ZAP by Checkmarx Scanning Report

Generated with ZAP on Thu 7 Aug 2025, at 10:41:31

ZAP Version: 2.16.1

ZAP by Checkmarx

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://localhost

(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%)	1 (5.9%)	0 (0.0%)	1 (5.9%)
	Medium	0 (0.0%)	2 (11.8%)	3 (17.6%)	1 (5.9%)	6 (35.3%)
	Low	0 (0.0%)	1 (5.9%)	4 (23.5%)	0 (0.0%)	5 (29.4%)
	Informational	0 (0.0%)	2 (11.8%)	2 (11.8%)	1 (5.9%)	5 (29.4%)

	Confidence				
	User Confirmed	High	Medium	Low	Total
Total	0 (0.0%)	5 (29.4%)	10 (58.8%)	2 (11.8%)	17 (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)
Site	http://localhost	1 (1)	6 (7)	5 (12)	5 (17)

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
Path Traversal	High	2 (11.8%)
Absence of Anti-CSRF Tokens	Medium	35 (205.9%)
Content Security Policy (CSP) Header Not Set	Medium	16 (94.1%)
Directory Browsing	Medium	4 (23.5%)
Hidden File Found	Medium	1 (5.9%)
Missing Anti-clickjacking Header	Medium	15 (88.2%)
XSLT Injection	Medium	2 (11.8%)
Application Error Disclosure	Low	1 (5.9%)
Cookie No HttpOnly Flag	Low	3 (17.6%)
Cookie without SameSite Attribute	Low	3 (17.6%)
Total		17

Alert type	Risk	Count
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	32 (188.2%)
X-Content-Type-Options Header Missing	Low	18 (105.9%)
Authentication Request Identified	Informational	1 (5.9%)
GET for POST	Informational	1 (5.9%)
Session Management Response Identified	Informational	2 (11.8%)
User Agent Fuzzer	Informational	216 (1,270.6%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	10 (58.8%)
Total		17

Alerts

Risk=High, Confidence=Medium (1)

http://localhost (1)

Path Traversal (1)

▶ GET http://localhost/bWAPP/directory_traversal_1.php?page=%2Fetc%2Fpasswd

Risk=Medium, Confidence=High (2)

http://localhost (2)

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

▶ GET http://localhost/bWAPP/login.php

Hidden File Found (1)

▶ GET http://localhost/server-status

Risk=Medium, Confidence=Medium (3)

http://localhost (3)

Directory Browsing (1)

▶ GET http://localhost/bWAPP/fonts/

Missing Anti-clickjacking Header (1)

▶ GET http://localhost/bWAPP/login.php

XSLT Injection (1)

▶ POST http://localhost/bWAPP/

insecure_direct_object_ref_3.php

Risk=Medium, Confidence=Low (1)

http://localhost (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://localhost/bWAPP/login.php

Risk=Low, Confidence=High (1)

http://localhost (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET http://localhost/bWAPP/stylesheets/stylesheet.css

Risk=Low, Confidence=Medium (4)

http://localhost (4)

Application Error Disclosure (1)

▶ GET http://localhost/bWAPP/sqli_1.php

Cookie No HttpOnly Flag (1)

▶ GET http://localhost/bWAPP/login.php

Cookie without SameSite Attribute (1)

▶ GET http://localhost/bWAPP/login.php

X-Content-Type-Options Header Missing (1)

▶ GET http://localhost/bWAPP/js/html5.js

Risk=Informational, Confidence=High (2)

http://localhost (2)

Authentication Request Identified (1)

▶ POST http://localhost/bWAPP/login.php

GET for POST (1)

▶ GET http://localhost/bWAPP/login.php

Risk=Informational, Confidence=Medium (2)

http://localhost (2)

Session Management Response Identified (1)

▶ GET http://localhost/bWAPP/login.php

User Agent Fuzzer (1)

▶ POST http://localhost/bWAPP/ba_pwd_attacks_1.php

Risk=Informational, Confidence=Low (1)

http://localhost (1)

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

▶ POST http://localhost/bWAPP/login.php

Appendix

Alert Types

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

Path Traversal

Source	raised by an active scanner (Path Traversal)
CWE ID	22
WASC ID	33
Reference	▪ https://owasp.org/www-community/attacks/Path_Traversal ▪ https://cwe.mitre.org/data/definitions/22.html

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	▪ https://cheatsheetseries.owasp.org/

cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

- 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 - https://www.w3.org/TR/CSP/ - https://w3c.github.io/webappsec-csp/ - https://web.dev/articles/csp - https://caniuse.com/#feat=contentsecuritypolicy - https://content-security-policy.com/

Directory Browsing

Source	raised by an active scanner (Directory Browsing)
CWE ID	548
WASC ID	48
Reference	▪ https://httpd.apache.org/docs/mod/core.html#options

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13
Reference	▪ https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html ▪ https://httpd.apache.org/docs/current/mod/mod_status.html

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

XSLT Injection

Source	raised by an active scanner (XSLT Injection)
CWE ID	91
WASC ID	23
Reference	▪ https://www.contextis.com/blog/xslt-server-side-injection-attacks

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	550
WASC ID	13

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

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

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
WASC ID	13
Reference	▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) ▪ https://www.troyhunt.com/shhh-dont-let-your-response-headers/

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://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

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	▪ https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html