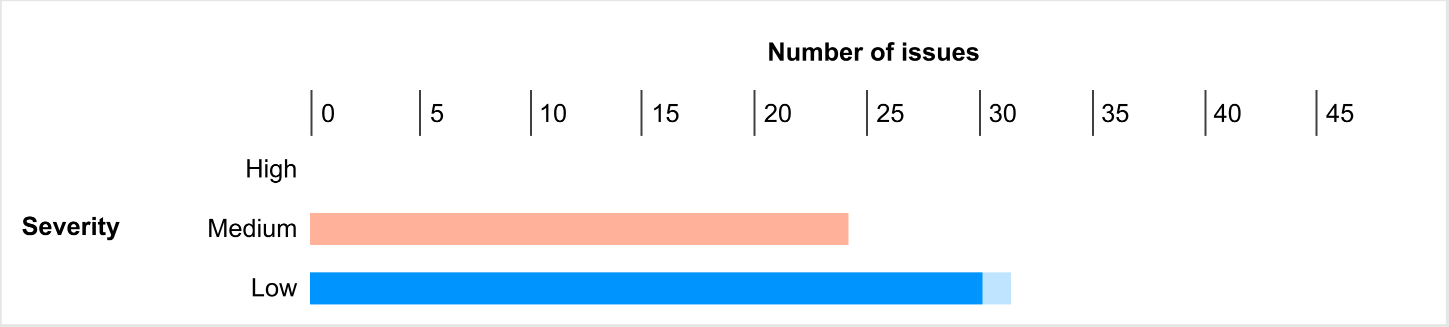
Burp Scanner Report

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low, Information or False Positive. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	0	0
	Medium	0	20	0	20
	Low	25	0	1	26
	Information	45	1	0	46
	False Positive	0	0	0	0

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

9. Content security policy: allows form hijacking

10. Cross-domain script include

10.1. https://news.wheelmap.org/en/apps/
10.2. https://wheelmap.org/

11. Frameable response (potential Clickjacking)

12. Browser cross-site scripting filter disabled

12.1. https://fonts.googleapis.com/css
12.2. https://fonts.gstatic.com/s/ubuntu/v20/4iCv6KVjbNBYlgoCjC3jsGyN.woff2
12.3. http://www.google.com/gen_204

13. Email addresses disclosed

13.1. https://v2.accessibility.cloud/mapping-events.json
13.2. https://wheelmap.org/

14. Credit card numbers disclosed

15. Cacheable HTTPS response

15.1. https://ac-o-0.global.ssl.fastly.net/api/v1/legacy/api/nodes/
15.2. https://ac-o-1.global.ssl.fastly.net/api/v1/legacy/api/nodes/
15.3. https://ac-o-2.global.ssl.fastly.net/api/v1/legacy/api/nodes/
15.4. https://ac-o-3.global.ssl.fastly.net/api/v1/legacy/api/nodes/
15.5. https://accessibility-cloud-v2.freetls.fastly.net/equipment-infos.json
15.6. https://accessibility-cloud-v2.freetls.fastly.net/images.json
15.7. https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json
15.8. https://api.mapbox.com/
15.9. https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Italic,Arial%20Unicode%20MS%20Regular/0-255.pbf
15.10. https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf
15.11. https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q
15.12. https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json
15.13. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json
15.14. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf
15.15. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf
15.16. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf
15.17. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf
15.18. https://news.wheelmap.org/en/apps/
15.19. https://osm-api.wheelmap.tech/api/v1/legacy/api/nodes
15.20. https://photon.komoot.io/api/
15.21. https://v2.accessibility.cloud/mapping-events.json
15.22. https://v2.accessibility.cloud/sources/LB5rYeCZ9PxthQ3Rg.json
15.23. https://v2.accessibility.cloud/tracking-events/report
15.24. https://wheelmap.org/
15.25. https://wheelmap.org/clientEnv.js
15.26. https://wheelmap.org/images/triangle.svg
15.27. https://wheelmap.pro/organizations/LPb4y2ri7b6fLxLFa/survey-projects/wx4mM8xFiQAsB5aLi/show

---

1. Session token in URL

There are 20 instances of this issue:

- https://accessibility-cloud-v2.freetls.fastly.net/equipment-infos.json
- https://accessibility-cloud-v2.freetls.fastly.net/images.json
- https://accessibility-cloud-v2.freetls.fastly.net/licenses/ns5HmC6xFrakRdoJ5.json
- https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json
- https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json
- https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json
- https://api.mapbox.com/
- https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf
- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q
- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json
- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.png
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf
- https://events.mapbox.com/events/v2
- https://v2.accessibility.cloud/mapping-events.json
- https://v2.accessibility.cloud/sources/LB5rYeCZ9PxthQ3Rg.json
- https://v2.accessibility.cloud/tracking-events/report

Issue background

Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. URLs may also be displayed on-screen, bookmarked or emailed around by users. They may be disclosed to third parties via the Referer header when any off-site links are followed. Placing session tokens into the URL increases the risk that they will be captured by an attacker.

Issue remediation

Applications should use an alternative mechanism for transmitting session tokens, such as HTTP cookies or hidden fields in forms that are submitted using the POST method.

Vulnerability classifications

- CWE-200: Information Exposure
- CWE-384: Session Fixation
- CWE-598: Information Exposure Through Query Strings in GET Request
- CAPEC-593: Session Hijacking

1.1. https://accessibility-cloud-v2.freetls.fastly.net/equipment-infos.json

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://accessibility-cloud-v2.freetls.fastly.net**
Path:	**/equipment-infos.json**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://accessibility-cloud-v2.freetls.fastly.net/equipment-infos.json?&x=2619&y=6333&z=14&appToken=27be4b5216aced82122d7cf8f69e4a07&includePlacesWithoutAccessibility=1

Request

```
GET /equipment-infos.json?
&x=2619&y=6333&z=14&appToken=27be4b5216aced82122d7cf8f69e4a07&includePlacesWithoutAccessibility=1 HTTP/2
Host: accessibility-cloud-v2.freetls.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Cache-Control: max-age=600
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

```
X-Fastly-Webpsupport: false
Accept-Ranges: bytes
Age: 0
Date: Fri, 29 Nov 2024 00:21:20 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970027-YUL
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1732839680.684848,VS0,VE483
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 1557

{"type":"FeatureCollection","featureCount":2,"totalFeatureCount":2,"related":{"licenses":{"2WCCM3YWWacqnEMTX":
{"_id":"2WCCM3YWWacqnEMTX","name":"Open Data Commons Open Database License","shortName":"O
...[SNIP]...
```

1.2. https://accessibility-cloud-v2.freetls.fastly.net/images.json

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://accessibility-cloud-v2.freetls.fastly.net**
Path:	**/images.json**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://accessibility-cloud-v2.freetls.fastly.net/images.json?context=surveyResult&objectId=etY5jXaQbwGaxmqCt&appToken=27be4b5216aced82122d7cf8f69e4a07

Request

```
GET /images.json?context=surveyResult&objectId=etY5jXaQbwGaxmqCt&appToken=27be4b5216aced82122d7cf8f69e4a07
HTTP/2
Host: accessibility-cloud-v2.freetls.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent, X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Cache-Control: max-age=120
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Fastly-Webpsupport: false
Accept-Ranges: bytes
Age: 0
Date: Fri, 29 Nov 2024 00:22:58 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970054-YUL
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1732839779.884012,VS0,VE112
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 28

{"totalCount":0,"images":[]}
```

1.3. https://accessibility-cloud-v2.freetls.fastly.net/licenses/ns5HmC6xFrakRdoJ5.json

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://accessibility-cloud-v2.freetls.fastly.net**

Path: **/licenses/ns5HmC6xFrakRdoJ5.json**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://accessibility-cloud-v2.freetls.fastly.net/licenses/ns5HmC6xFrakRdoJ5.json?appToken=27be4b5216aced82122d7cf8f69e4a07

Request

```
GET /licenses/ns5HmC6xFrakRdoJ5.json?appToken=27be4b5216aced82122d7cf8f69e4a07 HTTP/2
Host: accessibility-cloud-v2.freetls.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
```

```
Access-Control-Max-Age: 86400
Cache-Control: max-age=120
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Fastly-Webpsupport: false
Accept-Ranges: bytes
Age: 0
Date: Fri, 29 Nov 2024 00:23:38 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970040-YUL
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1732839818.788223,VS0,VE415
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 278

{"_id":"ns5HmC6xFrakRdoJ5","name":"CC-BY 4.0 International","shortName":"CC-BY 4.0
Int.","websiteURL":"https://creativecommons.org/licenses/by/4.0/","fullTextURL":"https://creativecommons.org/licenses
...[SNIP]...
```

1.4. https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://accessibility-cloud-v2.freetls.fastly.net**
Path:	**/place-infos.json**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json?excludeSourceIds=LiBTS67TjmBcXdEmX,pbT4qym6cAwKifCcN,ZyDaF8ZrJeGL3m4Cq,Yra2ze6vW9ttX7Tiz,JiTwDMcX5c8erJx95,cvus37h4bvef2pJzd,axsmapv2,T8j8nnnqMpbxpLxZu,ehgoCgSPEfNdpg5fG,cnQiiH4qpyyn6fBNr,TNmCbw6xD4DoXnhb7,WKkGrSNMXn3sd6ubT,dBCyrMSJdHZSxKgK5,sPSreQtMg8Soy5TDr&x=83831&y=202680&z=19&appToken=27be4b5216aced82122d7cf8f69e4a07&includePlacesWithoutAccessibility=1

Request

```
GET /place-infos.json?
excludeSourceIds=LiBTS67TjmBcXdEmX,pbT4qym6cAwKifCcN,ZyDaF8ZrJeGL3m4Cq,Yra2ze6vW9ttX7Tiz,JiTwDMcX5c8erJ
x95,cvus37h4bvef2pJzd,axsmapv2,T8j8nnnqMpbxpLxZu,ehgoCgSPEfNdpg5fG,cnQiiH4qpyyn6fBNr,TNmCbw6xD4DoXnhb7,
WKkGrSNMXn3sd6ubT,dBCyrMSJdHZSxKgK5,sPSreQtMg8Soy5TDr&x=83831&y=202680&z=19&appToken=27be4b5216ace
d82122d7cf8f69e4a07&includePlacesWithoutAccessibility=1 HTTP/1.1
Host: accessibility-cloud-v2.freetls.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Cache-Control: max-age=1200
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Fastly-Webpsupport: false
Accept-Ranges: bytes
Age: 0
Date: Fri, 29 Nov 2024 00:21:20 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970027-YUL
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1732839679.398170,VS0,VE625
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 52679

{"type":"FeatureCollection","featureCount":74,"totalFeatureCount":74,"related":{"licenses":{"2WCCM3YWWacqnEMTX":
{"_id":"2WCCM3YWWacqnEMTX","name":"Open Data Commons Open Database License","shortName":
...[SNIP]...
```

1.5. https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://accessibility-cloud-v2.freetls.fastly.net**
Path:	**/place-infos.json**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json?parentPlaceInfoId=xgt9bT3QYyjw3zPSt&limit=100&appToken=27be4b5216aced82122d7cf8f69e4a07

Request

```
GET /place-infos.json?parentPlaceInfoId=xgt9bT3QYyjw3zPSt&limit=100&appToken=27be4b5216aced82122d7cf8f69e4a07
HTTP/2
Host: accessibility-cloud-v2.freetls.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
```

```
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Cache-Control: max-age=1200
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Fastly-Webpsupport: false
Accept-Ranges: bytes
Age: 0
Date: Fri, 29 Nov 2024 00:22:41 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970036-YUL
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1732839761.948256,VS0,VE918
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 119

{"type":"FeatureCollection","featureCount":0,"totalFeatureCount":0,"related":{"licenses":{},"images":{}},"features":[]}
```

1.6. https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://accessibility-cloud-v2.freetls.fastly.net**
Path:	**/place-infos.json**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json?excludeSourceIds=LiBTS67TjmBcXdEmX&latitude=37.7577&longitude=-122.4376&accuracy=300&limit=20&appToken=27be4b5216aced82122d7cf8f69e4a07

Request

```
GET /place-infos.json?
excludeSourceIds=LiBTS67TjmBcXdEmX&latitude=37.7577&longitude=-122.4376&accuracy=300&limit=20&appToken=27be4
b5216aced82122d7cf8f69e4a07 HTTP/2
Host: accessibility-cloud-v2.freetls.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
```

```
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Cache-Control: max-age=1200
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Fastly-Webpsupport: false
Accept-Ranges: bytes
Age: 0
Date: Fri, 29 Nov 2024 00:22:59 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970054-YUL
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1732839779.790891,VS0,VE472
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 13976
```

{"type":"FeatureCollection","featureCount":20,"totalFeatureCount":null,"related":{"licenses":{"2WCCM3YWWacqnEMTX":

```
{"_id":"2WCCM3YWWacqnEMTX","name":"Open Data Commons Open Database License","shortName
...[SNIP]...
```

1.7. https://api.mapbox.com/

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api.mapbox.com**
Path:	**/**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Italic,Arial%20Unicode%20MS%20Regular/0-255.pbf?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

This issue was found in multiple locations under the reported path.

Request

```
GET /fonts/v1/sozialhelden/DIN%20Pro%20Italic,Arial%20Unicode%20MS%20Regular/0-255.pbf?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 73513
Date: Mon, 28 Oct 2024 16:40:45 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: Mbx-Fonts
Timing-Allow-Origin: *
Cache-Control: max-age=5184000, stale-while-revalidate=3600, stale-if-error=18000
Etag: W/"af7a-Nz1ssxur6nsO2p0x1nwNWs8GbWI"
```

```
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: gIhIgHTPa8W8nQkBAFgGzk-qScGe0kOUycPTBwOQGGSBc-bswoqedQ==
Age: 2706055


...
(DIN Pro Italic, Arial Unicode MS Regular..0-255...... .(.018...... .(.018.... .. .(.018.....!.....3LaorrrgS.#A^y.....g
*Ii......r./On......q.5Tt......j.:Zy......d @_  .....|]&Ee......uV+Kk......
...[SNIP]...
```

1.8. https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api.mapbox.com**
Path:	**/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

Request

```
GET /fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 68970
Date: Mon, 18 Nov 2024 22:35:17 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: Mbx-Fonts
Timing-Allow-Origin: *
Cache-Control: max-age=5184000, stale-while-revalidate=3600, stale-if-error=18000
Etag: W/"9381-SLipJvr+Rq1bv9MIBVb1HAUP+3c"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: L5ol3NEssF0-aamOhwFSOInRxfBVgtRsehSj153jpqT9_Z4Dx2y1LQ==
Age: 870382



...
)DIN Pro Regular, Arial Unicode MS Regular..0-255...... .(.018...... .(.018.... .. .
(.018.....!...LbprrrgT_z.....hi......sj......ti......sh......sh......rg......qg......qf......pe......oe......o
...[SNIP]...
```

1.9. https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api.mapbox.com**
Path:	**/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

Request

```
GET /styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/1.1
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: mbx-styles
Timing-Allow-Origin: *
X-Dns-Prefetch-Control: off
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: origin
Date: Fri, 29 Nov 2024 00:21:19 GMT
Cache-Control: max-age=900, stale-while-revalidate=900, stale-if-error=3600
Etag: W/"149dc-VxeuyDGpYLOxKpBskraSOt44THw"
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: EVEIy7QiCiqnN9QgPBWnewDjBn090BsAvD5bNusFc5zLCZH-pl8QQg==
Age: 489

{"version":8,"name":"Streets","metadata":{"mapbox:type":"default","mapbox:origin":"streets-v11","mapbox:sdk-support":
{"android":"9.3.0","ios":"5.10.0","js":"2.0.0"},"mapbox:autocomposite":true,"mapbox
...[SNIP]...
```

1.10. https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api.mapbox.com**
Path:	**/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

Request

```
GET /styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Date: Sun, 11 Aug 2024 20:29:50 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: mbx-styles
Timing-Allow-Origin: *
X-Dns-Prefetch-Control: off
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: origin
Cache-Control: max-age=31536000, stale-if-error=18000
Etag: "sprite-4.5.8-v1/6qsolfec7nhi04bt9085kqnu6"
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: TerwV_Lz5r06Kx2An0ZIug7cQRSzzCqOgtS4iCLfgHE800_s841EQA==
Age: 9431494

{"pedestrian-polygon":{"x":0,"y":0,"width":128,"height":128,"pixelRatio":2,"visible":true},"turning-circle-outline":{"x":128,"y":0,"width":92,"height":92,"pixelRatio":2,"visible":true},"turning-circle
...[SNIP]...
```

1.11. https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.png

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api.mapbox.com**

Path: **/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.png**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.png?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

Request

```
GET /styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.png?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: image/webp,*/*
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: image/png
Content-Length: 70813
Date: Mon, 19 Aug 2024 16:27:03 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: mbx-styles
Timing-Allow-Origin: *
Cache-Control: max-age=31536000, stale-if-error=18000
Etag: "sprite-4.5.8-v1/6qsolfec7nhi04bt9085kqnu6"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: eqHKWBIuHGeoCkyOj3-YLYyVJSEgmb9zWKdM18yzOT3cu9MKHQVPNw==
Age: 8754860

