ZAP by Checkmarx Scanning Report

Generated with ZAP on Sun 20 Apr 2025, at 04:40:28

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://192.168.1.27:8088`

(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 (2.9%)	0 (0.0%)	1 (2.9%)
	Medium	0 (0.0%)	2 (5.9%)	4 (11.8%)	1 (2.9%)	7 (20.6%)
	Low	0 (0.0%)	1 (2.9%)	5 (14.7%)	3 (8.8%)	9 (26.5%)
	Informational	0 (0.0%)	4 (11.8%)	12 (35.3%)	1 (2.9%)	17 (50.0%)
	Total	0 (0.0%)	7 (20.6%)	22 (64.7%)	5 (14.7%)	34 (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://192.168.1.27:8088	1 (1)	7 (8)	9 (17)	17 (34)

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	2 (5.9%)
Absence of Anti-CSRF Tokens	Medium	3 (8.8%)
Anti-CSRF Tokens Check	Medium	1 (2.9%)
Content Security Policy (CSP) Header Not Set	Medium	115 (338.2%)
Total		34

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	61 (179.4%)
Relative Path Confusion	Medium	68 (200.0%)
Source Code Disclosure - SQL	Medium	1 (2.9%)
Sub Resource Integrity Attribute Missing	Medium	1 (2.9%)
Cookie Slack Detector	Low	77 (226.5%)
Cookie without SameSite Attribute	Low	1 (2.9%)
Cross-Domain JavaScript Source File Inclusion	Low	1 (2.9%)
Dangerous JS Functions	Low	1 (2.9%)
Insufficient Site Isolation Against Spectre Vulnerability	Low	222 (652.9%)
Permissions Policy Header Not Set	Low	117 (344.1%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	161 (473.5%)
Timestamp Disclosure - Unix	Low	2 (5.9%)
X-Content-Type-Options Header Missing	Low	100 (294.1%)
Total		34

Alert type	Risk	Count
Base64 Disclosure	Informational	5 (14.7%)
Cookie Slack Detector	Informational	2 (5.9%)
Information Disclosure - Suspicious Comments	Informational	10 (29.4%)
Modern Web Application	Informational	6 (17.6%)
Non-Storable Content	Informational	3 (8.8%)
Sec-Fetch-Dest Header is Missing	Informational	161 (473.5%)
Sec-Fetch-Mode Header is Missing	Informational	161 (473.5%)
Sec-Fetch-Site Header is Missing	Informational	161 (473.5%)
Sec-Fetch-User Header is Missing	Informational	161 (473.5%)
Session Management Response Identified	Informational	2 (5.9%)
Storable and Cacheable Content	Informational	158 (464.7%)
Tech Detected - Adobe Flash	Informational	1 (2.9%)
Tech Detected - Apache Tomcat	Informational	1 (2.9%)
Total		34

Alert type	Risk	Count
Tech Detected - Java	Informational	1 (2.9%)
Tech Detected - React	Informational	1 (2.9%)
Tech Detected - Swagger UI	Informational	1 (2.9%)
User Agent Fuzzer	Informational	121 (355.9%)
Total		34

Alerts

Risk=High, Confidence=Medium (1)

http://192.168.1.27:8088 (1)

Cross Site Scripting (Reflected) (1)

▶ POST http://192.168.1.27:8088/altoromutual/sendFeedback

Risk=Medium, Confidence=High (2)

http://192.168.1.27:8088 (2)

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

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Sub Resource Integrity Attribute Missing (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_investments.htm

Risk=Medium, Confidence=Medium (4)

http://192.168.1.27:8088 (4)

Anti-CSRF Tokens Check (1)

▶ POST http://192.168.1.27:8088/altoromutual/sendFeedback

Missing Anti-clickjacking Header (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Relative Path Confusion (1)

▶ GET http://192.168.1.27:8088/altoromutual/default.jsp

Source Code Disclosure - SQL (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=inside_trainee.htm

Risk=Medium, Confidence=Low (1)

http://192.168.1.27:8088 (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://192.168.1.27:8088/altoromutual/feedback.jsp

Risk=Low, Confidence=High (1)

http://192.168.1.27:8088 (1)

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

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Risk=Low, Confidence=Medium (5)

http://192.168.1.27:8088 (5)

Cookie without SameSite Attribute (1)

▶ GET http://192.168.1.27:8088/altoromutual/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_investments.htm

Insufficient Site Isolation Against Spectre Vulnerability (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Permissions Policy Header Not Set (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

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

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Risk=Low, Confidence=Low (3)

http://192.168.1.27:8088 (3)

Cookie Slack Detector (1)

▶ POST http://192.168.1.27:8088/altoromutual/doLogin

Dangerous JS Functions (1)

▶ GET http://192.168.1.27:8088/altoromutual/status_check.jsp

Timestamp Disclosure - Unix (1)

▶ GET http://192.168.1.27:8088/altoromutual/swagger/swagger-ui-standalone-preset.js

Risk=Informational, Confidence=High (4)

http://192.168.1.27:8088 (4)

Sec-Fetch-Dest Header is Missing (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Sec-Fetch-Mode Header is Missing (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Sec-Fetch-Site Header is Missing (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Sec-Fetch-User Header is Missing (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Risk=Informational, Confidence=Medium (12)

http://192.168.1.27:8088 (12)

