ZAP by Checkmarx Scanning Report

Generated with ZAP on Mon 28 Jul 2025, at 22:14:59

ZAP Version: 2.16.1

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://chromewebstore.googleapis.com
- https://beacons.gcp.gvt2.com
- https://clientservices.googleapis.com
- https://update.googleapis.com
- https://passwordsleakcheck-pa.googleapis.com
- https://api.medmind.com
- https://cognito-idp.us-east-1.amazonaws.com
- https://strapi.medmind.com
- https://www.google-analytics.com

- https://www.googletagmanager.com
- https://optimizationguide-pa.googleapis.com
- https://content-autofill.googleapis.com
- https://android.clients.google.com
- https://medmind.com
- https://www.googleapis.com
- http://clients2.google.com
- https://accounts.google.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%)	1 (3.8%)	0 (0.0%)	1 (3.8%)	2 (7.7%)
	Medium	0 (0.0%)	3 (11.5%)	2 (7.7%)	0 (0.0%)	5 (19.2%)
	Low	0 (0.0%)	2 (7.7%)	7 (26.9%)	1 (3.8%)	10 (38.5%)
	Informational	0 (0.0%)	2 (7.7%)	4 (15.4%)	3 (11.5%)	9 (34.6%)
	Total	0 (0.0%)	8 (30.8%)	13 (50.0%)	5 (19.2%)	26 (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://cognito-idp.us-east-1.amazonaws.	0 (0)	0 (0)	0 (0)	1 (1)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://strapi.medmind.com	0 (0)	0 (0)	5 (5)	1 (6)
https://www.google-analytics.com	0 (0)	1 (1)	1 (2)	0 (2)
https://optimizationguide-pa.googleapis.com	0 (0)	1 (1)	0 (1)	0 (1)
https://content-autofill.googleapis.com	0 (0)	0 (0)	0 (0)	1 (1)
https://medmind.com	2 (2)	3 (5)	3 (8)	6 (14)
https://www.googleapis.com	0 (0)	0 (0)	1 (1)	0 (1)

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
Total		26

Alert type	Risk	Count
PII Disclosure	High	1 (3.8%)
Path Traversal	High	2 (7.7%)
Content Security Policy (CSP) Header Not Set	Medium	53 (203.8%)
Cross-Domain Misconfiguration	Medium	141 (542.3%)
Information Disclosure - JWT in Browser localStorage	Medium	3 (11.5%)
Missing Anti-clickjacking Header	Medium	53 (203.8%)
Session ID in URL Rewrite	Medium	5 (19.2%)
Cookie No HttpOnly Flag	Low	16 (61.5%)
Cookie Without Secure Flag	Low	8 (30.8%)
Cookie with SameSite Attribute None	Low	8 (30.8%)
Cookie without SameSite Attribute	Low	8 (30.8%)
Information Disclosure - Sensitive Information in Browser localStorage	Low	1 (3.8%)
Total		26

Alert type	Risk	Count
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	31 (119.2%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	6 (23.1%)
Strict-Transport-Security Header Not Set	Low	37 (142.3%)
Timestamp Disclosure - Unix	Low	49 (188.5%)
X-Content-Type-Options Header Missing	Low	190 (730.8%)
Authentication Request Identified	Informational	1 (3.8%)
Information Disclosure - Information in Browser localStorage	Informational	9 (34.6%)
Information Disclosure - Information in Browser sessionStorage	Informational	11 (42.3%)
Information Disclosure - Sensitive Information in URL	Informational	2 (7.7%)
Information Disclosure - Suspicious Comments	Informational	40 (153.8%)
Modern Web Application	Informational	4 (15.4%)
Re-examine Cache-control Directives	Informational	62 (238.5%)
Total		26

Alert type	Risk	Count
Retrieved from Cache	Informational	2768 (10,646.2%)
Session Management Response Identified	Informational	9 (34.6%)
Total		26

Alerts

Risk=High, Confidence=High (1)

https://medmind.com (1)

PII Disclosure (1)

▶ GET https://medmind.com/

Risk=High, Confidence=Low (1)

https://medmind.com (1)

Path Traversal (1)

▶ POST https://medmind.com/monitoring?o=4508132443488256&p=4508132459216896&r=monitoring

Risk=Medium, Confidence=High (3)

https://www.google-analytics.com (1)

Session ID in URL Rewrite (1)

