ZAP by Checkmarx Scanning Report

Generated with ZAP on Sun 1 Jun 2025, at 16:25:51

ZAP Version: 2.16.1

ZAP by Checkmarx

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- http://testphp.vulnweb.com

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	1 (10.0%)	0 (0.0%)	0 (0.0%)	1 (10.0%)
	Medium	0 (0.0%)	1 (10.0%)	1 (10.0%)	1 (10.0%)	3 (30.0%)
	Low	0 (0.0%)	1 (10.0%)	2 (20.0%)	0 (0.0%)	3 (30.0%)
	Informational	0 (0.0%)	0 (0.0%)	2 (20.0%)	1 (10.0%)	3 (30.0%)
	Total	0 (0.0%)	3 (30.0%)	5 (50.0%)	2 (20.0%)	10 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://testphp.vulnweb.com	1 (1)	3 (4)	3 (7)	3 (10)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Cross Site Scripting (DOM Based)	High	7 (70.0%)
Absence of Anti-CSRF Tokens	Medium	8 (80.0%)
Content Security Policy (CSP) Header Not Set	Medium	7 (70.0%)
Total		10

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	7 (70.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	8 (80.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	10 (100.0%)
X-Content-Type-Options Header Missing	Low	9 (90.0%)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	7 (70.0%)
Modern Web Application	Informational	2 (20.0%)
User Agent Fuzzer	Informational	48 (480.0%)
Total		10

Alerts

Risk=High, Confidence=High (1)

http://testphp.vulnweb.com (1)

Cross Site Scripting (DOM Based) (1)

▶ GET http://testphp.vulnweb.com#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e

Risk=Medium, Confidence=High (1)

http://testphp.vulnweb.com (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET http://testphp.vulnweb.com/

Risk=Medium, Confidence=Medium (1)

http://testphp.vulnweb.com (1)

Missing Anti-clickjacking Header (1)

▶ GET http://testphp.vulnweb.com/

Risk=Medium, Confidence=Low (1)

http://testphp.vulnweb.com (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://testphp.vulnweb.com/

Risk=Low, Confidence=High (1)

http://testphp.vulnweb.com (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

- GET http://testphp.vulnweb.com/

Risk=Low, Confidence=Medium (2)

http://testphp.vulnweb.com (2)

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

- GET http://testphp.vulnweb.com/

X-Content-Type-Options Header Missing (1)

- GET http://testphp.vulnweb.com/

Risk=Informational, Confidence=Medium (2)

http://testphp.vulnweb.com (2)

Modern Web Application (1)

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

User Agent Fuzzer (1)

- GET http://testphp.vulnweb.com/AJAX

Risk=Informational, Confidence=Low (1)

http://testphp.vulnweb.com (1)

Charset Mismatch (Header Versus Meta Content-Type Charset) (1)

▶ GET http://testphp.vulnweb.com/

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Cross Site Scripting (DOM Based)

Source raised by an active scanner (Cross Site Scripting (DOM Based))

CWE ID 79

WASC ID 8

Reference
- https://owasp.org/www-community/attacks/xss/
- https://cwe.mitre.org/data/definitions/79.html

Absence of Anti-CSRF Tokens

Source raised by a passive scanner (Absence of Anti-CSRF Tokens)

CWE ID 352

WASC ID 9

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
- https://cwe.mitre.org/data/definitions/352.html

Content Security Policy (CSP) Header Not Set

Source raised by a passive scanner (Content Security Policy (CSP) Header Not Set)

CWE ID 693

WASC ID 15

Reference

- https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://www.w3.org/TR/CSP/
- https://w3c.github.io/webappsec-csp/
- https://web.dev/articles/csp
- https://caniuse.com/#feat=contentsecuritypolicy
- https://content-security-policy.com/

Missing Anti-clickjacking Header

Source raised by a passive scanner (Anti-clickjacking Header)

CWE ID	1021
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
CWE ID	497
WASC ID	13
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework ▪ https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
WASC ID	13
Reference	▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens

- https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)

- https://www.troyhunt.com/shhh-dont-let-your-response-headers/

X-Content-Type-Options Header Missing

Source raised by a passive scanner (X-Content-Type-Options Header Missing)

CWE ID 693

WASC ID 15

Reference
- https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)

- https://owasp.org/www-community/Security_Headers

Charset Mismatch (Header Versus Meta Content-Type Charset)

Source raised by a passive scanner (Charset Mismatch)

CWE ID 436

WASC ID 15

Reference
- https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

Modern Web Application

Source raised by a passive scanner (Modern Web

Application)

User Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	▪ https://owasp.org/wstg