

# ZAP by Checkmarx Scanning Report

Generated with  [ZAP](#) on Sat 11 Jan 2025, at 16:34:39

ZAP Version: 2.15.0

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 \(3\)](#)
- [Risk=Medium, Confidence=Medium \(1\)](#)
- [Risk=Low, Confidence=High \(1\)](#)
- [Risk=Low, Confidence=Medium \(1\)](#)
- [Risk=Informational, Confidence=Medium \(1\)](#)
- [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://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
	Medium	0	3	1	0	0	4
	Low	0	1	1	0	0	2
	Informational	0	0	1	2	0	3
	Total	0	4	3	2	0	9
		(0.0%)	(44.4%)	(33.3%)	(22.2%)	(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.)

Site	Risk				Informational al)
	High (= High)	Medium (>= Medium)	Low (>= Informational) (>= Low)		
	0 (0)	2 (2)	0 (2)	0 (2)	
<a href="https://beta.pupt-flss.com">https://beta.pupt-flss.com</a>	0 (0)	2 (2)	0 (2)	0 (2)	0 (2)

### 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="#">CSP: Wildcard Directive</a>	Medium	6 (66.7%)
Total		9

Alert type	Risk	Count
<a href="#"><u>CSP: script-src unsafe-inline</u></a>	Medium	6 (66.7%)
<a href="#"><u>CSP: style-src unsafe-inline</u></a>	Medium	6 (66.7%)
<a href="#"><u>Missing Anti-clickjacking Header</u></a>	Medium	6 (66.7%)
<a href="#"><u>Strict-Transport-Security Header Not Set</u></a>	Low	40 (444.4%)
<a href="#"><u>X-Content-Type-Options Header Missing</u></a>	Low	40 (444.4%)
<a href="#"><u>Information Disclosure - Suspicious Comments</u></a>	Informational	31 (344.4%)
<a href="#"><u>Modern Web Application</u></a>	Informational	6 (66.7%)
<a href="#"><u>Re-examine Cache-control Directives</u></a>	Informational	6 (66.7%)
Total		9

# Alerts

**Risk=Medium, Confidence=High (3)**

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

**CSP: script-src unsafe-inline (1)**

- ▶ GET https://beta.pupt-flss.com/

**CSP: style-src unsafe-inline (1)**

- ▶ GET https://beta.pupt-flss.com/

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

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

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

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

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

# Appendix

## Alert types

---

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

### CSP: Wildcard Directive

<b>Source</b>	raised by a passive scanner ( <a href="#">CSP</a> )
<b>CWE ID</b>	<a href="#">693</a>
<b>WASC ID</b>	15
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a></li><li>▪ <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a></li><li>▪ <a href="https://content-security-policy.com/">https://content-security-policy.com/</a></li><li>▪ <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a></li><li>▪ <a href="https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources">https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</a></li></ul>

### CSP: script-src unsafe-inline

<b>Source</b>	raised by a passive scanner ( <a href="#">CSP</a> )
<b>CWE ID</b>	<a href="#">693</a>
<b>WASC ID</b>	15
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a></li><li>▪ <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a></li><li>▪ <a href="https://content-security-policy.com/">https://content-security-policy.com/</a></li><li>▪ <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a></li><li>▪ <a href="https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources">https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</a></li></ul>

## CSP: style-src unsafe-inline

<b>Source</b>	raised by a passive scanner ( <a href="#">CSP</a> )
<b>CWE ID</b>	<a href="#">693</a>
<b>WASC ID</b>	15
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a></li></ul>

- <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](https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources)

## Missing Anti-clickjacking Header

<b>Source</b>	raised by a passive scanner ( <a href="#">Anti-clickjacking Header</a> )
<b>CWE ID</b>	<a href="#">1021</a>
<b>WASC ID</b>	15
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <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></li></ul>

## Strict-Transport-Security Header Not Set

<b>Source</b>	raised by a passive scanner ( <a href="#">Strict-Transport-Security Header</a> )
<b>CWE ID</b>	<a href="#">319</a>
<b>WASC ID</b>	15

**Reference**

- [https://cheatsheetseries.owasp.org/cheatsheets/HTTP Strict Transport Security Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html)
- [https://owasp.org/www-community/Security\\_Headers](https://owasp.org/www-community/Security_Headers)
- [https://en.wikipedia.org/wiki/HTTP Strict Transport Security](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://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85))
- [https://owasp.org/www-community/Security\\_Headers](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://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/>