▶ POST https://www.google-analytics.com/g/collect?v=2&tid=G-DKFZQ6FE4H&gtm=45je57n0v9125337445za200zd9125337445&_p=1753717148961&gcd=13l3l3l3l1l1&npa=0&dma=0&tag_exp=101509157~103116026~103200004~103233427~104684208~104684211~104948813~105134979~105134981&cid=1013652829.1753717149&ul=en-us&sr=1536x864&uaa=x86&uab=64&uafvl=Not)A%253BBrand%3B8.0.0.0%7CChromium%3B138.0.7204.169%7CGoogle%2520Chrome%3B138.0.7204.169&uamb=0&uam=&uap=Windows&uapv=19.0.0&uaw=0&are=1&frm=0&pscdl=noapi&_s=1&sid=1753717149&sct=1&seg=0&dl=https%3A%2F%2Fmedmind.com%2F&dt=Medmind%20-%20Empowering%20Your%20Health%20Journey%20with%20Intelligent%20AI%20Support&en=page_view&_fv=1&_nsi=1&_ss=1&_ee=1&tfd=2525

https://medmind.com (2)

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

▶ GET https://medmind.com/

Information Disclosure - JWT in Browser localStorage (1)

▶ GET https://medmind.com/login

Risk=Medium, Confidence=Medium (2)

https://optimizationguide-pa.googleapis.com (1)

Missing Anti-clickjacking Header (1)

▶ GET https://optimizationguide-pa.googleapis.com/downloads?name=1745312779&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDICTIONS

https://medmind.com (1)

Cross-Domain Misconfiguration (1)

▼ GET https://medmind.com/_next/static/media/6905431624c34d00-s.p.woff2

Alert tags

- OWASP_2021_A01
- POLICY_QA_STD =
- POLICY_PENTEST =
- OWASP_2017_A05
- CWE-264

Alert description

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Other info

The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

Request

▼ Request line and header section (559 bytes)

```
GET https://medmind.com/_next/static/media/6905431624c34d00-s.p.woff2 HTTP/1.1
host: medmind.com
```

```
Connection: keep-alive
Origin: https://medmind.com
sec-ch-ua-platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/138.0.0.0
Safari/537.36
sec-ch-ua: "Not)A;Brand";v="8",
"Chromium";v="138", "Google
Chrome";v="138"
sec-ch-ua-mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: font
Referer: https://medmind.com/
Accept-Language: en-US,en;q=0.9
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (578 bytes)

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Age: 1704568
Cache-Control: public,max-
age=31536000,immutable
Content-Disposition: inline;
filename="6905431624c34d00-s.p.woff2"
Content-Length: 50560
Content-Type: font/woff2
Date: Mon, 28 Jul 2025 15:39:03 GMT
Etag:
"5b3db6889bd28d3ebeef0fe9ae345c4e"
Last-Modified: Tue, 08 Jul 2025
22:09:34 GMT
```

Server: Vercel
Strict-Transport-Security: max-age=63072000
X-Matched-Path: /_next/static/media/6905431624c34d00-s.p.woff2
X-Vercel-Cache: HIT
X-Vercel-Id: dxb1::rwtr6-1753717143211-9d72b80c58f5

▶ Response body (50560 bytes)

Evidence `Access-Control-Allow-Origin: *`

Solution Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

Risk=Low, Confidence=High (2)

https://www.google-analytics.com (1)

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

▶ POST https://www.google-analytics.com/g/collect?v=2&tid=G-DKFZQ6FE4H&gtm=45je57n0v9125337445za200zd9125337445&_p=1753717148961&gcd=13l3l3l3l1l1&npa=0&dma=0&tag_exp=101509157~103116026~1032

00004~103233427~104684208~104684211~104948813~105134979~105134981&cid=1013652829.1753717149&ul=en-us&sr=1536x864&uaa=x86&uab=64&uafvl=Not)A%253BBrand%3B8.0.0.0%7CChromium%3B138.0.7204.169%7CGoogle%2520Chrome%3B138.0.7204.169&uamb=0&uam=&uap=Windows&uapv=19.0.0&uaw=0&are=1&frm=0&pscdl=noapi&_s=1&sid=1753717149&sct=1&seg=0&dl=https%3A%2F%2Fmedmind.com%2F&dt=Medmind%20-%20Empowering%20Your%20Health%20Journey%20with%20Intelligent%20AI%20Support&en=page_view&_fv=1&_nsi=1&_ss=1&_ee=1&tfd=2525

https://www.googleapis.com (1)

Strict-Transport-Security Header Not Set (1)

