ZAP Scanning Report

Generated with ZAP on Sun 15 Sept 2024, at 09:20:47

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

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://kioptrix.local`

(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 (20.0%)	2 (40.0%)	0 (0.0%)	3 (60.0%)
	Low	0 (0.0%)	1 (20.0%)	1 (20.0%)	0 (0.0%)	2 (40.0%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	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** **(>= Mediu**	**Low** **(>= Low)**	**Informational**

			m)		(>= Informational)
Site	**http://kioptrix.local**	0 (0)	3 (3)	2 (5)	0 (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	10 (200.0%)
Directory Browsing	Medium	3 (60.0%)
Missing Anti-clickjacking Header	Medium	1 (20.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	12 (240.0%)
X-Content-Type-Options Header Missing	Low	3 (60.0%)
Total		5

Alerts

Risk=Medium, Confidence=High (1)

http://kioptrix.local (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET http://kioptrix.local

Risk=Medium, Confidence=Medium (2)

http://kioptrix.local (2)

Directory Browsing (1)

▶ GET http://kioptrix.local/manual/

Missing Anti-clickjacking Header (1)

▶ GET http://kioptrix.local

Risk=Low, Confidence=High (1)

http://kioptrix.local (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET http://kioptrix.local

Risk=Low, Confidence=Medium (1)

http://kioptrix.local (1)

X-Content-Type-Options Header Missing (1)

▶ GET http://kioptrix.local

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 ▪ https://www.w3.org/TR/CSP/ ▪ https://w3c.github.io/webappsec-csp/ ▪ https://web.dev/articles/csp ▪ https://caniuse.com/#feat=contentsecuritypolicy ▪ https://content-security-policy.com/

Directory Browsing

Source	raised by an active scanner (Directory

	Browsing)
CWE ID	548
WASC ID	48
Reference	▪ https://httpd.apache.org/docs/mod/core.html#options

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 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	▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) ▪ https://www.troyhunt.com/shhh-dont-let-

your-response-headers/

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	▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) ▪ https://owasp.org/www-community/Security_Headers