ZAP by Checkmarx Scanning Report

Generated with ZAP on Thu 19 Dec 2024, at 17:40:24

ZAP Version: 2.15.0

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://beta.pupt-flss.com

(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%)	3 (33.3%)	1 (11.1%)	0 (0.0%)	4 (44.4%)
	Low	0 (0.0%)	1 (11.1%)	1 (11.1%)	0 (0.0%)	2 (22.2%)
	Informational	0 (0.0%)	0 (0.0%)	1 (11.1%)	2 (22.2%)	3 (33.3%)
	Total	0 (0.0%)	4 (44.4%)	3 (33.3%)	2 (22.2%)	9 (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://beta.pupt-flss.com	0 (0)	4 (4)	2 (6)	3 (9)

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
CSP: Wildcard Directive	Medium	4 (44.4%)
Total		9

Alert type	Risk	Count
CSP: script-src unsafe-inline	Medium	4 (44.4%)
CSP: style-src unsafe-inline	Medium	4 (44.4%)
Missing Anti-clickjacking Header	Medium	4 (44.4%)
Strict-Transport-Security Header Not Set	Low	41 (455.6%)
X-Content-Type-Options Header Missing	Low	41 (455.6%)
Information Disclosure - Suspicious Comments	Informational	29 (322.2%)
Modern Web Application	Informational	4 (44.4%)
Re-examine Cache-control Directives	Informational	4 (44.4%)
Total		9

Alerts

Risk=Medium, Confidence=High (3)

https://beta.pupt-flss.com (3)

CSP: Wildcard Directive (1)

▶ GET https://beta.pupt-flss.com/login

CSP: script-src unsafe-inline (1)

▶ GET https://beta.pupt-flss.com/login

CSP: style-src unsafe-inline (1)

▶ GET https://beta.pupt-flss.com/login

Risk=Medium, Confidence=Medium (1)

https://beta.pupt-flss.com (1)

Missing Anti-clickjacking Header (1)

▶ GET https://beta.pupt-flss.com/login

Risk=Low, Confidence=High (1)

https://beta.pupt-flss.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://beta.pupt-flss.com/login

Risk=Low, Confidence=Medium (1)

https://beta.pupt-flss.com (1)

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

▶ GET https://beta.pupt-flss.com/login

Risk=Informational, Confidence=Medium (1)

https://beta.pupt-flss.com (1)

Modern Web Application (1)

▶ GET https://beta.pupt-flss.com/login

Risk=Informational, Confidence=Low (2)

https://beta.pupt-flss.com (2)

Information Disclosure - Suspicious Comments (1)

▶ GET https://beta.pupt-flss.com/chunk-WYGBBPGQ.js

Re-examine Cache-control Directives (1)

▶ GET https://beta.pupt-flss.com/login

Appendix

Alert types

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

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693

WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: script-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp

	▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

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

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

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
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/