

# insecure ZAP Scanning Report

Generated with  ZAP on Sun 31 Mar 2024, at 13:28:20

ZAP Version: 2.14.0

## 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=Medium, Confidence=High \(2\)](#)
  - [Risk=Medium, Confidence=Medium \(1\)](#)
  - [Risk=Low, Confidence=Medium \(2\)](#)
- [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:

- <http://localhost:8001>

(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        |              |              |             |              |
|------|---------------|-------------------|--------------|--------------|-------------|--------------|
| Risk |               | User<br>Confirmed | High         | Medium       | Low         | Total        |
|      | High          | 0<br>(0.0%)       | 0<br>(0.0%)  | 0<br>(0.0%)  | 0<br>(0.0%) | 0<br>(0.0%)  |
|      | Medium        | 0<br>(0.0%)       | 2<br>(40.0%) | 1<br>(20.0%) | 0<br>(0.0%) | 3<br>(60.0%) |
|      | Low           | 0<br>(0.0%)       | 0<br>(0.0%)  | 2<br>(40.0%) | 0<br>(0.0%) | 2<br>(40.0%) |
|      | Informational | 0<br>(0.0%)       | 0<br>(0.0%)  | 0<br>(0.0%)  | 0<br>(0.0%) | 0<br>(0.0%)  |
|      | Total         | 0<br>(0.0%)       | 2<br>(40.0%) | 3<br>(60.0%) | 0<br>(0.0%) | 5<br>(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      |     | Medium             |     |
|   |  | Low       |     | Informational      |     |
|   |  | (>= High) |     | (>= Medium)        |     |
|   |  | (>= Low)  |     | (>= Informational) |     |
| <a href="http://localhost:8001">http://localhost:8001</a> |  | 0         | 3   | 2                  | 0   |
| Site  |  | (0)       | (3) | (5)                | (5) |

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         |
|---|--------|---------------|
| <a href="#">CSP: Wildcard Directive</a>   | Medium | 1<br>(20.0%)  |
| <a href="#">Content Security Policy (CSP) Header Not Set</a>                              | Medium | 5<br>(100.0%) |
| <a href="#">Missing Anti-clickjacking Header</a>  | Medium | 5<br>(100.0%) |
| <a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a> | Low    | 7<br>(140.0%) |
| <a href="#">X-Content-Type-Options Header Missing</a>                                     | Low    | 5<br>(100.0%) |
| Total   |        | 5             |

Alerts

**Risk=Medium, Confidence=High (2)****http://localhost:8001 (2)****CSP: Wildcard Directive (1)**

► GET http://localhost:8001/favicon.ico

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

► GET http://localhost:8001/login

**Risk=Medium, Confidence=Medium (1)****http://localhost:8001 (1)****Missing Anti-clickjacking Header (1)**

► GET http://localhost:8001/login

**Risk=Low, Confidence=Medium (2)****http://localhost:8001 (2)****Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)**

► GET http://localhost:8001/login

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

► GET http://localhost:8001/login

# 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 ( <a href="#">CSP</a> )   |
| CWE ID    | <a href="#">693</a>   |
| WASC ID   | 15  |
| Reference | <ul style="list-style-type: none"><li>▪ <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a></li><li>▪ <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a></li><li>▪ <a href="https://content-security-policy.com/">https://content-security-policy.com/</a></li><li>▪ <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a></li><li>▪ <a href="https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources">https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</a></li></ul> |

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

|         |  |
|---------|--|
| Source  | raised by a passive scanner ( <a href="#">Content Security Policy (CSP) Header Not Set</a> ) |
| CWE ID  | <a href="#">693</a>  |
| WASC ID | 15   |

Reference

- [https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\\_Content\\_Security\\_Policy](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://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 ( <a href="#">Anti-clickjacking Header</a> )  |
| CWE ID    | <a href="#">1021</a>  |
| WASC ID   | 15  |
| Reference | ▪ <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a> |

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

|        |   |
|--------|---|
| Source | raised by a passive scanner ( <a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a> ) |
| CWE ID | <a href="#">200</a>   |

|           |   |
|-----------|---|
| WASC ID   | 13  |
| Reference | <ul style="list-style-type: none"><li>▪ <a href="https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework</a></li><li>▪ <a href="https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html">https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html</a></li></ul> |

**X-Content-Type-Options Header Missing**

|           |   |
|-----------|---|
| Source    | raised by a passive scanner ( <a href="#">X-Content-Type-Options Header Missing</a> )   |
| CWE ID    | <a href="#">693</a>   |
| WASC ID   | 15  |
| Reference | <ul style="list-style-type: none"><li>▪ <a href="https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)</a></li><li>▪ <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a></li></ul> |