ZAP by Checkmarx Scanning Report

Generated with [The ZAP logoZAP](https://zaproxy.org/) on Mon 24 Mar 2025, at 08:01:19 ZAP Version: 2.16.0

ZAP by [Checkmarx](https://checkmarx.com/)

# Contents

1. About this report
   1. Report description
   2. Report parameters
2. Summaries
   1. Alert counts by risk and confidence
   2. Alert counts by site and risk
   3. Alert counts by alert type
3. Alerts
   1. Risk=Medium, Confidence=High (1)
   2. Risk=Medium, Confidence=Medium (1)
   3. Risk=Medium, Confidence=Low (1)
   4. Risk=Low, Confidence=High (1)

* 1. Risk=Low, Confidence=Medium (3)
  2. Risk=Low, Confidence=Low (1)
  3. Risk=Informational, Confidence=Medium (3)

1. Appendix
   1. Alert types

# About this report

## Report description

Pentesting - altoro mutual Web app using zap

## Report parameters

**Contexts**

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

**Sites**

The following sites were included:  [http://altoro.testfire.net](http://altoro.testfire.net/)

(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** |
|  | **High** | 0  (0.0%) | 0  (0.0%) | 0  (0.0%) | 0  (0.0%) | 0  (0.0%) |
|  | **Medium** | 0  (0.0%) | 1  (9.1%) | 1  (9.1%) | 1  (9.1%) | 3  (27.3%) |
| **Risk** | **Low** | 0  (0.0%) | 1  (9.1%) | 3  (27.3%) | 1  (9.1%) | 5  (45.5%) |
|  | **Informational** | 0  (0.0%) | 0  (0.0%) | 3  (27.3%) | 0  (0.0%) | 3  (27.3%) |
|  | **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://altoro.testfire.net**](http://altoro.testfire.net/) | 0  (0) | 3  (3) | 5  (8) | 3  (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** |
| **Absence of Anti-CSRF Tokens** | Medium | 1  (9.1%) |
| **Content Security Policy (CSP) Header Not Set** | Medium | 164  (1,490.9%) |
| **Missing Anti-clickjacking Header** | Medium | 62  (563.6%) |
| **Cookie without SameSite Attribute** | Low | 3  (27.3%) |
| **Cross-Domain JavaScript Source File Inclusion** | Low | 1  (9.1%) |
| **Server Leaks Version Information via "Server" HTTP Response Header Field** | Low | 206  (1,872.7%) |
| **Timestamp Disclosure - Unix** | Low | 2  (18.2%) |
| **X-Content-Type-Options Header Missing** | Low | 101  (918.2%) |
| **Information Disclosure - Suspicious Comments** | Informational | 15  (136.4%) |
| **Modern Web Application** | Informational | 6  (54.5%) |
| **Session Management Response Identified** | Informational | 4  (36.4%) |
| **Total** |  | 11 |

# Alerts

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

* 1. [**http://altoro.testfire.net**](http://altoro.testfire.net/) **(1)**
     1. **Content Security Policy (CSP) Header Not Set (1)**
        1.  GET <http://altoro.testfire.net/>

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

* 1. [**http://altoro.testfire.net**](http://altoro.testfire.net/) **(1)**
     1. **Missing Anti-clickjacking Header (1)**
        1.  GET <http://altoro.testfire.net/>

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

* 1. [**http://altoro.testfire.net**](http://altoro.testfire.net/) **(1)**
     1. **Absence of Anti-CSRF Tokens (1)**
        1.  POST <http://altoro.testfire.net/sendFeedback>

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

* 1. [**http://altoro.testfire.net**](http://altoro.testfire.net/) **(1)**
     1. **Server Leaks Version Information via "Server" HTTP Response Header Field (1)**
        1.  GET <http://altoro.testfire.net/>

