ZAP Scanning Report Basic2

Generated with ZAP on Fri 5 Jan 2024, at 17:01:38

ZAP Version: 2.14.0

Contents

About this report

Report description

Medium and low 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`, `Low`

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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (20.0%)	1 (20.0%)	0 (0.0%)	2 (40.0%)
	Low	0 (0.0%)	1 (20.0%)	2 (40.0%)	0 (0.0%)	3 (60.0%)
	Total	0 (0.0%)	2 (40.0%)	3 (60.0%)	0 (0.0%)	5 (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)
Site	http://testphp.vulnweb.com	0 (0)	2 (2)	3 (5)

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
Content Security Policy (CSP) Header Not Set	Medium	48 (960.0%)
Missing Anti-clickjacking Header	Medium	44 (880.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	62 (1,240.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	74 (1,480.0%)
X-Content-Type-Options Header Missing	Low	68 (1,360.0%)
Total		5

Alerts

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=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

Appendix

Alert types

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

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

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

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
WASC ID	13
Reference	▪ http://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 ▪ 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