ZAP by Checkmarx Scanning Report

Generated with ZAP on Tue 8 Jul 2025, at 14:51:27

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%)	2 (11.1%)	0 (0.0%)	2 (11.1%)
	Medium	0 (0.0%)	1 (5.6%)	3 (16.7%)	1 (5.6%)	5 (27.8%)
	Low	0 (0.0%)	1 (5.6%)	5 (27.8%)	0 (0.0%)	6 (33.3%)
	Informational	0 (0.0%)	1 (5.6%)	2 (11.1%)	2 (11.1%)	5 (27.8%)
	Total	0 (0.0%)	3 (16.7%)	12 (66.7%)	3 (16.7%)	18 (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	2 (2)	5 (7)	6 (13)	5 (18)

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
Cross Site Scripting (Reflected)	High	5 (27.8%)
SQL Injection - MySQL	High	4 (22.2%)
Total		18

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	9 (50.0%)
Application Error Disclosure	Medium	2 (11.1%)
Content Security Policy (CSP) Header Not Set	Medium	11 (61.1%)
Missing Anti-clickjacking Header	Medium	8 (44.4%)
Vulnerable JS Library	Medium	2 (11.1%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	2 (11.1%)
Cookie No HttpOnly Flag	Low	1 (5.6%)
Cookie without SameSite Attribute	Low	1 (5.6%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	12 (66.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	30 (166.7%)
X-Content-Type-Options Header Missing	Low	23 (127.8%)
Authentication Request Identified	Informational	1 (5.6%)
Total		18

Alert type	Risk	Count
Information Disclosure - Suspicious Comments	Informational	3 (16.7%)
Modern Web Application	Informational	7 (38.9%)
Session Management Response Identified	Informational	2 (11.1%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	2 (11.1%)
Total		18

Alerts

Risk=High, Confidence=Medium (2)

http://localhost (2)

Cross Site Scripting (Reflected) (1)

▶ POST http://localhost/home-rental/auth/login.php

SQL Injection - MySQL (1)

▶ POST http://localhost/home-rental/index.php

Risk=Medium, Confidence=High (1)

http://localhost (1)

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

▶ GET http://localhost/sitemap.xml

Risk=Medium, Confidence=Medium (3)

http://localhost (3)

Application Error Disclosure (1)

▶ GET http://localhost/home-rental/app/register.php

Missing Anti-clickjacking Header (1)

▶ GET http://localhost/home-rental/

Vulnerable JS Library (1)

▶ GET http://localhost/home-rental/assets/plugins/bootstrap/js/bootstrap.min.js

Risk=Medium, Confidence=Low (1)

http://localhost (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://localhost/home-rental/auth/register.php

Risk=Low, Confidence=High (1)

http://localhost (1)

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

▶ GET http://localhost/home-rental/assets/css/rent.css

Risk=Low, Confidence=Medium (5)

http://localhost (5)

Big Redirect Detected (Potential Sensitive Information Leak) (1)

▶ GET http://localhost/home-rental/app/register.php

Cookie No HttpOnly Flag (1)

▶ GET http://localhost/home-rental/

Cookie without SameSite Attribute (1)

▶ GET http://localhost/home-rental/

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▶ GET http://localhost/home-rental/auth/register.php

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

▶ GET http://localhost/home-rental/assets/css/style.css

Risk=Informational, Confidence=High (1)

http://localhost (1)

Authentication Request Identified (1)

▶ POST http://localhost/home-rental/auth/login.php

Risk=Informational, Confidence=Medium (2)

http://localhost (2)

Modern Web Application (1)

▶ GET http://localhost/home-rental/

Session Management Response Identified (1)

▶ GET http://localhost/home-rental/

Risk=Informational, Confidence=Low (2)

http://localhost (2)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost/home-rental/assets/js/contact_me.js

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

▶ POST http://localhost/home-rental/auth/register.php

Appendix

Alert Types

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

Cross Site Scripting (Reflected)

Source	raised by an active scanner (Cross Site Scripting (Reflected))
CWE ID	79
WASC ID	8
Reference	- https://owasp.org/www-community/attacks/xss/ - https://cwe.mitre.org/data/definitions/79.html

SQL Injection - MySQL

Source	raised by an active scanner (SQL Injection)
CWE ID	89
WASC ID	19
Reference	- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.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

Application Error Disclosure

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

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/

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

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	1395
Reference	- https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Big Redirect Detected (Potential Sensitive Information Leak)

Source	raised by a passive scanner (Big Redirect Detected (Potential Sensitive Information Leak))
CWE ID	201
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 Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
CWE ID	497
WASC ID	13
Reference	- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-

Information_Gathering/08-Fingerprint_Web_Application_Framework

- https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

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/

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	615
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 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