.PNG
.
...IHDR.............~p.....PLTELiq.........fe\...................&.....%..&..............
..................... ........&..d...E\...."$-........$........F*+3..$.....#336..$..%..%.BB......
...[SNIP]...
```

1.12. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json?secure&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

Request

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json?
secure&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-
AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732340266
Last-Modified: Fri, 25 Aug 2023 07:39:41 GMT
Timing-Allow-Origin: *
Date: Fri, 29 Nov 2024 00:21:24 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "aec9c7f4fcbb8ce46a34a7729283a612"
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
```

```
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: FU1AMgX2hq0ukyg4RDMYEuytgALWrNZYeHxAWXd3NmMWjeBfzgPF2A==
Age: 278

{"attribution":"<a href=\"https://www.mapbox.com/about/maps/\" target=\"_blank\" title=\"Mapbox\" aria-label=\"Mapbox\">&copy; Mapbox</a> <a href=\"https://www.openstreetmap.org/about/\" target=\"_bla
...[SNIP]...
```

1.13. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf?sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

Request

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf?sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 89570
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
```

```
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732634791
Last-Modified: Mon, 25 Nov 2024 17:26:02 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:37 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "48a2ebaf3c06b5445978f57916aa2257"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: KgHEPQWsMZ0aI59WpYwG3Ue0IzfV8Z2IITK919J8OiNUTnWCxgAb2w==
Age: 290

...x.
   hillshade(. ......."..    ...$........?...     .    ...@@....  .    ..@............    .......@@....  .    .+?:........?....@......_....    ...?
j..........@....  ......0..      .....  ..? ?.    ...R.@.............?..@  ....
...[SNIP]...
```

1.14. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf?sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

Request

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

```
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 72751
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732656614
Last-Modified: Mon, 25 Nov 2024 17:26:01 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:37 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "95bfcf6dcc7025ed71b84195e9c96031"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: hHeREAdeDQe33FNJERSs_P9qIfbzfcIC_7rod8YM-A2BScVH0OKhdw==
Age: 290

..x.
   hillshade(. ......."..    ............?...      .    ...@@....  .    ..@............    .......@@....  .    .+?:........?....@......_....
   ...;B.........@....  ......0..  .    .._B...# ..........?..@  .....    .!.D...@.....
...[SNIP]...
```

1.15. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf?sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

Request

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
```

```
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 95205
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732645643
Last-Modified: Mon, 25 Nov 2024 17:26:01 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:39 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "4cd778583d27c21fe970d7bd75ac4080"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: Zusuj4xRihPpjsKnWq4mVMJhYRkpS5xYCM-3gL0OenmnZzZMZ8CIgg==
Age: 292

...x.
  hillshade(. ......."..   .$.$........?...     .    ...@@....  .    ..@............    .......@@....  .    .*.."... .....?...    _.CR`_..? ?............ ...`___.
  ....R.@.............?..@  .........  .    ...I...@.....?
...[SNIP]...
```

1.16. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf?sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

Request

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 73869
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732634791
Last-Modified: Mon, 25 Nov 2024 17:26:07 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:37 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "ba2c99c10975464cef1acc458b4dac1f"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: qGSHoo4VS4PtlBO9AXafbDJy1NhTNbBsHFZEfxYW05XmEqccCyh_Ew==
Age: 290

..x.
   hillshade(. ......."..   .$..........?...     .    ...@@....  .    ..@............    .......@@....  .    .*.."... .....?...    _.@*......... ...`_.    .._B...#
..........?..@  .....   .!.D...@.....?.    ..  .....?....?.    ...
...[SNIP]...
```

1.17. https://events.mapbox.com/events/v2

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://events.mapbox.com**
Path:	**/events/v2**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://events.mapbox.com/events/v2?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA

Request

```
POST /events/v2?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/1.1
Host: events.mapbox.com
Content-Length: 206
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Content-Type: text/plain
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive

[{"event":"appUserTurnstile","created":"2024-11-29T00:21:25.254Z","sdkIdentifier":"mapbox-gl-
js","sdkVersion":"2.2.0","skuId":"01","userId":"32ce1d01-c4f4-47e6-be7b-602517d02082","enabled.telemetry":f
...[SNIP]...
```

Response

```
HTTP/2 204 No Content
Date: Fri, 29 Nov 2024 00:21:36 GMT
X-Powered-By: Express
Access-Control-Allow-Origin: *
```

1.18. https://v2.accessibility.cloud/mapping-events.json

Summary

Severity:	**Medium**

Confidence:	**Firm**
Host:	**https://v2.accessibility.cloud**
Path:	**/mapping-events.json**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://v2.accessibility.cloud/mapping-events.json?appToken=27be4b5216aced82122d7cf8f69e4a07&includeRelated=images

Request

```
GET /mapping-events.json?appToken=27be4b5216aced82122d7cf8f69e4a07&includeRelated=images HTTP/2
Host: v2.accessibility.cloud
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:22:30 GMT
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
```

```
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Surrogate-Control: max-age=86400, stale-while-revalidate=30, stale-if-error=3600
Cache-Control: max-age=120
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=1T4PC8%2BEdAq3gzwJNWZS8fuyWL35V8dZF0sd8iE12mxUGbzZSjkAmVFH4ceErIUGzkJI7F2DITG80vOmD02XnwjW3rV
629ywqAxVu6sk%2FIynVkSr1zQV4aFXMCRPTO31Mwm%2FIrUZzJnq"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e7195dc8ba296-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4554&min_rtt=4449&rtt_var=1443&sent=5&recv=9&lost=0&retrans=0&sent_bytes=781&recv_bytes=1552&deli
very_rate=304721&cwnd=246&unsent_bytes=0&cid=a31fc582c370cbfd&ts=510&x=0"

{"count":400,"totalCount":400,"related":{"images":{"97QSEx3Pzi8T4YNyM":
{"_id":"97QSEx3Pzi8T4YNyM","objectId":"2CBbFTpcmLb6kJoht","mimeType":"image/jpeg","context":"event","type":"photo","mo
derationReq
...[SNIP]...
```

1.19. https://v2.accessibility.cloud/sources/LB5rYeCZ9PxthQ3Rg.json

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://v2.accessibility.cloud**
Path:	**/sources/LB5rYeCZ9PxthQ3Rg.json**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://v2.accessibility.cloud/sources/LB5rYeCZ9PxthQ3Rg.json?appToken=27be4b5216aced82122d7cf8f69e4a07

Request

```
GET /sources/LB5rYeCZ9PxthQ3Rg.json?appToken=27be4b5216aced82122d7cf8f69e4a07 HTTP/2
Host: v2.accessibility.cloud
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
```

```
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:22:59 GMT
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Surrogate-Control: max-age=120, stale-while-revalidate=30, stale-if-error=3600
Cache-Control: max-age=120
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vrfmxvGjMgjZghg4yEEUEzk40qgARU%2F5tsh2KQ6RrgnOBnXa60Fy9myD6RuE4I4xtJGmL5MSU2wXjFkM2n08uew9XXoI
RiHGW2bg60%2FrZr2%2Fcag9PkQZKbN9kj4bbEIE7%2BvU8LRrVg6B"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e724b2874a255-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4646&min_rtt=3420&rtt_var=1819&sent=6&recv=9&lost=0&retrans=0&sent_bytes=781&recv_bytes=1546&deli
very_rate=424561&cwnd=251&unsent_bytes=0&cid=a2ae56aef645320a&ts=348&x=0"

{"_id":"LB5rYeCZ9PxthQ3Rg","organizationId":"LPb4y2ri7b6fLxLFa","isFreelyAccessible":true,"accessRestrictedTo":
[],"name":"Sozialhelden e.V. - Wheelmap S","shortName":"Wheelmap","licenseId":"ns5HmC6xFr
...[SNIP]...
```

1.20. https://v2.accessibility.cloud/tracking-events/report

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://v2.accessibility.cloud**
Path:	**/tracking-events/report**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://v2.accessibility.cloud/tracking-events/report?appToken=27be4b5216aced82122d7cf8f69e4a07

Request

```
OPTIONS /tracking-events/report?appToken=27be4b5216aced82122d7cf8f69e4a07 HTTP/1.1
Host: v2.accessibility.cloud
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type
Origin: https://wheelmap.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:19 GMT
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
```

```
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=ABjuq%2FccA8NoiGVXBXNqf9kgTo%2FzNQi5%2F1tdg6tKXv%2FBzzmqgMpsjp%2Fja%2FRBTOqZLPgE6bP7HGKiUmKR
XuXHs2WDiwSuPGc3trtdyCZddK3yMCpcSmNFrPYmdKOTMVX0xnbAKh5Frsyd"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6fd9f926a28c-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4978&min_rtt=3686&rtt_var=2547&sent=7&recv=11&lost=0&retrans=0&sent_bytes=3699&recv_bytes=1251&d
elivery_rate=579178&cwnd=239&unsent_bytes=0&cid=d4d14fd1aa13460c&ts=394&x=0"
```

2. Vulnerable JavaScript dependency

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://wheelmap.org**
Path:	**/_next/static/chunks/main-9b34891982685c08.js**

Issue detail

We observed a vulnerable JavaScript library.

We detected **nextjs** version **12.3.4**, which has the following vulnerability:

- CVE-2023-46298: Next.js missing cache-control header may lead to CDN caching empty reply

Issue background

The use of third-party JavaScript libraries can introduce a range of DOM-based vulnerabilities, including some that can be used to hijack user accounts like DOM-XSS.

Common JavaScript libraries typically enjoy the benefit of being heavily audited. This may mean that bugs are quickly identified and patched upstream, resulting in a steady stream of security updates that need to be applied. Although it may be tempting to ignore updates, using a library with missing security patches can make your website exceptionally easy to exploit. Therefore, it's important to ensure that any available security updates are applied promptly.

Some library vulnerabilities expose every application that imports the library, but others only affect applications that use certain library features. Accurately identifying which library vulnerabilities apply to your website can be difficult, so we recommend applying all available security updates regardless.

Issue remediation

Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.

Vulnerability classifications

- CWE-1104: Use of Unmaintained Third Party Components
- A9: Using Components with Known Vulnerabilities

Request

```
GET /_next/static/chunks/main-9b34891982685c08.js HTTP/2
Host: wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:08 GMT
Content-Type: application/javascript; charset=UTF-8
Cache-Control: public, max-age=31536000, immutable
Cf-Bgj: minify
Cf-Polished: origSize=109337
Etag: W/"1ab19-1924c92b118"
Last-Modified: Wed, 02 Oct 2024 09:32:15 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Accept-Encoding
X-Powered-By: Express
Cf-Cache-Status: HIT
Age: 201580
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=lAFvGN8r0Q3BNafnRalJ%2Fu6QovscrR48UyvSXeLZ7HjM2g2P8rxYIDxV1aWkK7VYATzfT5ePIZXnH4kTyUJHZpRsky%2F
TB%2BQsL9mMlaF4VHYpq7fboH6HUOFXrsW1sw%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6f97faaaa2ae-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4600&min_rtt=2902&rtt_var=1365&sent=173&recv=95&lost=0&retrans=1&sent_bytes=197169&recv_bytes=18
52&delivery_rate=11598602&cwnd=251&unsent_bytes=0&cid=56c8de4124ebb565&ts=654&x=0"

(self.webpackChunk_N_E=self.webpackChunk_N_E||[]).push([[179],{37290:function(e,t){"use
strict";Object.defineProperty(t,"__esModule",{value:!0}),t.default=function(e,t){(null==t||t>e.length)&&(t=e.len
...[SNIP]...
3),y=d(r(94988)),m=r(49756),g=r(22627),_=r(2734),b=r(99603),P=r(94915),w=r(29388),S=d(r(790)),j=d(r(87838)),O=d(r(80313
)),E=r(14608),x=r(15817),M=r(60016),C=r(80300),R=r(89960),A=r(67554),k=r(31542);t.version="12.3.4",t.router=p;var
T=y.default();t.emitter=T;var L,I,N,D,B,Z,q,H,F,U,W=function(e){return[].slice.call(e)},z=void 0,G=!1;self.__next_require__=r;var
V=function(e){o(r,e);var t=c(r);function r(){return n(this,r),t.apply(this,arguments)}return a(r,
[{key:"componentDidCatch",value:function(e,t){this.props.fn(e,t)}},{key:"componentDidMount",value:function()
{this.scrollToHash(),p.isSsr&&"/404"!==L.page&&"/_error"!==L.page&&(L.isFallback||L.nextExport&&
(g.isDynamicRoute(p.pathname)||location.search||G)||L.props&&L.props.__N_SSG&&
(location.search||G))&&p.replace(p.pathname+"?"+String(_.assign(_.urlQueryToSearchParams(p.query),new
URLSearchParams(location.search))),I,{_h:1,shallow:!L.isFallback&&!G}).catch((function(e){if(!e.cancelled)throw e}))}},
{key:"componentDidUpdate",value:function(){this.scrollToHash()}},{key:"scrollToHash",value:function(){var
```

```
e=location.hash;if(e=e&&e.substring(1)){var t=document.getElementById(e);t&&setTimeout((function(){return
t.scrollIntoView()}),0)}}},{key:"render",value:function(){return this.props.children}}]),r}(h.default.Component);function K(){return
K=I((function(){var e,t,n=arguments;return s(this,(function(a){return n.length>0&&void 0!==n[0]?n[0]:
{},L=JSON.parse(document.getElementById("__NEXT_DATA__").textContent),window.__NEXT_DATA__=L,z=L.defaultLocale,
e=L.assetPrefix||"",r.p="".concat(e,"/_next/"),b.setConfig({serverRuntimeConfig:{},publicRuntimeConfig:L.runtimeConfig||
{}}),I=P.getURL(),A.hasBasePath(I)&&(I
...[SNIP]...
```

3. Unencrypted communications

There are 2 instances of this issue:

- http://connectivitycheck.gstatic.com/
- http://www.google.com/

Issue description

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Please note that using a mixture of encrypted and unencrypted communications is an ineffective defense against active attackers, because they can easily remove references to encrypted resources when these references are transmitted over an unencrypted connection.

Issue remediation

Applications should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server. The Strict-Transport-Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection.

References

- Marking HTTP as non-secure
- Configuring Server-Side SSL/TLS
- HTTP Strict Transport Security

Vulnerability classifications

- CWE-326: Inadequate Encryption Strength
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

3.1. http://connectivitycheck.gstatic.com/

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**http://connectivitycheck.gstatic.com**
Path:	**/**

3.2. http://www.google.com/

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**http://www.google.com**
Path:	**/**

---

4. Strict transport security not enforced

There are 23 instances of this issue:

- https://api.mapbox.com/
- https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf
- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q
- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json
- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.png
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf
- https://events.mapbox.com/events/v2
- https://fonts.gstatic.com/s/ubuntu/v20/4iCv6KVjbNBYlgoCjC3jsGyN.woff2
- https://matomo.sozialhelden.de/matomo.js
- https://matomo.sozialhelden.de/matomo.php
- https://news.wheelmap.org/en
- https://news.wheelmap.org/en/apps/
- https://news.wheelmap.org/en/wp-content/themes/hello-elementor/style.min.css
- https://news.wheelmap.org/en/wp-content/themes/hello-elementor/theme.min.css
- https://news.wheelmap.org/en/wp-includes/css/dist/block-library/style.min.css
- https://photon.komoot.io/api/
- https://service.sozialhelden.de/pwproxy.php
- https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015
- https://www.google.com/generate_204

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

4.1. https://api.mapbox.com/

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/**

Issue detail

This issue was found in multiple locations under the reported path.

Request

```
GET /fonts/v1/sozialhelden/DIN%20Pro%20Italic,Arial%20Unicode%20MS%20Regular/0-255.pbf?access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 73513
Date: Mon, 28 Oct 2024 16:40:45 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: Mbx-Fonts
Timing-Allow-Origin: *
Cache-Control: max-age=5184000, stale-while-revalidate=3600, stale-if-error=18000
Etag: W/"af7a-Nz1ssxur6nsO2p0x1nwNWs8GbWI"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: gIhIgHTPa8W8nQkBAFgGzk-qScGe0kOUycPTBwOQGGSBc-bswoqedQ==
Age: 2706055


...
(DIN Pro Italic, Arial Unicode MS Regular..0-255...... .(.018...... .(.018.... .. .(.018.....!.....3LaorrrgS.#A^y.....g
*Ii......r./On......q.5Tt......j.:Zy......d @_  .....|]&Ee......uV+Kk......
...[SNIP]...
```

4.2. https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf**

Request

```
GET /fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 68970
Date: Mon, 18 Nov 2024 22:35:17 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: Mbx-Fonts
Timing-Allow-Origin: *
Cache-Control: max-age=5184000, stale-while-revalidate=3600, stale-if-error=18000
Etag: W/"9381-SLipJvr+Rq1bv9MIBVb1HAUP+3c"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: L5ol3NEssF0-aamOhwFSOInRxfBVgtRsehSj153jpqT9_Z4Dx2y1LQ==
Age: 870382



...
)DIN Pro Regular, Arial Unicode MS Regular..0-255...... .(.018...... .(.018.... .. .
(.018.....!...LbprrrgT_z.....hi......sj......ti......sh......sh......rg......qg......qf......pe......oe......o
...[SNIP]...
```

4.3. https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q**

Request

