ZAP Scanning Report

Generated with ZAP on Fri 8 Dec 2023, at 21:02:33

ZAP Version: 2.14.0

Contents

About this report

Report description

Identify common vulnerabilities such as SQL injection and cross site scripting.

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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (9.1%)	1 (9.1%)	1 (9.1%)	3 (27.3%)
	Low	0 (0.0%)	1 (9.1%)	2 (18.2%)	0 (0.0%)	3 (27.3%)
	Informational	0 (0.0%)	0 (0.0%)	1 (9.1%)	4 (36.4%)	5 (45.5%)
	Total	0 (0.0%)	2 (18.2%)	4 (36.4%)	5 (45.5%)	11 (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	0 (0)	3 (3)	3 (6)	5 (11)

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
Absence of Anti-CSRF Tokens	Medium	40 (363.6%)
Content Security Policy (CSP) Header Not Set	Medium	48 (436.4%)
Missing Anti-clickjacking Header	Medium	44 (400.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	62 (563.6%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	74 (672.7%)
X-Content-Type-Options Header Missing	Low	68 (618.2%)
Authentication Request Identified	Informational	1
Total		11

Alert type	Risk	Count
		(9.1%)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	31 (281.8%)
Information Disclosure - Suspicious Comments	Informational	1 (9.1%)
Modern Web Application	Informational	9 (81.8%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3 (27.3%)
Total		11

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=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 (1)

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

Modern Web Application (1)

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

Risk=Informational, Confidence=Low (4)

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

Authentication Request Identified (1)

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

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

User Controllable HTML Element Attribute (Potential XSS) (1)

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

Appendix

Alert types

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

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 ▪ 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 ▪ 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

Authentication Request Identified

Source	raised by a passive scanner (Authentication Request Identified)
Reference	- https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

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

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

User Controllable HTML Element Attribute (Potential XSS)

Source	raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))
CWE ID	20
WASC ID	20
Reference	▪ http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute