CyberNauts CYBERSECURITY LEARNING CIRCLE

TASK - 0 Report 💻

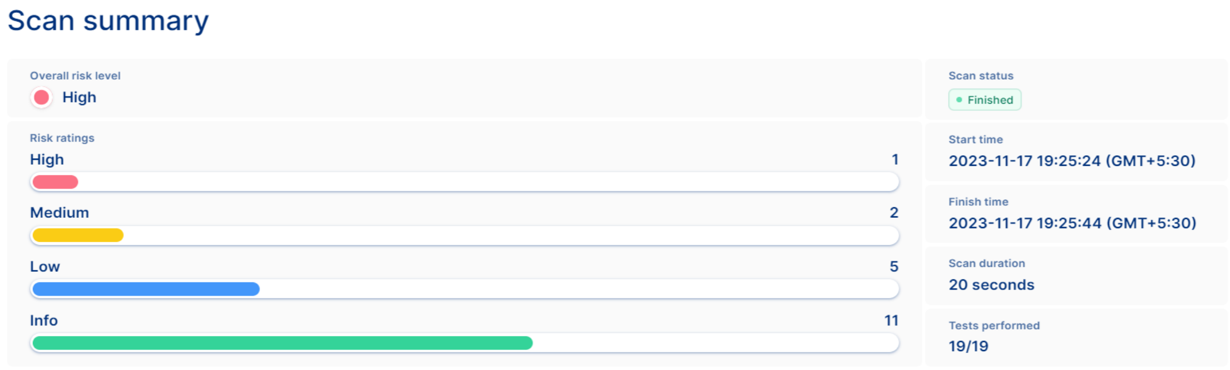
#Team_Members

● Tom Sibu	-	Tom Sibu
● Edwin Joseph	-	Edwin Joseph
● Alex George	-	kulampallil.alex@gmail.com
● Andrea Tresa Tom	-	andreatresa2004@gmail.com
● Aleena V Sunil	-	aleena6187@gmail.com

#Problem Description

Conduct a *web application vulnerability assessment on http://testphp.vulnweb.com/* and create a report documenting identified vulnerabilities and their potential impact.

#Report



Scan summary

Overall risk level
● High

Risk ratings

Rating	Count
High	1
Medium	2
Low	5
Info	11

Scan status
● Finished

Start time
2023-11-17 19:25:24 (GMT+5:30)

Finish time
2023-11-17 19:25:44 (GMT+5:30)

