# ZAP by Checkmarx Scanning Report

Generated with ZAP on Sat 5 Apr 2025, at 18:18:10

ZAP Version: 2.16.0

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://localhost:8000

(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 (6.2%) | 1 (6.2%) | 1 (6.2%) | 3 (18.8%) |
| | Low | 0 (0.0%) | 1 (6.2%) | 4 (25.0%) | 1 (6.2%) | 6 (37.5%) |
| | Informational | 0 (0.0%) | 0 (0.0%) | 3 (18.8%) | 4 (25.0%) | 7 (43.8%) |
| | Total | 0 (0.0%) | 2 (12.5%) | 8 (50.0%) | 6 (37.5%) | 16 (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:8000 | 0 (0) | 3 (3) | 6 (9) | 7 (16) |

## 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 |
|---|---|---|
| Absence of Anti-CSRF Tokens | Medium | 9 (56.2%) |
| Content Security Policy (CSP) Header Not Set | Medium | 19 (118.8%) |
| Total | | 16 |

| Alert type | Risk | Count |
|---|---|---|
| Missing Anti-clickjacking Header | Medium | 10 (62.5%) |
| Cookie No HttpOnly Flag | Low | 9 (56.2%) |
| Cookie without SameSite Attribute | Low | 9 (56.2%) |
| Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) | Low | 37 (231.2%) |
| Server Leaks Version Information via "Server" HTTP Response Header Field | Low | 56 (350.0%) |
| Timestamp Disclosure - Unix | Low | 3 (18.8%) |
| X-Content-Type-Options Header Missing | Low | 41 (256.2%) |
| Charset Mismatch | Informational | 2 (12.5%) |
| Cookie Poisoning | Informational | 3 (18.8%) |
| Information Disclosure - Suspicious Comments | Informational | 5 (31.2%) |
| Modern Web Application | Informational | 9 (56.2%) |
| Session Management Response Identified | Informational | 7 (43.8%) |
| Total | | 16 |

| Alert type | Risk | Count |
|---|---|---|
| User Agent Fuzzer | Informational | 288 (1,800.0%) |
| User Controllable HTML Element Attribute (Potential XSS) | Informational | 39 (243.8%) |
| Total | | 16 |

# Alerts

### Risk=Medium, Confidence=High (1)

#### http://localhost:8000 (1)

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

▶ GET http://localhost:8000/robots.txt

### Risk=Medium, Confidence=Medium (1)

#### http://localhost:8000 (1)

##### Missing Anti-clickjacking Header (1)

▶ GET http://localhost:8000

### Risk=Medium, Confidence=Low (1)

#### http://localhost:8000 (1)

### Absence of Anti-CSRF Tokens (1)

▶ GET http://localhost:8000/?p=1

## Risk=Low, Confidence=High (1)

#### http://localhost:8000 (1)

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

▶ GET http://localhost:8000/wp-content/themes/twentytwentyfive/style.css?ver=1.0

## Risk=Low, Confidence=Medium (4)

#### http://localhost:8000 (4)

### Cookie No HttpOnly Flag (1)

▶ GET http://localhost:8000/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Flocalhost%3A8000%2Fwp-admin%2F

### Cookie without SameSite Attribute (1)

▶ GET http://localhost:8000/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Flocalhost%3A8000%2Fwp-admin%2F

### Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▶ GET http://localhost:8000

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

▶ GET http://localhost:8000/wp-content/themes/twentytwentyfive/style.css?ver=1.0

### Risk=Low, Confidence=Low (1)

#### http://localhost:8000 (1)

##### Timestamp Disclosure - Unix (1)

▶ GET http://localhost:8000/wp-includes/js/zxcvbn.min.js

### Risk=Informational, Confidence=Medium (3)

#### http://localhost:8000 (3)

##### Modern Web Application (1)

▶ GET http://localhost:8000

##### Session Management Response Identified (1)

▶ GET http://localhost:8000/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Flocalhost%3A8000%2Fwp-admin%2F

##### User Agent Fuzzer (1)

▶ GET http://localhost:8000/index.php?rest_route=%2Foembed%2F1.0%2Fembed&url=http%3A%2F%2Flocalhost%3A8000%2F%3Fp%3D1

### Risk=Informational, Confidence=Low (4)

#### http://localhost:8000 (4)

### Charset Mismatch (1)

▶ GET http://localhost:8000/index.php?format=xml&rest_route=%2Foembed%2F1.0%2Fembed&url=http%3A%2F%2Flocalhost%3A8000%2F%3Fp%3D1

### Cookie Poisoning (1)

▶ POST http://localhost:8000/wp-comments-post.php

### Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:8000/wp-admin/load-scripts.php?c=0&load%5Bchunk_0%5D=clipboard,jquery-core,jquery-migrate,zxcvbn-async,wp-hooks&ver=6.7.2

### User Controllable HTML Element Attribute (Potential XSS) (1)

▶ GET http://localhost:8000/?p=1

# Appendix

## Alert types

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

### Absence of Anti-CSRF Tokens

| | |
|---|---|
| **Source** | raised by a passive scanner (Absence of Anti-CSRF Tokens) |
| **CWE ID** | 352 |
| **WASC ID** | 9 |

**Reference**

- https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
- https://cwe.mitre.org/data/definitions/352.html

## 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 |

### Cookie No HttpOnly Flag

| | |
|---|---|
| **Source** | raised by a passive scanner (Cookie No HttpOnly Flag) |
| **CWE ID** | 1004 |
| **WASC ID** | 13 |
| **Reference** | ▪ https://owasp.org/www-community/HttpOnly |

### Cookie without SameSite Attribute

| | |
|---|---|
| **Source** | raised by a passive scanner (Cookie without SameSite Attribute) |
| **CWE ID** | 1275 |
| **WASC ID** | 13 |
| **Reference** | ▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site |

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

| | |
|---|---|
| **Source** | raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)) |
| **CWE ID** | 497 |
| **WASC ID** | 13 |
| **Reference** | • https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework<br>• https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html |

### 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<br>• https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)<br>• 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 |

### 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)<br>▪ https://owasp.org/www-community/Security_Headers |

### Charset Mismatch

| | |
|---|---|
| **Source** | raised by a passive scanner (Charset Mismatch) |
| **CWE ID** | 436 |
| **WASC ID** | 15 |
| **Reference** | ▪ https://code.google.com/p/browsersec/wiki/Part2 |

#Character_set_handling_and_detection

### Cookie Poisoning

| | |
|---|---|
| **Source** | raised by a passive scanner (Cookie Poisoning) |
| **CWE ID** | 565 |
| **WASC ID** | 20 |
| **Reference** | ▪ https://en.wikipedia.org/wiki/HTTP_cookie<br>▪ https://cwe.mitre.org/data/definitions/565.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) |

### Session Management Response Identified

| | |
|---|---|
| **Source** | raised by a passive scanner (Session Management Response Identified) |
| **Reference** | ▪ https://www.zaproxy.org/docs/desktop/addons/a |

uthentication-helper/session-mgmt-id

### User Agent Fuzzer

| | |
|---|---|
| **Source** | raised by an active scanner (User Agent Fuzzer) |
| **Reference** | ▪ https://owasp.org/wstg |

### User Controllable HTML Element Attribute (Potential XSS)

| | |
|---|---|
| **Source** | raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS)) |
| **CWE ID** | 20 |
| **WASC ID** | 20 |
| **Reference** | ▪ https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html |