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

* 1. [**http://altoro.testfire.net**](http://altoro.testfire.net/) **(3)**
     1. **Cookie without SameSite Attribute (1)**
        1.  GET <http://altoro.testfire.net/>
     2. **Cross-Domain JavaScript Source File Inclusion (1)**
        1.  GET <http://altoro.testfire.net/index.jsp?content=personal_investments.htm>
     3. **X-Content-Type-Options Header Missing (1)**
        1.  GET <http://altoro.testfire.net/>

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

* 1. [**http://altoro.testfire.net**](http://altoro.testfire.net/) **(1)**
     1. **Timestamp Disclosure - Unix (1)**
        1.  GET <http://altoro.testfire.net/swagger/swagger-ui-standalone-preset.js>

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

* 1. [**http://altoro.testfire.net**](http://altoro.testfire.net/) **(3)**
     1. **Information Disclosure - Suspicious Comments (1)**
        1.  GET <http://altoro.testfire.net/login.jsp>
     2. **Modern Web Ap** **p lication (1)**
        1.  GET <http://altoro.testfire.net/index.jsp?content=inside.htm>
     3. **Session Management Response Identified (1)**
        1.  GET <http://altoro.testfire.net/>

# Appendix

## Alert types

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

1. **Absence of Anti-CSRF Tokens**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Absence of Anti-CSRF Tokens](https://www.zaproxy.org/docs/alerts/10202/)) |
| **CWE ID** | [352](https://cwe.mitre.org/data/definitions/352.html) |
| **WASC ID** | 9 |
| **Reference** | 1. <https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html> 2. <https://cwe.mitre.org/data/definitions/352.html> |

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

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Content Security Policy (CSP) Header Not Set](https://www.zaproxy.org/docs/alerts/10038/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **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](https://caniuse.com/#feat%3Dcontentsecuritypolicy)      1. <https://content-security-policy.com/> |

1. **Missing Anti-clickjacking Header**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Anti-clickjacking Header](https://www.zaproxy.org/docs/alerts/10020/)) |
| **CWE ID** | [1021](https://cwe.mitre.org/data/definitions/1021.html) |
| **WASC ID** | 15 |
| **Reference** | 1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options> |

1. **Cookie without SameSite Attribute**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Cookie without SameSite Attribute](https://www.zaproxy.org/docs/alerts/10054/)) |
| **CWE ID** | [1275](https://cwe.mitre.org/data/definitions/1275.html) |
| **WASC ID** | 13 |
| **Reference** | 1. <https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site> |

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

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Cross-Domain JavaScript Source File Inclusion](https://www.zaproxy.org/docs/alerts/10017/)) |
| **CWE ID** | [829](https://cwe.mitre.org/data/definitions/829.html) |
| **WASC ID** | 15 |

1. **Server Leaks Version Information via "Server" HTTP Response Header Field**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([HTTP Server Response Header](https://www.zaproxy.org/docs/alerts/10036/)) |
| **CWE ID** | [200](https://cwe.mitre.org/data/definitions/200.html) |
| **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)](https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v%3Dpandp.10)) 3. <https://www.troyhunt.com/shhh-dont-let-your-response-headers/> |

1. **Timestamp Disclosure - Unix**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Timestamp Disclosure](https://www.zaproxy.org/docs/alerts/10096/)) |
| **CWE ID** | [200](https://cwe.mitre.org/data/definitions/200.html) |
| **WASC ID** | 13 |
| **Reference** | 1. <https://cwe.mitre.org/data/definitions/200.html> |

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

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([X-Content-Type-Options Header Missing](https://www.zaproxy.org/docs/alerts/10021/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | 1. [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%3Dvs.85))      1. <https://owasp.org/www-community/Security_Headers> |

1. **Information Disclosure - Suspicious Comments**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Information Disclosure - Suspicious Comments](https://www.zaproxy.org/docs/alerts/10027/)) |
| **CWE ID** | [200](https://cwe.mitre.org/data/definitions/200.html) |
| **WASC ID** | 13 |

1. **Modern Web Application**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Modern Web Application](https://www.zaproxy.org/docs/alerts/10109/)) |

1. **Session Management Response Identified**