

Website Vulnerability Scanner Report



See what the FULL scanner can do



Perform in-depth website scanning and discover high risk vulnerabilities.

Testing areas	Light scan	Full scan
Website fingerprinting	✓	✓
Version-based vulnerability detection	✓	✓
Common configuration issues	✓	✓
SQL injection	✗	✓
Cross-Site Scripting	✗	✓
Local/Remote File Inclusion	✗	✓
Remote command execution	✗	✓
Discovery of sensitive files	✗	✓

Get a PRO Account to unlock the full capabilities of this scanner!

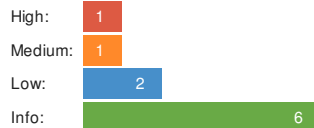
✓ <http://testphp.vulnweb.com>

Summary

Overall risk level:

High

Risk ratings:



Scan information:

Start time: 2019-07-24 14:11:20 UTC+03
Finish time: 2019-07-24 14:11:42 UTC+03
Scan duration: 22 sec
Tests performed: 10/10
Scan status: **Finished**

Findings

Insecure client access policy

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

▼ Details

Risk description:

The `crossdomain.xml` file controls the access of externally hosted Flash scripts to this website. 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.

Recommendation:

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

More information about this issue:

<http://blog.h3xstream.com/2015/04/crossdomainxml-beware-of-wildcards.html>

Communication is not secure

http://testphp.vulnweb.com/

Details

Risk description:

The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to 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.

Server software and technology found

Software / Version	Category
 Nginx 1.4.1	Web Servers
 PHP 5.3.10	Programming Languages
 DreamWeaver	Editors

Details

Risk description:

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 permit the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

More information about this issue:

[https://www.owasp.org/index.php/Fingerprint_Web_Server_\(OTG-INFO-002\)](https://www.owasp.org/index.php/Fingerprint_Web_Server_(OTG-INFO-002)).

Missing HTTP security headers

HTTP Security Header	Header Role	Status
X-Frame-Options	Protects against Clickjacking attacks	Not set
X-XSS-Protection	Mitigates Cross-Site Scripting (XSS) attacks	Not set
X-Content-Type-Options	Prevents possible phishing or XSS attacks	Not set

Details

Risk description:

Because the **X-Frame-Options** header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:

<https://www.owasp.org/index.php/Clickjacking>

The **X-XSS-Protection** HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

The HTTP **X-Content-Type-Options** header is addressed to Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:

We recommend you to add the **X-Frame-Options** HTTP response header to every page that you want to be protected against Clickjacking attacks.

More information about this issue:

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

We recommend setting the **X-XSS-Protection** header to "X-XSS-Protection: 1; mode=block".

More information about this issue:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection>

We recommend setting the `X-Content-Type-Options` header to "X-Content-Type-Options: nosniff".


More information about this issue:

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

 No vulnerabilities found for server-side software

 No security issue found regarding HTTP cookies

 Robots.txt file not found

 Directory listing not found (quick scan)

 No password input found (auto-complete test)

 No password input found (clear-text submission test)

Scan coverage information

List of tests performed (10/10)

- ✔ Fingerprinting the server software and technology...
- ✔ Checking for vulnerabilities of server-side software...
- ✔ Analyzing the security of HTTP cookies...
- ✔ Analyzing HTTP security headers...
- ✔ Checking for secure communication...
- ✔ Checking robots.txt file...
- ✔ Checking client access policies...
- ✔ Checking for directory listing (quick scan)...
- ✔ Checking for password auto-complete (quick scan)...
- ✔ Checking for clear-text submission of passwords (quick scan)...

Scan parameters

Website URL: http://testphp.vulnweb.com
Scan type: Light
Authentication: False
