ZAP by Checkmarx Scanning Report

Generated with ZAP on Mon 1 Dec 2025, at 22:18:49

ZAP Version: 2.16.1

ZAP by Checkmarx

Contents

- About This Report
  - Report Parameters
- Summaries
  - Alert Counts by Risk and Confidence
  - Alert Counts by Site and Risk
  - Alert Counts by Alert Type
- Alerts
  - Risk=High, Confidence=Medium (1)
  - Risk=Medium, Confidence=High (4)
  - Risk=Low, Confidence=High (1)
  - Risk=Low, Confidence=Medium (1)

    - Risk=Low, Confidence=Low (1)
    - Risk=Informational, Confidence=Medium (2)
    - Risk=Informational, Confidence=Low (2)
- Appendix
    - Alert Types

About This Report

Report Parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- `https://app.kinnect.us`

(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 (8.3%)	0 (0.0%)	1 (8.3%)
	Medium	0 (0.0%)	4 (33.3%)	0 (0.0%)	0 (0.0%)	4 (33.3%)
	Low	0 (0.0%)	1 (8.3%)	1 (8.3%)	1 (8.3%)	3 (25.0%)
	Informational	0 (0.0%)	0 (0.0%)	2 (16.7%)	2 (16.7%)	4 (33.3%)
	Total	0 (0.0%)	5 (41.7%)	4 (33.3%)	3 (25.0%)	12 (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://app.kinnect.us**	1 (1)	4 (5)	3 (8)	4 (12)

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 (8.3%)
CSP: Failure to Define Directive with No Fallback	Medium	6 (50.0%)
CSP: Wildcard Directive	Medium	6 (50.0%)
Total		12

Alert type	Risk	Count
CSP: script-src unsafe-inline	Medium	6 (50.0%)
CSP: style-src unsafe-inline	Medium	6 (50.0%)
Cross-Domain JavaScript Source File Inclusion	Low	12 (100.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	12 (100.0%)
Timestamp Disclosure - Unix	Low	163 (1,358.3%)
Information Disclosure - Suspicious Comments	Informational	2 (16.7%)
Modern Web Application	Informational	6 (50.0%)
Re-examine Cache-control Directives	Informational	6 (50.0%)
Retrieved from Cache	Informational	12 (100.0%)
Total		12

Alerts

Risk=High, Confidence=Medium (1)

https://app.kinnect.us (1)

Vulnerable JS Library (1)

▶ GET https://app.kinnect.us/main.2bb3f9be7d3baeb3.js

Risk=Medium, Confidence=High (4)

https://app.kinnect.us (4)

CSP: Failure to Define Directive with No Fallback (1)

▶ GET https://app.kinnect.us

CSP: Wildcard Directive (1)

▶ GET https://app.kinnect.us

CSP: script-src unsafe-inline (1)

▶ GET https://app.kinnect.us

CSP: style-src unsafe-inline (1)

▶ GET https://app.kinnect.us

Risk=Low, Confidence=High (1)

https://app.kinnect.us (1)

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

▶ GET https://app.kinnect.us/polyfills.71c20159e16df7fd.js

Risk=Low, Confidence=Medium (1)

https://app.kinnect.us (1)

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://app.kinnect.us

Risk=Low, Confidence=Low (1)

https://app.kinnect.us (1)

Timestamp Disclosure - Unix (1)

▶ GET https://app.kinnect.us/main.2bb3f9be7d3baeb3.js

Risk=Informational, Confidence=Medium (2)

https://app.kinnect.us (2)

Modern Web Application (1)

▶ GET https://app.kinnect.us

Retrieved from Cache (1)

▶ GET https://app.kinnect.us/polyfills.71c20159e16df7fd.js

Risk=Informational, Confidence=Low (2)

https://app.kinnect.us (2)

Information Disclosure - Suspicious Comments (1)

▶ GET https://app.kinnect.us/scripts.f4c55e9ea35629fa.js

Re-examine Cache-control Directives (1)

▶ GET https://app.kinnect.us

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	1395
Reference	▪ https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

CSP: Failure to Define Directive with No Fallback

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+

policy

- https://content-security-policy.com/
- https://github.com/HtmlUnit/htmlunit-csp
- https://web.dev/articles/csp#resource-options

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://web.dev/articles/csp#resource-options

CSP: script-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/

- https://caniuse.com/#search=content+security+policy
- https://content-security-policy.com/
- https://github.com/HtmlUnit/htmlunit-csp
- https://web.dev/articles/csp#resource-options

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://web.dev/articles/csp#resource-options

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
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/

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	497
WASC ID	13
Reference	▪ https://cwe.mitre.org/data/definitions/200.html

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	615

WASC ID	13

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/

Retrieved from Cache

Source	raised by a passive scanner (Retrieved from Cache)
CWE ID	525
Reference	▪ https://datatracker.ietf.org/doc/html/rfc7234

- https://datatracker.ietf.org/doc/html/rfc7231
- https://www.rfc-editor.org/rfc/rfc9110.html