


Vulnerability Scanning Report

Generated with  ZAP on Wed 10 May 2023, at 18:02:23
Recruitment Management System - ~ Anuruddha Basnayake®

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=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:

- <http://localhost:9002>

(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				
Risk		User Confirmed	High	Medium	Low	Total
	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (20.0%)	0 (0.0%)	0 (0.0%)	1 (20.0%)
	Low	0 (0.0%)	0 (0.0%)	1 (20.0%)	0 (0.0%)	1 (20.0%)
	Informational	0 (0.0%)	0 (0.0%)	1 (20.0%)	2 (40.0%)	3 (60.0%)
	1					
Total	0 (0.0%)	1 (20.0%)	2 (40.0%)	2 (40.0%)	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

		Informational			
		High (= High)	Medium (>= Medium)	Low (>= Low)	(>= Informational)
http://localhost:9000		0	1	1	3
Site	2	(0)	(1)	(2)	(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
Content Security Policy (CSP) Header Not Set	Medium	2 (40.0%)
Cookie without SameSite Attribute	Low	1 (20.0%)
Charset Mismatch (Header Versus Meta Charset)	Informational	2 (40.0%)
Loosely Scoped Cookie	Informational	2 (40.0%)
User Agent Fuzzer	Informational	57 (1,140.0%)
Total		5

Alerts

Risk=Medium, Confidence=High (1)

<http://localhost:9002> (1)

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

► GET <http://localhost:9002/user/userRegister>

Risk=Low, Confidence=Medium (1)

<http://localhost:9002> (1)

Cookie without SameSite Attribute (1)

► GET <http://localhost:9002/user/userRegister>

Risk=Informational, Confidence=Medium (1)

<http://localhost:9002> (1)

User Agent Fuzzer (1)

► GET <http://localhost:9002/user>

Risk=Informational, Confidence=Low (2)

<http://localhost:9002> (2)

Charset Mismatch (Header Versus Meta Charset) (1)

► GET http://localhost:9002/user/userRegister

Loosely Scoped Cookie (1)

► GET http://localhost:9002/user/userRegister

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	<ul style="list-style-type: none">▪ 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▪ http://www.w3.org/TR/CSP/▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html

- <http://www.html5rocks.com/en/tutorials/security/content-security-policy/>
- <http://caniuse.com/#feat=contentsecuritypolicy>
- <http://content-security-policy.com/>

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

Charset Mismatch (Header Versus Meta Charset)

Source	raised by a passive scanner (Charset Mismatch)
CWE ID	436
WASC ID	15
Reference	■ http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

Loosely Scoped Cookie

Source	raised by a passive scanner (Loosely Scoped Cookie)
--------	---

CWE ID	565
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://tools.ietf.org/html/rfc6265#section-4.1▪ 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▪ http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

User Agent Fuzzer

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