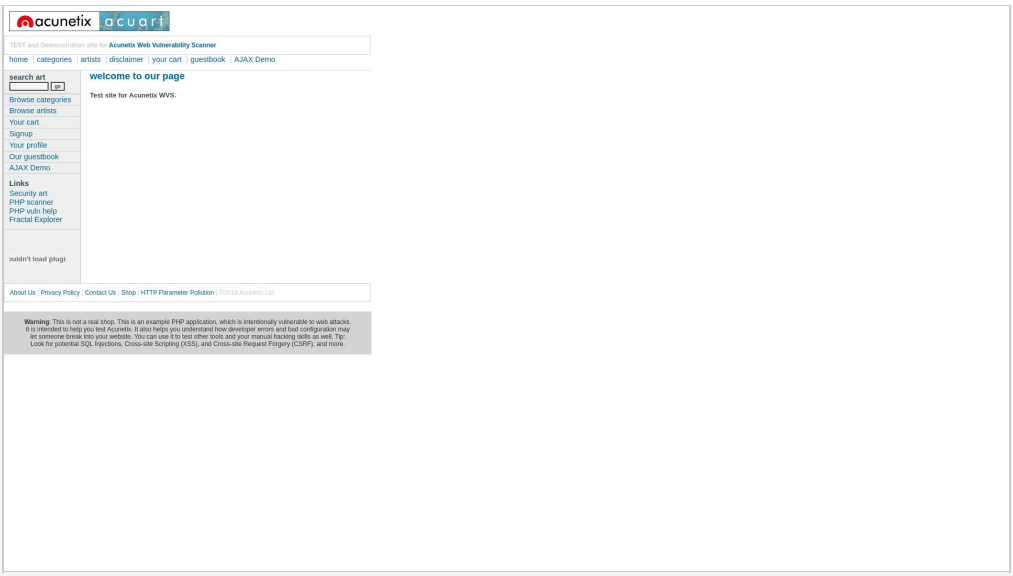



Figure 3. Website Screenshot

## Interesting files found

UNCONFIRMED

| URL | Page Title | Page Size | Summary |
|---|---|---|---|
| http://testphp.vulnweb.com/admin/ | Index of /admin | 262 B | This might be interesting. |
| http://testphp.vulnweb.com/images/ | Index of /image | 377 B | Directory indexing found. |
| http://testphp.vulnweb.com/login.php | login page | 5.39 KB | Admin login page/section found. |

Details

**Risk description:**
The risk is that these files/folders usually contain sensitive information which may help attackers to mount further attacks against the server. Manual validation is required.

**Recommendation:**
We recommend you to analyze if the mentioned files/folders contain any sensitive information and restrict their access according to the business purposes of the application.

**Classification:**
CWE : CWE-200
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Enumerable Parameter

UNCONFIRMED

| URL | Method | Vulnerable Parameter | Evidence |
|---|---|---|---|
| http://testphp.vulnweb.com/artists.php | GET | artist (Query Parameter) | The **artist query parameter** appears to contain an enumerable numeric part. We modified its initial value **3** to **4** and the two responses were **77%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability. Request / Response |
| http://testphp.vulnweb.com/hpp | GET | pp (Query Parameter) | The **pp query parameter** appears to contain an enumerable numeric part. We modified its initial value **12** to **11** and the two responses were **99%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability. Request / Response |
| http://testphp.vulnweb.com/hpp/params.php | GET | pp (Query Parameter) | The **pp query parameter** appears to contain an enumerable numeric part. We modified its initial value **12** to **11** and the two responses were **75%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability. Request / Response |

| | | | |
|---|---|---|---|
| http://testphp.vulnweb.com/listproducts.php | GET | artist (Query Parameter) | The **artist query parameter** appears to contain an enumerable numeric part. We modified its initial value **3** to **2** and the two responses were **91%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability.<br>Request / Response |
| http://testphp.vulnweb.com/listproducts.php | GET | cat (Query Parameter) | The **cat query parameter** appears to contain an enumerable numeric part. We modified its initial value **3** to **2** and the two responses were **89%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability.<br>Request / Response |
| http://testphp.vulnweb.com/product.php | GET | pic (Query Parameter) | The **pic query parameter** appears to contain an enumerable numeric part. We modified its initial value **2** to **1** and the two responses were **99%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability.<br>Request / Response |

Details

**Risk description:**
The vulnerability allows attackers to brute-force parameter values to uncover and access unauthorized resources and functionalities.

**Recommendation:**
Ensure that parameter values would not reveal sensitive information and that the application properly checks the user's authorization to access the resource. Also, the resource IDs should not be predictable.