Scan duration
20 seconds

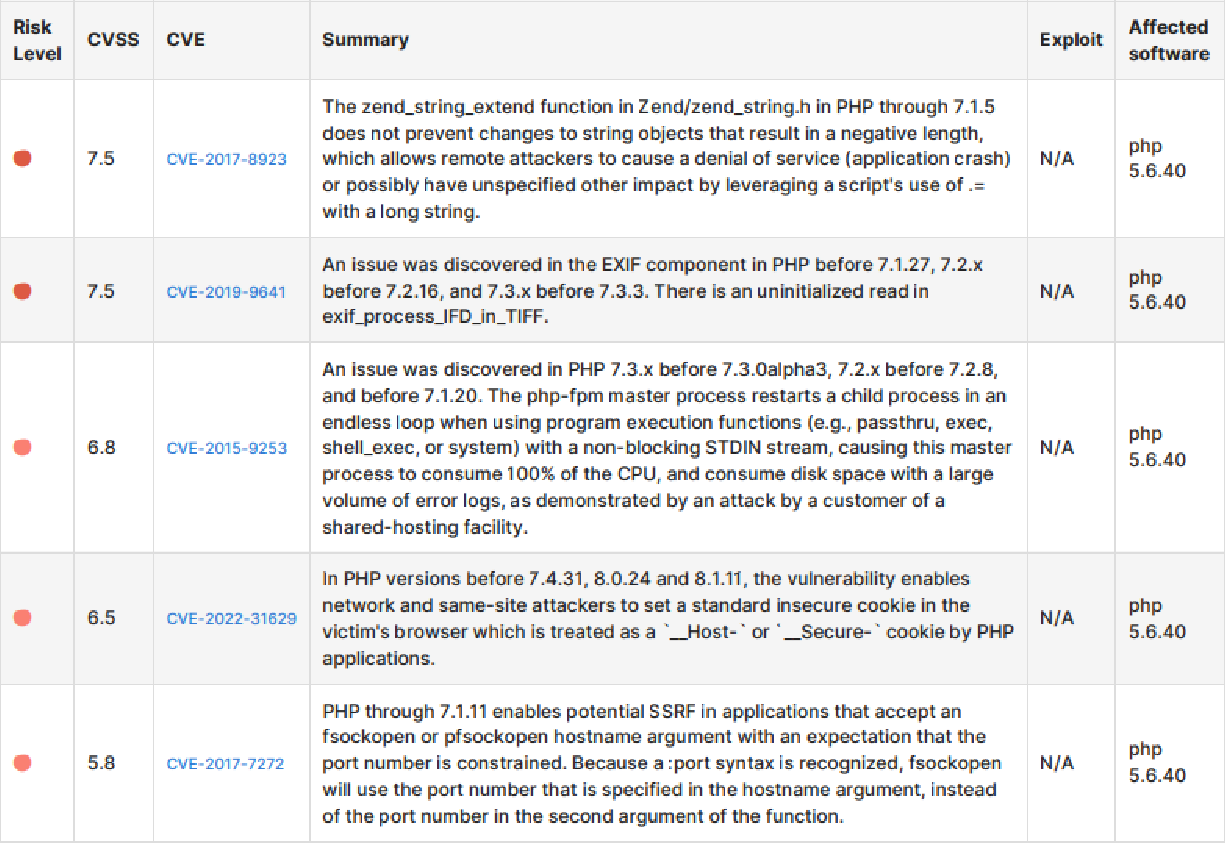
Tests performed
19/19

Performed the vulnerability testing on the website : testphp.vulnweb.com, using an online vulnerability scanner.
Found 1 : High, 2: Medium and 5: Low level vulnerabilities.
Overall vulnerability is high. Action recommended.

#Findings

Vulnerabilities found for server-side software

UNCONFIRMED

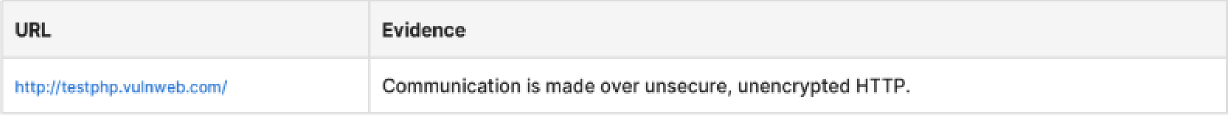


Risk Level	CVSS	CVE	Summary	Exploit	Affected software
●	7.5	CVE-2017-8923	The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.	N/A	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.	N/A	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.	N/A	php 5.6.40
●	6.5	CVE-2022-31629	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications.	N/A	php 5.6.40
●	5.8	CVE-2017-7272	PHP through 7.1.11 enables potential SSRF in applications that accept an fsockopen or pfsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.	N/A	php 5.6.40

- **Risk Description**
  These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. 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 - 2013 : A9 - Using Components with Known Vulnerabilities
  OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities

Communication is not secure

CONFIRMED



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

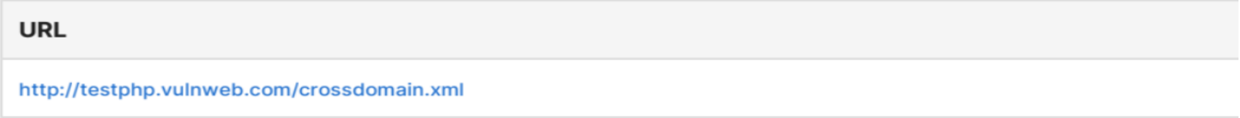
- **Risk description**
  The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who

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.
- **Classification**
  CWE : CWE-311
  OWASP Top 10 - 2013 : A6 - Sensitive Data Exposure
  OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure

