ZAP by Checkmarx Scanning Report

Generated with ZAP on Thu 12 Dec 2024, at 22:44:50

ZAP Version: 2.15.0

ZAP by Checkmarx

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://52.90.153.234:8080

(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%)	1 (11.1%)	0 (0.0%)	1 (11.1%)
	Medium	0 (0.0%)	1 (11.1%)	2 (22.2%)	0 (0.0%)	3 (33.3%)
	Low	0 (0.0%)	0 (0.0%)	1 (11.1%)	1 (11.1%)	2 (22.2%)
	Informational	0 (0.0%)	0 (0.0%)	2 (22.2%)	1 (11.1%)	3 (33.3%)
	Total	0 (0.0%)	1 (11.1%)	6 (66.7%)	2 (22.2%)	9 (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://52.90.153.234:8080	1 (1)	3 (4)	2 (6)	3 (9)

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
Vulnerable JS Library	High	1 (11.1%)
Content Security Policy (CSP) Header Not Set	Medium	1 (11.1%)
Missing Anti-clickjacking Header	Medium	1 (11.1%)
Total		9

Alert type	Risk	Count
Spring Actuator Information Leak	Medium	1 (11.1%)
Timestamp Disclosure - Unix	Low	74 (822.2%)
X-Content-Type-Options Header Missing	Low	8 (88.9%)
Information Disclosure - Suspicious Comments	Informational	2 (22.2%)
Modern Web Application	Informational	1 (11.1%)
User Agent Fuzzer	Informational	11 (122.2%)
Total		9

Alerts

Risk=High, Confidence=Medium (1)

http://52.90.153.234:8080 (1)

Vulnerable JS Library (1)

▶ GET http://52.90.153.234:8080/swagger-ui/swagger-ui-bundle.js

Risk=Medium, Confidence=High (1)

http://52.90.153.234:8080 (1)

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

▶ GET http://52.90.153.234:8080/swagger-ui/index.html

Risk=Medium, Confidence=Medium (2)

http://52.90.153.234:8080 (2)

Missing Anti-clickjacking Header (1)

▶ GET http://52.90.153.234:8080/swagger-ui/index.html

Spring Actuator Information Leak (1)

▶ GET http://52.90.153.234:8080/actuator/health

Risk=Low, Confidence=Medium (1)

http://52.90.153.234:8080 (1)

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

▶ GET http://52.90.153.234:8080/swagger-ui/swagger-initializer.js

Risk=Low, Confidence=Low (1)

http://52.90.153.234:8080 (1)

Timestamp Disclosure - Unix (1)

▶ GET http://52.90.153.234:8080/swagger-ui/swagger-ui-standalone-preset.js

Risk=Informational, Confidence=Medium (2)

http://52.90.153.234:8080 (2)

Modern Web Application (1)

▶ GET http://52.90.153.234:8080/swagger-ui/index.html

User Agent Fuzzer (1)

▶ GET http://52.90.153.234:8080/swagger-ui

Risk=Informational, Confidence=Low (1)

http://52.90.153.234:8080 (1)

Information Disclosure - Suspicious Comments (1)

▶ GET http://52.90.153.234:8080/swagger-ui/swagger-ui-standalone-preset.js

Appendix

Alert types

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

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	▪ https://github.com/advisories/GHSA-gx9m-whjm-85jf ▪ https://github.com/cure53/DOMPurify/commit/6ea80cd8b47640c20f2f230c7920b1f4ce4fdf7a ▪ https://github.com/advisories/GHSA-p3vf-v8qc-cwcr ▪ https://github.com/cure53/DOMPurify/commit/0ef5e537a514f904b6aa1d7ad9e749e365d7185f ▪ https://github.com/cure53/DOMPurify/security/advisories/GHSA-p3vf-v8qc-cwcr ▪ https://nvd.nist.gov/vuln/detail/CVE-2024-45801 ▪ https://github.com/cure53/DOMPurify/security/advisories/GHSA-mmhx-hmjr-r674 ▪ https://github.com/cure53/DOMPurify/commit/d1dd0374caef2b4c56c3bd09fe1988c3479166dc ▪ https://github.com/cure53/DOMPurify ▪ https://github.com/advisories/GHSA-mmhx-hmjr-r674

- https://github.com/cure53/DOMPurify/commit/26e1d69ca7f769f5c558619d644d90dd8bf26ebc
- https://nvd.nist.gov/vuln/detail/CVE-2024-47875
- https://github.com/cure53/DOMPurify/security/advisories/GHSA-gx9m-whjm-85jf
- https://github.com/cure53/DOMPurify/blob/0ef5e537a514f904b6aa1d7ad9e749e365d7185f/test/test-suite.js#L2098
- https://github.com/cure53/DOMPurify/commit/1e520262bf4c66b5efda49e2316d6d1246ca7b21
- https://nvd.nist.gov/vuln/detail/CVE-2024-48910

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/

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

Spring Actuator Information Leak

Source	raised by an active scanner (Spring Actuator Information Leak)
CWE ID	215
WASC ID	13
Reference	• https://docs.spring.io/spring-boot/docs/current/actuator-api/htmlsingle/#overview

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ https://cwe.mitre.org/data/definitions/200.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	▪ 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

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