


ZAP Scanning Report2

Generated with  ZAP on Tue 12 Dec 2023, at 18:35:26

ZAP Version: 2.14.0

Contents

- [About this report](#)
 - [Report description](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=High, Confidence=High \(1\)](#)
 - [Risk=High, Confidence=Medium \(3\)](#)
 - [Risk=Medium, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(2\)](#)
- [Appendix](#)
 - [Alert types](#)

About this report

Report description

High & medium level vulnerabilities

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](#)

Excluded: [High](#), [Medium](#), [Low](#), [Informational](#)

Confidence levels

Included: [User Confirmed](#), [High](#), [Medium](#), [False Positive](#)

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				
Risk		User Confirmed	High	Medium	False Positive	Total
	High	0 (0.0%)	1 (14.3%)	3 (42.9%)	0 (0.0%)	4 (57.1%)
	Medium	0 (0.0%)	1 (14.3%)	2 (28.6%)	0 (0.0%)	3 (42.9%)
	Total	0 (0.0%)	2 (28.6%)	5 (71.4%)	0 (0.0%)	7 (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	
Site		High (= High)	Medium (>= Medium)
		4 (4)	3 (7)

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	4 (57.1%)
Cross Site Scripting (Reflected)	High	1 (14.3%)
SQL Injection	High	2 (28.6%)
SQL Injection - MySQL	High	2 (28.6%)
.htaccess Information Leak	Medium	1 (14.3%)
Content Security Policy (CSP) Header Not Set	Medium	51 (728.6%)
Missing Anti-clickjacking Header	Medium	47 (671.4%)
Total		7

Alerts

Risk=High, Confidence=High (1)

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

Cross Site Scripting (DOM Based) (1)

► GET [http://testphp.vulnweb.com/index.php#jaVaScRipt:/*-/*`/*\`/*'/*"/**/\(/* */oNcliCk=alert\(5397\) \)//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNlOAd=alert\(5397\)//>\x3e](http://testphp.vulnweb.com/index.php#jaVaScRipt:/*-/*`/*\`/*'/*)

Risk=High, Confidence=Medium (3)

<http://testphp.vulnweb.com> (3)

Cross Site Scripting (Reflected) (1)

► GET <http://testphp.vulnweb.com/listproducts.php?cat=%27%22%3Cimg+src%3Dx+onerror%3Dprompt%28%29%3E>

SQL Injection (1)

► GET <http://testphp.vulnweb.com/artists.php?artist=5-2>

SQL Injection - MySQL (1)

► GET <http://testphp.vulnweb.com/artists.php?artist=3>

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 (2)

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

[.htaccess Information Leak \(1\)](#)

- ▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess

[Missing Anti-clickjacking Header \(1\)](#)

- ▶ 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 (plugin ID: 40026)
CWE ID	79
WASC ID	8
Reference	<ul style="list-style-type: none">▪ http://projects.webappsec.org/Cross-Site-Scripting▪ https://cwe.mitre.org/data/definitions/79.html

Cross Site Scripting (Reflected)

Source	raised by an active scanner (plugin ID: 40012)
CWE ID	79
WASC ID	8
Reference	<ul style="list-style-type: none">▪ http://projects.webappsec.org/Cross-Site-Scripting▪ https://cwe.mitre.org/data/definitions/79.html

SQL Injection

Source	raised by an active scanner (plugin ID: 40018)
CWE ID	89
WASC ID	19
Reference	<ul style="list-style-type: none">▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL Injection - MySQL

Source	raised by an active scanner (plugin ID: 40019)
CWE ID	89
WASC ID	19
Reference	<ul style="list-style-type: none">▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

.htaccess Information Leak

Source	raised by an active scanner (plugin ID: 40032)
CWE ID	94
WASC ID	14
Reference	<ul style="list-style-type: none">▪ http://www.htaccess-guide.com/

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	<ul style="list-style-type: none">▪ 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▪ http://www.w3.org/TR/CSP/▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html▪ http://www.html5rocks.com/en/tutorials/security/content-security-policy/▪ http://caniuse.com/#feat=contentsecuritypolicy

- <http://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