Insecure client access policy

CONFIRMED

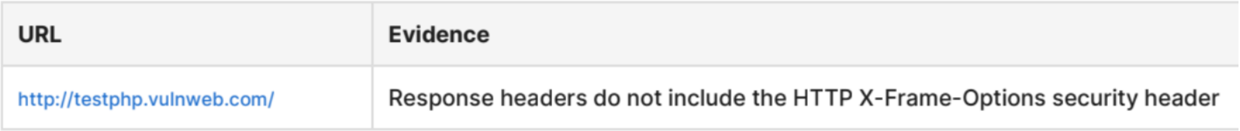


URL
http://testphp.vulnweb.com/crossdomain.xml

- **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.
  The clientaccesspolicy.xml file specifies that other websites can read content from this website - which is normally denied by the Same Origin Policy. If the allowed domains are too permissive (ex. wildcard) 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 - 2013 : A5 - Security Misconfiguration
  OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header :X-frame-options

CONFIRMED

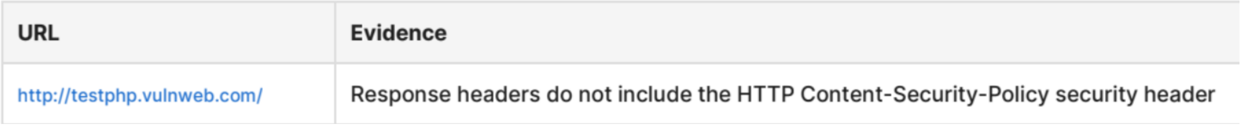


URL	Evidence
http://testphp.vulnweb.com/	Response headers do not include the HTTP X-Frame-Options security header

- **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 consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here: https://owasp.org/www-community/attacks/Clickjacking
- **Recommendation**
  We recommend you to add the X-Frame-Options HTTP header with the values DENY or SAMEORIGIN to every page that you want to be protected against Clickjacking attacks.
- **References**
  https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html
- **Classification**
  CWE : CWE-693
  OWASP Top 10 - 2013 : A5 - Security Misconfiguration
  OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header :Content-Security-Policy

CONFIRMED

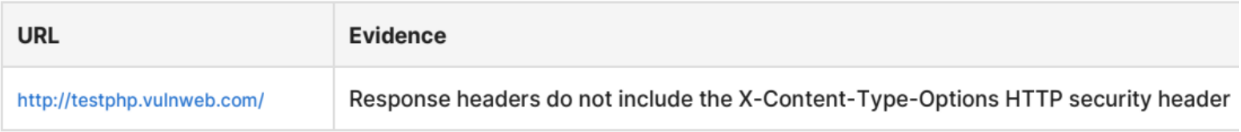


URL	Evidence
http://testphp.vulnweb.com/	Response headers do not include the HTTP Content-Security-Policy security header

- **Risk description**
  The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). 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 - 2013 : A5 - Security Misconfiguration
  OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: X-Content-Type-Options

CONFIRMED

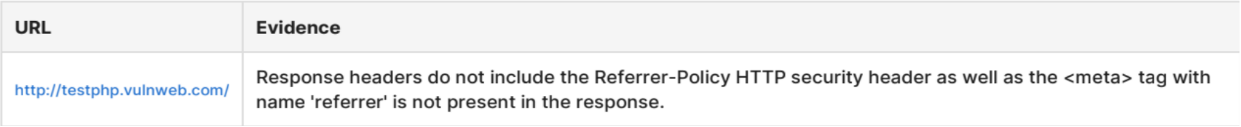


URL	Evidence
http://testphp.vulnweb.com/	Response headers do not include the X-Content-Type-Options HTTP security header

- **Risk description**
  The HTTP header X-Content-Type-Options is addressed to the 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 setting the X-Content-Type-Options header such as
  X-Content-Type-Options: nosniff .
- **Reference**:
  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
- **Classification**
  CWE : CWE-693
  OWASP Top 10 - 2013 : A5 - Security Misconfiguration
  OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED



