ZAP by Checkmarx Scanning Report

Generated with ZAP on Mon 7 Jul 2025, at 14:42:57

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=Low, Confidence=High (1)
  - Risk=Low, Confidence=Medium (2)

    - Risk=Informational, Confidence=High (1)
    - Risk=Informational, Confidence=Medium (3)
    - Risk=Informational, Confidence=Low (2)
- 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:

- `https://automationintesting.online`

(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 (9.1%)	1 (9.1%)	0 (0.0%)	2 (18.2%)
	Low	0 (0.0%)	1 (9.1%)	2 (18.2%)	0 (0.0%)	3 (27.3%)
	Informational	0 (0.0%)	1 (9.1%)	3 (27.3%)	2 (18.2%)	6 (54.5%)
	Total	0 (0.0%)	3 (27.3%)	6 (54.5%)	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	**https://automationtesting.online**	0 (0)	2 (2)	3 (5)	5 (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	4 (36.4%)
Missing Anti-clickjacking Header	Medium	4 (36.4%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	4 (36.4%)

Strict-Transport-Security Header Not Set	Low	68 (618.2%)
X-Content-Type-Options Header Missing	Low	67 (609.1%)
Authentication Request Identified	Informational	1 (9.1%)
Information Disclosure - Suspicious Comments	Informational	14 (127.3%)
Modern Web Application	Informational	2 (18.2%)
Re-examine Cache-control Directives	Informational	30 (272.7%)
Retrieved from Cache	Informational	47 (427.3%)
Session Management Response Identified	Informational	1 (9.1%)
Total		11

Alerts

Risk=Medium, Confidence=High (1)

https://automationintesting.online (1)

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

▶ GET https://automationintesting.online/

Risk=Medium, Confidence=Medium (1)

https://automationintesting.online (1)

Missing Anti-clickjacking Header (1)

▶ GET https://automationintesting.online/

Risk=Low, Confidence=High (1)

https://automationintesting.online (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://automationintesting.online/_next/static/css/21cf7b845cb0f7d7.css

Risk=Low, Confidence=Medium (2)

https://automationintesting.online (2)

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

▶ GET https://automationintesting.online/

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

▶ GET https://automationintesting.online/_next/static/css/21cf7b845cb0f7d7.css

Risk=Informational, Confidence=High (1)

https://automationintesting.online (1)

Authentication Request Identified (1)

▶ POST https://automationintesting.online/api/auth/login

Risk=Informational, Confidence=Medium (3)

https://automationintesting.online (3)

Modern Web Application (1)

▶ GET https://automationintesting.online/

Retrieved from Cache (1)

▶ GET https://automationintesting.online/_next/static/css/21cf7b845cb0f7d7.css

Session Management Response Identified (1)

▶ POST https://automationintesting.online/api/auth/login

Risk=Informational, Confidence=Low (2)

https://automationintesting.online (1)

Re-examine Cache-control Directives (1)

▶ GET https://automationintesting.online/

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

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

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/

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)

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/

Retrieved from Cache

Source	raised by a passive scanner (Retrieved from Cache)
Reference	- https://tools.ietf.org/html/rfc7234 - https://tools.ietf.org/html/rfc7231 - https://www.rfc-editor.org/rfc/rfc9110.html

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