**References:**
Testing for Insecure Direct Object References

**Classification:**
CWE : CWE-284
OWASP Top 10 - 2017 : A5 - Broken Access Control
OWASP Top 10 - 2021 : A1 - Broken Access Control

## Error message containing sensitive information

UNCONFIRMED

| URL | Method | Parameters | Evidence |
|---|---|---|---|
| http://testphp.vulnweb.com/listproducts.php | GET | **Query:**<br>cat=https://pentest-tools.com/file.txt<br>**Headers:**<br>User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 | Error message **You have an error in your SQL syntax** found in:<br>`e="content_rgn" -->\n<div id="content">\n\tError: You have an error in your SQL syntax; check the manual that corresponds to your MySQL`<br>Request / Response |

Details

**Risk description:**
The risk is that an attacker may use the contents of error messages to help launch another, more focused attack. For example, an attempt to exploit a path traversal weakness (CWE-22) might yield the full pathname of the installed application.

**Recommendation:**
It is recommended treating all exceptions of the application flow. Ensure that error messages only contain minimal details.

**Classification:**
CWE : CWE-209
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A4 - Insecure Design

## Login Interface Found

CONFIRMED

| URL | Evidence |
|---|---|

| | |
|---|---|
| http://testphp.vulnweb.com/login.php | `<input name="uname" size="20" style="width:120px;" type="text"/>`<br>`<input name="pass" size="20" style="width:120px;" type="password"/>`<br>`<input style="width:75px;" type="submit" value="login"/>`<br><br>Request / Response |
| http://testphp.vulnweb.com/signup.php | `<input name="uemail" style="width:200px" type="text"/>`<br>`<input name="upass" style="width:200px" type="password"/>`<br>`<input name="signup" type="submit" value="signup"/>`<br><br>Request / Response |

Details

**Risk description:**
The risk is that an attacker could use this interface to mount brute force attacks against known passwords and usernames combinations leaked throughout the web.

**Recommendation:**
Ensure each interface is not bypassable using common knowledge of the application or leaked credentials using occasional password audits.

**References:**
https://pentest-tools.com/network-vulnerability-scanning/password-auditor
http://capec.mitre.org/data/definitions/16.html