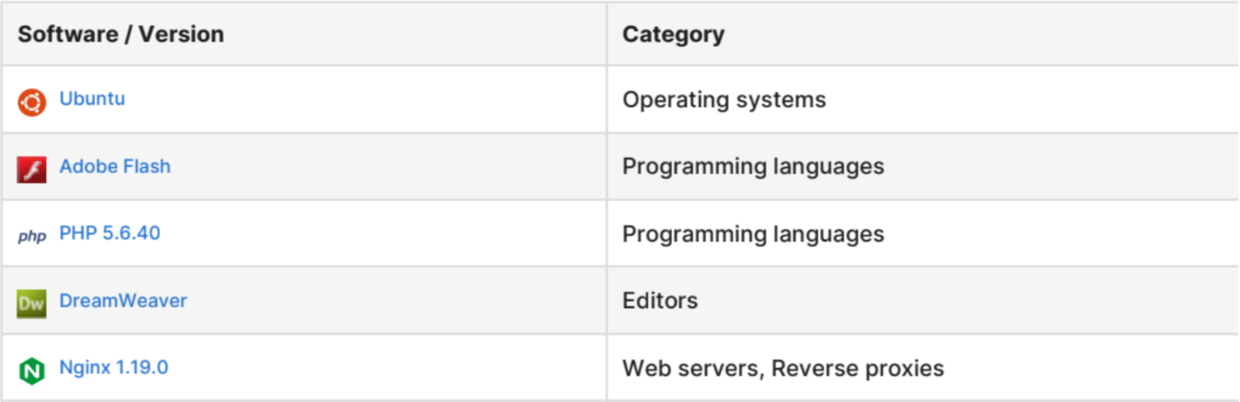
URL	Evidence
http://testphp.vulnweb.com/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.

- **Risk description**
  The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application.
  For instance, if a user visits the web page "http://example.com/pricing/" and it 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 ReferrerPolicy 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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Server software and technology found

UNCONFIRMED

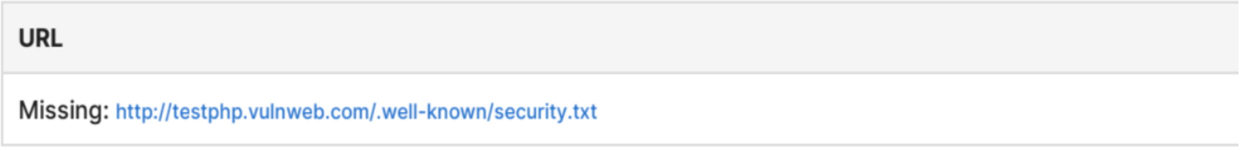


Software / Version	Category
Ubuntu	Operating systems
Adobe Flash	Programming languages
PHP 5.6.40	Programming languages
DreamWeaver	Editors
Nginx 1.19.0	Web servers, Reverse proxies

- **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 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 - 2013 : A5 - Security Misconfiguration
  OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Security.txt file is missing

CONFIRMED



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

- **Risk description**
  We have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid 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 - 2013 : A5 - Security Misconfiguration
  OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Website is accessible

Nothing was found for robots.txt file

Nothing was found for use of untrusted certificates

Nothing was found for enabled HTTP debug methods

Nothing was found for directory listing

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

Nothing was found for domain too loose set for cookies

Nothing was found for HttpOnly flag of cookie

Nothing was found for Secure flag of cookie

Nothing was found for unsafe HTTP header Content Security Policy

#Remediation

1. **Use Parameterized Statements or Prepared Statements**
   - Use parameterized queries or prepared statements provided by your programming language or ORM (Object-Relational Mapping) library.
   - Parameterized queries ensure that user input is treated as data, not as executable code.
2. **Input Validation and Sanitization**
   - Implement strict input validation on both client and server sides to ensure that user inputs match expected formats.
   - Sanitize user inputs by removing or encoding special characters that may be interpreted as SQL code.
3. **Least Privilege Principle**
   - Restrict database user permissions to the minimum required for normal operation.
   - Avoid using accounts with excessive privileges in your application.

