

ZAP by Checkmarx Scanning Report

1,128–1,435 minutes

Contents

1. [About this report](#)
1. [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=Low, Confidence=Medium \(3\)](#)
 4. [Risk=Low, Confidence=Low \(1\)](#)
 5. [Risk=Informational, Confidence=Medium \(2\)](#)
 6. [Risk=Informational, Confidence=Low \(2\)](#)
4. [Appendix](#)
 1. [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:

- <https://www.ecommerceprojgroup9.site>

(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 (10.0%)	1 (10.0%)	0 (0.0%)	2 (20.0%)
	Low	0 (0.0%)	0 (0.0%)	3 (30.0%)	1 (10.0%)	4 (40.0%)
	Informational	0 (0.0%)	0 (0.0%)	2 (20.0%)	2 (20.0%)	4 (40.0%)
	Total	0 (0.0%)	1 (10.0%)	6 (60.0%)	3 (30.0%)	10 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number 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 the risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https:// www.ecommerceprojgroup9.site	0 (0)	2 (2)	4 (6)	4 (10)

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	1 (10.0%)
Missing Anti-clickjacking Header	Medium	1 (10.0%)
Cross-Domain JavaScript Source File Inclusion	Low	41 (410.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	4 (40.0%)
Timestamp Disclosure - Unix	Low	1 (10.0%)
X-Content-Type-Options Header Missing	Low	1 (10.0%)
Information Disclosure - Suspicious Comments	Informational	1 (10.0%)
Modern Web Application	Informational	1 (10.0%)
Re-examine Cache-control Directives	Informational	1 (10.0%)
Total		10

Alert type	Risk	Count
User Agent Fuzzer	Informational	60 (600.0%)
Total		10

Alerts

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

1. <https://www.ecommerceprojgroup9.site> (1)

1. [Content Security Policy \(CSP\) Header Not Set](#) (1)

1. ► GET <https://www.ecommerceprojgroup9.site>

2. Risk=Medium, Confidence=Medium (1)

1. <https://www.ecommerceprojgroup9.site> (1)

1. [Missing Anti-clickjacking Header](#) (1)

1. ► GET <https://www.ecommerceprojgroup9.site>

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

1. <https://www.ecommerceprojgroup9.site> (3)

1. [Cross-Domain JavaScript Source File Inclusion](#) (1)

1. ► GET <https://www.ecommerceprojgroup9.site>

2. [Server Leaks Information via "X-Powered-By" HTTP Response Header Field\(s\)](#) (1)

1. ► GET https://www.ecommerceprojgroup9.site/sitemap.xml

3. [X-Content-Type-Options Header Missing](#) (1)

1. ► GET https://www.ecommerceprojgroup9.site

4. **Risk=Low, Confidence=Low (1)**

1. **https://www.ecommerceprojgroup9.site (1)**

1. [Timestamp Disclosure - Unix](#) (1)

1. ► GET https://www.ecommerceprojgroup9.site

5. **Risk=Informational, Confidence=Medium (2)**

1. **https://www.ecommerceprojgroup9.site (2)**

1. [Modern Web Application](#) (1)

1. ► GET https://www.ecommerceprojgroup9.site

2. [User Agent Fuzzer](#) (1)

1. ► GET https://www.ecommerceprojgroup9.site/wp/

6. **Risk=Informational, Confidence=Low (2)**

1. **https://www.ecommerceprojgroup9.site (2)**

1. [Information Disclosure - Suspicious Comments](#) (1)

1. ► GET https://www.ecommerceprojgroup9.site

2. [Re-examine Cache-control Directives](#) (1)

1. ► GET <https://www.ecommerceprojgroup9.site>

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	<ol style="list-style-type: none">1. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html3. https://www.w3.org/TR/CSP/4. https://w3c.github.io/webappsec-csp/5. https://web.dev/articles/csp6. https://caniuse.com/#feat=contentsecuritypolicy7. 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	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

3. Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

4. 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 2. https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

5. 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

6. 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) 2. https://owasp.org/www-community/Security-Headers

7. Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	615
WASC ID	13

8. Modern Web Application

Source	raised by a passive scanner (Modern Web Application)
---------------	------------------------------------------------------------------------

9. Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	<ol style="list-style-type: none">https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-cachinghttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Controlhttps://grayduck.mn/2021/09/13/cache-control-recommendations/

10. User Agent Fuzzer

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