```
GET /styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/1.1
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: mbx-styles
Timing-Allow-Origin: *
X-Dns-Prefetch-Control: off
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: origin
Date: Fri, 29 Nov 2024 00:21:19 GMT
Cache-Control: max-age=900, stale-while-revalidate=900, stale-if-error=3600
Etag: W/"149dc-VxeuyDGpYLOxKpBskraSOt44THw"
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: EVEIy7QiCiqnN9QgPBWnewDjBn090BsAvD5bNusFc5zLCZH-pl8QQg==
Age: 489

{"version":8,"name":"Streets","metadata":{"mapbox:type":"default","mapbox:origin":"streets-v11","mapbox:sdk-support":
{"android":"9.3.0","ios":"5.10.0","js":"2.0.0"},"mapbox:autocomposite":true,"mapbox
...[SNIP]...
```

4.4. https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json

Summary

Severity:	**Low**
Confidence:	**Certain**

Host: **https://api.mapbox.com**

Path: **/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json**

Request

```
GET /styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Date: Sun, 11 Aug 2024 20:29:50 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: mbx-styles
Timing-Allow-Origin: *
X-Dns-Prefetch-Control: off
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: origin
Cache-Control: max-age=31536000, stale-if-error=18000
Etag: "sprite-4.5.8-v1/6qsolfec7nhi04bt9085kqnu6"
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: TerwV_Lz5r06Kx2An0ZIug7cQRSzzCqOgtS4iCLfgHE800_s841EQA==
Age: 9431494

{"pedestrian-polygon":{"x":0,"y":0,"width":128,"height":128,"pixelRatio":2,"visible":true},"turning-circle-outline":
{"x":128,"y":0,"width":92,"height":92,"pixelRatio":2,"visible":true},"turning-circle
...[SNIP]...
```

4.5. https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.png

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.png**

Request

```
GET /styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.png?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: image/webp,*/*
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: image/png
Content-Length: 70813
Date: Mon, 19 Aug 2024 16:27:03 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: mbx-styles
Timing-Allow-Origin: *
Cache-Control: max-age=31536000, stale-if-error=18000
Etag: "sprite-4.5.8-v1/6qsolfec7nhi04bt9085kqnu6"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: eqHKWBIuHGeoCkyOj3-YLYyVJSEgmb9zWKdM18yzOT3cu9MKHQVPNw==
Age: 8754860

.PNG
.
...IHDR..............~p.....PLTELiq.........fe\....................&.....%..&..............
..................... ........&..d...E\...."$-........$........F*+3..$.....#336..$..%..%.BB......
...[SNIP]...
```

4.6. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json**

Request

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json?
secure&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-
AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732340266
Last-Modified: Fri, 25 Aug 2023 07:39:41 GMT
Timing-Allow-Origin: *
Date: Fri, 29 Nov 2024 00:21:24 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "aec9c7f4fcbb8ce46a34a7729283a612"
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: FU1AMgX2hq0ukyg4RDMYEuytgALWrNZYeHxAWXd3NmMWjeBfzgPF2A==
Age: 278

{"attribution":"<a href=\"https://www.mapbox.com/about/maps/\" target=\"_blank\" title=\"Mapbox\" aria-
label=\"Mapbox\">&copy; Mapbox</a> <a href=\"https://www.openstreetmap.org/about/\" target=\"_bla
...[SNIP]...
```

4.7. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf**

Request

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 89570
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732634791
Last-Modified: Mon, 25 Nov 2024 17:26:02 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:37 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "48a2ebaf3c06b5445978f57916aa2257"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: KgHEPQWsMZ0aI59WpYwG3Ue0IzfV8Z2IITK919J8OiNUTnWCxgAb2w==
Age: 290

...x.
   hillshade(. ......."..    ...$........?...      .    ...@@....  .    ..@............    .......@@....  .    .+?:........?....@......_....    ...?
j..........@....  ......0..      .....  ..? ?.    ...R.@.............?..@  ....
...[SNIP]...
```

4.8. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf**

Request

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 72751
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732656614
Last-Modified: Mon, 25 Nov 2024 17:26:01 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:37 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "95bfcf6dcc7025ed71b84195e9c96031"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: hHeREAdeDQe33FNJERSs_P9qIfbzfcIC_7rod8YM-A2BScVH0OKhdw==
Age: 290
```

```
..x.
  hillshade(. ......."..    ............?...      .    ...@@....  .    ..@............    .......@@....  .    .+?:........?....@......_....
  ...;B.........@....  ......0..  .    .._B...# ..........?..@  .....    .!.D...@.....
...[SNIP]...
```

4.9. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf**

Request

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 95205
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732645643
Last-Modified: Mon, 25 Nov 2024 17:26:01 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:39 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "4cd778583d27c21fe970d7bd75ac4080"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
```

```
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: Zusuj4xRihPpjsKnWq4mVMJhYRkpS5xYCM-3gL0OenmnZzZMZ8CIgg==
Age: 292

...x.
  hillshade(. ......."..    .$.$........?...      .    ...@@....  .    ..@............    .......@@....  .    .*.."... .....?...    _.CR`_..? ?............ ...`___.
  ....R.@.............?..@  .........  .    ...I...@.....?
...[SNIP]...
```

4.10. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf**

Request

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 73869
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732634791
Last-Modified: Mon, 25 Nov 2024 17:26:07 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:37 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "ba2c99c10975464cef1acc458b4dac1f"
```

```
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: qGSHoo4VS4PtlBO9AXafbDJy1NhTNbBsHFZEfxYW05XmEqccCyh_Ew==
Age: 290

..x.
  hillshade(. ......."..    .$..........?...      .    ...@@....  .    ..@............    .......@@....  .    .*.."... .....?...    _.@*......... ...`_.    .._B...#
..........?..@  .....    .!.D...@.....?.    ..  .....?....?.    ...
...[SNIP]...
```

4.11. https://events.mapbox.com/events/v2

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://events.mapbox.com**
Path:	**/events/v2**

Request

```
POST /events/v2?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-jU7SUA HTTP/1.1
Host: events.mapbox.com
Content-Length: 206
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Content-Type: text/plain
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive

[{"event":"appUserTurnstile","created":"2024-11-29T00:21:25.254Z","sdkIdentifier":"mapbox-gl-js","sdkVersion":"2.2.0","skuId":"01","userId":"32ce1d01-c4f4-47e6-be7b-602517d02082","enabled.telemetry":f
...[SNIP]...
```

Response

```
HTTP/2 204 No Content
Date: Fri, 29 Nov 2024 00:21:36 GMT
X-Powered-By: Express
```

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

4.12. https://fonts.gstatic.com/s/ubuntu/v20/4iCv6KVjbNBYlgoCjC3jsGyN.woff2

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://fonts.gstatic.com**
Path:	**/s/ubuntu/v20/4iCv6KVjbNBYlgoCjC3jsGyN.woff2**

Request

```
GET /s/ubuntu/v20/4iCv6KVjbNBYlgoCjC3jsGyN.woff2 HTTP/1.1
Host: fonts.gstatic.com
Origin: https://news.wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: font
Referer: https://fonts.googleapis.com/
Accept-Encoding: gzip, deflate, br
Priority: u=4
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/apps-themes
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="apps-themes"
Report-To: {"group":"apps-themes","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/apps-
themes"}]}
Timing-Allow-Origin: *
Content-Length: 30480
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Fri, 22 Nov 2024 12:25:23 GMT
Expires: Sat, 22 Nov 2025 12:25:23 GMT
Cache-Control: public, max-age=31536000
Age: 561247
Last-Modified: Wed, 27 Apr 2022 16:04:03 GMT
Content-Type: font/woff2
```

```
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

wOF2......w.......!...v...........................T..2.`..V......    .#..
..\..n..,...(.6.$..T. ..d..X..9[[.q.k..W}.....5{Z._0......(.5TeDp.@T..9.......".i7m.....?....2*A.#).\..`..D......e...`UM.mp.    ...
...[SNIP]...
```

4.13. https://matomo.sozialhelden.de/matomo.js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://matomo.sozialhelden.de**
Path:	**/matomo.js**

Request

```
GET /matomo.js HTTP/1.1
Host: matomo.sozialhelden.de
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://news.wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Last-Modified: Wed, 23 Oct 2024 10:00:47 GMT
Etag: "10784-62521f5bd9bb7-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 67460
Content-Type: text/javascript
Date: Fri, 29 Nov 2024 00:19:29 GMT
Server: Apache

/*!!
* Matomo - free/libre analytics platform
*
* JavaScript tracking client
*
* @link https://piwik.org
* @source https://github.com/matomo-org/matomo/blob/master/js/piwik.js
* @license https:
...[SNIP]...
```

4.14. https://matomo.sozialhelden.de/matomo.php

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://matomo.sozialhelden.de**
Path:	**/matomo.php**

Request

```
POST /matomo.php?
action_name=Apps%20%E2%80%93%20Wheelmap.org&idsite=4&rec=1&r=046657&h=19&m=19&s=29&url=https%3A%2F%
2Fnews.wheelmap.org%2Fen%2Fapps%2F&_id=&_idn=1&send_image=0&_refts=0&pv_id=vF9d3y&pf_net=607&pf_srv=7697
0&pf_tfr=6&pf_dm1=45384&uadata=%7B%22fullVersionList%22%3A%5B%5D%2C%22mobile%22%3Afalse%2C%22model%
22%3A%22%22%2C%22platform%22%3A%22Windows%22%2C%22platformVersion%22%3A%22%22%7D&pdf=1&qt=0&re
alp=0&wma=0&fla=0&java=0&ag=0&cookie=1&res=1280x800 HTTP/2
Host: matomo.sozialhelden.de
Content-Length: 0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://news.wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
Referer: https://news.wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 204 No Content
Access-Control-Allow-Origin: https://news.wheelmap.org
Access-Control-Allow-Credentials: true
Date: Fri, 29 Nov 2024 00:21:07 GMT
Server: Apache
```

4.15. https://news.wheelmap.org/en

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://news.wheelmap.org**
Path:	**/en**

Issue detail

This issue was found in multiple locations under the reported path.

Request

```
GET /en/wp-content/plugins/elementor/assets/lib/swiper/v8/css/swiper.min.css?ver=8.4.5 HTTP/2
Host: news.wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: text/css,*/*;q=0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Referer: https://news.wheelmap.org/en/apps/
Accept-Encoding: gzip, deflate, br
Priority: u=0
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:18:44 GMT
Content-Type: text/css
Content-Length: 16471
Last-Modified: Sun, 10 Nov 2024 13:13:17 GMT
Etag: "4057-6268ebf554d32-gzip"
Vary: Accept-Encoding
Cache-Control: max-age=14400
Cf-Cache-Status: HIT
Accept-Ranges: bytes
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=zv3y0RgZ3UVTF7hfrz5RsfcPPpFMBF68HXeer%2FsXrP%2Bdjz0r44NhaHroX2df5RVBrmJCgC6aEbHyEBnSsImOqJO6YA
XejzehLiWWGXSnas2HVFKWv0GqXPxevcTKmhFygJYR"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6c105bcaa2b1-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=33809&min_rtt=3071&rtt_var=54249&sent=58&recv=50&lost=0&retrans=2&sent_bytes=36373&recv_bytes=41
63&delivery_rate=4980277&cwnd=256&unsent_bytes=0&cid=486f1b40d622f412&ts=1902&x=0"

/**
* Swiper 8.4.5
* Most modern mobile touch slider and framework with hardware accelerated transitions
* https://swiperjs.com
*
* Copyright 2014-2022 Vladimir Kharlampidi
*
```

```
* Released under t
...[SNIP]...
```

4.16. https://news.wheelmap.org/en/apps/

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://news.wheelmap.org**
Path:	**/en/apps/**

Request

```
GET /en/apps/ HTTP/1.1
Host: news.wheelmap.org
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:18:42 GMT
Content-Type: text/html; charset=UTF-8
Link: <https://news.wheelmap.org/en/wp-json/>; rel="https://api.w.org/", <https://news.wheelmap.org/en/wp-
json/wp/v2/pages/5777>; rel="alternate"; title="JSON"; type="application/json", <https://news.wheelmap.org/en/?p=5777>;
rel=shortlink
Vary: Accept-Encoding
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=CTFPLXPh87yBwgqZxoDhiNOnyADdx%2B0cIMevZ%2FntXKTXyP17J5lXXsUFM20w8D%2Bw4m9o5y2UmglNXtiEvj%2Bc
xf2jRZL2uOqEWswR2UE%2FKLSG%2BtaeKpy5XBwV1vxgtbh5PSTF"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6c05bd74a2b1-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=11041&min_rtt=4177&rtt_var=8284&sent=8&recv=11&lost=0&retrans=1&sent_bytes=3915&recv_bytes=1315&
delivery_rate=347617&cwnd=254&unsent_bytes=0&cid=486f1b40d622f412&ts=789&x=0"
```

```
<!doctype html>
<html lang="en-US">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="profile" href="https://gmpg.org/xfn/11">
  <title>Ap
...[SNIP]...
```

4.17. https://news.wheelmap.org/en/wp-content/themes/hello-elementor/style.min.css

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://news.wheelmap.org**
Path:	**/en/wp-content/themes/hello-elementor/style.min.css**

Request

```
GET /en/wp-content/themes/hello-elementor/style.min.css?ver=3.1.1 HTTP/2
Host: news.wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: text/css,*/*;q=0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Referer: https://news.wheelmap.org/en/apps/
Accept-Encoding: gzip, deflate, br
Priority: u=0
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:18:43 GMT
Content-Type: text/css
Content-Length: 5501
Last-Modified: Sun, 18 Aug 2024 18:18:27 GMT
Etag: "157d-61ff938030392-gzip"
Vary: Accept-Encoding
Cache-Control: max-age=14400
Cf-Cache-Status: HIT
Accept-Ranges: bytes
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=XLo7CLC53h1yRGJJR1JQeadBqeq4NzS7glnTOY61x8GgK1Erz9E%2Fbvk0IuD6AphmjLPKet7Gk7nkPHDlpwOkSFgpgIiYViBBxx8AfG5WFZ7SX7qwdbW07wVKFrN%2FR1DSkZof"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
```

```
Server: cloudflare
Cf-Ray: 8e9e6c0d4f42a2b1-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=117861&min_rtt=4177&rtt_var=122885&sent=38&recv=20&lost=0&retrans=2&sent_bytes=34028&recv_bytes=
1709&delivery_rate=347617&cwnd=256&unsent_bytes=0&cid=486f1b40d622f412&ts=1664&x=0"

html{line-height:1.15;-webkit-text-size-adjust:100%}*,:after,:before{box-sizing:border-box}body{margin:0;font-family:-apple-
system,BlinkMacSystemFont,Segoe UI,Roboto,Helvetica Neue,Arial,Noto Sans,san
...[SNIP]...
```

4.18. https://news.wheelmap.org/en/wp-content/themes/hello-elementor/theme.min.css

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://news.wheelmap.org**
Path:	**/en/wp-content/themes/hello-elementor/theme.min.css**

Request

```
GET /en/wp-content/themes/hello-elementor/theme.min.css?ver=3.1.1 HTTP/2
Host: news.wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: text/css,*/*;q=0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Referer: https://news.wheelmap.org/en/apps/
Accept-Encoding: gzip, deflate, br
Priority: u=0
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:18:43 GMT
Content-Type: text/css
Content-Length: 5146
Last-Modified: Sun, 18 Aug 2024 18:18:27 GMT
Etag: "141a-61ff938031332-gzip"
Vary: Accept-Encoding
Cache-Control: max-age=14400
Cf-Cache-Status: HIT
Accept-Ranges: bytes
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=0R%2BeZ6uLtoHkyfG2cfz5ewTXrppB6pcjGZ5f%2FTDgoHHxTDj2WHBeUc3PQQVGvB3X%2F4IjEdWsd46q5qjbQx2JquELf
naAPeqRgSkyNkR0yqC%2FI%2BGzdkrqVI5qwb4VXCJPGtW9"}],"group":"cf-nel","max_age":604800}
```

```
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6c0d4f40a2b1-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=117861&min_rtt=4177&rtt_var=122885&sent=35&recv=20&lost=0&retrans=2&sent_bytes=32186&recv_bytes=
1709&delivery_rate=347617&cwnd=256&unsent_bytes=0&cid=486f1b40d622f412&ts=1664&x=0"

@charset "UTF-8";.comments-area a,.page-content a{text-decoration:underline}.alignright{float:right;margin-
left:1rem}.alignleft{float:left;margin-right:1rem}.aligncenter{clear:both;display:block;margi
...[SNIP]...
```

4.19. https://news.wheelmap.org/en/wp-includes/css/dist/block-library/style.min.css

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://news.wheelmap.org**
Path:	**/en/wp-includes/css/dist/block-library/style.min.css**