4. **Stored Procedures**
   - Use stored procedures to encapsulate and control database operations.
   - This reduces the risk of injection by not allowing direct execution of arbitrary SQL code.
5. **ORMs (Object-Relational Mapping)**
   - If possible, use ORM frameworks that automatically handle SQL query generation and parameterization.
   - ORM frameworks can provide an additional layer of security.
6. **Web Application Firewalls (WAF)**
   - Implement a Web Application Firewall to monitor and filter HTTP traffic between a web application and the Internet.
   - WAFs can help detect and block SQL injection attempts.
7. **Error Handling**
   - Customize error messages to provide minimal information to users in case of an error.
   - Log detailed error messages internally for the development team.
8. **Security Audits and Code Reviews**
   - Regularly perform security audits on your application's codebase.
   - Conduct thorough code reviews to identify and fix potential vulnerabilities.
9. **Update and Patch Software**
   - Keep database systems, web servers, and application frameworks up-to-date with the latest security patches.
   - Regularly check for updates and security announcements.
10. **Monitoring and Intrusion Detection**
    - Implement real-time monitoring and intrusion detection systems to identify and respond to suspicious activities.
    - Set up alerts for unusual database queries or patterns.

By implementing a combination of these measures, you can significantly reduce the risk of SQL injection vulnerabilities in your application and enhance its overall security posture. Regularly reassess and update your security measures as new threats and best practices emerge.

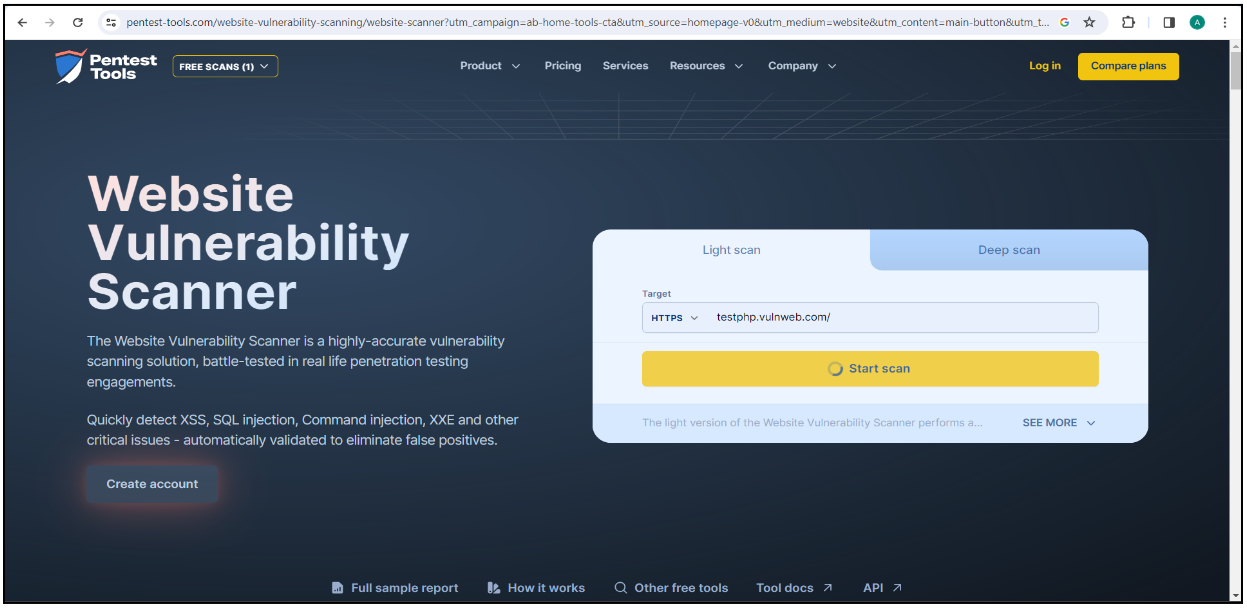
#Scans Performed

List of tests performed (19/19)

- ☑ Checking for website accessibility...
- ☑ Checking for missing HTTP header - X-Frame-Options...
- ☑ Checking for missing HTTP header - Content Security Policy...
- ☑ Checking for missing HTTP header - X-Content-Type-Options...
- ☑ Checking for secure communication...
- ☑ Checking for missing HTTP header - Referrer...
- ☑ 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 use of untrusted certificates...
- ☑ Checking for enabled HTTP debug methods...
- ☑ Checking for directory listing...
- ☑ Checking for missing HTTP header - Strict-Transport-Security...
- ☑ Checking for domain too loose set for cookies...
- ☑ Checking for HttpOnly flag of cookie...
- ☑ Checking for Secure flag of cookie...
- ☑ Checking for unsafe HTTP header Content Security Policy...

