ZAP by Checkmarx Scanning Report

Generated with The ZAP logoZAP on Wed 30 Jul 2025, at 15:35:32

ZAP Version: 2.16.1

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://localhost:3000

(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 (9.1%)	0 (0.0%)	1 (9.1%)
	Medium	0 (0.0%)	2 (18.2%)	2 (18.2%)	0 (0.0%)	4 (36.4%)
	Low	0 (0.0%)	0 (0.0%)	3 (27.3%)	1 (9.1%)	4 (36.4%)
	Informational	0 (0.0%)	0 (0.0%)	1 (9.1%)	1 (9.1%)	2 (18.2%)
	Total	0 (0.0%)	2 (18.2%)	7 (63.6%)	2 (18.2%)	11 (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:3000	1 (1)	4 (5)	4 (9)	2 (11)

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
SQL Injection - SQLite	High	1 (9.1%)
Content Security Policy (CSP) Header Not Set	Medium	69 (627.3%)
Cross-Domain Misconfiguration	Medium	106 (963.6%)
Missing Anti-clickjacking Header	Medium	10 (90.9%)
Session ID in URL Rewrite	Medium	46 (418.2%)
Cross-Domain JavaScript Source File Inclusion	Low	100 (909.1%)
Private IP Disclosure	Low	1 (9.1%)
Timestamp Disclosure - Unix	Low	165 (1,500.0%)
X-Content-Type-Options Header Missing	Low	46 (418.2%)
Information Disclosure - Suspicious Comments	Informational	2 (18.2%)
Modern Web Application	Informational	51 (463.6%)
Total		11

Alerts

1. **Risk=High, Confidence=Medium (1)**
    1. **http://localhost:3000 (1)**
        1. SQL Injection - SQLite (1)
            1. ▶ GET http://localhost:3000/rest/products/search?q=%27%28
2. **Risk=Medium, Confidence=High (2)**
    1. **http://localhost:3000 (2)**
        1. Content Security Policy (CSP) Header Not Set (1)
            1. ▶ GET http://localhost:3000
        2. Session ID in URL Rewrite (1)
            1. ▶ GET http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXQoAoi&sid=W4_DERWv7h7yG9WwAAAC
3. **Risk=Medium, Confidence=Medium (2)**
    1. **http://localhost:3000 (2)**
        1. Cross-Domain Misconfiguration (1)
            1. ▶ GET http://localhost:3000/robots.txt
        2. Missing Anti-clickjacking Header (1)
            1. ▶ POST http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXQoAof&sid=W4_DERWv7h7yG9WwAAAC
4. **Risk=Low, Confidence=Medium (3)**
    1. **http://localhost:3000 (3)**
        1. Cross-Domain JavaScript Source File Inclusion (1)
            1. ▶ GET http://localhost:3000
        2. Private IP Disclosure (1)
            1. ▶ GET http://localhost:3000/rest/admin/application-configuration
        3. X-Content-Type-Options Header Missing (1)
            1. ▶ GET http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXQoAPa
5. **Risk=Low, Confidence=Low (1)**
    1. **http://localhost:3000 (1)**
        1. Timestamp Disclosure - Unix (1)
            1. ▶ GET http://localhost:3000
6. **Risk=Informational, Confidence=Medium (1)**
    1. **http://localhost:3000 (1)**
        1. Modern Web Application (1)
            1. ▶ GET http://localhost:3000/sitemap.xml
7. **Risk=Informational, Confidence=Low (1)**
    1. **http://localhost:3000 (1)**
        1. Information Disclosure - Suspicious Comments (1)
            1. ▶ GET http://localhost:3000/main.js

Appendix

Alert types

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

1. **SQL Injection - SQLite**

    Source raised by an active scanner (SQL Injection)
    CWE ID 89
    WASC ID 19
    Reference 1. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

2. **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
    1. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
    2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
    3. https://www.w3.org/TR/CSP/
    4. https://w3c.github.io/webappsec-csp/
    5. https://web.dev/articles/csp
    6. https://caniuse.com/#feat=contentsecuritypolicy
    7. https://content-security-policy.com/

3. **Cross-Domain Misconfiguration**

    Source raised by a passive scanner (Cross-Domain Misconfiguration)
    CWE ID 264
    WASC ID 14
    Reference 1. https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

4. **Missing Anti-clickjacking Header**

    Source raised by a passive scanner (Anti-clickjacking Header)
    CWE ID 1021
    WASC ID 15
    Reference 1. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

5. **Session ID in URL Rewrite**

    Source raised by a passive scanner (Session ID in URL Rewrite)
    CWE ID 598
    WASC ID 13
    Reference 1. https://seclists.org/webappsec/2002/q4/111

6. **Cross-Domain JavaScript Source File Inclusion**

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

7. **Private IP Disclosure**

    Source raised by a passive scanner (Private IP Disclosure)
    CWE ID 497
    WASC ID 13
    Reference 1. https://tools.ietf.org/html/rfc1918

8. **Timestamp Disclosure - Unix**

    Source raised by a passive scanner (Timestamp Disclosure)
    CWE ID 497
    WASC ID 13
    Reference 1. https://cwe.mitre.org/data/definitions/200.html

9. **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
    1. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)
    2. https://owasp.org/www-community/Security_Headers

10. **Information Disclosure - Suspicious Comments**

    Source raised by a passive scanner (Information Disclosure - Suspicious Comments)
    CWE ID 615
    WASC ID 13

11. **Modern Web Application**

    Source raised by a passive scanner (Modern Web Application)