Request

```
GET /en/wp-includes/css/dist/block-library/style.min.css?ver=6.6.2 HTTP/2
Host: news.wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: text/css,*/*;q=0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Referer: https://news.wheelmap.org/en/apps/
Accept-Encoding: gzip, deflate, br
Priority: u=0
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:18:43 GMT
Content-Type: text/css
Content-Length: 112427
Last-Modified: Tue, 10 Sep 2024 20:19:06 GMT
Etag: "1b72b-621c995d8db02-gzip"
Vary: Accept-Encoding
Cache-Control: max-age=14400
Cf-Cache-Status: MISS
Accept-Ranges: bytes
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=CWPkDzBc1pTUuEG7WCSv1UUDaOjtOAd%2BPvFgaAEoecUw5R2ivkOibdGIS6lYBX1eGfiND61BjVZ5hDIjT3QDxvT%2Fp
U0OT33OHg5ryknD4jjZDfJl3a7Pe9rNy5yYi7BeIGq9"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6c0d2f0ea2b1-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=117861&min_rtt=4177&rtt_var=122885&sent=22&recv=20&lost=0&retrans=2&sent_bytes=16523&recv_bytes=
1709&delivery_rate=347617&cwnd=256&unsent_bytes=0&cid=486f1b40d622f412&ts=1662&x=0"

@charset "UTF-8";.wp-block-archives{box-sizing:border-box}.wp-block-archives-dropdown label{display:block}.wp-block-
avatar{line-height:0}.wp-block-avatar,.wp-block-avatar img{box-sizing:border-box}.wp
...[SNIP]...
```

4.20. https://photon.komoot.io/api/

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://photon.komoot.io**
Path:	**/api/**

Request

```
GET /api/?q=concordia%5C%5C%5C&limit=30&lang=en HTTP/1.1
Host: photon.komoot.io
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Fri, 29 Nov 2024 00:22:59 GMT
Content-Type: application/json;charset=utf-8
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Request-Method: get
Access-Control-Allow-Headers: *
Expires: Fri, 29 Nov 2024 01:22:59 GMT
Cache-Control: max-age=3600
```

```
Content-Length: 11295

{"features":[{"geometry":{"coordinates":[-91.6714379,31.3941887],"type":"Point"},"type":"Feature","properties":
{"osm_type":"R","osm_id":1837802,"extent":[-91.867607,31.762226,-91.3785942,30.9969969],"
...[SNIP]...
```

4.21. https://service.sozialhelden.de/pwproxy.php

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://service.sozialhelden.de**
Path:	**/pwproxy.php**

Request

```
GET /pwproxy.php HTTP/1.1
Host: service.sozialhelden.de
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Vary: Accept-Encoding
Last-Modified: Fri, 29 Nov 2024 00:21:19 GMT
Content-Length: 67450
Content-Type: application/javascript; charset=UTF-8
Date: Fri, 29 Nov 2024 00:21:19 GMT
Server: Apache

/*!!
* Matomo - free/libre analytics platform
*
* JavaScript tracking client
*
* @link https://piwik.org
* @source https://github.com/matomo-org/matomo/blob/master/js/piwik.js
* @license https:
...[SNIP]...
```

4.22. https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://static.cloudflareinsights.com**
Path:	**/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015**

Request

```
GET /beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015 HTTP/1.1
Host: static.cloudflareinsights.com
Origin: https://news.wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: script
Referer: https://news.wheelmap.org/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:19:28 GMT
Content-Type: text/javascript;charset=UTF-8
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=86400
Etag: W/"2024.6.1"
Last-Modified: Thu, 06 Jun 2024 15:52:56 GMT
Cross-Origin-Resource-Policy: cross-origin
Vary: Accept-Encoding
Server: cloudflare
Cf-Ray: 8e9e6d2878d5a305-YUL

!function(){var e={343:function(e){"use strict";for(var t=[],n=0;n<256;++n)t[n]=
(n+256).toString(16).substr(1);e.exports=function(e,n){var r=n||0,i=t;return[i[e[r++]],i[e[r++]],i[e[r++]],i[e[r++]],"-"
...[SNIP]...
```

4.23. https://www.google.com/generate_204

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://www.google.com**
Path:	**/generate_204**

Request

```
GET /generate_204 HTTP/1.1
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.32 Safari/537.36
Host: www.google.com
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 204 No Content
Content-Length: 0
Cross-Origin-Resource-Policy: cross-origin
Date: Fri, 29 Nov 2024 00:19:29 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

5. Content security policy: allowlisted script resources

There are 2 instances of this issue:

- https://v2.accessibility.cloud/tracking-events/report
- https://wheelmap.org/

Issue background

Content Security Policy (CSP) is a security mechanism designed to mitigate cross-site scripting attacks by disabling dangerous behaviours such as untrusted JavaScript execution. Websites can specify their security policy in a response header or meta tag, enabling fine-grained control over dangerous features like scripts and stylesheets.

Issue remediation

To prevent untrusted JavaScript execution, replace allowlisted resources in script-based directives with a secure, random nonce of at least 8 characters 'nonce-RANDOM'.

References

- Web Security Academy: What is CSP?
- Web Security Academy: What is XSS?
- Web Security Academy: Mitigating XSS attacks using CSP
- Web Security Academy: Preventing XSS
- Content Security Policy (CSP)

Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-588: DOM-Based XSS

5.1. https://v2.accessibility.cloud/tracking-events/report

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://v2.accessibility.cloud**
Path:	**/tracking-events/report**

Issue detail

The Content Security Policy relies on an allowlist to control script-based resource loading. However, this approach is vulnerable if allowlisted domains host scripts susceptible to reflected or DOM-based XSS attacks. Additionally, JSONP-based endpoints can be abused too. These vulnerabilities could enable attackers to bypass the CSP, leading to untrusted JavaScript execution.

Request

```
OPTIONS /tracking-events/report?appToken=27be4b5216aced82122d7cf8f69e4a07 HTTP/1.1
Host: v2.accessibility.cloud
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type
Origin: https://wheelmap.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:19 GMT
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
```

```
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=ABjuq%2FccA8NoiGVXBXNqf9kgTo%2FzNQi5%2F1tdg6tKXv%2FBzzmqgMpsjp%2Fja%2FRBTOqZLPgE6bP7HGKiUmKR
XuXHs2WDiwSuPGc3trtdyCZddK3yMCpcSmNFrPYmdKOTMVX0xnbAKh5Frsyd"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6fd9f926a28c-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4978&min_rtt=3686&rtt_var=2547&sent=7&recv=11&lost=0&retrans=0&sent_bytes=3699&recv_bytes=1251&d
elivery_rate=579178&cwnd=239&unsent_bytes=0&cid=d4d14fd1aa13460c&ts=394&x=0"
```

5.2. https://wheelmap.org/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://wheelmap.org**
Path:	**/**

Issue detail

The Content Security Policy relies on an allowlist to control script-based resource loading. However, this approach is vulnerable if allowlisted domains host scripts susceptible to reflected or DOM-based XSS attacks. Additionally, JSONP-based endpoints can be abused too. These vulnerabilities could enable attackers to bypass the CSP, leading to untrusted JavaScript execution.

Request

```
GET / HTTP/1.1
Host: wheelmap.org
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
```

```
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://news.wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:08 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: Next.js
Cache-Control: max-age=3600, public
Vary: X-User-Agent-Variant, X-Locale-Variant, Content-Language, Accept-Encoding
X-Locale-Variant: en-us
Content-Language: en-us
X-User-Agent-Variant: Windows
X-Frame-Options: deny
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=DLH2DZNWER%2BKKRYqqn5KbKk%2FzrCdWckNo9lbMa3t98wD%2FMsj%2FHohPBy72XUVzH2WneQ9xF9%2Bui0xllP6
GfB2Vxy5vVWoszPtwclubBavQ4qwQBt7tLHky6N4%2Fld3IA%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6f941d9ca2ae-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=3696&min_rtt=2902&rtt_var=1701&sent=9&recv=11&lost=0&retrans=0&sent_bytes=3716&recv_bytes=1322&d
elivery_rate=703147&cwnd=249&unsent_bytes=0&cid=56c8de4124ebb565&ts=190&x=0"

<!DOCTYPE html><html lang="en-US"><head><meta charSet="utf-8"/><meta name="viewport" content="width=device-width,
height=device-height, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, viewpor
...[SNIP]...
<meta http-equiv="Content-Security-Policy" content="
default-src
&#x27;self&#x27;
ws:
data:
blob:
&#x27;self&#x27;
&#x27;unsafe-eval&#x27;
&#x27;unsafe-inline&#x27;
https://sozialhelden.de
https://service.sozialhelden.de
https://photon.komoot.io
https://api.mapbox.com
https://api.tiles.mapbox.com
https://events.mapbox.com
https://ac-o-0.global.ssl.fastly.net
https://ac-o-1.global.ssl.fastly.net
https://ac-o-2.global.ssl.fastly.net
```

```
https://ac-o-3.global.ssl.fastly.net
https://osm-api.wheelmap.tech
https://ac-o-{n}.global.ssl.fastly.net
https://accessibility-cloud-v2.freetls.fastly.net
https://v2.accessibility.cloud
;
style-src
&#x27;self&#x27;
https://api.tiles.mapbox.com
&#x27;unsafe-inline&#x27;;
frame-src
&#x27;self&#x27;;
media-src
&#x27;self&#x27;;
img-src
&#x27;self&#x27;
data:
blob:
https://accessibility-cloud-uploads.s3.amazonaws.com
https://service.sozialhelden.de
https://api.mapbox.com
https://asset0.wheelmap.org
https://asset1.wheelmap.org
https://asset2.wheelmap.org
https://asset3.wheelmap.org
https://asset4.wheelmap.org
https://accessibility-cloud-v2.freetls.fastly.net
https://v2.accessibility.cloud
;
"/>
...[SNIP]...
```

6. Content security policy: allows untrusted script execution

There are 3 instances of this issue:

- https://v2.accessibility.cloud/tracking-events/report
- https://wheelmap.org/
- https://wheelmap.pro/organizations/LPb4y2ri7b6fLxLFa/survey-projects/wx4mM8xFiQAsB5aLi/show

Issue background

Content Security Policy (CSP) is a security mechanism designed to mitigate cross-site scripting attacks by disabling dangerous behaviours such as untrusted JavaScript execution. Websites can specify their security policy in a response header or meta tag, enabling fine-grained control over dangerous features like scripts and stylesheets.

Issue remediation

Mitigate cross-site scripting by avoiding 'unsafe-inline', 'unsafe-eval', data: URLs, and global wildcards in script directives. Use a secure, random nonce of at least 8 characters 'nonce-RANDOM' to prevent untrusted JavaScript execution.

References

- Web Security Academy: What is CSP?
- Web Security Academy: What is XSS?
- Web Security Academy: Mitigating XSS attacks using CSP
- Web Security Academy: Preventing XSS
- Content Security Policy (CSP)

Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-588: DOM-Based XSS

6.1. https://v2.accessibility.cloud/tracking-events/report

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://v2.accessibility.cloud**
Path:	**/tracking-events/report**

Issue detail

The content security policy fails to prevent untrusted JavaScript from being executed. As a result, it may fail to mitigate cross-site scripting attacks.

The policy has the following issues:

The policy contains unsafe-inline which can allow arbitrary scripts to be executed.

Allowing dynamic JavaScript execution through unsafe-eval in the policy fails to mitigate some DOM-based cross-site scripting vulnerabilities.

The policy allows data: URLs which allows arbitrary scripts to be executed.

Request

```
OPTIONS /tracking-events/report?appToken=27be4b5216aced82122d7cf8f69e4a07 HTTP/1.1
Host: v2.accessibility.cloud
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type
Origin: https://wheelmap.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:19 GMT
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=ABjuq%2FccA8NoiGVXBXNqf9kgTo%2FzNQi5%2F1tdg6tKXv%2FBzzmqgMpsjp%2Fja%2FRBTOqZLPgE6bP7HGKiUmKR
XuXHs2WDiwSuPGc3trtdyCZddK3yMCpcSmNFrPYmdKOTMVX0xnbAKh5Frsyd"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6fd9f926a28c-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4978&min_rtt=3686&rtt_var=2547&sent=7&recv=11&lost=0&retrans=0&sent_bytes=3699&recv_bytes=1251&d
elivery_rate=579178&cwnd=239&unsent_bytes=0&cid=d4d14fd1aa13460c&ts=394&x=0"
```

6.2. https://wheelmap.org/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://wheelmap.org**
Path:	**/**

Issue detail

The content security policy fails to prevent untrusted JavaScript from being executed. As a result, it may fail to mitigate cross-site scripting attacks.

The policy has the following issues:

The policy contains unsafe-inline which can allow arbitrary scripts to be executed.

Allowing dynamic JavaScript execution through unsafe-eval in the policy fails to mitigate some DOM-based cross-site scripting vulnerabilities.

The policy allows data: URLs which allows arbitrary scripts to be executed.

Request

```
GET / HTTP/1.1
Host: wheelmap.org
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://news.wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:08 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: Next.js
Cache-Control: max-age=3600, public
Vary: X-User-Agent-Variant, X-Locale-Variant, Content-Language, Accept-Encoding
X-Locale-Variant: en-us
Content-Language: en-us
X-User-Agent-Variant: Windows
X-Frame-Options: deny
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=DLH2DZNWER%2BKKRYqqn5KbKk%2FzrCdWckNo9lbMa3t98wD%2FMsj%2FHohPBy72XUVzH2WneQ9xF9%2Bui0xlIP6
GfB2Vxy5vVWoszPtwclubBavQ4qwQBt7tLHky6N4%2Fld3IA%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6f941d9ca2ae-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=3696&min_rtt=2902&rtt_var=1701&sent=9&recv=11&lost=0&retrans=0&sent_bytes=3716&recv_bytes=1322&d
elivery_rate=703147&cwnd=249&unsent_bytes=0&cid=56c8de4124ebb565&ts=190&x=0"

<!DOCTYPE html><html lang="en-US"><head><meta charSet="utf-8"/><meta name="viewport" content="width=device-width,
height=device-height, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, viewpor
...[SNIP]...
<meta http-equiv="Content-Security-Policy" content="
default-src
&#x27;self&#x27;
```

```
ws:
data:
blob:
&#x27;self&#x27;
&#x27;unsafe-eval&#x27;
&#x27;unsafe-inline&#x27;
https://sozialhelden.de
https://service.sozialhelden.de
https://photon.komoot.io
https://api.mapbox.com
https://api.tiles.mapbox.com
https://events.mapbox.com
https://ac-o-0.global.ssl.fastly.net
https://ac-o-1.global.ssl.fastly.net
https://ac-o-2.global.ssl.fastly.net
https://ac-o-3.global.ssl.fastly.net
https://osm-api.wheelmap.tech
https://ac-o-{n}.global.ssl.fastly.net
https://accessibility-cloud-v2.freetls.fastly.net
https://v2.accessibility.cloud
;
style-src
&#x27;self&#x27;
https://api.tiles.mapbox.com
&#x27;unsafe-inline&#x27;;
frame-src
&#x27;self&#x27;;
media-src
&#x27;self&#x27;;
img-src
&#x27;self&#x27;
data:
blob:
https://accessibility-cloud-uploads.s3.amazonaws.com
https://service.sozialhelden.de
https://api.mapbox.com
https://asset0.wheelmap.org
https://asset1.wheelmap.org
https://asset2.wheelmap.org
https://asset3.wheelmap.org
https://asset4.wheelmap.org
https://accessibility-cloud-v2.freetls.fastly.net
https://v2.accessibility.cloud
;
"/>
...[SNIP]...
```

6.3. https://wheelmap.pro/organizations/LPb4y2ri7b6fLxLFa/survey-projects/wx4mM8xFiQAsB5aLi/show

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://wheelmap.pro**
Path:	**/organizations/LPb4y2ri7b6fLxLFa/survey-projects/wx4mM8xFiQAsB5aLi/show**

Issue detail

The content security policy fails to prevent untrusted JavaScript from being executed. As a result, it may fail to mitigate cross-site scripting attacks.

The policy has the following issues:

The policy contains unsafe-inline which can allow arbitrary scripts to be executed.

Allowing dynamic JavaScript execution through unsafe-eval in the policy fails to mitigate some DOM-based cross-site scripting vulnerabilities.

The policy allows data: URLs which allows arbitrary scripts to be executed.

Request

```
GET /organizations/LPb4y2ri7b6fLxLFa/survey-projects/wx4mM8xFiQAsB5aLi/show?
d%5Bmapping_event_id%5D=undefined&d%5BuniqueSurveyId%5D=af3d83a0-38b3-41e2-a5b2-
0f0f6af14689&d%5BosmId%5D=undefined%2Fundefined HTTP/1.1
Host: wheelmap.pro
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:23:38 GMT
Content-Type: text/html; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
```

```
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=hGcQWMAHHWbkatPS8gmcAbpJObfX3pu5LUSMMC4jzUiR7YBJh0T%2FuUyKNCkw7%2FUTIi556lJJbms6EgId%2BWxX
wnIUHgcFxr3fHMJ4zOX2vhcBCd51nUjZE9y%2FFdy0jLA%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e733d6e8ba269-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=15371&min_rtt=9222&rtt_var=12754&sent=11&recv=12&lost=0&retrans=0&sent_bytes=3698&recv_bytes=145
2&delivery_rate=218641&cwnd=248&unsent_bytes=0&cid=13492432fa2054cf&ts=446&x=0"

<!DOCTYPE html>
<html lang="en">
<head>


</head>
<body><noscript
>...... Sorry, this app needs JavaScript to work. Please enable JavaScript in your
browser.</noscript
>
<div id="react-ap
...[SNIP]...
```

7. Content security policy: allows untrusted style execution

There are 3 instances of this issue:

- https://v2.accessibility.cloud/tracking-events/report
- https://wheelmap.org/
- http://www.google.com/gen_204

Issue background

Content Security Policy (CSP) is a security mechanism designed to mitigate cross-site scripting attacks by disabling dangerous behaviours such as untrusted JavaScript execution. Websites can specify their security policy in a response header or meta tag, enabling fine-grained control over dangerous features like scripts and stylesheets.

Issue remediation

Mitigate style-based data exfiltration by avoiding 'unsafe-inline', data: URLs, and global wildcards in style directives. Use a secure, random nonce of at least 8 characters 'nonce-RANDOM' in the relevant directive.

References

- Web Security Academy: What is CSP?
- PortSwigger Research: Blind CSS exfiltration
- PortSwigger Research: Offensive CSS research
- Content Security Policy (CSP)

Vulnerability classifications

- CWE-116: Improper Encoding or Escaping of Output

- CWE-159: Failure to Sanitize Special Element
- CAPEC-468: Generic Cross-Browser Cross-Domain Theft

7.1. https://v2.accessibility.cloud/tracking-events/report

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://v2.accessibility.cloud**
Path:	**/tracking-events/report**

Issue detail

The content security policy fails to prevent untrusted style execution. As a result, it may fail to mitigate style based data exfiltration.

The policy contains unsafe-inline which can allow arbitrary styles to be executed.

The policy allows data: URLs which allows arbitrary styles to be executed.

Request

```
OPTIONS /tracking-events/report?appToken=27be4b5216aced82122d7cf8f69e4a07 HTTP/1.1
Host: v2.accessibility.cloud
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type
Origin: https://wheelmap.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:19 GMT
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
```

```
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=ABjuq%2FccA8NoiGVXBXNqf9kgTo%2FzNQi5%2F1tdg6tKXv%2FBzzmqgMpsjp%2Fja%2FRBTOqZLPgE6bP7HGKiUmKR
XuXHs2WDiwSuPGc3trtdyCZddK3yMCpcSmNFrPYmdKOTMVX0xnbAKh5Frsyd"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6fd9f926a28c-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4978&min_rtt=3686&rtt_var=2547&sent=7&recv=11&lost=0&retrans=0&sent_bytes=3699&recv_bytes=1251&d
elivery_rate=579178&cwnd=239&unsent_bytes=0&cid=d4d14fd1aa13460c&ts=394&x=0"
```

7.2. https://wheelmap.org/

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://wheelmap.org**

Path: **/**

Issue detail

The content security policy fails to prevent untrusted style execution. As a result, it may fail to mitigate style based data exfiltration.

The policy contains unsafe-inline which can allow arbitrary styles to be executed.

The policy allows data: URLs which allows arbitrary styles to be executed.

Request

```
GET / HTTP/1.1
Host: wheelmap.org
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
```

```
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://news.wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:08 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: Next.js
Cache-Control: max-age=3600, public
Vary: X-User-Agent-Variant, X-Locale-Variant, Content-Language, Accept-Encoding
X-Locale-Variant: en-us
Content-Language: en-us
X-User-Agent-Variant: Windows
X-Frame-Options: deny
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=DLH2DZNWER%2BKKRYqqn5KbKk%2FzrCdWckNo9lbMa3t98wD%2FMsj%2FHohPBy72XUVzH2WneQ9xF9%2Bui0xlIP6
GfB2Vxy5vVWoszPtwclubBavQ4qwQBt7tLHky6N4%2Fld3IA%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6f941d9ca2ae-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=3696&min_rtt=2902&rtt_var=1701&sent=9&recv=11&lost=0&retrans=0&sent_bytes=3716&recv_bytes=1322&d
elivery_rate=703147&cwnd=249&unsent_bytes=0&cid=56c8de4124ebb565&ts=190&x=0"

<!DOCTYPE html><html lang="en-US"><head><meta charSet="utf-8"/><meta name="viewport" content="width=device-width,
height=device-height, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, viewpor
...[SNIP]...
<meta http-equiv="Content-Security-Policy" content="
default-src
&#x27;self&#x27;
ws:
data:
blob:
&#x27;self&#x27;
&#x27;unsafe-eval&#x27;
&#x27;unsafe-inline&#x27;
https://sozialhelden.de
https://service.sozialhelden.de
https://photon.komoot.io
https://api.mapbox.com
https://api.tiles.mapbox.com
https://events.mapbox.com
https://ac-o-0.global.ssl.fastly.net
https://ac-o-1.global.ssl.fastly.net
```

```
https://ac-o-2.global.ssl.fastly.net
https://ac-o-3.global.ssl.fastly.net
https://osm-api.wheelmap.tech
https://ac-o-{n}.global.ssl.fastly.net
https://accessibility-cloud-v2.freetls.fastly.net
https://v2.accessibility.cloud
;
style-src
&#x27;self&#x27;
https://api.tiles.mapbox.com
&#x27;unsafe-inline&#x27;;
frame-src
&#x27;self&#x27;;
media-src
&#x27;self&#x27;;
img-src
&#x27;self&#x27;
data:
blob:
https://accessibility-cloud-uploads.s3.amazonaws.com
https://service.sozialhelden.de
https://api.mapbox.com
https://asset0.wheelmap.org
https://asset1.wheelmap.org
https://asset2.wheelmap.org
https://asset3.wheelmap.org
https://asset4.wheelmap.org
https://accessibility-cloud-v2.freetls.fastly.net
https://v2.accessibility.cloud
;
"/>
...[SNIP]...
```

7.3. http://www.google.com/gen_204

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://www.google.com**
Path:	**/gen_204**

Issue detail

The content security policy fails to prevent untrusted style execution. As a result, it may fail to mitigate style based data exfiltration.

The policy allows global wildcard URLs which allows arbitrary styles to be executed.

The policy allows data: URLs which allows arbitrary styles to be executed.

Request

```
GET /gen_204 HTTP/1.1
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.32 Safari/537.36
Host: www.google.com
```

```
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/1.1 204 No Content
Content-Type: text/html; charset=UTF-8
Content-Security-Policy: object-src 'none';base-uri 'self';script-src 'nonce-WUmCg9AA-jUlY8uNNhbvyw' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Permissions-Policy: unload=()
Date: Fri, 29 Nov 2024 00:19:29 GMT
Server: gws
Content-Length: 0
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

8. Content security policy: malformed syntax

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://wheelmap.org**
Path:	**/**

Issue detail

Malformed syntax in the policy means the following directives, which do not conform to the CSP specification, will not be enforced:

Directive default-src has illegal value component: https://ac-o-{n}.global.ssl.fastly.net

Issue background

Content Security Policy (CSP) is a security mechanism designed to mitigate cross-site scripting attacks by disabling dangerous behaviours such as untrusted JavaScript execution. Websites can specify their security policy in a response header or meta tag, enabling fine-grained control over dangerous features like scripts and stylesheets.

Issue remediation

Using malformed syntax in your policy causes the browser to ignore the directive. Ensure that you use the correct syntax in your policy.

References

- Web Security Academy: What is CSP?
- Content Security Policy (CSP)

Request

```
GET / HTTP/1.1
Host: wheelmap.org
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://news.wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:08 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: Next.js
Cache-Control: max-age=3600, public
Vary: X-User-Agent-Variant, X-Locale-Variant, Content-Language, Accept-Encoding
X-Locale-Variant: en-us
Content-Language: en-us
X-User-Agent-Variant: Windows
X-Frame-Options: deny
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=DLH2DZNWER%2BKKRYqqn5KbKk%2FzrCdWckNo9lbMa3t98wD%2FMsj%2FHohPBy72XUVzH2WneQ9xF9%2Bui0xlIP6
GfB2Vxy5vVWoszPtwclubBavQ4qwQBt7tLHky6N4%2Fld3IA%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6f941d9ca2ae-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=3696&min_rtt=2902&rtt_var=1701&sent=9&recv=11&lost=0&retrans=0&sent_bytes=3716&recv_bytes=1322&d
elivery_rate=703147&cwnd=249&unsent_bytes=0&cid=56c8de4124ebb565&ts=190&x=0"

<!DOCTYPE html><html lang="en-US"><head><meta charSet="utf-8"/><meta name="viewport" content="width=device-width,
height=device-height, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, viewpor
...[SNIP]...
<meta http-equiv="Content-Security-Policy" content="
default-src
&#x27;self&#x27;
ws:
data:
blob:
&#x27;self&#x27;
&#x27;unsafe-eval&#x27;
&#x27;unsafe-inline&#x27;
https://sozialhelden.de
https://service.sozialhelden.de
https://photon.komoot.io
https://api.mapbox.com
https://api.tiles.mapbox.com
```

```
https://events.mapbox.com
https://ac-o-0.global.ssl.fastly.net
https://ac-o-1.global.ssl.fastly.net
https://ac-o-2.global.ssl.fastly.net
https://ac-o-3.global.ssl.fastly.net
https://osm-api.wheelmap.tech
https://ac-o-{n}.global.ssl.fastly.net
https://accessibility-cloud-v2.freetls.fastly.net
https://v2.accessibility.cloud
;
style-src
&#x27;self&#x27;
https://api.tiles.mapbox.com
&#x27;unsafe-inline&#x27;;
frame-src
&#x27;self&#x27;;
media-src
&#x27;self&#x27;;
img-src
&#x27;self&#x27;
data:
blob:
https://accessibility-cloud-uploads.s3.amazonaws.com
https://service.sozialhelden.de
https://api.mapbox.com
https://asset0.wheelmap.org
https://asset1.wheelmap.org
https://asset2.wheelmap.org
https://asset3.wheelmap.org
https://asset4.wheelmap.org
https://accessibility-cloud-v2.freetls.fastly.net
https://v2.accessibility.cloud
;
"/>
...[SNIP]...
```

9. Content security policy: allows form hijacking

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://www.google.com**
Path:	**/gen_204**

Issue detail

The content security policy doesn't prevent form hijacking, where attackers with HTML injection hijack forms using action attributes. This can lead to credential theft by autofilling passwords from a manager and sending them to an attacker's server upon form submission.

Issue background

Content Security Policy (CSP) is a security mechanism designed to mitigate cross-site scripting attacks by disabling dangerous behaviours such as untrusted JavaScript execution. Websites can specify their security policy in a response header or meta tag, enabling fine-grained control over dangerous features like scripts and stylesheets.

Issue remediation

We recommend using the form-action directive in the CSP response header to control form post destinations. If no form actions are used, set form-action to 'none' to block untrusted forms. For applications without external form URLs, use 'self' to allow only same-origin URLs. If needed, allow list hosts for external URL form submissions, but be aware this lets attackers submit to these external resources.

References

- PortSwigger Research: Stealing passwords from infosec Mastodon - without bypassing CSP
- Web Security Academy: What is CSP?
- Content Security Policy (CSP)

Vulnerability classifications

- CWE-116: Improper Encoding or Escaping of Output

Request

```
GET /gen_204 HTTP/1.1
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.32 Safari/537.36
Host: www.google.com
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/1.1 204 No Content
Content-Type: text/html; charset=UTF-8
Content-Security-Policy: object-src 'none';base-uri 'self';script-src 'nonce-WUmCg9AA-jUIY8uNNhbvyw' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Permissions-Policy: unload=()
Date: Fri, 29 Nov 2024 00:19:29 GMT
Server: gws
Content-Length: 0
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

10. Cross-domain script include

There are 2 instances of this issue:

- https://news.wheelmap.org/en/apps/
- https://wheelmap.org/

Issue background

When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do, such as accessing application data and performing actions within the context of the current user.

If you include a script from an external domain, then you are trusting that domain with the data and functionality of your application, and you are trusting the domain's own security to prevent an attacker from modifying the script to perform malicious actions within your application.

Issue remediation

Scripts should ideally not be included from untrusted domains. Applications that rely on static third-party scripts should consider using Subresource Integrity to make browsers verify them, or copying the contents of these scripts onto their own domain and including them from there. If that is not possible (e.g. for licensing reasons) then consider reimplementing the script's functionality within application code.

References

- Subresource Integrity

Vulnerability classifications

- CWE-829: Inclusion of Functionality from Untrusted Control Sphere

---

10.1. https://news.wheelmap.org/en/apps/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://news.wheelmap.org**
Path:	**/en/apps/**

Issue detail

The response dynamically includes the following script from another domain:

- https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015

Request

```
GET /en/apps/ HTTP/1.1
Host: news.wheelmap.org
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:18:42 GMT
Content-Type: text/html; charset=UTF-8
Link: <https://news.wheelmap.org/en/wp-json/>; rel="https://api.w.org/", <https://news.wheelmap.org/en/wp-
json/wp/v2/pages/5777>; rel="alternate"; title="JSON"; type="application/json", <https://news.wheelmap.org/en/?p=5777>;
rel=shortlink
Vary: Accept-Encoding
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=CTFPLXPh87yBwgqZxoDhiNOnyADdx%2B0cIMevZ%2FntXKTXyP17J5lXXsUFM20w8D%2Bw4m9o5y2UmglNXtiEvj%2Bc
xf2jRZL2uOqEWswR2UE%2FKLSG%2BtaeKpy5XBwV1vxgtbh5PSTF"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6c05bd74a2b1-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=11041&min_rtt=4177&rtt_var=8284&sent=8&recv=11&lost=0&retrans=1&sent_bytes=3915&recv_bytes=1315&
delivery_rate=347617&cwnd=254&unsent_bytes=0&cid=486f1b40d622f412&ts=789&x=0"

<!doctype html>
<html lang="en-US">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="profile" href="https://gmpg.org/xfn/11">
  <title>Ap
...[SNIP]...
</script>

<script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015"
integrity="sha512-
ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-
beacon='{"rayId":"8e9e6c05bd74a2b1","version":"2024.10.5","serverTiming":{"name":
{"cfExtPri":true,"cfL4":true,"cfSpeedBrain":true,"cfCacheStatus":true}},"token":"e984cce862cc4d6fa172e7817939ffc1","b":1}'
crossorigin="anonymous"></script>
...[SNIP]...
```

10.2. https://wheelmap.org/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://wheelmap.org**
Path:	**/**

Issue detail

The response dynamically includes the following script from another domain:

- https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015

Request

```
GET / HTTP/1.1
Host: wheelmap.org
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://news.wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:08 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: Next.js
Cache-Control: max-age=3600, public
Vary: X-User-Agent-Variant, X-Locale-Variant, Content-Language, Accept-Encoding
X-Locale-Variant: en-us
Content-Language: en-us
X-User-Agent-Variant: Windows
X-Frame-Options: deny
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=DLH2DZNWER%2BKKRYqqn5KbKk%2FzrCdWckNo9lbMa3t98wD%2FMsj%2FHohPBy72XUVzH2WneQ9xF9%2Bui0xlIP6
GfB2Vxy5vVWoszPtwclubBavQ4qwQBt7tLHky6N4%2Fld3IA%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6f941d9ca2ae-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=3696&min_rtt=2902&rtt_var=1701&sent=9&recv=11&lost=0&retrans=0&sent_bytes=3716&recv_bytes=1322&d
elivery_rate=703147&cwnd=249&unsent_bytes=0&cid=56c8de4124ebb565&ts=190&x=0"

<!DOCTYPE html><html lang="en-US"><head><meta charSet="utf-8"/><meta name="viewport" content="width=device-width,
height=device-height, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, viewpor
...[SNIP]...
</script><script defer
src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015"
integrity="sha512-
ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf84rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-
beacon='{"rayId":"8e9e6f941d9ca2ae","version":"2024.10.5","serverTiming":{"name":
{"cfExtPri":true,"cfL4":true,"cfSpeedBrain":true,"cfCacheStatus":true}},"token":"e984cce862cc4d6fa172e7817939ffc1","b":1}'
```

```
crossorigin="anonymous"></script>
...[SNIP]...
```

11. Frameable response (potential Clickjacking)

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://news.wheelmap.org**
Path:	**/en/apps/**

Issue description

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

References

- Web Security Academy: Clickjacking
- X-Frame-Options

Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CWE-1021: Improper Restriction of Rendered UI Layers or Frames
- CAPEC-103: Clickjacking

Request

```
GET /en/apps/ HTTP/1.1
Host: news.wheelmap.org
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:18:42 GMT
Content-Type: text/html; charset=UTF-8
Link: <https://news.wheelmap.org/en/wp-json/>; rel="https://api.w.org/", <https://news.wheelmap.org/en/wp-
json/wp/v2/pages/5777>; rel="alternate"; title="JSON"; type="application/json", <https://news.wheelmap.org/en/?p=5777>;
rel=shortlink
Vary: Accept-Encoding
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=CTFPLXPh87yBwgqZxoDhiNOnyADdx%2B0cIMevZ%2FntXKTXyP17J5lXXsUFM20w8D%2Bw4m9o5y2UmglNXtiEvj%2Bc
xf2jRZL2uOqEWswR2UE%2FKLSG%2BtaeKpy5XBwV1vxgtbh5PSTF"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6c05bd74a2b1-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=11041&min_rtt=4177&rtt_var=8284&sent=8&recv=11&lost=0&retrans=1&sent_bytes=3915&recv_bytes=1315&
delivery_rate=347617&cwnd=254&unsent_bytes=0&cid=486f1b40d622f412&ts=789&x=0"