#Screenshots



pentest-tools.com/website-vulnerability-scanning/website-scanner?utm_campaign=ab-home-tools-cta&utm_source=homepage-v0&utm_medium=website&utm_content=main-button&utm_t...

Website Vulnerability Scanner

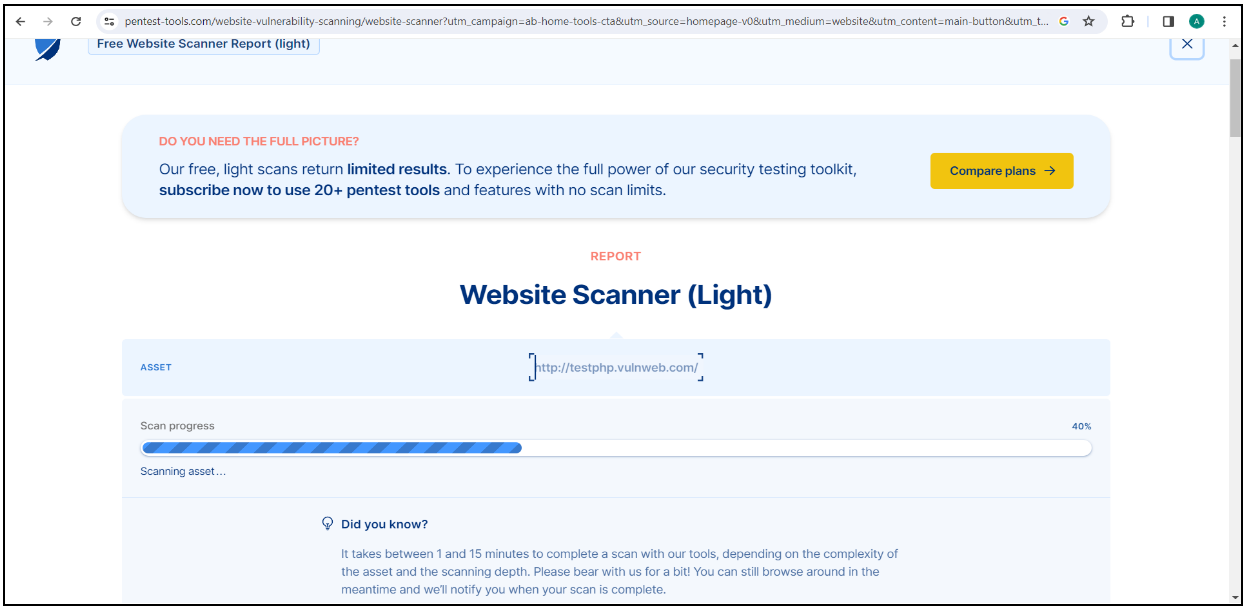
The Website Vulnerability Scanner is a highly-accurate vulnerability scanning solution, battle-tested in real life penetration testing engagements.

Quickly detect XSS, SQL injection, Command injection, XXE and other critical issues - automatically validated to eliminate false positives.

Target: HTTPS testphp.vulnweb.com/

The light version of the Website Vulnerability Scanner performs a...

The above image depicts the website of Pentest tools, a penetration testing toolkit, founded by Adrian Furtuna.



pentest-tools.com/website-vulnerability-scanning/website-scanner?utm_campaign=ab-home-tools-cta&utm_source=homepage-v0&utm_medium=website&utm_content=main-button&utm_t...

Free Website Scanner Report (light)

DO YOU NEED THE FULL PICTURE?

