

ZAP Scanning Report

Generated with  ZAP on Fri 22 Mar 2024, at 19:53:13

ZAP Version: 2.14.0

ZAP is supported by the [Crash Override Open Source Fellowship](#)

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=Low, Confidence=Medium \(2\)](#)
 - [Risk=Informational, Confidence=Medium \(2\)](#)
 - [Risk=Informational, Confidence=Low \(1\)](#)
- [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://timelog-diegobrito-dev.apps.sandbox-m2.119k.p1.openshiftapps.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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Low	0 (0.0%)	0 (0.0%)	2 (40.0%)	0 (0.0%)	2 (40.0%)
	Informational	0 (0.0%)	0 (0.0%)	2 (40.0%)	1 (20.0%)	3 (60.0%)
	Total	0 (0.0%)	0 (0.0%)	4 (80.0%)	1 (20.0%)	5 (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 (>= Information al)	Informational
https://timelog-diegobrito-dev.apps.sandbox-m2.119k.p1.openshiftapps.com	0 (0)	0 (0)	2 (2)	3 (5)

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
Cookie Without Secure Flag	Low	1 (20.0%)
Cookie without SameSite Attribute	Low	1 (20.0%)
Authentication Request Identified	Informational	1 (20.0%)
Session Management Response Identified	Informational	1 (20.0%)
User Agent Fuzzer	Informational	12 (240.0%)
Total		5

Alerts

Risk=Low, Confidence=Medium (2)

<https://timelog-diegobrito-dev.apps.sandbox-m2.119k.p1.openshiftapps.com> (2)

[Cookie Without Secure Flag \(1\)](#)

► POST <https://timelog-diegobrito-dev.apps.sandbox-m2.119k.p1.openshiftapps.com/authenticate>

[Cookie without SameSite Attribute \(1\)](#)

► POST <https://timelog-diegobrito-dev.apps.sandbox-m2.119k.p1.openshiftapps.com/authenticate>

Risk=Informational, Confidence=Medium (2)

<https://timelog-diegobrito-dev.apps.sandbox-m2.119k.p1.openshiftapps.com> (2)

Session Management Response Identified (1)

► POST <https://timelog-diegobrito-dev.apps.sandbox-m2.119k.p1.openshiftapps.com/authenticate>

User Agent Fuzzer (1)

► POST <https://timelog-diegobrito-dev.apps.sandbox-m2.119k.p1.openshiftapps.com/authenticate>

Risk=Informational, Confidence=Low (1)

<https://timelog-diegobrito-dev.apps.sandbox-m2.119k.p1.openshiftapps.com> (1)

Authentication Request Identified (1)

► POST <https://timelog-diegobrito-dev.apps.sandbox-m2.119k.p1.openshiftapps.com/authenticate>

Appendix

Alert types

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

Cookie Without Secure Flag

Source	raised by a passive scanner (Cookie Without Secure Flag)
CWE ID	614
WASC ID	13
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Cookie without SameSite Attribute

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275

WASC ID 13

Reference

- <https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site>

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/>

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>