<!doctype html>
<html lang="en-US">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="profile" href="https://gmpg.org/xfn/11">
  <title>Ap
...[SNIP]...
```

---

12. Browser cross-site scripting filter disabled

There are 3 instances of this issue:

- https://fonts.googleapis.com/css
- https://fonts.gstatic.com/s/ubuntu/v20/4iCv6KVjbNBYlgoCjC3jsGyN.woff2
- http://www.google.com/gen_204

Issue description

Some browsers, including Internet Explorer, contain built-in filters designed to protect against cross-site scripting (XSS) attacks. Applications can instruct browsers to disable this filter by setting the following response header:

X-XSS-Protection: 0

This behavior does not in itself constitute a vulnerability; in some cases XSS filters may themselves be leveraged to perform attacks against application users. However, in typical situations XSS filters do provide basic protection for application users against some XSS vulnerabilities in applications. The presence of this header should be reviewed to establish whether it affects the application's security posture.

Issue remediation

Review whether the application needs to disable XSS filters. In most cases you can gain the protection provided by XSS filters without the associated risks by using the following response header:

X-XSS-Protection: 1; mode=block

When this header is set, browsers that detect an XSS attack will simply render a blank page instead of attempting to sanitize the injected script. This behavior is considerably less likely to introduce new security issues.

References

- Web Security Academy: Cross-site scripting
- Controlling the XSS Filter

Vulnerability classifications

- CWE-16: Configuration
- CAPEC-63: Cross-Site Scripting (XSS)

12.1. https://fonts.googleapis.com/css

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://fonts.googleapis.com**
Path:	**/css**

Request

```
GET /css?
family=Roboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2
C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CUbuntu%3A100%2C100italic%2C200
%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2
C800%2C800italic%2C900%2C900italic&display=auto&ver=6.6.2 HTTP/1.1
Host: fonts.googleapis.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: text/css,*/*;q=0.1
X-Client-Data: CljcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
```

```
Sec-Fetch-Dest: style
Referer: https://news.wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=0
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: text/css; charset=utf-8
Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site
Access-Control-Allow-Origin: *
Timing-Allow-Origin: *
Link: <https://fonts.gstatic.com>; rel=preconnect; crossorigin
Strict-Transport-Security: max-age=31536000
Expires: Fri, 29 Nov 2024 00:19:28 GMT
Date: Fri, 29 Nov 2024 00:19:28 GMT
Cache-Control: private, max-age=86400, stale-while-revalidate=604800
Last-Modified: Fri, 29 Nov 2024 00:19:28 GMT
Cross-Origin-Opener-Policy: same-origin-allow-popups
Cross-Origin-Resource-Policy: cross-origin
Server: ESF
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

/* cyrillic-ext */
@font-face {
font-family: 'Roboto';
font-style: italic;
font-weight: 100;
src: url(https://fonts.gstatic.com/s/roboto/v32/KFOiCnqEu92Fr1Mu51QrEz0dL_nz.woff2) format('woff2')
...[SNIP]...
```

12.2. https://fonts.gstatic.com/s/ubuntu/v20/4iCv6KVjbNBYlgoCjC3jsGyN.woff2

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://fonts.gstatic.com**
Path:	**/s/ubuntu/v20/4iCv6KVjbNBYlgoCjC3jsGyN.woff2**

Request

```
GET /s/ubuntu/v20/4iCv6KVjbNBYlgoCjC3jsGyN.woff2 HTTP/1.1
Host: fonts.gstatic.com
Origin: https://news.wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
```

```
Sec-Ch-Ua-Mobile: ?0
Accept: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: font
Referer: https://fonts.googleapis.com/
Accept-Encoding: gzip, deflate, br
Priority: u=4
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/apps-themes
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="apps-themes"
Report-To: {"group":"apps-themes","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/apps-themes"}]}
Timing-Allow-Origin: *
Content-Length: 30480
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Fri, 22 Nov 2024 12:25:23 GMT
Expires: Sat, 22 Nov 2025 12:25:23 GMT
Cache-Control: public, max-age=31536000
Age: 561247
Last-Modified: Wed, 27 Apr 2022 16:04:03 GMT
Content-Type: font/woff2
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

wOF2......w.......!...v............................T..2.`..V......    .#..
..\..n..,...(.6.$..T. ..d..X..9[[.q.k..W}.....5{Z._0......(.5TeDp.@T..9.......".i7m.....?....2*A.#).\..`..D......e...`UM.mp.    ...
...[SNIP]...
```

12.3. http://www.google.com/gen_204

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://www.google.com**
Path:	**/gen_204**

Request

```
GET /gen_204 HTTP/1.1
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.32 Safari/537.36
Host: www.google.com
```

```
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/1.1 204 No Content
Content-Type: text/html; charset=UTF-8
Content-Security-Policy: object-src 'none';base-uri 'self';script-src 'nonce-WUmCg9AA-jUlY8uNNhbvyw' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Permissions-Policy: unload=()
Date: Fri, 29 Nov 2024 00:19:29 GMT
Server: gws
Content-Length: 0
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

13. Email addresses disclosed

There are 2 instances of this issue:

- https://v2.accessibility.cloud/mapping-events.json
- https://wheelmap.org/

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure
- CAPEC-37: Retrieve Embedded Sensitive Data

13.1. https://v2.accessibility.cloud/mapping-events.json

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://v2.accessibility.cloud**
Path:	**/mapping-events.json**

Issue detail

The following email addresses were disclosed in the response:

- elberg.anna@lebenshilfe-nrw.de
- info@incluscience.org
- sylvie@menschen-in-hanau.eu
- presse@sozialkontor.de

Request

```
GET /mapping-events.json?appToken=27be4b5216aced82122d7cf8f69e4a07&includeRelated=images HTTP/2
Host: v2.accessibility.cloud
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:22:30 GMT
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
```

```
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Surrogate-Control: max-age=86400, stale-while-revalidate=30, stale-if-error=3600
Cache-Control: max-age=120
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=1T4PC8%2BEdAq3gzwJNWZS8fuyWL35V8dZF0sd8iE12mxUGbzZSjkAmVFH4ceErIUGzkJI7F2DITG80vOmD02XnwjW3rV
629ywqAxVu6sk%2FIynVkSr1zQV4aFXMCRPTO31Mwm%2FIrUZzJnq"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e7195dc8ba296-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4554&min_rtt=4449&rtt_var=1443&sent=5&recv=9&lost=0&retrans=0&sent_bytes=781&recv_bytes=1552&deli
very_rate=304721&cwnd=246&unsent_bytes=0&cid=a31fc582c370cbfd&ts=510&x=0"

{"count":400,"totalCount":400,"related":{"images":{"97QSEx3Pzi8T4YNyM":
{"_id":"97QSEx3Pzi8T4YNyM","objectId":"2CBbFTpcmLb6kJoht","mimeType":"image/jpeg","context":"event","type":"photo","mo
derationReq
...[SNIP]...
Teil des VHS-Kurses \"Wheelmap-Botschafter werden\". im Rahmen des Projekts Inklusion Olpe (IKO), Lebenshilfe Wohnen
NRW gGmbH! Zus..tzliche Anmeldungen f..r die Tour bitte per E-Mail an Anna Elberg: elberg.anna@lebenshilfe-
nrw.de","welcomeMessage":"Willkommen bei der Mapping-Aktion des Projekts Inklusion Olpe (IKO)!","area":{"geometry":
{"coordinates":[7.8424193,51.0297603],"type":"Point"},"properties":{"osm_id":163179,"osm_typ
...[SNIP]...
en f..hrt. \n3. Es werden nur Orte angezeigt, die mit dem Thema Gesundheit zu tun haben. Wenn du andere Orte suchst oder
bewerten willst, wechsel bitte zu Wheelmap.org.\nFragen? Melde dich gerne unter info@incluscience.org","startTime":"2023-
07-03T10:00:00.517Z","visibility":"listed","name":"IncluScience: Barrierefreiheit in Arztpraxen
erheben","description":"............**Bitte lesen**............ \n\n\nHier kannst du
...[SNIP]...
rt. \n3. Es werden nur Orte angezeigt, die mit dem Thema Gesundheit zu tun haben. Wenn du andere Orte suchst oder
bewerten willst, wechsel bitte zu Wheelmap.org.\n\n\nBei Fragen melde dich gerne unter
info@incluscience.org\n\n............Bitte lesen............\n\nUnd am Ende auf Teilnehmen klicken .........","statistics":
{"invitedParticipantCount":178,"joinedParticipantCount":560,"surveyCompletedCount":203}},{"_id":"Hx
...[SNIP]...
rfahrung mit dem Thema Barrierefreiheit ist f..r die Spazierg..nge nicht notwendig. Wir freuen uns ..ber jeden der mitkommt,
denn jeder Eindruck z..hlt. Anmeldung vorab bitte bei Sylvie Janka, E-Mail: sylvie@menschen-in-hanau.eu, da der Treffpunkt in
Hanau variiert. https://menschen-in-hanau.eu/event-pro/stadtspaziergang-mit-dem-checker-team/","endTime":"2023-11-
21T18:30:00.000Z","statistics":{"invitedParticipantCount":0}},{"
...[SNIP]...
```

13.2. https://wheelmap.org/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://wheelmap.org**
Path:	**/**

Issue detail

The following email addresses were disclosed in the response:

- qwertybat1234@gmail.com
- silkemariageorgi@gmail.com
- bugs@wheelmap.org
- gabor.babos@gmail.com
- as.matichard@gmail.com
- bejokeup@gmail.com
- ferityazgan@gmail.com
- danieldegroot18@gmail.com
- parukhin@gmail.com
- holger@sozialhelden.de
- joaquin.garcima@gmail.com
- maximilian@sozialhelden.de
- xymarior@yandex.com
- bjoern@sozialhelden.de

Numerous email addresses were found to be disclosed and the above are a sample subset.

This issue was found in multiple locations under the reported path.

Request 1

```
GET /_next/static/chunks/pages/_app-f09ed82b9deb00bd.js HTTP/2
Host: wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
```

Response 1

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:08 GMT
Content-Type: application/javascript; charset=UTF-8
Cache-Control: public, max-age=31536000, immutable
Cf-Bgj: minify
Cf-Polished: origSize=3064279
Etag: W/"2ec1d7-1924c92b118"
Last-Modified: Wed, 02 Oct 2024 09:32:15 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Accept-Encoding
```

```
X-Powered-By: Express
Cf-Cache-Status: HIT
Age: 82413
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=ImfHzcG7nU%2Fax5W8jiYKtyw00rQeDi8jvz1d2uCh0SAddPDNVeY7dhh5INwvoYTHCRzoc7bWhhiIWGWzu7a8YXx9rfYVq
JkEEv22MbCweXXWoXJxhN%2BHh6S06gPm0w%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6f982adea2ae-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=7689&min_rtt=2902&rtt_var=2886&sent=200&recv=110&lost=0&retrans=1&sent_bytes=230414&recv_bytes=2
049&delivery_rate=11598602&cwnd=251&unsent_bytes=0&cid=56c8de4124ebb565&ts=705&x=0"

(self.webpackChunk_N_E=self.webpackChunk_N_E||[]).push([[888],{24782:function(e,t){"use strict";t.byteLength=function(e)
{var t=c(e),o=t[0],r=t[1];return 3*(o+r)/4-r},t.toByteArray=function(e){var t,o,
...[SNIP]...
<qwertybat1234@gmail.com>
...[SNIP]...
<qwertybat1234@gmail.com>
...[SNIP]...
<qwertybat1234@gmail.com>
...[SNIP]...
<silkemariageorgi@gmail.com>
...[SNIP]...
<bejokeup@gmail.com>
...[SNIP]...
<bejokeup@gmail.com>
...[SNIP]...
<bejokeup@gmail.com>
...[SNIP]...
```

Request 2

```
GET /_next/static/chunks/pages/main-3e8c28b930adce7d.js HTTP/2
Host: wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
```

Response 2

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:08 GMT
Content-Type: application/javascript; charset=UTF-8
Cache-Control: public, max-age=31536000, immutable
Cf-Bgj: minify
Etag: W/"721de-1924c92b118"
Last-Modified: Wed, 02 Oct 2024 09:32:15 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Accept-Encoding
X-Powered-By: Express
Cf-Cache-Status: HIT
```

```
Age: 932619
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=FkDVrua%2FvAREMexQkpIiNgAEkAI%2Bvmz2Xw71N0z4h6zi3P6RLa6Av1jJJ9risim6EV0bKIzz%2BV81xSI%2BdXcK04A
%2FzwjQw%2FI1c9gaVgxLpyCEstISz4xKIFDadIvsMw%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6f99dd08a2ae-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=11853&min_rtt=2902&rtt_var=124&sent=746&recv=385&lost=0&retrans=1&sent_bytes=971864&recv_bytes=2
243&delivery_rate=30864886&cwnd=313&unsent_bytes=0&cid=56c8de4124ebb565&ts=957&x=0"

(self.webpackChunk_N_E=self.webpackChunk_N_E||[]).push([[671],{8377:function(n,e,t)
{(window.__NEXT_P=window.__NEXT_P||[]).push(["/main",function(){return t(48467)}])},97506:function(n,e,t){"use strict
...[SNIP]...
arker),We=t(6333);function Ue(){var n=(0,h.Z)(["Add more details"]);return Ue=function(){return n},n}function qe(){var n=(0,h.Z)
(["Sorry, something went wrong! Please retry later, or write an email to bugs@wheelmap.org if the issue persists."]);return
qe=function(){return n},n}function Ke(){var n=(0,h.Z)(["\n margin-top: 12px;\n width: 100%;\n\n .loadingIndicator {\n margin-left:
12px;\n }\n\n .errorBlock {\
...[SNIP]...
s.category||this.props.parentCategory,a=o?(0,at.WN)
(o):null,s=jo(),l=s.reportBody,c=s.reportSubject,u=s.apologyAndSolution,d=s.contactButtonCaption,h=s.backButtonCaption,p=c
(i.name,a),f=l(r),v="mailto:bugs@wheelmap.org?
subject=".concat(encodeURIComponent(p),"&body=").concat(encodeURIComponent(f));return(0,m.jsxs)("section",
{role:"dialog","aria-labelledby":"apology-and-solution",children:[(0,m.jsx)("p",{id:"apology-a
...[SNIP]...
```

14. Credit card numbers disclosed

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://photon.komoot.io**
Path:	**/api/**

Issue detail

The following credit card number was disclosed in the response:

- 340191400000002

Issue background

Applications sometimes disclose sensitive financial information such as credit card numbers. Responses containing credit card numbers may not represent any security vulnerability - for example, a number may belong to the logged-in user to whom it is displayed. If a credit card number is identified during a security assessment it should be verified, then application logic reviewed to identify whether its disclosure within the application is necessary and appropriate.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure
- CWE-388: Error Handling
- CAPEC-37: Retrieve Embedded Sensitive Data

Request 1

```
GET /api/?q=concordia%5C%5C%5C&limit=30&lang=en HTTP/1.1
Host: photon.komoot.io
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Fri, 29 Nov 2024 00:22:59 GMT
Content-Type: application/json;charset=utf-8
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Request-Method: get
Access-Control-Allow-Headers: *
Expires: Fri, 29 Nov 2024 01:22:59 GMT
Cache-Control: max-age=3600
Content-Length: 11295

{"features":[{"geometry":{"coordinates":[-91.6714379,31.3941887],"type":"Point"},"type":"Feature","properties":
{"osm_type":"R","osm_id":1837802,"extent":[-91.867607,31.762226,-91.3785942,30.9969969],"
...[SNIP]...
osm_key":"place","countrycode":"US","osm_value":"town","postcode":"66901","name":"Concordia","county":"Cloud
County","state":"Kansas","type":"city"}},{"geometry":{"coordinates":
[-58.02636417596116,-31.340191400000002],"type":"Point"},"type":"Feature","properties":
{"osm_type":"R","osm_id":2826131,"extent":
[-58.1510605,-31.2255642,-57.9382715,-31.4564703],"country":"Argentina","osm_key":"boundary","countrycode":"AR"
...[SNIP]...
```

15. Cacheable HTTPS response

There are 27 instances of this issue:

- https://ac-o-0.global.ssl.fastly.net/api/v1/legacy/api/nodes/
- https://ac-o-1.global.ssl.fastly.net/api/v1/legacy/api/nodes/
- https://ac-o-2.global.ssl.fastly.net/api/v1/legacy/api/nodes/
- https://ac-o-3.global.ssl.fastly.net/api/v1/legacy/api/nodes/
- https://accessibility-cloud-v2.freetls.fastly.net/equipment-infos.json

- https://accessibility-cloud-v2.freetls.fastly.net/images.json
- https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json
- https://api.mapbox.com/
- https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Italic,Arial%20Unicode%20MS%20Regular/0-255.pbf
- https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf
- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q
- https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf
- https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf
- https://news.wheelmap.org/en/apps/
- https://osm-api.wheelmap.tech/api/v1/legacy/api/nodes
- https://photon.komoot.io/api/
- https://v2.accessibility.cloud/mapping-events.json
- https://v2.accessibility.cloud/sources/LB5rYeCZ9PxthQ3Rg.json
- https://v2.accessibility.cloud/tracking-events/report
- https://wheelmap.org/
- https://wheelmap.org/clientEnv.js
- https://wheelmap.org/images/triangle.svg
- https://wheelmap.pro/organizations/LPb4y2ri7b6fLxLFa/survey-projects/wx4mM8xFiQAsB5aLi/show

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

15.1. https://ac-o-0.global.ssl.fastly.net/api/v1/legacy/api/nodes/

Summary

Severity:	**Information**

Confidence: **Certain**

Host: **https://ac-o-0.global.ssl.fastly.net**

Path: **/api/v1/legacy/api/nodes/**

Request 1

```
GET /api/v1/legacy/api/nodes/?
api_key=3s8GNQvBCmwm45zro_jP&per_page=25&bbox=-122.4371,37.7571,-122.4364,37.7577&per_page=10000&limit=100
00&ts=0 HTTP/1.1
Host: ac-o-0.global.ssl.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1