Our free, light scans return **limited results**. To experience the full power of our security testing toolkit, **subscribe now to use 20+ pentest tools** and features with no scan limits.

REPORT

Website Scanner (Light)

ASSET http://testphp.vulnweb.com/

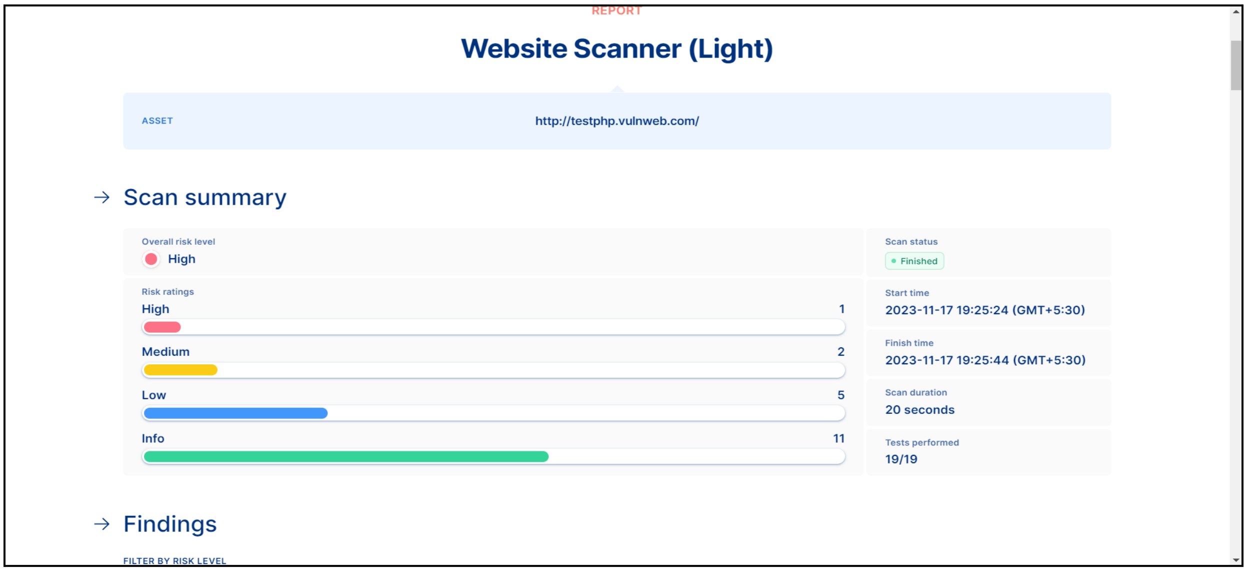
Scan progress 40%

Scanning asset…

Did you know?

It takes between 1 and 15 minutes to complete a scan with our tools, depending on the complexity of the asset and the scanning depth. Please bear with us for a bit! You can still browse around in the meantime and we'll notify you when your scan is complete.

The above image shows the vulnerability scanner performing the above mentioned scans on the site http://testphp.vulnweb.com/



REPORT

Website Scanner (Light)

ASSET http://testphp.vulnweb.com/

→ Scan summary

Overall risk level

● High

Risk ratings

High	1
Medium	2
Low	5
Info	11

Scan status: Finished

Start time: 2023-11-17 19:25:24 (GMT+5:30)

Finish time: 2023-11-17 19:25:44 (GMT+5:30)

