ZAP by Checkmarx Scanning Report-Roomhub

Generated with ZAP on Mon 2 Dec 2024, at 22:06:10

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://fonts.gstatic.com
- https://www.gstatic.com
- https://roomhubflutter.vercel.app
- https://img.icons8.com
- https://beacons.gcp.gvt2.com
- https://7hm4udd9s2.execute-api.ca-central-1.amazonaws.com
- https://cognito-idp.ca-central-1.amazonaws.com

- https://update.googleapis.com
- https://optimizationguide-pa.googleapis.com
- https://content-autofill.googleapis.com
- https://accounts.google.com
- https://room-hub.vercel.app

(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

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (5.3%)	1 (5.3%)
	Medium	0 (0.0%)	1 (5.3%)	2 (10.5%)	1 (5.3%)	4 (21.1%)
	Low	0 (0.0%)	1 (5.3%)	3 (15.8%)	1 (5.3%)	5 (26.3%)
	Informational	0 (0.0%)	0 (0.0%)	6 (31.6%)	3 (15.8%)	9 (47.4%)
	Total	0 (0.0%)	2 (10.5%)	11 (57.9%)	6 (31.6%)	19 (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://roomhubfluttter.vercel.app	0 (0)	0 (0)	0 (0)	1 (1)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://7hm4udd9s2.execute-api.ca-central-1.amazonaws.com	0 (0)	0 (0)	2 (2)	1 (3)
https://cognito-idp.ca-central-1.amazonaws.com	0 (0)	0 (0)	0 (0)	2 (2)
https://room-hub.vercel.app	1 (1)	4 (5)	3 (8)	5 (13)

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	2 (10.5%)
Content Security Policy (CSP) Header Not Set	Medium	22 (115.8%)
Cross-Domain Misconfiguration	Medium	56 (294.7%)
Total		19

Alert type	Risk	Count
Hidden File Found	Medium	4 (21.1%)
Missing Anti-clickjacking Header	Medium	16 (84.2%)
Application Error Disclosure	Low	1 (5.3%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	18 (94.7%)
Strict-Transport-Security Header Not Set	Low	74 (389.5%)
Timestamp Disclosure - Unix	Low	73 (384.2%)
X-Content-Type-Options Header Missing	Low	54 (284.2%)
Authentication Request Identified	Informational	1 (5.3%)
Information Disclosure - Sensitive Information in URL	Informational	4 (21.1%)
Information Disclosure - Suspicious Comments	Informational	20 (105.3%)
Modern Web Application	Informational	23 (121.1%)
Re-examine Cache-control Directives	Informational	52 (273.7%)
Total		19

Alert type	Risk	Count
Retrieved from Cache	Informational	58 (305.3%)
Session Management Response Identified	Informational	1 (5.3%)
User Agent Fuzzer	Informational	624 (3,284.2%)
Vulnerable JS Library	Informational	1 (5.3%)
Total		19

Alerts

Risk=High, Confidence=Low (1)

https://room-hub.vercel.app (1)

Cloud Metadata Potentially Exposed (1)

▶ GET https://room-hub.vercel.app/latest/meta-data/

Risk=Medium, Confidence=High (1)

https://room-hub.vercel.app (1)

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

▶ GET https://room-hub.vercel.app/sitemap.xml

Risk=Medium, Confidence=Medium (2)

https://room-hub.vercel.app (2)

Cross-Domain Misconfiguration (1)

▶ GET https://room-hub.vercel.app/favicon.ico

Missing Anti-clickjacking Header (1)

▶ GET https://room-hub.vercel.app/

Risk=Medium, Confidence=Low (1)

https://room-hub.vercel.app (1)

Hidden File Found (1)

▶ GET https://room-hub.vercel.app/.hg

Risk=Low, Confidence=High (1)

https://room-hub.vercel.app (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://room-hub.vercel.app/static/js/main.0fc38355.js

Risk=Low, Confidence=Medium (3)

https://7hm4udd9s2.execute-api.ca-central-1.amazonaws.com (2)

Application Error Disclosure (1)

▶ POST https://7hm4udd9s2.execute-api.ca-central-1.amazonaws.com/dev/notification/join-room-request

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▶ GET https://7hm4udd9s2.execute-api.ca-central-1.amazonaws.com/dev/user/hungludao@gmail.com/get-room

https://room-hub.vercel.app (1)

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

▶ GET https://room-hub.vercel.app/logo2.png

Risk=Low, Confidence=Low (1)

https://room-hub.vercel.app (1)

Timestamp Disclosure - Unix (1)

▶ GET https://room-hub.vercel.app/static/js/main.0fc38355.js

Risk=Informational, Confidence=Medium (6)

https://roomhubflutter.vercel.app (1)

User Agent Fuzzer (1)

▶ GET https://roomhubflutter.vercel.app/assets/packages/cupertino_icons/assets/CupertinoIcons.ttf

https://7hm4udd9s2.execute-api.ca-central-1.amazonaws.com (1)

Information Disclosure - Sensitive Information in URL (1)

▶ GET https://7hm4udd9s2.execute-api.ca-central-1.amazonaws.com/dev/room/get-pending-tasks?frm=hungludao%40gmail.com

https://cognito-idp.ca-central-1.amazonaws.com (1)

Session Management Response Identified (1)

▶ POST https://cognito-idp.ca-central-1.amazonaws.com/

https://room-hub.vercel.app (3)

Modern Web Application (1)

▶ GET https://room-hub.vercel.app/sitemap.xml

Retrieved from Cache (1)

▶ GET https://room-hub.vercel.app/favicon.ico

Vulnerable JS Library (1)

▶ GET https://room-hub.vercel.app/static/js/main.0fc38355.js

Risk=Informational, Confidence=Low (3)

https://cognito-idp.ca-central-1.amazonaws.com (1)

Authentication Request Identified (1)

▶ POST https://cognito-idp.ca-central-1.amazonaws.com/

https://room-hub.vercel.app (2)

Information Disclosure - Suspicious Comments (1)

▶ GET https://room-hub.vercel.app/static/js/main.0fc38355.js

Re-examine Cache-control Directives (1)

▶ GET https://room-hub.vercel.app/manifest.json

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/

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?id=desc.config.dotnet.html5_overly_permissive_cors_policy

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

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
CWE ID	200

WASC ID 13

Reference
- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework
- https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

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

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
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

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/

Information Disclosure - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

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/

Retrieved from Cache

Source raised by a passive scanner (Retrieved from Cache)

Reference
- https://tools.ietf.org/html/rfc7234
- https://tools.ietf.org/html/rfc7231
- https://www.rfc-editor.org/rfc/rfc9110.html

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

Vulnerable JS Library

Source raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))

CWE ID 829