```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 205
Content-Type: application/json; charset=utf-8
x-powered-by: Express
access-control-allow-origin: *
Cache-Control: public, max-age=86400
etag: W/"cd-dqPegU3WDf/5NU5ZqRCCUgU3g+0"
strict-transport-security: max-age=31536000; includeSubDomains
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=87h9kbBEctR1O6KyGG7P4Zu63Xd0NeKEOxOiQPJ3I47jcj%2BcWyDlk841HxcQqmIG45fdnLyaCSarEmEn2FJaI5Y2Mv2tv5
ptQdqu0x%2Fo%2Bkfm1LuR9yacgBVUylveZBfbexsYpsldhcA%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 8e55f9b5ff1ca2d0-YUL
server-timing: cfL4;desc="?
proto=TCP&rtt=603&sent=5&recv=7&lost=0&retrans=0&sent_bytes=2993&recv_bytes=1589&delivery_rate=3866488&cwnd=2
52&unsent_bytes=0&cid=1b304e3dcf672f0c&ts=331&x=0"
X-Fastly-WebpSupport: false
Accept-Ranges: bytes
Age: 759817
Date: Fri, 29 Nov 2024 00:21:22 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970023-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732839682.444353,VS0,VE1
Vary: Accept-Encoding

{"conditions":{"limit":10000,"offset":0,"page":"limit-number","per_page":"limit-number","format":"parse url
param","bbox":"-122.4371,37.7571,-122.4364,37.7577"},"type":"LegacyFeatureCollection","nodes
...[SNIP]...
```

15.2. https://ac-o-1.global.ssl.fastly.net/api/v1/legacy/api/nodes/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://ac-o-1.global.ssl.fastly.net**
Path:	**/api/v1/legacy/api/nodes/**

Request 1

```
GET /api/v1/legacy/api/nodes/?
api_key=3s8GNQvBCmwm45zro_jP&per_page=25&bbox=-122.4382,37.7577,-122.4378,37.758&per_page=10000&limit=1000
0&ts=0 HTTP/1.1
Host: ac-o-1.global.ssl.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1

```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 204
Content-Type: application/json; charset=utf-8
x-powered-by: Express
access-control-allow-origin: *
Cache-Control: public, max-age=86400
etag: W/"cc-ExzTwN/6G2bJD347dGartZ/iZf8"
strict-transport-security: max-age=31536000; includeSubDomains
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=%2B%2B2A%2BHLjykTjh%2FdD%2BZzkoUjqWSt2TxWLUdxS1gKyOmfzr%2BK05dXEo%2B6OS1jP8o2KN%2BluVYVeIYB
%2BLHjh%2BEYA1Tus3ioQ1y09nPyLo9KM4Plxb0n%2F0g1F4pOJXwJzIz8b5APBzqPI0YQ%3D"}],"group":"cf-
nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 8e59fd699973a306-YUL
server-timing: cfL4;desc="?
```

```
proto=TCP&rtt=546&sent=8&recv=10&lost=0&retrans=0&sent_bytes=4649&recv_bytes=2585&delivery_rate=5125663&cwnd=
254&unsent_bytes=0&cid=e4107d242e440a9a&ts=55368&x=0"
X-Fastly-WebpSupport: false
Accept-Ranges: bytes
Age: 717795
Date: Fri, 29 Nov 2024 00:22:35 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970073-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732839755.444567,VS0,VE1
Vary: Accept-Encoding

{"conditions":{"limit":10000,"offset":0,"page":"limit-number","per_page":"limit-number","format":"parse url
param","bbox":"-122.4382,37.7577,-122.4378,37.758"},"type":"LegacyFeatureCollection","nodes"
...[SNIP]...
```

15.3. https://ac-o-2.global.ssl.fastly.net/api/v1/legacy/api/nodes/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://ac-o-2.global.ssl.fastly.net**
Path:	**/api/v1/legacy/api/nodes/**

Request 1

```
GET /api/v1/legacy/api/nodes/?
api_key=3s8GNQvBCmwm45zro_jP&per_page=25&bbox=-122.4385,37.7582,-122.4378,37.7588&per_page=10000&limit=100
00&ts=0 HTTP/1.1
Host: ac-o-2.global.ssl.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1

```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 205
Content-Type: application/json; charset=utf-8
```

```
x-powered-by: Express
access-control-allow-origin: *
Cache-Control: public, max-age=86400
etag: W/"cd-Dr5davedaJV3pt3gnNbKnEbQIu8"
strict-transport-security: max-age=31536000; includeSubDomains
cf-cache-status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=osAuDeuXTFh7NboDRcRy8Rw9VZ%2BNIjH2RZGr7cl958uELby3gLkLwHmy%2F%2BCN78aMJnTxm%2FKFpPzq3puOsy
%2FxyLccGBAZ4M%2Br4DOSOAk%2FO8iNVbn7uBs4AmNJEu5oS4zK8w%2B96pVmzuo%3D"}],"group":"cf-
nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 8e843ecfae95a2dc-YUL
server-timing: cfL4;desc="?
proto=TCP&rtt=394&sent=5&recv=8&lost=0&retrans=0&sent_bytes=2993&recv_bytes=1851&delivery_rate=6295652&cwnd=2
52&unsent_bytes=0&cid=b0f99dc1e9b2a119&ts=320&x=0"
X-Fastly-WebpSupport: false
Accept-Ranges: bytes
Age: 274639
Date: Fri, 29 Nov 2024 00:21:19 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970028-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732839680.527801,VS0,VE2
Vary: Accept-Encoding

{"conditions":{"limit":10000,"offset":0,"page":"limit-number","per_page":"limit-number","format":"parse url
param","bbox":"-122.4385,37.7582,-122.4378,37.7588"},"type":"LegacyFeatureCollection","nodes
...[SNIP]...
```

15.4. https://ac-o-3.global.ssl.fastly.net/api/v1/legacy/api/nodes/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://ac-o-3.global.ssl.fastly.net**
Path:	**/api/v1/legacy/api/nodes/**

Request 1

```
GET /api/v1/legacy/api/nodes/?
api_key=3s8GNQvBCmwm45zro_jP&per_page=25&bbox=-122.4378,37.7582,-122.4371,37.7588&per_page=10000&limit=100
00&ts=0 HTTP/1.1
Host: ac-o-3.global.ssl.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
```

```
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

```

Response 1

```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 205
Content-Type: application/json; charset=utf-8
x-powered-by: Express
access-control-allow-origin: *
Cache-Control: public, max-age=86400
etag: W/"cd-I9D1NIRRkCZYmsQ8brl/5bXjK8Q"
strict-transport-security: max-age=31536000; includeSubDomains
cf-cache-status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=absEP37SSYrGZhdYffB2VD5MSamZGmwMLofaa65SVTa6A0XdHbl5GszsThFa%2BGDMszq3VKd2jogjXSfpqNSdLqUZaj9
a6jg%2FXCvia7B5euC5WzuKAHeS9tqnhHSJ%2B3sAFLBQzZjs3os%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 8e8ccca94d566e02-YUL
server-timing: cfL4;desc="?
proto=TCP&rtt=664&min_rtt=387&rtt_var=349&sent=5&recv=7&lost=0&retrans=0&sent_bytes=2994&recv_bytes=1648&delive
ry_rate=6895238&cwnd=251&unsent_bytes=0&cid=1f008cd9e94b59cc&ts=332&x=0"
X-Fastly-WebpSupport: false
Accept-Ranges: bytes
Age: 184945
Date: Fri, 29 Nov 2024 00:21:22 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970042-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732839683.613469,VS0,VE2
Vary: Accept-Encoding

{"conditions":{"limit":10000,"offset":0,"page":"limit-number","per_page":"limit-number","format":"parse url
param","bbox":"-122.4378,37.7582,-122.4371,37.7588"},"type":"LegacyFeatureCollection","nodes
...[SNIP]...
```

15.5. https://accessibility-cloud-v2.freetls.fastly.net/equipment-infos.json

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://accessibility-cloud-v2.freetls.fastly.net**
Path:	**/equipment-infos.json**

Request 1

```
GET /equipment-infos.json?
&x=2619&y=6333&z=14&appToken=27be4b5216aced82122d7cf8f69e4a07&includePlacesWithoutAccessibility=1 HTTP/2
```

```
Host: accessibility-cloud-v2.freetls.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent, X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Cache-Control: max-age=600
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Fastly-Webpsupport: false
Accept-Ranges: bytes
Age: 0
Date: Fri, 29 Nov 2024 00:21:20 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970027-YUL
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1732839680.684848,VS0,VE483
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
```

```
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 1557

{"type":"FeatureCollection","featureCount":2,"totalFeatureCount":2,"related":{"licenses":{"2WCCM3YWWacqnEMTX":
{"_id":"2WCCM3YWWacqnEMTX","name":"Open Data Commons Open Database License","shortName":"O
...[SNIP]...
```

15.6. https://accessibility-cloud-v2.freetls.fastly.net/images.json

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://accessibility-cloud-v2.freetls.fastly.net**
Path:	**/images.json**

Request 1

```
GET /images.json?context=surveyResult&objectId=etY5jXaQbwGaxmqCt&appToken=27be4b5216aced82122d7cf8f69e4a07
HTTP/2
Host: accessibility-cloud-v2.freetls.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
```

```
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Cache-Control: max-age=120
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Fastly-Webpsupport: false
Accept-Ranges: bytes
Age: 0
Date: Fri, 29 Nov 2024 00:22:58 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970054-YUL
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1732839779.884012,VS0,VE112
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 28

{"totalCount":0,"images":[]}
```

15.7. https://accessibility-cloud-v2.freetls.fastly.net/place-infos.json

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://accessibility-cloud-v2.freetls.fastly.net**
Path:	**/place-infos.json**

Request 1

```
GET /place-infos.json?
excludeSourceIds=LiBTS67TjmBcXdEmX,pbT4qym6cAwKifCcN,ZyDaF8ZrJeGL3m4Cq,Yra2ze6vW9ttX7Tiz,JiTwDMcX5c8erJ
x95,cvus37h4bvef2pJzd,axsmapv2,T8j8nnnqMpbxpLxZu,ehgoCgSPEfNdpg5fG,cnQiiH4qpyyn6fBNr,TNmCbw6xD4DoXnhb7,
WKkGrSNMXn3sd6ubT,dBCyrMSJdHZSxKgK5,sPSreQtMg8Soy5TDr&x=83831&y=202680&z=19&appToken=27be4b5216ace
d82122d7cf8f69e4a07&includePlacesWithoutAccessibility=1 HTTP/1.1
Host: accessibility-cloud-v2.freetls.fastly.net
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
```

```
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Cache-Control: max-age=1200
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Fastly-Webpsupport: false
Accept-Ranges: bytes
Age: 0
Date: Fri, 29 Nov 2024 00:21:20 GMT
Via: 1.1 varnish
X-Served-By: cache-yul1970027-YUL
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1732839679.398170,VS0,VE625
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 52679

{"type":"FeatureCollection","featureCount":74,"totalFeatureCount":74,"related":{"licenses":{"2WCCM3YWWacqnEMTX":
{"_id":"2WCCM3YWWacqnEMTX","name":"Open Data Commons Open Database License","shortName":
...[SNIP]...
```

15.8. https://api.mapbox.com/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/**

Issue detail

This issue was found in multiple locations under the reported path.

Request 1

```
GET /fonts/v1/sozialhelden/DIN%20Pro%20Medium,Arial%20Unicode%20MS%20Regular/0-255.pbf?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 72144
Date: Tue, 12 Nov 2024 04:15:22 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: Mbx-Fonts
Timing-Allow-Origin: *
Cache-Control: max-age=5184000, stale-while-revalidate=3600, stale-if-error=18000
Etag: W/"9c12-5pn0WeJ7Ttb6Bi93KFqV4/UwhrE"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: x0HiMhiyjVGcx9eXHt-YI2-TjiARM0MvhNs4jBnzVh4VfNljLp8ufg==
Age: 1454778


...
```

```
(DIN Pro Medium, Arial Unicode MS Regular..0-255...... .(.018...... .(.018.... .. .(.018.....!...SfqrrrpcNf......
{`q.......jr.......kp.......io.......hm.......gl.......ek.......di.......ch......
...[SNIP]...
```

15.9. https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Italic,Arial%20Unicode%20MS%20Regular/0-255.pbf

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/fonts/v1/sozialhelden/DIN%20Pro%20Italic,Arial%20Unicode%20MS%20Regular/0-255.pbf**

Request 1

```
GET /fonts/v1/sozialhelden/DIN%20Pro%20Italic,Arial%20Unicode%20MS%20Regular/0-255.pbf?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 73513
Date: Mon, 28 Oct 2024 16:40:45 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: Mbx-Fonts
Timing-Allow-Origin: *
Cache-Control: max-age=5184000, stale-while-revalidate=3600, stale-if-error=18000
Etag: W/"af7a-Nz1ssxur6nsO2p0x1nwNWs8GbWI"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: gIhIgHTPa8W8nQkBAFgGzk-qScGe0kOUycPTBwOQGGSBc-bswoqedQ==
Age: 2706055
```

```
...
(DIN Pro Italic, Arial Unicode MS Regular..0-255...... .(.018...... .(.018.... .. .(.018.....!.....3LaorrrgS.#A^y.....g
*Ii......r./On......q.5Tt......j.:Zy......d @_  .....|]&Ee......uV+Kk......
...[SNIP]...
```

15.10. https://api.mapbox.com/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf**

Request 1

```
GET /fonts/v1/sozialhelden/DIN%20Pro%20Regular,Arial%20Unicode%20MS%20Regular/0-255.pbf?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 68970
Date: Mon, 18 Nov 2024 22:35:17 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: Mbx-Fonts
Timing-Allow-Origin: *
Cache-Control: max-age=5184000, stale-while-revalidate=3600, stale-if-error=18000
Etag: W/"9381-SLipJvr+Rq1bv9MIBVb1HAUP+3c"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: L5ol3NEssF0-aamOhwFSOInRxfBVgtRsehSj153jpqT9_Z4Dx2y1LQ==
Age: 870382


...
)DIN Pro Regular, Arial Unicode MS Regular..0-255...... .(.018...... .(.018.... .. .
(.018.....!...LbprrrgT_z.....hi......sj......ti......sh......sh......rg......qg......qf......pe......oe......o
...[SNIP]...
```

15.11. https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q**

Request 1

```
GET /styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/1.1
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: mbx-styles
Timing-Allow-Origin: *
X-Dns-Prefetch-Control: off
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: origin
Date: Fri, 29 Nov 2024 00:21:19 GMT
Cache-Control: max-age=900, stale-while-revalidate=900, stale-if-error=3600
Etag: W/"149dc-VxeuyDGpYLOxKpBskraSOt44THw"
```

```
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: EVEIy7QiCiqnN9QgPBWnewDjBn090BsAvD5bNusFc5zLCZH-pl8QQg==
Age: 489

{"version":8,"name":"Streets","metadata":{"mapbox:type":"default","mapbox:origin":"streets-v11","mapbox:sdk-support":
{"android":"9.3.0","ios":"5.10.0","js":"2.0.0"},"mapbox:autocomposite":true,"mapbox
...[SNIP]...
```

15.12. https://api.mapbox.com/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json**

Request 1

```
GET /styles/v1/sozialhelden/cko1h26xf0tg717qieiftte7q/6qsolfec7nhi04bt9085kqnu6/sprite@2x.json?
access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-AZBY56hv-
jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Date: Sun, 11 Aug 2024 20:29:50 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Origin: mbx-styles
Timing-Allow-Origin: *
X-Dns-Prefetch-Control: off
X-Frame-Options: DENY
```

```
X-Content-Type-Options: nosniff
Referrer-Policy: origin
Cache-Control: max-age=31536000, stale-if-error=18000
Etag: "sprite-4.5.8-v1/6qsolfec7nhi04bt9085kqnu6"
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: TerwV_Lz5r06Kx2An0ZIug7cQRSzzCqOgtS4iCLfgHE800_s841EQA==
Age: 9431494

{"pedestrian-polygon":{"x":0,"y":0,"width":128,"height":128,"pixelRatio":2,"visible":true},"turning-circle-outline":
{"x":128,"y":0,"width":92,"height":92,"pixelRatio":2,"visible":true},"turning-circle
...[SNIP]...
```

15.13. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json**

Request 1

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8.json?
secure&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ.kGBP3x-
AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Link
X-Rate-Limit-Limit: 100000
```

```
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732340266
Last-Modified: Fri, 25 Aug 2023 07:39:41 GMT
Timing-Allow-Origin: *
Date: Fri, 29 Nov 2024 00:21:24 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "aec9c7f4fcbb8ce46a34a7729283a612"
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: FU1AMgX2hq0ukyg4RDMYEuytgALWrNZYeHxAWXd3NmMWjeBfzgPF2A==
Age: 278

{"attribution":"<a href=\"https://www.mapbox.com/about/maps/\" target=\"_blank\" title=\"Mapbox\" aria-
label=\"Mapbox\">&copy; Mapbox</a> <a href=\"https://www.openstreetmap.org/about/\" target=\"_bla
...[SNIP]...
```