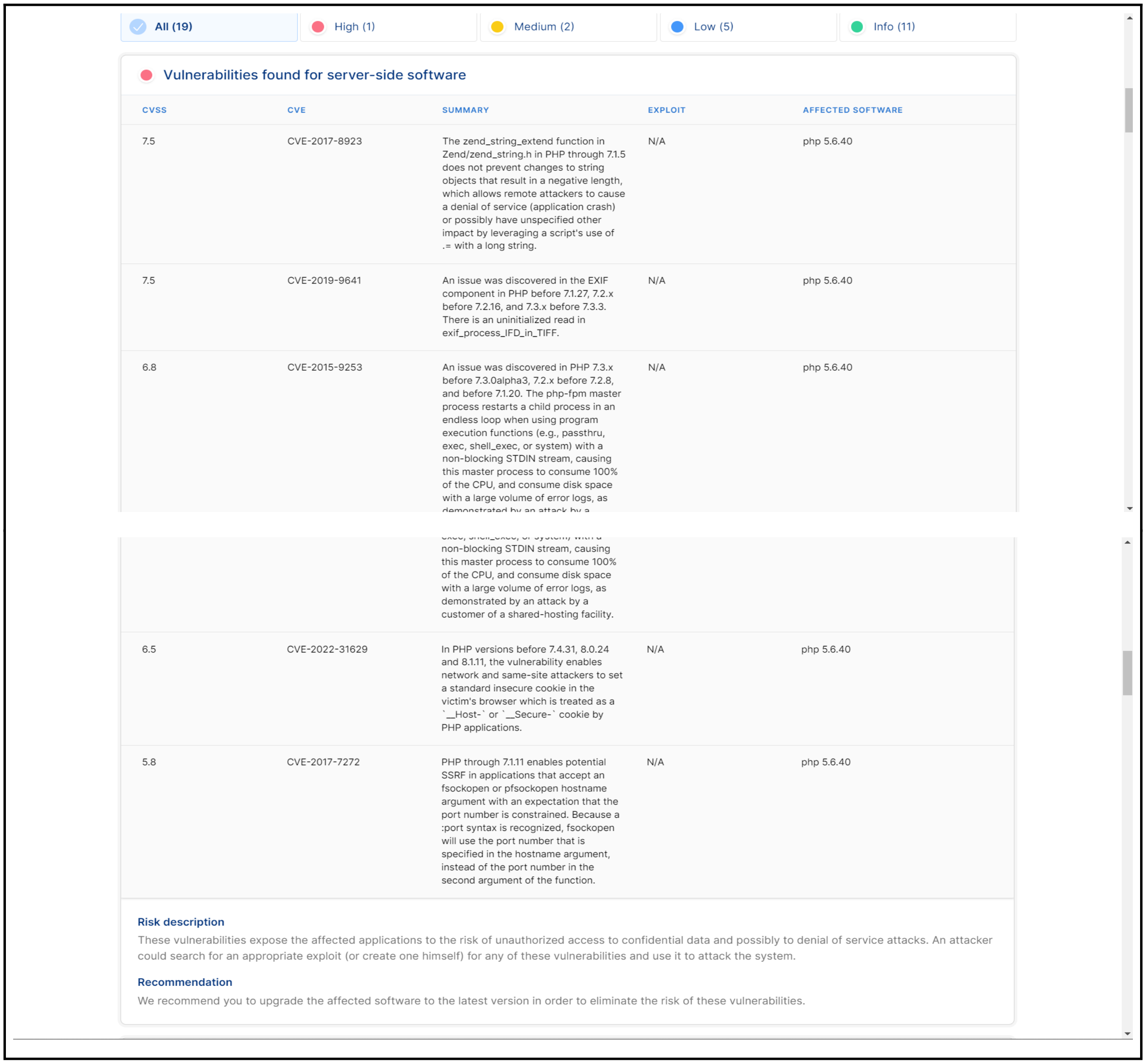
Scan duration: 20 seconds

Tests performed: 19/19

→ Findings

FILTER BY RISK LEVEL

The above image shows the light scan summary and the following two screenshots depicts the vulnerability reports.



✓ All (19) | ● High (1) | ● Medium (2) | ● Low (5) | ● Info (11)

● Vulnerabilities found for server-side software

CVSS	CVE	SUMMARY	EXPLOIT	AFFECTED SOFTWARE
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.	N/A	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.	N/A	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.	N/A	php 5.6.40
6.5	CVE-2022-31629	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a \`__Host-\` or \`__Secure-\` cookie by PHP applications.	N/A	php 5.6.40
5.8	CVE-2017-7272	PHP through 7.1.11 enables potential SSRF in applications that accept an fsockopen or pfsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.	N/A	php 5.6.40

Risk description

These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. 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.