ZAP Scanning Report

Generated with ZAP on Fri 20 May 2022, at 18:48:28

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%)	0 (0.0%)	2 (20.0%)	0 (0.0%)	2 (20.0%)
	Medium	0 (0.0%)	1 (10.0%)	2 (20.0%)	1 (10.0%)	4 (40.0%)
	Low	0 (0.0%)	0 (0.0%)	2 (20.0%)	0 (0.0%)	2 (20.0%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	2 (20.0%)	2 (20.0%)
	Total	0 (0.0%)	1 (10.0%)	6 (60.0%)	3 (30.0%)	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	2 (2)	4 (6)	2 (8)	2 (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 (Reflected)	High	16 (160.0%)
SQL Injection	High	7 (70.0%)
.htaccess Information Leak	Medium	7 (70.0%)
Absence of Anti-CSRF Tokens	Medium	39 (390.0%)
Content Security Policy (CSP) Header Not Set	Medium	48 (480.0%)
Missing Anti-clickjacking Header	Medium	45 (450.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	63 (630.0%)
X-Content-Type-Options Header Missing	Low	67 (670.0%)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	29 (290.0%)
Information Disclosure - Suspicious Comments	Informational	1 (10.0%)
Total		10

Alerts

Risk=High, Confidence=Medium (2)

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

Cross Site Scripting (Reflected) (1)

▶ POST http://testphp.vulnweb.com/guestbook.php

SQL Injection (1)

▶ POST http://testphp.vulnweb.com/secured/newuser.php

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/

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (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=Low (2)

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

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

▶ GET http://testphp.vulnweb.com/

Information Disclosure - Suspicious Comments (1)

▶ GET http://testphp.vulnweb.com/AJAX/index.php

Appendix

Alert types

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

Cross Site Scripting (Reflected)

Source	raised by an active scanner (Cross Site Scripting (Reflected))
CWE ID	79
WASC ID	8
Reference	▪ http://projects.webappsec.org/Cross-Site-Scripting ▪ http://cwe.mitre.org/data/definitions/79.html

SQL Injection

Source	raised by an active scanner (SQL Injection)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

.htaccess Information Leak

Source	raised by an active scanner (.htaccess Information Leak)
CWE ID	94
WASC ID	14
Reference	▪ http://www.htaccess-guide.com/

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://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 ▪ 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

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	200
WASC ID	13
Reference	- http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx - http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

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	- http://msdn.microsoft.com/en-

us/library/ie/gg622941%28v=vs.85%29.aspx

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

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13