Basic Principles of Cyber Security

SEC 105

Term Assignment

APPLICATION SECURITY ASSESSMENT & SUGGESTION FOR REMEDIATION

Submitted by: TEAM ARCHER
ID: 2101008, 2101013, 2101015

Submitted to: DR. ABUL KALAM AZAD(AKA) ADJUNCT FACULTY DEPARTMENT OF IRE, BDU

Submission date: 03-11-23

ZAP Scanning Report

Generated with ZAP on Mon 30 Oct 2023, at 22:45:20

ZAP Version: 2.14.0

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- http://127.0.0.1:8080

(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 (11.1%)	1 (11.1%)	1 (11.1%)	3 (33.3%)
	Low	0 (0.0%)	0 (0.0%)	2 (22.2%)	0 (0.0%)	2 (22.2%)
	Informational	0 (0.0%)	1 (11.1%)	2 (22.2%)	1 (11.1%)	4 (44.4%)
	Total	0 (0.0%)	2 (22.2%)	5 (55.6%)	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)
http://127.0.0.1:808 0	0 (0)	3 (3)	2 (5)	4 (9)

Site

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
Absence of Anti-CSRF Tokens	Medium	5 (55.6%)
Content Security Policy (CSP) Header Not Set	Medium	5 (55.6%)
Parameter Tampering	Medium	1 (11.1%)
Cookie No HttpOnly Flag	Low	1 (11.1%)
Cookie without SameSite Attribute	Low	1
Total		9

Alert type	Risk	Count
		(11.1%)
Authentication Request Identified	Informational	1 (11.1%)
Session Management Response Identified	Informational	2 (22.2%)
User Agent Fuzzer	Informational	98 (1,088.9%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	5 (55.6%)
Total		9

Alerts

Risk=Medium, Confidence=High (1)

http://127.0.0.1:8080 (1)

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

▶ GET http://127.0.0.1:8080/WebGoat

Risk=Medium, Confidence=Medium (1)

http://127.0.0.1:8080 (1)

Parameter Tampering (1)

▶ POST http://127.0.0.1:8080/WebGoat/register.mvc

Risk=Medium, Confidence=Low (1)

http://127.0.0.1:8080 (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://127.0.0.1:8080/WebGoat

Risk=Low, Confidence=Medium (2)

http://127.0.0.1:8080 (2)

Cookie No HttpOnly Flag (1)

▶ GET http://127.0.0.1:8080/WebGoat/

Cookie without SameSite Attribute (1)

▶ GET http://127.0.0.1:8080/WebGoat/

Risk=Informational, Confidence=High (1)

http://127.0.0.1:8080 (1)

Authentication Request Identified (1)

▶ POST http://127.0.0.1:8080/WebGoat/login

Risk=Informational, Confidence=Medium (2)

http://127.0.0.1:8080 (2)

Session Management Response Identified (1)

▶ GET http://127.0.0.1:8080/WebGoat/

User Agent Fuzzer (1)

▶ GET http://127.0.0.1:8080/WebGoat/

Risk=Informational, Confidence=Low (1)

http://127.0.0.1:8080 (1)

User Controllable HTML Element Attribute (Potential XSS) (1)

▶ POST http://127.0.0.1:8080/WebGoat/register.mvc

Appendix

Alert types

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

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9

Reference

- http://projects.webappsec.org/Cross-Site-Request-Forgery
- https://cwe.mitre.org/data/definitions/352.html

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
- 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/

Parameter Tampering

Source	raised by an active scanner (Parameter Tampering)
CWE ID	472
WASC ID	20

Cookie No HttpOnly Flag

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	▪ https://owasp.org/www-community/HttpOnly

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

User Controllable HTML Element Attribute (Potential XSS)

Source	raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))
CWE ID	20
WASC ID	20
Reference	▪ http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute