ZAP by Checkmarx Scanning Report

Generated with ZAP on Sat 30 Nov 2024, at 22:29:45

ZAP Version: 2.15.0

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://myprojectnetwork.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%)	1 (7.7%)	1 (7.7%)
	Medium	0 (0.0%)	1 (7.7%)	1 (7.7%)	1 (7.7%)	3 (23.1%)
	Low	0 (0.0%)	1 (7.7%)	4 (30.8%)	0 (0.0%)	5 (38.5%)
	Informational	0 (0.0%)	1 (7.7%)	2 (15.4%)	1 (7.7%)	4 (30.8%)
	Total	0 (0.0%)	3 (23.1%)	7 (53.8%)	3 (23.1%)	13 (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://myprojectnetwork.com	1 (1)	1 (2)	2 (4)	2 (6)

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
Cloud Metadata Potentially Exposed	High	1 (7.7%)
Content Security Policy (CSP) Header Not Set	Medium	11 (84.6%)
Total		13

Alert type	Risk	Count
Hidden File Found	Medium	4 (30.8%)
Missing Anti-clickjacking Header	Medium	6 (46.2%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	5 (38.5%)
Cookie No HttpOnly Flag	Low	11 (84.6%)
Cross-Domain JavaScript Source File Inclusion	Low	8 (61.5%)
Strict-Transport-Security Header Not Set	Low	13 (100.0%)
X-Content-Type-Options Header Missing	Low	7 (53.8%)
Authentication Request Identified	Informational	1 (7.7%)
Re-examine Cache-control Directives	Informational	7 (53.8%)
Session Management Response Identified	Informational	15 (115.4%)
User Agent Fuzzer	Informational	12 (92.3%)
Total		13

Alerts

Risk=High, Confidence=Low (1)

https://myprojectnetwork.com (1)

Cloud Metadata Potentially Exposed (1)

▶ GET https://myprojectnetwork.com/latest/meta-data/

Risk=Medium, Confidence=High (1)

Risk=Medium, Confidence=Medium (1)

Risk=Medium, Confidence=Low (1)

https://myprojectnetwork.com (1)

Hidden File Found (1)

▶ GET https://myprojectnetwork.com/.hg

Risk=Low, Confidence=High (1)

Risk=Low, Confidence=Medium (4)

https://myprojectnetwork.com (2)

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

▶ GET https://myprojectnetwork.com/auth/redirect

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://myprojectnetwork.com/

Risk=Informational, Confidence=High (1)

https://myprojectnetwork.com (1)

Authentication Request Identified (1)

▶ POST https://myprojectnetwork.com/login

Risk=Informational, Confidence=Medium (2)

https://myprojectnetwork.com (1)

User Agent Fuzzer (1)

▶ GET https://myprojectnetwork.com/register

Risk=Informational, Confidence=Low (1)

Appendix

Alert types

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

Cloud Metadata Potentially Exposed

Source	raised by an active scanner (Cloud Metadata Potentially Exposed)

Reference	▪ https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/

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/

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13

Reference	▪ https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html

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

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

Cross-Domain JavaScript Source File Inclusion

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

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html ▪ https://owasp.org/www-community/Security_Headers ▪ https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ https://caniuse.com/stricttransportsecurity ▪ https://datatracker.ietf.org/doc/html/rfc6797

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/

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

- https://grayduck.mn/2021/09/13/cache-control-recommendations/

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