ZAP by Checkmarx Scanning Report

Generated with ZAP on Mon 2 Feb 2026, at 07:20:24

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:

- http://localhost:8080

(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%)	7 (41.2%)	1 (5.9%)	0 (0.0%)	8 (47.1%)
	Low	0 (0.0%)	0 (0.0%)	3 (17.6%)	0 (0.0%)	3 (17.6%)
	Informational	0 (0.0%)	2 (11.8%)	3 (17.6%)	1 (5.9%)	6 (35.3%)
	Total	0 (0.0%)	9 (52.9%)	7 (41.2%)	1 (5.9%)	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:8080	0 (0)	8 (8)	3 (11)	6 (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
CSP: Failure to Define Directive with No Fallback	Medium	4 (23.5%)
CSP: Wildcard Directive	Medium	4 (23.5%)
CSP: script-src unsafe-eval	Medium	4 (23.5%)
CSP: script-src unsafe-inline	Medium	4 (23.5%)
CSP: style-src unsafe-inline	Medium	4 (23.5%)
Content Security Policy (CSP) Header Not Set	Medium	5 (29.4%)
Total		17

Alert type	Risk	Count
Session ID in URL Rewrite	Medium	5 (29.4%)
Spring Actuator Information Leak	Medium	1 (5.9%)
Application Error Disclosure	Low	8 (47.1%)
Cookie without SameSite Attribute	Low	2 (11.8%)
X-Content-Type-Options Header Missing	Low	5 (29.4%)
Authentication Request Identified	Informational	1 (5.9%)
GET for POST	Informational	1 (5.9%)
Information Disclosure - Suspicious Comments	Informational	4 (23.5%)
Modern Web Application	Informational	4 (23.5%)
Session Management Response Identified	Informational	37 (217.6%)
User Agent Fuzzer	Informational	3 (17.6%)
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	9
Low	Warning		ZAP warnings logged - see the zap.log file for details	391
Low	Exceeded High	http://localhost:8080	Percentage of slow responses	50 %
Info	Informational		Percentage of network failures	1 %
Info	Informational	http://clientservices.googleapis.com	Percentage of responses with status code 3xx	100 %
Info	Informational	http://clientservices.googleapis.com	Percentage of endpoints with method GET	100 %
Info	Informational	http://clientservices.googleapis.com	Count of total endpoints	1
Info	Informational	http://detectpor	Percentage of responses with	100 %

Level	Reason	Site	Description	Statistic
		tal.brave-http-only.com	status code 2xx	
Info	Informational	http://detectportal.brave-http-only.com	Percentage of endpoints with method GET	100 %
Info	Informational	http://detectportal.brave-http-only.com	Count of total endpoints	1
Info	Informational	http://detectportal.brave-http-only.com	Percentage of slow responses	100 %
Info	Informational	http://example.com	Percentage of responses with status code 2xx	100 %
Info	Informational	http://example.com	Percentage of endpoints with content type text/html	100 %
Info	Informational	http://example.com	Percentage of endpoints with method GET	100 %
Info	Informational	http://example.	Count of total endpoints	1

Level	Reason	Site	Description	Statistic
		com		
Info	Informational	http://example.com	Percentage of slow responses	75 %
Info	Informational	http://ipv6.msftconnecttest.com	Percentage of endpoints with content type text/plain	100 %
Info	Informational	http://ipv6.msftconnecttest.com	Percentage of endpoints with method GET	100 %
Info	Informational	http://ipv6.msftconnecttest.com	Count of total endpoints	1
Info	Informational	http://localhost:8080	Percentage of responses with status code 2xx	63 %
Info	Informational	http://localhost:8080	Percentage of responses with status code 3xx	31 %
Info	Informational	http://localhost:8080	Percentage of responses with status code 4xx	3 %
Info	Informational	http://localhost:8080	Percentage of responses with status code 5xx	2 %
Info	Informational	http://localhost:8080	Percentage of endpoints with content type application/json	1 %

Level	Reason	Site	Description	Statistic
Info	Informational	http://localhost:8080	Percentage of endpoints with content type application/xml	10 %
Info	Informational	http://localhost:8080	Percentage of endpoints with content type font/ttf	1 %
Info	Informational	http://localhost:8080	Percentage of endpoints with content type image/png	2 %
Info	Informational	http://localhost:8080	Percentage of endpoints with content type image/x-icon	1 %
Info	Informational	http://localhost:8080	Percentage of endpoints with content type text/css	6 %
Info	Informational	http://localhost:8080	Percentage of endpoints with content type text/html	22 %
Info	Informational	http://localhost:8080	Percentage of endpoints with content type text/javascript	6 %
Info	Informational	http://localhost:8080	Percentage of endpoints with content type text/xml	11 %

