ZAP by Checkmarx Scanning Report

Generated with The ZAP logoZAP on Thu 14 Nov 2024, at 20:51:08

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://127.0.0.1:5000

(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 (25.0%)	1 (25.0%)	0 (0.0%)	2 (50.0%)
	Low	0 (0.0%)	1 (25.0%)	1 (25.0%)	0 (0.0%)	2 (50.0%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Total	0 (0.0%)	2 (50.0%)	2 (50.0%)	0 (0.0%)	4 (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://127.0.0.1:5000	0 (0)	2 (2)	2 (4)	0 (4)

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
Content Security Policy (CSP) Header Not Set	Medium	5 (125.0%)
Missing Anti-clickjacking Header	Medium	2 (50.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	5 (125.0%)
X-Content-Type-Options Header Missing	Low	2 (50.0%)
Total		4

Alerts

1. **Risk=Medium, Confidence=High (1)**
    1. **http://127.0.0.1:5000 (1)**
        1. Content Security Policy (CSP) Header Not Set (1)
            1. ▶ GET http://127.0.0.1:5000/sitemap.xml
2. **Risk=Medium, Confidence=Medium (1)**
    1. **http://127.0.0.1:5000 (1)**
        1. Missing Anti-clickjacking Header (1)
            1. ▶ POST http://127.0.0.1:5000/add
3. **Risk=Low, Confidence=High (1)**
    1. **http://127.0.0.1:5000 (1)**
        1. Server Leaks Version Information via "Server" HTTP Response Header Field (1)
            1. ▶ POST http://127.0.0.1:5000/add
4. **Risk=Low, Confidence=Medium (1)**
    1. **http://127.0.0.1:5000 (1)**
        1. X-Content-Type-Options Header Missing (1)
            1. ▶ POST http://127.0.0.1:5000/add

Appendix

Alert types

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

1. **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/

2. **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

3. **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
    1. https://httpd.apache.org/docs/current/mod/core.html#servertokens
    2. https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)
    3. https://www.troyhunt.com/shhh-dont-let-your-response-headers/

4. **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