ZAP Scanning Report

Generated with ZAP on Tue 6 Feb 2024, at 15:56:05

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:

- `https://fdsa-rocky.addi-services.org`

(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 (16.7%)	0 (0.0%)	0 (0.0%)	1 (16.7%)
	Low	0 (0.0%)	1 (16.7%)	0 (0.0%)	1 (16.7%)	2 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	2 (33.3%)	1 (16.7%)	3 (50.0%)
	Total	0 (0.0%)	2 (33.3%)	2 (33.3%)	2 (33.3%)	6 (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	https://fdsa-rocky.addi-services.org	0 (0)	1 (1)	2 (3)	3 (6)

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
CSP: Wildcard Directive	Medium	1 (16.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	2 (33.3%)
Timestamp Disclosure - Unix	Low	2 (33.3%)
Information Disclosure - Suspicious Comments	Informational	24 (400.0%)
Modern Web Application	Informational	2 (33.3%)
User Agent Fuzzer	Informational	24 (400.0%)
Total		6

Alerts

Risk=Medium, Confidence=High (1)

https://fdsa-rocky.addi-services.org (1)

CSP: Wildcard Directive (1)

▶ GET https://fdsa-rocky.addi-services.org/admin

Risk=Low, Confidence=High (1)

https://fdsa-rocky.addi-services.org (1)

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

▶ GET https://fdsa-rocky.addi-services.org

Risk=Low, Confidence=Low (1)

https://fdsa-rocky.addi-services.org (1)

Timestamp Disclosure - Unix (1)

▶ GET https://fdsa-rocky.addi-services.org/admin/js/chunk-vendors.js

Risk=Informational, Confidence=Medium (2)

https://fdsa-rocky.addi-services.org (2)

Modern Web Application (1)

▶ GET https://fdsa-rocky.addi-services.org

User Agent Fuzzer (1)

▶ GET https://fdsa-rocky.addi-services.org/admin

Risk=Informational, Confidence=Low (1)

https://fdsa-rocky.addi-services.org (1)

Information Disclosure - Suspicious Comments (1)

▶ GET https://fdsa-rocky.addi-services.org

Appendix

Alert types

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

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

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

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200

WASC ID	13
Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

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 Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	▪ https://owasp.org/wstg