Base64 Disclosure (1)

▶ GET http://192.168.1.27:8088/altoromutual/login.jsp

Information Disclosure - Suspicious Comments (1)

▶ GET http://192.168.1.27:8088/altoromutual/login.jsp

Modern Web Application (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_other.htm

Non-Storable Content (1)

▶ GET http://192.168.1.27:8088/altoromutual/admin/clients.xls

Session Management Response Identified (1)

▶ GET http://192.168.1.27:8088/altoromutual/

Storable and Cacheable Content (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Tech Detected - Adobe Flash (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=inside_contact.htm

Tech Detected - Apache Tomcat (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Tech Detected - Java (1)

▶ GET http://192.168.1.27:8088/altoromutual/index.jsp?content=personal_cards.htm

Tech Detected - React (1)

▶ GET http://192.168.1.27:8088/altoromutual/swagger/swagger-ui-bundle.js

Tech Detected - Swagger UI (1)

▶ GET http://192.168.1.27:8088/altoromutual/swagger/index.html

User Agent Fuzzer (1)

▶ GET http://192.168.1.27:8088/altoromutual/admin

Risk=Informational, Confidence=Low (1)

http://192.168.1.27:8088 (1)

Cookie Slack Detector (1)

▶ GET http://192.168.1.27:8088/altoromutual/login.jsp

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

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

Anti-CSRF Tokens Check

Source	raised by an active scanner (Anti-CSRF Tokens Check)
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/

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

Relative Path Confusion

Source	raised by an active scanner (Relative Path Confusion)
CWE ID	20
WASC ID	20
Reference	▪ https://arxiv.org/abs/1811.00917 ▪ https://hsivonen.fi/doctype/ ▪ https://www.w3schools.com/tags/tag_base.asp

Source Code Disclosure - SQL

Source	raised by a passive scanner (Source Code Disclosure)
CWE ID	540
WASC ID	13
Reference	▪ https://www.wsj.com/articles/BL-CIOB-2999

Sub Resource Integrity Attribute Missing

Source	raised by a passive scanner (Sub Resource Integrity Attribute Missing)
CWE ID	345
WASC ID	15

Reference	- https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Cookie Slack Detector

Source	raised by an active scanner (Cookie Slack Detector)
CWE ID	205
WASC ID	45
Reference	- https://cwe.mitre.org/data/definitions/205.html

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

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

Dangerous JS Functions

Source	raised by a passive scanner (Dangerous JS Functions)
CWE ID	749
Reference	▪ https://angular.io/guide/security

Insufficient Site Isolation Against Spectre Vulnerability

Source	raised by a passive scanner (Insufficient Site Isolation Against Spectre Vulnerability)
CWE ID	693
WASC ID	14
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy

Permissions Policy Header Not Set

Source	raised by a passive scanner (Permissions Policy Header Not Set)
CWE ID	693
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy ▪ https://developer.chrome.com/blog/feature-policy/ ▪ https://scotthelme.co.uk/a-new-security-header-feature-policy/

	▪ https://w3c.github.io/webappsec-feature-policy/ ▪ https://www.smashingmagazine.com/2018/12/feature-policy/

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/

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	497
WASC ID	13
Reference	▪ https://cwe.mitre.org/data/definitions/200.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	▪ 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

Base64 Disclosure

Source	raised by a passive scanner (Base64 Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ https://projects.webappsec.org/w/page/13246936/Information%20Leakage

Cookie Slack Detector

Source	raised by an active scanner (Cookie Slack Detector)
CWE ID	205
WASC ID	45
Reference	▪ https://cwe.mitre.org/data/definitions/205.html

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)

Non-Storable Content

Source	raised by a passive scanner (Content Cacheability)
CWE ID	524
WASC ID	13
Reference	▪ https://datatracker.ietf.org/doc/html/rfc7234 ▪ https://datatracker.ietf.org/doc/html/rfc7231 ▪ https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html

Sec-Fetch-Dest Header is Missing

Source	raised by a passive scanner (Fetch Metadata Request Headers)
CWE ID	352

WASC ID	9
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Dest

Sec-Fetch-Mode Header is Missing

Source	raised by a passive scanner (Fetch Metadata Request Headers)
CWE ID	352
WASC ID	9
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Mode

Sec-Fetch-Site Header is Missing

Source	raised by a passive scanner (Fetch Metadata Request Headers)
CWE ID	352
WASC ID	9
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Site

Sec-Fetch-User Header is Missing

Source	raised by a passive scanner (Fetch Metadata Request Headers)
CWE ID	352
WASC ID	9
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-User

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

Storable and Cacheable Content

Source	raised by a passive scanner (Content Cacheability)
CWE ID	524
WASC ID	13
Reference	▪ https://datatracker.ietf.org/doc/html/rfc7234 ▪ https://datatracker.ietf.org/doc/html/rfc7231 ▪ https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html

Tech Detected - Adobe Flash

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://www.adobe.com/products/flashplayer

Tech Detected - Apache Tomcat

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://tomcat.apache.org

Tech Detected - Java

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://java.com

Tech Detected - React

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://reactjs.org

Tech Detected - Swagger UI

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://swagger.io/tools/swagger-ui

User Agent Fuzzer

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