

# ZAP by Checkmarx

# Scanning Report

Generated with  ZAP on Mon 23 Jun 2025, at 15:03:16

ZAP Version: 2.16.1

ZAP by Checkmarx

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

- [Risk=Informational, Confidence=Medium \(2\)](#)
- [Risk=Informational, Confidence=Low \(1\)](#)
- [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:5173>

(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 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 (12.5%)	1 (12.5%)	1 (12.5%)	3 (37.5%)
	Low	0 (0.0%)	0 (0.0%)	2 (25.0%)	0 (0.0%)	2 (25.0%)
	Informational	0 (0.0%)	0 (0.0%)	2 (25.0%)	1 (12.5%)	3 (37.5%)
	1					
Total		0 (0.0%)	1 (12.5%)	5 (62.5%)	2 (25.0%)	8 (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			Informational
		High (= High)	Medium (>= Medium)	Low (>= Low)	
	<a href="http://localhost:517">http://localhost:517</a>	0	3	2	3
Site	3	(0)	(3)	(5)	(8)

### 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="#">Content Security Policy (CSP) Header Not Set</a>	Medium	3 (37.5%)
<a href="#">Hidden File Found</a>	Medium	4 (50.0%)
<a href="#">Missing Anti-clickjacking Header</a>	Medium	3 (37.5%)
Total		8

Alert type	Risk	Count
<a href="#">Cross-Domain JavaScript Source File Inclusion</a>	Low	3 (37.5%)
<a href="#">X-Content-Type-Options Header Missing</a>	Low	21 (262.5%)
<a href="#">Information Disclosure - Sensitive Information in URL</a>	Informational	1 (12.5%)
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	8 (100.0%)
<a href="#">Modern Web Application</a>	Informational	3 (37.5%)
Total		8

## Alerts

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

<http://localhost:5173> (1)

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

► GET <http://localhost:5173/>

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

<http://localhost:5173> (1)

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

► GET http://localhost:5173/

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

http://localhost:5173 (1)

#### **Hidden File Found (1)**

► GET http://localhost:5173/.hg

### **Risk=Low, Confidence=Medium (2)**

http://localhost:5173 (2)

#### **Cross-Domain JavaScript Source File Inclusion (1)**

► GET http://localhost:5173/

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

► GET http://localhost:5173/vite.svg

### **Risk=Informational, Confidence=Medium (2)**

http://localhost:5173 (2)

#### **Information Disclosure - Sensitive Information in URL (1)**

► GET http://localhost:5173/?token=jBLTkmbxSUBC

#### **Modern Web Application (1)**

► GET http://localhost:5173/

**Risk=Informational, Confidence=Low (1)**<http://localhost:5173> (1)**Information Disclosure - Suspicious Comments (1)**► GET <http://localhost:5173/src/index.css>

# Appendix

## Alert Types

---

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

### 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	<ul style="list-style-type: none"><li>▪ <a href="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</a></li><li>▪ <a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a></li><li>▪ <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a></li><li>▪ <a href="https://w3c.github.io/webappsec-csp/">https://w3c.github.io/webappsec-csp/</a></li></ul>

- <https://web.dev/articles/csp>
- <https://caniuse.com/#feat=contentsecuritypolicy>
- <https://content-security-policy.com/>

## Hidden File Found

Source	raised by an active scanner ( <a href="#">Hidden File Finder</a> )
CWE ID	<a href="#">538</a>
WASC ID	13
Reference	▪ <a href="https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html">https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html</a>

## 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>

## Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner ( <a href="#">Cross-Domain JavaScript Source File Inclusion</a> )
CWE ID	<a href="#">829</a>



**WASC ID** 15

## 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\(v=vs.85\)](https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85))
- <https://owasp.org/www-community/Security-Headers>

## Information Disclosure - Sensitive Information in URL

**Source** raised by a passive scanner ([Information Disclosure - Sensitive Information in URL](#))

**CWE ID** [598](#)

**WASC ID** 13

## 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](#))