is_ii

Generated with ZAP on Wed 27 Dec 2023, at 11:06:14

ZAP Version: 2.14.0

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://localhost:8080`

(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%)	1 (14.3%)	1 (14.3%)
	Medium	0 (0.0%)	1 (14.3%)	0 (0.0%)	1 (14.3%)	2 (28.6%)
	Low	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Informational	0 (0.0%)	0 (0.0%)	2 (28.6%)	2 (28.6%)	4 (57.1%)
	Total	0 (0.0%)	1 (14.3%)	2 (28.6%)	4 (57.1%)	7 (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://localhost:8080	1 (1)	2 (3)	0 (3)	4 (7)

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
Cloud Metadata Potentially Exposed	High	1 (14.3%)
Absence of Anti-CSRF Tokens	Medium	1338 (19,114.3%)
CSP: Wildcard Directive	Medium	1382 (19,742.9%)
Authentication Request Identified	Informational	2 (28.6%)
Information Disclosure - Sensitive Information in URL	Informational	39 (557.1%)
User Agent Fuzzer	Informational	12 (171.4%)
Total		7

Alert type	Risk	Count
User Controllable HTML Element Attribute (Potential XSS)	Informational	4134 (59,057.1%)
Total		7

Alerts

Risk=High, Confidence=Low (1)

http://localhost:8080 (1)

Cloud Metadata Potentially Exposed (1)

▶ GET http://localhost:8080/latest/meta-data/

Risk=Medium, Confidence=High (1)

http://localhost:8080 (1)

CSP: Wildcard Directive (1)

▶ GET http://localhost:8080/OTHER/network/other/proxy.pac/?apinonce=58f6fa3a8f6b3d6d

Risk=Medium, Confidence=Low (1)

http://localhost:8080 (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://localhost:8080/UI/acsrf/view/optionPartialMatchingEnable d/

Risk=Informational, Confidence=Medium (2)

http://localhost:8080 (2)

Information Disclosure - Sensitive Information in URL (1)

▶ GET http://localhost:8080/UI/ajaxSpider/action/scanAsUser/override?apikey=ZAP&contextName=ZAP&subtreeOnly=ZAP&url=https%3A%2F%2Fzap.example.com&userName=ZAP

User Agent Fuzzer (1)

▶ GET http://localhost:8080/

Risk=Informational, Confidence=Low (2)

http://localhost:8080 (2)

Authentication Request Identified (1)

▶ GET http://localhost:8080/UI/network/action/setHttpProxy/override?apikey=ZAP&host=ZAP&password=ZAP&port=ZAP&realm=ZAP&username=ZAP

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

▶ GET http://localhost:8080/UI/ajaxSpider/view/fullResults/override?apikey=ZAP

Appendix

Alert types

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

Cloud Metadata Potentially Exposed

Source	raised by an active scanner (Cloud Metadata Potentially Exposed)
Reference	▪ https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/

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

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15

Reference	▪ http://www.w3.org/TR/CSP2/ ▪ http://www.w3.org/TR/CSP/ ▪ http://caniuse.com/#search=content+security+policy ▪ http://content-security-policy.com/ ▪ https://github.com/shapesecurity/salvation ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

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/

Information Disclosure - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

User Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)

Reference	- https://owasp.org/wstg

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