ZAP by Checkmarx Scanning Report

Generated with ZAP on Mon 10 Mar 2025, at 16:21:59

ZAP Version: 2.16.0

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://testfire.net

(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%)	1 (6.2%)	0 (0.0%)	0 (0.0%)	1 (6.2%)
	Medium	0 (0.0%)	1 (6.2%)	1 (6.2%)	1 (6.2%)	3 (18.8%)
	Low	0 (0.0%)	1 (6.2%)	6 (37.5%)	1 (6.2%)	8 (50.0%)
	Informational	0 (0.0%)	0 (0.0%)	3 (18.8%)	1 (6.2%)	4 (25.0%)
	Total	0 (0.0%)	3 (18.8%)	10 (62.5%)	3 (18.8%)	16 (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://testfire.net	1 (1)	3 (4)	8 (12)	4 (16)

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
PII Disclosure	High	4 (25.0%)
Absence of Anti-CSRF Tokens	Medium	3 (18.8%)
Content Security Policy (CSP) Header Not Set	Medium	170 (1,062.5%)
Total		16

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	65 (406.2%)
Application Error Disclosure	Low	2 (12.5%)
Cookie No HttpOnly Flag	Low	1 (6.2%)
Cookie without SameSite Attribute	Low	4 (25.0%)
Cross-Domain JavaScript Source File Inclusion	Low	1 (6.2%)
Information Disclosure - Debug Error Messages	Low	2 (12.5%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	215 (1,343.8%)
Timestamp Disclosure - Unix	Low	2 (12.5%)
X-Content-Type-Options Header Missing	Low	104 (650.0%)
Information Disclosure - Suspicious Comments	Informational	11 (68.8%)
Modern Web Application	Informational	6 (37.5%)
Session Management Response Identified	Informational	16 (100.0%)
Total		16

Alert type	Risk	Count
User Controllable HTML Element Attribute (Potential XSS)	Informational	1 (6.2%)
Total		16

Alerts

Risk=High, Confidence=High (1)

http://testfire.net (1)

PII Disclosure (1)

- GET http://testfire.net/bank/main.jsp

Risk=Medium, Confidence=High (1)

http://testfire.net (1)

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

- GET http://testfire.net/

Risk=Medium, Confidence=Medium (1)

http://testfire.net (1)

Missing Anti-clickjacking Header (1)

- GET http://testfire.net/

Risk=Medium, Confidence=Low (1)

http://testfire.net (1)

Absence of Anti-CSRF Tokens (1)

- GET http://testfire.net/login.jsp

Risk=Low, Confidence=High (1)

http://testfire.net (1)

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

- GET http://testfire.net/

Risk=Low, Confidence=Medium (6)

http://testfire.net (6)

Application Error Disclosure (1)

- POST http://testfire.net/doLogin

Cookie No HttpOnly Flag (1)

- POST http://testfire.net/doLogin

Cookie without SameSite Attribute (1)

- GET http://testfire.net/

Cross-Domain JavaScript Source File Inclusion (1)

- GET http://testfire.net/index.jsp?content=personal_investments.htm

Information Disclosure - Debug Error Messages (1)

- POST http://testfire.net/doLogin

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

- GET http://testfire.net/

Risk=Low, Confidence=Low (1)

http://testfire.net (1)

Timestamp Disclosure - Unix (1)

- GET http://testfire.net/swagger/swagger-ui-standalone-preset.js

Risk=Informational, Confidence=Medium (3)

http://testfire.net (3)

Information Disclosure - Suspicious Comments (1)

- GET http://testfire.net/login.jsp

Modern Web Application (1)

- GET http://testfire.net/index.jsp?content=inside.htm

Session Management Response Identified (1)

- GET http://testfire.net/

Risk=Informational, Confidence=Low (1)

http://testfire.net (1)

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

▶ GET http://testfire.net/bank/showAccount?listAccounts=800002

Appendix

Alert types

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

PII Disclosure

Source	raised by a passive scanner (PII Disclosure)
CWE ID	359
WASC ID	13

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/

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

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

Cross-Domain JavaScript Source File Inclusion

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

Information Disclosure - Debug Error Messages

Source	raised by a passive scanner (Information Disclosure - Debug Error Messages)
CWE ID	1295
WASC ID	13

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

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