▶ POST https://www.googleapis.com/chromewebstore/v1.1/items/verify

Risk=Low, Confidence=Medium (7)

https://strapi.medmind.com (5)

Cookie No HttpOnly Flag (1)

▶ OPTIONS https://strapi.medmind.com/api/white-papers

Cookie Without Secure Flag (1)

▶ OPTIONS https://strapi.medmind.com/api/white-papers

Cookie with SameSite Attribute None (1)

▶ OPTIONS https://strapi.medmind.com/api/infos

Cookie without SameSite Attribute (1)

▶ OPTIONS https://strapi.medmind.com/api/white-papers

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

▶ GET https://strapi.medmind.com/api/asks

https://medmind.com (2)

Information Disclosure - Sensitive Information in Browser localStorage (1)

▶ GET https://medmind.com/login

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

▶ GET https://medmind.com/.well-known/vercel/security/static/challenge.v2.min.js

Risk=Low, Confidence=Low (1)

https://medmind.com (1)

Timestamp Disclosure - Unix (1)

▶ GET https://medmind.com/

Risk=Informational, Confidence=High (2)

https://medmind.com (2)

Information Disclosure - Information in Browser localStorage (1)

▶ GET https://medmind.com/

Information Disclosure - Information in Browser sessionStorage (1)

▶ GET https://medmind.com/

Risk=Informational, Confidence=Medium (4)

https://strapi.medmind.com (1)

Session Management Response Identified (1)

▶ OPTIONS https://strapi.medmind.com/api/white-papers

https://medmind.com (3)

Information Disclosure - Sensitive Information in URL (1)

▶ POST https://medmind.com/monitoring?o=4508132443488256&p=4508132459216896&r=us

Modern Web Application (1)

▶ GET https://medmind.com/

Retrieved from Cache (1)

▶ GET https://medmind.com/_next/static/media/6905431624c34d00-s.p.woff2

Risk=Informational, Confidence=Low (3)

https://cognito-idp.us-east-1.amazonaws.com (1)

Authentication Request Identified (1)

▶ POST https://cognito-idp.us-east-1.amazonaws.com/

https://content-autofill.googleapis.com (1)

Re-examine Cache-control Directives (1)

▶ GET https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTM4LjAuNzIwNC4xNjkSXwmGS3OjwcZXeBIFDTQ30ysSBQ3c5MosEgUNBu27_xIFDQbtu_8SBQ0G7bv_EgUNBu27_xIFDQbtu_8SBQ0G7bv_EgUNBu27_xIFDQbtu_8SBQ0G7bv_ISBffLIw4TtZEiAJbpxO9YafN7gSBQ00N9MrEgUN3OTKLCEgX3yyMOE7WRJRCbTmrF5B_mW2EgUNBu27_xIFDQbtu_8SBQ0G7bv_EgUNBu27_xIFDQbtu_8SBQ0G7bv_EgUNBu27_xIFDQbtu_8SBQ0G7bv_ISBffLIw4TtZ?alt=proto

https://medmind.com (1)

Information Disclosure - Suspicious Comments (1)

▶ GET https://medmind.com/_next/static/chunks/main-app-92b9b7d06e37c540.js

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

Path Traversal

Source	raised by an active scanner (plugin ID: 6)
CWE ID	22
WASC ID	33
Reference	▪ https://owasp.org/www-community/attacks/Path_Traversal ▪ https://cwe.mitre.org/data/definitions/22.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/

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

Information Disclosure - JWT in Browser localStorage

Source	raised by a passive scanner (plugin ID: 120002)
CWE ID	922
WASC ID	13
Reference	• https://www.zaproxy.org/blog/2020-09-03-zap-jwt-scanner/

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

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

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 Secure Flag

Source	raised by a passive scanner (Cookie Without Secure Flag)
CWE ID	614
WASC ID	13

Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Cookie with SameSite Attribute None

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

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

Information Disclosure - Sensitive Information in Browser localStorage

Source	raised by a passive scanner (plugin ID: 120001)
CWE ID	359

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 497

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

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/

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	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

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 - Information in Browser localStorage

Source	raised by a passive scanner (plugin ID: 120000)
CWE ID	359
WASC ID	13

Information Disclosure - Information in Browser sessionStorage

Source	raised by a passive scanner (plugin ID: 120000)
CWE ID	359
WASC ID	13

Information Disclosure - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	598
WASC ID	13

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)

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)
CWE ID	525
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