ZAP Scanning Report Advanced

Generated with ZAP on Fri 5 Jan 2024, at 18:03:40

ZAP Version: 2.14.0

Contents

About this report

Report description

High and medium levell 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				
		User Confirmed	High	Medium	False Positive	Total
Risk	High	0 (0.0%)	1 (11.1%)	3 (33.3%)	0 (0.0%)	4 (44.4%)
	Medium	0 (0.0%)	1 (11.1%)	4 (44.4%)	0 (0.0%)	5 (55.6%)
	Total	0 (0.0%)	2 (22.2%)	7 (77.8%)	0 (0.0%)	9 (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)

		Risk	
		High (= High)	Medium (>= Medium)
Site	http://testphp.vulnweb.com	4 (4)	5 (9)

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	16 (177.8%)
Cross Site Scripting (Reflected)	High	14 (155.6%)
SQL Injection	High	8 (88.9%)
SQL Injection - MySQL	High	4 (44.4%)
.htaccess Information Leak	Medium	7 (77.8%)
Content Security Policy (CSP) Header Not Set	Medium	72 (800.0%)
Total		9

Alert type	Risk	Count
Directory Browsing	Medium	3 (33.3%)
Missing Anti-clickjacking Header	Medium	56 (622.2%)
XSLT Injection	Medium	2 (22.2%)
Total		9

Alerts

Risk=High, Confidence=High (1)

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

Cross Site Scripting (DOM Based) (1)

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

Risk=High, Confidence=Medium (3)

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

Cross Site Scripting (Reflected) (1)

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

SQL Injection (1)

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

SQL Injection - MySQL (1)

▶ POST http://testphp.vulnweb.com/search.php?test=query

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 (4)

http://testphp.vulnweb.com (4)

.htaccess Information Leak (1)

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

Directory Browsing (1)

▶ GET http://testphp.vulnweb.com/images/

Missing Anti-clickjacking Header (1)

▶ GET http://testphp.vulnweb.com/

XSLT Injection (1)

▶ GET http://testphp.vulnweb.com/showimage.php?file=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Ftestphp.vulnweb.com%3A22%27%29%22%2F%3E

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	▪ 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 (Cross Site Scripting (Reflected))
CWE ID	79
WASC ID	8
Reference	▪ http://projects.webappsec.org/Cross-Site-Scripting ▪ https://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

SQL Injection - MySQL

Source	raised by an active scanner (SQL Injection - MySQL)
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/

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/

Directory Browsing

Source	raised by a passive scanner (Directory Browsing)
CWE ID	548
WASC ID	16
Reference	▪ https://cwe.mitre.org/data/definitions/548.html

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

XSLT Injection

Source	raised by an active scanner (XSLT Injection)
CWE ID	91
WASC ID	23
Reference	▪ https://www.contextis.com/blog/xslt-server-side-injection-attacks