ZAP by- Checkmarx Scanning Report

Generated with ZAP on Wed 18 Feb 2026, at 21:16:42

ZAP Version: 2.17.0

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:

- https://testhtml5.vulnweb.com
- http://testhtml5.vulnweb.com

(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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (11.8%)	3 (17.6%)	1 (5.9%)	6 (35.3%)
	Low	0 (0.0%)	1 (5.9%)	5 (29.4%)	0 (0.0%)	6 (35.3%)
	Informational	0 (0.0%)	1 (5.9%)	3 (17.6%)	1 (5.9%)	5 (29.4%)
	Total	0 (0.0%)	4 (23.5%)	11 (64.7%)	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	https://testhtml5.vulnweb.com	0 (0)	1 (1)	0 (1)	0 (1)
	http://testhtml5.vulnweb.com	0 (0)	5 (5)	6 (11)	5 (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
Absence of Anti-CSRF Tokens	Medium	1 (5.9%)
Content Security Policy (CSP) Header Not Set	Medium	3 (17.6%)
Total		17

Alert type	Risk	Count
Cross-Domain Misconfiguration	Medium	1 (5.9%)
HTTP Only Site	Medium	1 (5.9%)
Missing Anti-clickjacking Header	Medium	1 (5.9%)
Sub Resource Integrity Attribute Missing	Medium	5 (29.4%)
Cookie No HttpOnly Flag	Low	1 (5.9%)
Cookie without SameSite Attribute	Low	1 (5.9%)
Cross-Domain JavaScript Source File Inclusion	Low	4 (23.5%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	5 (29.4%)
Vulnerable JS Library	Low	1 (5.9%)
X-Content-Type-Options Header Missing	Low	5 (29.4%)
Authentication Request Identified	Informational	1 (5.9%)
Cookie Poisoning	Informational	1 (5.9%)
Total		17

Alert type	Risk	Count
Information Disclosure - Suspicious Comments	Informational	2 (11.8%)
Modern Web Application	Informational	1 (5.9%)
User Agent Fuzzer	Informational	2 (11.8%)
Total		17

Insights

This table shows information that is likely to be very relevant to you, but which is not related to vulnerabilities, or potentially even related to the application in question.

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP errors logged - see the zap.log file for details	1
Low	Warning		ZAP warnings logged - see the zap.log file for details	11
Info	Informational		Percentage of network failures	8 %
Info	Informational	http://testhtml5.vulnweb.com	Percentage of responses with status code 2xx	23 %
Info	Informational	http://testhtml5.vulnweb.com	Percentage of responses with status code 3xx	1 %
Info	Informational	http://testhtml5.vulnweb.com	Percentage of responses with status code 4xx	75 %

Level	Reason	Site	Description	Statistic
Info	Informational	http://testhtml5.vulnweb.com	Percentage of endpoints with content type application/javascript	45 %
Info	Informational	http://testhtml5.vulnweb.com	Percentage of endpoints with content type image/png	9 %
Info	Informational	http://testhtml5.vulnweb.com	Percentage of endpoints with content type text/css	9 %
Info	Informational	http://testhtml5.vulnweb.com	Percentage of endpoints with content type text/html	36 %
Info	Informational	http://testhtml5.vulnweb.com	Percentage of endpoints with method GET	90 %
Info	Informational	http://testhtml5.vulnweb.com	Percentage of endpoints with method POST	9 %
Info	Informational	http://testhtml5.vulnweb.com	Count of total endpoints	11
Info	Informational	http://testhtml5.vulnweb.com	Percentage of slow responses	100 %
Info	Informational	https://testhtml5.vulnweb.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://testhtml5.vulnweb.com	Count of total endpoints	1

Alerts

Risk=Medium, Confidence=High (2)

http://testhtml5.vulnweb.com (2)

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

▶ GET http://testhtml5.vulnweb.com/sitemap.xml

Sub Resource Integrity Attribute Missing (1)

▶ GET http://testhtml5.vulnweb.com/

Risk=Medium, Confidence=Medium (3)

https://testhtml5.vulnweb.com (1)

HTTP Only Site (1)

▶ GET http://testhtml5.vulnweb.com/

http://testhtml5.vulnweb.com (2)

Cross-Domain Misconfiguration (1)

▶ GET http://testhtml5.vulnweb.com/

Missing Anti-clickjacking Header (1)

▶ GET http://testhtml5.vulnweb.com/

Risk=Medium, Confidence=Low (1)

http://testhtml5.vulnweb.com (1)

Absence of Anti-CSRF Tokens (1)

▶ `GET http://testhtml5.vulnweb.com/`

Risk=Low, Confidence=High (1)

`http://testhtml5.vulnweb.com` (1)

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

▶ `GET http://testhtml5.vulnweb.com/robots.txt`

Risk=Low, Confidence=Medium (5)

`http://testhtml5.vulnweb.com` (5)

Cookie No HttpOnly Flag (1)

▶ `POST http://testhtml5.vulnweb.com/login`

Cookie without SameSite Attribute (1)

▶ `POST http://testhtml5.vulnweb.com/login`

Cross-Domain JavaScript Source File Inclusion (1)

▶ `GET http://testhtml5.vulnweb.com/`

Vulnerable JS Library (1)

▶ `GET http://testhtml5.vulnweb.com/static/app/libs/sessvars.js`

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

▶ `GET http://testhtml5.vulnweb.com/`

Risk=Informational, Confidence=High (1)

http://testhtml5.vulnweb.com (1)

Authentication Request Identified (1)

▶ POST http://testhtml5.vulnweb.com/login

Risk=Informational, Confidence=Medium (3)

http://testhtml5.vulnweb.com (3)

Information Disclosure - Suspicious Comments (1)

▶ GET http://testhtml5.vulnweb.com/

Modern Web Application (1)

▶ GET http://testhtml5.vulnweb.com/

User Agent Fuzzer (1)

▶ GET http://testhtml5.vulnweb.com/

Risk=Informational, Confidence=Low (1)

http://testhtml5.vulnweb.com (1)

Cookie Poisoning (1)

▶ POST http://testhtml5.vulnweb.com/login

Appendix

Alert Types

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

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/HTTP/Guides/CSP ▪ 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/

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	▪ https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy

HTTP Only Site

Source	raised by an active scanner (HTTP Only Site)
CWE ID	311
WASC ID	4
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html ▪ https://letsencrypt.org/

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/Reference/Headers/X-Frame-Options

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 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://datatracker.ietf.org/doc/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

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/

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/

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/

Cookie Poisoning

Source	raised by a passive scanner (Cookie Poisoning)
CWE ID	565
WASC ID	20
Reference	- https://en.wikipedia.org/wiki/HTTP_cookie - https://cwe.mitre.org/data/definitions/565.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)

User Agent Fuzzer

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