ZAP Scanning Report

Generated with ZAP on 月 20 5月 2024, at 16:28:58

ZAP Version: 2.14.0

ZAP is supported by the Crash Override Open Source Fellowship

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://0.0.0.0:8000

(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: 高, 中, 低, 情報

Excluded: None

Confidence levels

Included: User Confirmed, 高, 中, 低

Excluded: User Confirmed, 高, 中, 低, False Positive（誤った警告）

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	高	中	低	Total
Risk	高	0 (0.0%)	0 (0.0%)	2 (14.3%)	0 (0.0%)	2 (14.3%)
	中	0 (0.0%)	1 (7.1%)	1 (7.1%)	0 (0.0%)	2 (14.3%)
	低	0 (0.0%)	1 (7.1%)	2 (14.3%)	0 (0.0%)	3 (21.4%)
	情報	0 (0.0%)	3 (21.4%)	2 (14.3%)	2 (14.3%)	7 (50.0%)
	Total	0 (0.0%)	5 (35.7%)	7 (50.0%)	2 (14.3%)	14 (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			
	高 (= 高)	中 (>= 中)	低 (>= 低)	情報 (>= 情報)

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
External Redirect	高	1 (7.1%)
Server Side Include	高	1 (7.1%)
Content Security Policy (CSP) Header Not Set	中	39 (278.6%)
Vulnerable JS Library	中	1 (7.1%)
Cookie No HttpOnly Flag	低	8 (57.1%)
Server Leaks Version Information via "Server" HTTP Response Header Field	低	72 (514.3%)
X-Content-Type-Options Header Missing	低	11 (78.6%)
Authentication Request Identified	情報	5 (35.7%)
Total		14

Alert type	Risk	Count
GET for POST	情報	4 (28.6%)
Information Disclosure - Suspicious Comments	情報	2 (14.3%)
Modern Web Application	情報	1 (7.1%)
Session Management Response Identified	情報	2206 (15,757.1%)
User Agent Fuzzer	情報	518 (3,700.0%)
User Controllable HTML Element Attribute (Potential XSS)	情報	1 (7.1%)
Total		14

Alerts

Risk=高, Confidence=中 (2)

Risk=中, Confidence=高 (1)

Risk=中, Confidence=中 (1)

Risk=低, Confidence=高 (1)

Risk=低, Confidence=中 (2)

Risk=情報, Confidence=高 (3)

Risk=情報, Confidence=中 (2)

Risk=情報, Confidence=低 (2)

Appendix

Alert types

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

External Redirect

Source	raised by an active scanner (External Redirect)
CWE ID	601
WASC ID	38
Reference	▪ http://projects.webappsec.org/URL-Redirector-Abuse ▪ https://cwe.mitre.org/data/definitions/601.html

Server Side Include

Source	raised by an active scanner (Server Side Include)
CWE ID	97
WASC ID	31
Reference	▪ http://www.carleton.ca/~dmcfet/html/ssi.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/

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

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

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
WASC ID	13
Reference	▪ http://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 ▪ http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx ▪ http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

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	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx ▪ https://owasp.org/www-community/Security_Headers

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/

GET for POST

Source	raised by an active scanner (GET for POST)
CWE ID	16
WASC ID	20

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)

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