**Screenshot:**

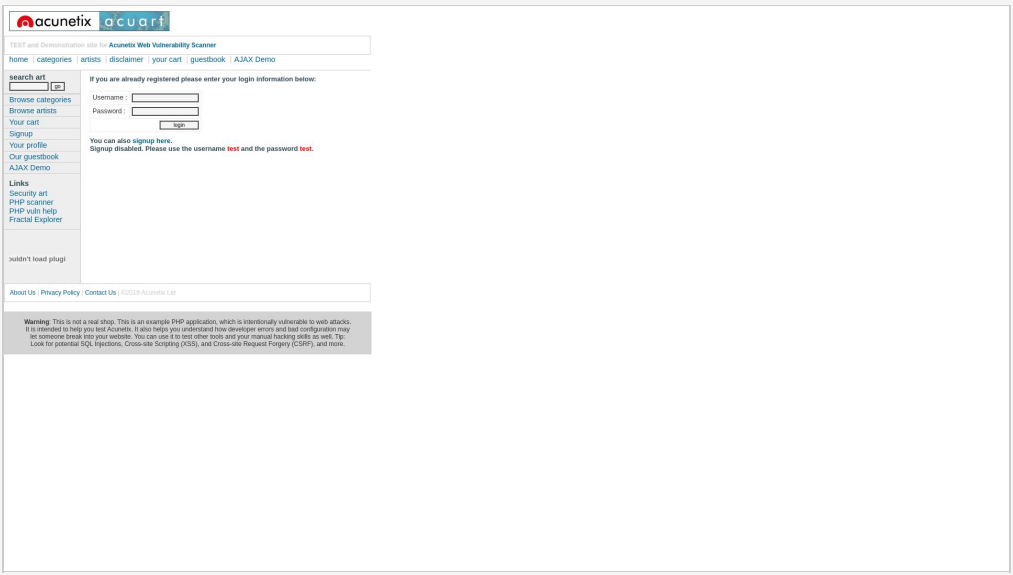



**Figure 4.** Login Interface

## Security.txt file is missing

CONFIRMED

| URL |
|---|
| Missing: http://testphp.vulnweb.com/.well-known/security.txt |

Details

**Risk description:**
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

**Recommendation:**
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

**References:**
https://securitytxt.org/

**Classification:**
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Spider results

| URL | Method | Parameters | Page Title | Page Size | Status Code |
|---|---|---|---|---|---|
| http://testphp.vulnweb.com/ | GET | | Home of Acunetix Art | 4.84 KB | 200 |
| http://testphp.vulnweb.com/AJAX | GET | | ajax test | 4.14 KB | 200 |
| http://testphp.vulnweb.com/Flash | GET | | Index of /Flash/ | 371 B | 200 |
| http://testphp.vulnweb.com/Flash/add.swf | GET | | | 16.32 KB | 200 |
| http://testphp.vulnweb.com/Mod_Rewrite_Shop | GET | | | 975 B | 200 |
| http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3 | GET | | 404 Not Found | 555 B | 404 |
| http://testphp.vulnweb.com/Mod_Rewrite_Shop/images | GET | | Index of /Mod_Rewrite_Shop/images/ | 513 B | 200 |
| http://testphp.vulnweb.com/admin | GET | | Index of /admin/ | 262 B | 200 |
| http://testphp.vulnweb.com/artists.php | GET | | artists | 5.2 KB | 200 |
| http://testphp.vulnweb.com/cart.php | POST | **Body:** addcart=2 price=800 | you cart | 4.79 KB | 200 |
| http://testphp.vulnweb.com/categories.php | GET | | picture categories | 5.97 KB | 200 |
| http://testphp.vulnweb.com/disclaimer.php | GET | | disclaimer | 5.39 KB | 200 |
| http://testphp.vulnweb.com/guestbook.php | GET | | guestbook | 5.26 KB | 200 |
| http://testphp.vulnweb.com/guestbook.php | POST | **Body:** name=anonymous user submit=add message text=1d3d2d231d2dd4 | guestbook | 5.29 KB | 200 |
| http://testphp.vulnweb.com/hpp | GET | | HTTP Parameter Pollution Example | 203 B | 200 |
| http://testphp.vulnweb.com/hpp/params.php | GET | **Query:** aaaa/=submit | | 0 | 200 |
| http://testphp.vulnweb.com/hpp/params.php | GET | **Query:** p=valid pp=12 | | 7 B | 200 |
| http://testphp.vulnweb.com/hpp | GET | **Query:** pp=12 | HTTP Parameter Pollution Example | 383 B | 200 |
| http://testphp.vulnweb.com/listproducts.php | GET | **Query:** artist=3 | pictures | 4.59 KB | 200 |
| http://testphp.vulnweb.com/listproducts.php | GET | **Query:** cat=2 | pictures | 5.19 KB | 200 |
| http://testphp.vulnweb.com/privacy.php | GET | | | 16 B | 404 |

| | | | | | |
|---|---|---|---|---|---|
| http://testphp.vulnweb.com/search.php | GET | **Query:**<br>test=query | search | 4.62 KB | 200 |
| http://testphp.vulnweb.com/search.php | POST | **Query:**<br>test=query<br>**Body:**<br>goButton=go<br>searchFor=1d3d2d231d2dd4 | search | 4.67 KB | 200 |
| http://testphp.vulnweb.com/secured | GET | | | 0 | 200 |
| http://testphp.vulnweb.com/secured/newuser.php | GET | | add new user | 415 B | 200 |
| http://testphp.vulnweb.com/secured/newuser.php | POST | **Body:**<br>signup=signup<br>uaddress=uaddress<br>ucc=1d3d2d231d2dd4<br>uemail=1d3d2d231d2dd4<br>upass=Secure123456$<br>upass2=Secure123456$<br>uphone=1d3d2d231d2dd4<br>urname=1d3d2d231d2dd4<br>uuname=1d3d2d231d2dd4 | add new user | 806 B | 200 |
| http://testphp.vulnweb.com/signup.php | GET | | signup | 5.89 KB | 200 |
| http://testphp.vulnweb.com/userinfo.php | POST | **Body:**<br>pass=Secure123456$<br>uname=1d3d2d231d2dd4 | login page | 5.39 KB | 200 |
| http://testphp.vulnweb.com/AJAX/index.php | GET | | ajax test | 4.14 KB | 200 |
| http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details | GET | | 404 Not Found | 555 B | 404 |
| http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer | GET | | 404 Not Found | 555 B | 404 |
| http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink | GET | | 404 Not Found | 555 B | 404 |
| http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1 | GET | | 404 Not Found | 555 B | 404 |
| http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech | GET | | 404 Not Found | 555 B | 404 |
| http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2 | GET | | 404 Not Found | 555 B | 404 |
| http://testphp.vulnweb.com/URLStr | GET | | 404 Not Found | 555 B | 404 |
| http://testphp.vulnweb.com/artists.php | GET | **Query:**<br>artist=1 | artists | 6.1 KB | 200 |
| http://testphp.vulnweb.com/cart.php | GET | | you cart | 4.79 KB | 200 |
| http://testphp.vulnweb.com/images | GET | | Index of /images/ | 377 B | 200 |
| http://testphp.vulnweb.com/index.php | GET | | Home of Acunetix Art | 4.84 KB | 200 |

| | | | | | |
|---|---|---|---|---|---|
| http://testphp.vulnweb.com/login.php | GET | | login page | 5.39 KB | 200 |
| http://testphp.vulnweb.com/product.php | GET | **Query:** pic=6 | picture details | 6.3 KB | 200 |
| http://testphp.vulnweb.com/userinfo.php | GET | | login page | 5.39 KB | 200 |

Details

**Risk description:**
The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

**Recommendation:**
We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

**References:**
All the URLs the scanner found, including duplicates (available for 90 days after the scan date)

## Cloud Hosted URLs

| URL | Cloud Provider | Found at URL |
|---|---|---|
| http://testphp.vulnweb.com/AJAX | AWS | http://testphp.vulnweb.com/ |

Details

**Risk description:**
The risk is that publicly accessible web addresses hosted in the cloud can expose sensitive information. If access to these resources is not carefully configured, it makes it easier for attackers to gain unauthorized access and cause data breaches.

**Recommendation:**
We recommend you to implement strong access controls and conduct regular security checks to protect these URLs. Ensure compliance with best practices to protect sensitive data.

## website is accessible.

## Nothing was found for robots.txt file.

## Outdated JavaScript libraries were merged into server-side software vulnerabilities.

## Nothing was found for use of untrusted certificates.

## Nothing was found for enabled HTTP debug methods.

## Nothing was found for sensitive files.

## Nothing was found for administration consoles.

## Nothing was found for information disclosure.

## Nothing was found for software identification.

Nothing was found for enabled HTTP OPTIONS method.

Nothing was found for debug messages.

Nothing was found for code comments.

Nothing was found for missing HTTP header - Strict-Transport-Security.

Nothing was found for domain too loose set for cookies.

Nothing was found for mixed content between HTTP and HTTPS.

Nothing was found for internal error code.

Nothing was found for HttpOnly flag of cookie.

Nothing was found for Secure flag of cookie.

Nothing was found for Server Side Request Forgery.

Nothing was found for Open Redirect.

Nothing was found for Exposed Backup Files.

Nothing was found for unsafe HTTP header Content Security Policy.

Nothing was found for OpenAPI files.

Nothing was found for file upload.

## Scan coverage information

### List of tests performed (39/39)

- Starting the scan...
- Checking for missing HTTP header - Content Security Policy...
- Checking for missing HTTP header - X-Content-Type-Options...
- Checking for missing HTTP header - Referrer...
- Checking for secure communication...
- Spidering target...
- Scanning for cloud URLs on target...
- Checking for directory listing...

- Checking for login interfaces...
- Checking for website technologies...
- Checking for vulnerabilities of server-side software...
- Checking for client access policies...
- Checking for robots.txt file...
- Checking for absence of the security.txt file...
- Checking for outdated JavaScript libraries...
- Checking for use of untrusted certificates...
- Checking for enabled HTTP debug methods...
- Checking for sensitive files...
- Checking for administration consoles...
- Checking for interesting files... (this might take a few hours)
- Checking for Insecure Direct Object Reference...
- Checking for error messages...
- Checking for information disclosure... (this might take a few hours)
- Checking for software identification...
- Checking for enabled HTTP OPTIONS method...
- Checking for debug messages...
- Checking for code comments...
- Checking for missing HTTP header - Strict-Transport-Security...
- Checking for domain too loose set for cookies...
- Checking for mixed content between HTTP and HTTPS...
- Checking for internal error code...
- Checking for HttpOnly flag of cookie...
- Checking for Secure flag of cookie...
- Checking for Server Side Request Forgery...
- Checking for Open Redirect...
- Checking for Exposed Backup Files...
- Checking for unsafe HTTP header Content Security Policy...
- Checking for OpenAPI files...
- Checking for file upload...

### Scan parameters

| | |
|---|---|
| Target: | http://testphp.vulnweb.com/ |
| Scan type: | Light |
| Authentication: | False |

### Scan stats

| | |
|---|---|
| Unique Injection Points Detected: | 44 |
| URLs spidered: | 71 |
| Total number of HTTP requests: | 15859 |
| Average time until a response was received: | 9ms |
| Total number of HTTP request errors: | 42 |