ZAP by Checkmarx Scanning Report

Generated with ZAP on Thu 31 Jul 2025, at 13:43:03

ZAP Version: 2.16.1

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:

- https://scrutinize.co.uk

(If no sites were selected, all sites were included by default.)

An included site must also be within the set of 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%)	2 (20.0%)	2 (20.0%)	0 (0.0%)	4 (40.0%)
	Informational	0 (0.0%)	2 (20.0%)	1 (10.0%)	1 (10.0%)	4 (40.0%)
	Total	0 (0.0%)	5 (50.0%)	4 (40.0%)	1 (10.0%)	10 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number 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	https://scrutinize.co.uk	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	2 (20.0%)
Missing Anti-clickjacking Header	Medium	2 (20.0%)
Cross-Domain JavaScript Source File Inclusion	Low	2 (20.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	6 (60.0%)
Strict-Transport-Security Header Not Set	Low	3 (30.0%)
X-Content-Type-Options Header Missing	Low	3 (30.0%)
Authentication Request Identified	Informational	1 (10.0%)
Re-examine Cache-control Directives	Informational	2 (20.0%)
Session Management Response Identified	Informational	4 (40.0%)
User Agent Fuzzer	Informational	12 (120.0%)
Total		10

Alerts

Risk=Medium, Confidence=High (1)

https://scrutinize.co.uk (1)

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

- GET https://scrutinize.co.uk/login

Risk=Medium, Confidence=Medium (1)

https://scrutinize.co.uk (1)

Missing Anti-clickjacking Header (1)

- GET https://scrutinize.co.uk/login

Risk=Low, Confidence=High (2)

https://scrutinize.co.uk (2)

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

- GET https://scrutinize.co.uk/static/img/scrutinize_logo.png

Strict-Transport-Security Header Not Set (1)

- GET https://scrutinize.co.uk/static/img/scrutinize_logo.png

Risk=Low, Confidence=Medium (2)

https://scrutinize.co.uk (2)

Cross-Domain JavaScript Source File Inclusion (1)

- GET https://scrutinize.co.uk/

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

- GET https://scrutinize.co.uk/static/img/scrutinize_logo.png

Risk=Informational, Confidence=High (3)

https://scrutinize.co.uk (3)

Authentication Request Identified (1)

- POST https://scrutinize.co.uk/login

Session Management Response Identified (1)

- GET https://scrutinize.co.uk/login

Risk=Informational, Confidence=Medium (1)

https://scrutinize.co.uk (1)

User Agent Fuzzer (1)

- GET https://scrutinize.co.uk/

Risk=Informational, Confidence=Low (1)

https://scrutinize.co.uk (1)

Re-examine Cache-control Directives (1)

- GET https://scrutinize.co.uk/

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 (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

Cross-Domain JavaScript Source File Inclusion

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

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 • https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) • https://www.troyhunt.com/shhh-dont-let-your-response-headers/

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	• https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html • https://owasp.org/www-community/Security_Headers • https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security • https://caniuse.com/stricttransportsecurity • https://datatracker.ietf.org/doc/html/rfc6797

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://owasp.org/www-community/Security_Headers

Authentication Request Identified

Source	raised by a passive scanner (Authentication Request Identified)
Reference	• https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	• https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching • https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control • https://grayduck.mn/2021/09/13/cache-control-recommendations/

Session Management Response Identified

Source	raised by a passive scanner (Session Management Response Identified)
Reference	• https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

User Agent Fuzzer

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