Level	Reason	Site	Description	Statistic
Info	Informational	http://localhost:8080	Percentage of endpoints with method GET	98 %
Info	Informational	http://localhost:8080	Percentage of endpoints with method POST	1 %
Info	Informational	http://localhost:8080	Count of total endpoints	80
Info	Informational	http://www.msftconnecttest.com	Percentage of responses with status code 2xx	100 %
Info	Informational	http://www.msftconnecttest.com	Percentage of endpoints with content type text/plain	100 %
Info	Informational	http://www.msftconnecttest.com	Percentage of endpoints with method GET	100 %
Info	Informational	http://www.msftconnecttest.com	Count of total endpoints	1
Info	Informational	https://localhost:8080	Percentage of endpoints with method GET	100 %
Info	Informational	https://localhost:8080	Count of total endpoints	1

Alerts

Risk=Medium, Confidence=High (7)

http://localhost:8080 (7)

CSP: Failure to Define Directive with No Fallback (1)

▶ GET http://localhost:8080/midpoint/login?0

CSP: Wildcard Directive (1)

▶ GET http://localhost:8080/midpoint/login?0

CSP: script-src unsafe-eval (1)

▶ GET http://localhost:8080/midpoint/login?0

CSP: script-src unsafe-inline (1)

▶ GET http://localhost:8080/midpoint/login?0

CSP: style-src unsafe-inline (1)

▶ GET http://localhost:8080/midpoint/login?0

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

▶ GET http://localhost:8080/midpoint/login;jsessionid=226003264B7791EAFC2DC7E6B72D0E34

Session ID in URL Rewrite (1)

▶ GET http://localhost:8080/midpoint/login;jsessionid=6CF70FB9917F8F3203D24D034FA3AEE0

Risk=Medium, Confidence=Medium (1)

http://localhost:8080 (1)

Spring Actuator Information Leak (1)

▶ GET http://localhost:8080/midpoint/actuator/health

Risk=Low, Confidence=Medium (3)

http://localhost:8080 (3)

Application Error Disclosure (1)

▶ GET http://localhost:8080/midpoint/fonts

Cookie without SameSite Attribute (1)

▶ GET http://localhost:8080/midpoint/self/dashboard

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

▶ GET http://localhost:8080/midpoint/css/font-evosome-feccb5b1b8af6616c0da6e4b72dd711d.css

Risk=Informational, Confidence=High (2)

http://localhost:8080 (2)

Authentication Request Identified (1)

▶ POST http://localhost:8080/midpoint/auth/gui-default/loginForm/spring_security_login

GET for POST (1)

▶ GET http://localhost:8080/midpoint/auth/gui-default/loginForm/spring_security_login

Risk=Informational, Confidence=Medium (3)

http://localhost:8080 (3)

Modern Web Application (1)

▶ GET http://localhost:8080/midpoint/login?0

Session Management Response Identified (1)

▶ GET http://localhost:8080/midpoint/self/dashboard

User Agent Fuzzer (1)

▶ GET http://localhost:8080/midpoint/admin/users?3-1.0-&windowName=ed5c2665-8837-41de-9bde-59f1ebc49400&_=1769990288987

Risk=Informational, Confidence=Low (1)

http://localhost:8080 (1)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:8080/midpoint/wicket/resource/org.apache.wicket.ajax.AbstractDefaultAjaxBehavior/res/js/wicket-ajax-jquery-ver-8CD946166F47E5DD4EADD165939FF57D.js

Appendix

Alert Types

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

CSP: Failure to Define Directive with No Fallback

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://web.dev/articles/csp#resource-options

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://web.dev/articles/csp#resource-options

CSP: script-src unsafe-eval

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://web.dev/articles/csp#resource-options

CSP: script-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://web.dev/articles/csp#resource-options

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://web.dev/articles/csp#resource-options

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/

Session ID in URL Rewrite

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	598
WASC ID	13
Reference	▪ https://seclists.org/webappsec/2002/q4/111

Spring Actuator Information Leak

Source	raised by an active scanner (Spring Actuator Information Leak)
CWE ID	215
WASC ID	13
Reference	▪ https://docs.spring.io/spring-boot/api/rest/actuator/index.html#overview

Application Error Disclosure

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

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

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

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 Agent Fuzzer

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