15.14. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf**

Request 1

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25334.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 89570
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
```

```
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732634791
Last-Modified: Mon, 25 Nov 2024 17:26:02 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:37 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "48a2ebaf3c06b5445978f57916aa2257"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: KgHEPQWsMZ0aI59WpYwG3Ue0IzfV8Z2IITK919J8OiNUTnWCxgAb2w==
Age: 290

...x.
  hillshade(. ......."..   ...$........?...     .    ...@@....  .   ..@............    .......@@....  .   .+?:........?....@......_....    ...?
j..........@....  ......0..     .....  ..? ?.   ...R.@.............?..@  ....
...[SNIP]...
```

15.15. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf**

Request 1

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10478/25335.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
```

```
Content-Length: 72751
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732656614
Last-Modified: Mon, 25 Nov 2024 17:26:01 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:37 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "95bfcf6dcc7025ed71b84195e9c96031"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: hHeREAdeDQe33FNJERSs_P9qIfbzfcIC_7rod8YM-A2BScVH0OKhdw==
Age: 290

..x.
   hillshade(. ......."..    ............?...      .    ...@@....  .    ..@............    .......@@....  .    .+?:........?....@......_....
   ...;B.........@....  ......0..  .    .._B...# ..........?..@  .....    .!.D...@.....
...[SNIP]...
```

15.16. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf**

Request 1

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25334.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 95205
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732645643
Last-Modified: Mon, 25 Nov 2024 17:26:01 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:39 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "4cd778583d27c21fe970d7bd75ac4080"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: Zusuj4xRihPpjsKnWq4mVMJhYRkpS5xYCM-3gL0OenmnZzZMZ8CIgg==
Age: 292

...x.
  hillshade(. ......."..   .$.$........?...     .    ...@@....  .    ..@............    .......@@....  .    .*..".. .....?...    _.CR`_..? ?............ ...`___.
  ....R.@.............?..@  .........  .    ...l...@.....?
...[SNIP]...
```

15.17. https://api.mapbox.com/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.mapbox.com**
Path:	**/v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf**

Request 1

```
GET /v4/mapbox.mapbox-terrain-v2,mapbox.mapbox-streets-v8/16/10479/25335.vector.pbf?
sku=101C3XiMKBIs9&access_token=pk.eyJ1Ijoic296aWFsaGVsZGVuIiwiYSI6ImNrbzFjZnZxejBvN3YycHBnZGxtaGY5eG0ifQ
.kGBP3x-AZBY56hv-jU7SUA HTTP/2
Host: api.mapbox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Content-Type: application/x-protobuf
Content-Length: 73869
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Timing-Allow-Origin: *
X-Rate-Limit-Limit: 100000
X-Rate-Limit-Interval: 60
X-Rate-Limit-Reset: 1732634791
Last-Modified: Mon, 25 Nov 2024 17:26:07 GMT
X-Mapbox-Language: {"mapbox.mapbox-streets-v8":null}
X-Mapbox-Worldview: {"mapbox.mapbox-streets-v8":null}
Date: Fri, 29 Nov 2024 00:21:37 GMT
Cache-Control: max-age=43200,s-maxage=300,stale-while-revalidate=300,stale-if-error=600
Etag: "ba2c99c10975464cef1acc458b4dac1f"
X-Cache: Hit from cloudfront
Via: 1.1 a6f2e7c3dd76750ec70d32e7fcf09838.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: qGSHoo4VS4PtlBO9AXafbDJy1NhTNbBsHFZEfxYW05XmEqccCyh_Ew==
Age: 290

..x.
  hillshade(. ......."..   .$..........?...     .    ...@@....  .    ..@............    .......@@....  .    .*..".. .....?...    _.@*......... ...`_.    .._B...#
..........?..@  .....    .!.D...@.....?.    ..  .....?....?.    ...
...[SNIP]...
```

15.18. https://news.wheelmap.org/en/apps/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://news.wheelmap.org**
Path:	**/en/apps/**

Request 1

```
GET /en/apps/ HTTP/1.1
Host: news.wheelmap.org
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
```

```
Priority: u=0, i
Connection: keep-alive
```

Response 1

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:18:42 GMT
Content-Type: text/html; charset=UTF-8
Link: <https://news.wheelmap.org/en/wp-json/>; rel="https://api.w.org/", <https://news.wheelmap.org/en/wp-
json/wp/v2/pages/5777>; rel="alternate"; title="JSON"; type="application/json", <https://news.wheelmap.org/en/?p=5777>;
rel=shortlink
Vary: Accept-Encoding
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=CTFPLXPh87yBwgqZxoDhiNOnyADdx%2B0cIMevZ%2FntXKTXyP17J5lXXsUFM20w8D%2Bw4m9o5y2UmglNXtiEvj%2Bc
xf2jRZL2uOqEWswR2UE%2FKLSG%2BtaeKpy5XBwV1vxgtbh5PSTF"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6c05bd74a2b1-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=11041&min_rtt=4177&rtt_var=8284&sent=8&recv=11&lost=0&retrans=1&sent_bytes=3915&recv_bytes=1315&
delivery_rate=347617&cwnd=254&unsent_bytes=0&cid=486f1b40d622f412&ts=789&x=0"

<!doctype html>
<html lang="en-US">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="profile" href="https://gmpg.org/xfn/11">
  <title>Ap
...[SNIP]...
```

15.19. https://osm-api.wheelmap.tech/api/v1/legacy/api/nodes

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://osm-api.wheelmap.tech**
Path:	**/api/v1/legacy/api/nodes**

Request 1

```
GET /api/v1/legacy/api/nodes?
bbox=-122.44103172124267,37.75498689056723,-122.43416827875734,37.76041310943277&per_page=20&wheelchair=ye
s&wheelchair_toilet=yes&api_key=3s8GNQvBCmwm45zro_jP HTTP/1.1
Host: osm-api.wheelmap.tech
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
```

```
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
```

Response 1

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:22:59 GMT
Content-Type: application/json; charset=utf-8
X-Powered-By: Express
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=86400
Surrogate-Control: max-age=31536000, stale-while-revalidate=60, stale-if-error=86400
Etag: W/"1064-hhJ//M/KBXxzo81oLomiDO1jsc4"
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=gqjFSuAOeZ0Z4HP65Fo8sqYIVQIOIRG7cY7SPCPVvapbNWzVFpfF0%2FM3OvpH6aWf5JWyiMTVZaq16BR%2FrKe1Nt7K
T8zx8u5V%2BIbhbbmb0U9h9f9OYJDEtP70J5LLurumJBbo5MuLVro%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e724c890ea269-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=10299&min_rtt=2797&rtt_var=13620&sent=9&recv=12&lost=0&retrans=0&sent_bytes=3703&recv_bytes=1354
&delivery_rate=935366&cwnd=248&unsent_bytes=0&cid=328df190eac3fcca&ts=374&x=0"

{"conditions":{"limit":10,"offset":0,"page":"limit-number","per_page":"limit-number","format":"parse url
param","bbox":"-122.44103172124267,37.75498689056723,-122.43416827875734,37.76041310943277"},"t
...[SNIP]...
```

15.20. https://photon.komoot.io/api/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://photon.komoot.io**
Path:	**/api/**

Request 1

```
GET /api/?q=concordia%5C%5C%5C&limit=30&lang=en HTTP/1.1
Host: photon.komoot.io
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Fri, 29 Nov 2024 00:22:59 GMT
Content-Type: application/json;charset=utf-8
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Request-Method: get
Access-Control-Allow-Headers: *
Expires: Fri, 29 Nov 2024 01:22:59 GMT
Cache-Control: max-age=3600
Content-Length: 11295

{"features":[{"geometry":{"coordinates":[-91.6714379,31.3941887],"type":"Point"},"type":"Feature","properties":
{"osm_type":"R","osm_id":1837802,"extent":[-91.867607,31.762226,-91.3785942,30.9969969],"
...[SNIP]...
```

15.21. https://v2.accessibility.cloud/mapping-events.json

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://v2.accessibility.cloud**
Path:	**/mapping-events.json**

Request 1

```
GET /mapping-events.json?appToken=27be4b5216aced82122d7cf8f69e4a07&includeRelated=images HTTP/2
Host: v2.accessibility.cloud
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:22:30 GMT
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Surrogate-Control: max-age=86400, stale-while-revalidate=30, stale-if-error=3600
Cache-Control: max-age=120
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=1T4PC8%2BEdAq3gzwJNWZS8fuyWL35V8dZF0sd8iE12mxUGbzZSjkAmVFH4ceErIUGzkJI7F2DITG80vOmD02XnwjW3rV
629ywqAxVu6sk%2FIynVkSr1zQV4aFXMCRPTO31Mwm%2FIrUZzJnq"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e7195dc8ba296-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4554&min_rtt=4449&rtt_var=1443&sent=5&recv=9&lost=0&retrans=0&sent_bytes=781&recv_bytes=1552&deli
very_rate=304721&cwnd=246&unsent_bytes=0&cid=a31fc582c370cbfd&ts=510&x=0"

{"count":400,"totalCount":400,"related":{"images":{"97QSEx3Pzi8T4YNyM":
{"_id":"97QSEx3Pzi8T4YNyM","objectId":"2CBbFTpcmLb6kJoht","mimeType":"image/jpeg","context":"event","type":"photo","mo
derationReq
...[SNIP]...
```

15.22. https://v2.accessibility.cloud/sources/LB5rYeCZ9PxthQ3Rg.json

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://v2.accessibility.cloud**
Path:	**/sources/LB5rYeCZ9PxthQ3Rg.json**

Request 1

```
GET /sources/LB5rYeCZ9PxthQ3Rg.json?appToken=27be4b5216aced82122d7cf8f69e4a07 HTTP/2
Host: v2.accessibility.cloud
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response 1

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:22:59 GMT
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
```

```
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Methods: GET
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: PATCH
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Surrogate-Control: max-age=120, stale-while-revalidate=30, stale-if-error=3600
Cache-Control: max-age=120
Vary: x-app-token, x-user-token, x-token, Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=vrfmxvGjMgjZghg4yEEUEzk40qgARU%2F5tsh2KQ6RrgnOBnXa60Fy9myD6RuE4I4xtJGmL5MSU2wXjFkM2n08uew9XXoI
RiHGW2bg60%2FrZr2%2Fcag9PkQZKbN9kj4bbEIE7%2BvU8LRrVg6B"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e724b2874a255-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4646&min_rtt=3420&rtt_var=1819&sent=6&recv=9&lost=0&retrans=0&sent_bytes=781&recv_bytes=1546&deli
very_rate=424561&cwnd=251&unsent_bytes=0&cid=a2ae56aef645320a&ts=348&x=0"

{"_id":"LB5rYeCZ9PxthQ3Rg","organizationId":"LPb4y2ri7b6fLxLFa","isFreelyAccessible":true,"accessRestrictedTo":
[],"name":"Sozialhelden e.V. - Wheelmap S","shortName":"Wheelmap","licenseId":"ns5HmC6xFr
...[SNIP]...
```

15.23. https://v2.accessibility.cloud/tracking-events/report

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://v2.accessibility.cloud**
Path:	**/tracking-events/report**

Request 1

```
POST /tracking-events/report?appToken=27be4b5216aced82122d7cf8f69e4a07 HTTP/2
Host: v2.accessibility.cloud
Content-Length: 508
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Origin: https://wheelmap.org
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

```
{"type":"AppOpened","query":{},"appId":"wheelmap.org","mappingEventId":null,"mappingEvent":null,"userUUID":"ff3b3204-
bec0-46b4-a1fc-a39e9524fceb","timestamp":1732839670,"userAgent":{"ua":"Mozilla/5.0
...[SNIP]...
```

Response 1

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:24 GMT
Content-Type: application/json
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: OPTIONS
Access-Control-Allow-Headers: Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Referer, User-Agent,
X-Requested-With, X-Token, X-App-Token, X-User-Token, Content-Type, elastic-apm-traceparent
Access-Control-Max-Age: 86400
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=ygEKkwiWTE4Qv06NRhR1mYXKTDi3g12ydcfX8v4VFlOPQtJuGidbStjKn1o4casRRLFi2V4cRdDcsZItXl9s46tyky9MTi9foqEt
d1LkMHPHI8tHDgbEHQ0T8F%2BvSl9wpvdf4wSijuhN"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6ff87be2a28c-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=11836&min_rtt=3686&rtt_var=15076&sent=13&recv=16&lost=0&retrans=0&sent_bytes=6350&recv_bytes=203
6&delivery_rate=579178&cwnd=242&unsent_bytes=0&cid=d4d14fd1aa13460c&ts=5080&x=0"

{"success":true}
```

15.24. https://wheelmap.org/

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://wheelmap.org**

Path: **/**

Request 1

```
GET / HTTP/1.1
Host: wheelmap.org
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://news.wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response 1

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:08 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: Next.js
Cache-Control: max-age=3600, public
Vary: X-User-Agent-Variant, X-Locale-Variant, Content-Language, Accept-Encoding
X-Locale-Variant: en-us
Content-Language: en-us
X-User-Agent-Variant: Windows
X-Frame-Options: deny
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=DLH2DZNWER%2BKKRYqqn5KbKk%2FzrCdWckNo9lbMa3t98wD%2FMsj%2FHohPBy72XUVzH2WneQ9xF9%2Bui0xlIP6
GfB2Vxy5vVWoszPtwclubBavQ4qwQBt7tLHky6N4%2Fld3IA%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6f941d9ca2ae-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=3696&min_rtt=2902&rtt_var=1701&sent=9&recv=11&lost=0&retrans=0&sent_bytes=3716&recv_bytes=1322&d
elivery_rate=703147&cwnd=249&unsent_bytes=0&cid=56c8de4124ebb565&ts=190&x=0"

<!DOCTYPE html><html lang="en-US"><head><meta charSet="utf-8"/><meta name="viewport" content="width=device-width,
height=device-height, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, viewpor
...[SNIP]...
```

15.25. https://wheelmap.org/clientEnv.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://wheelmap.org**

Path: **/clientEnv.js**

Request 1

```
GET /clientEnv.js HTTP/2
Host: wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1
```

Response 1

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:21:08 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: Express
Cache-Control: max-age=14400
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: HIT
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=js3FSUUpzmOLAVgDMe4W8MWeHvx3uHVURIrjp8BtC2QPPHF3JeSj0O3UBXeZ4X%2FdEeWF1sdL3Cg7EVp%2BPa2oU
HWROSQ1B2bv%2B9kC8tDC22o7fbXZmMvHg66sCVw4qQ%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e6f9658b0a2ae-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=7510&min_rtt=2902&rtt_var=1165&sent=126&recv=70&lost=0&retrans=0&sent_bytes=149207&recv_bytes=14
45&delivery_rate=10648507&cwnd=251&unsent_bytes=0&cid=56c8de4124ebb565&ts=543&x=0"

window.env =
{"REACT_APP_ACCESSIBILITY_CLOUD_UNCACHED_BASE_URL":"https://v2.accessibility.cloud","REACT_APP_ACCESSI
BILITY_CLOUD_APP_TOKEN":"27be4b5216aced82122d7cf8f69e4a07","REACT_APP_ALLOW_ADDITIONA
...[SNIP]...
```

15.26. https://wheelmap.org/images/triangle.svg

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://wheelmap.org**
Path:	**/images/triangle.svg**

Request 1

```
GET /images/triangle.svg HTTP/2
Host: wheelmap.org
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://wheelmap.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response 1

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:22:13 GMT
Content-Type: image/svg+xml
X-Powered-By: Express
Cache-Control: public, max-age=14400
Last-Modified: Wed, 02 Oct 2024 09:30:13 GMT
Etag: W/"4d7-1924c90d488"
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: HIT
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=HhdwTApqIRrKegfOFmsfn7XNR1%2FcaacIfgmydLBkrFaIAC%2BeTOTtyIwoyPKC%2BpbkB8s8Mj99GQKz2YbRgb49Qhu%
2Fw8Qxo4Kblf3IltsbZnEJImsbnPWBEnr9TCHx9A%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e712ca90ca2ee-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=4908&min_rtt=4462&rtt_var=1788&sent=7&recv=10&lost=0&retrans=0&sent_bytes=819&recv_bytes=1515&de
livery_rate=564321&cwnd=245&unsent_bytes=0&cid=80af5e296d765711&ts=148&x=0"

<?xml version="1.0" encoding="UTF-8"?>
<svg width="12px" height="8px" viewBox="0 0 12 8" version="1.1" xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink">
<defs>
```

```
...[SNIP]...
```

15.27. https://wheelmap.pro/organizations/LPb4y2ri7b6fLxLFa/survey-projects/wx4mM8xFiQAsB5aLi/show

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://wheelmap.pro**
Path:	**/organizations/LPb4y2ri7b6fLxLFa/survey-projects/wx4mM8xFiQAsB5aLi/show**

Request 1

```
GET /organizations/LPb4y2ri7b6fLxLFa/survey-projects/wx4mM8xFiQAsB5aLi/show?
d%5Bmapping_event_id%5D=undefined&d%5BuniqueSurveyId%5D=af3d83a0-38b3-41e2-a5b2-
0f0f6af14689&d%5BosmId%5D=undefined%2Fundefined HTTP/1.1
Host: wheelmap.pro
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response 1

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 00:23:38 GMT
Content-Type: text/html; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' http://api.mapbox.com https://api.mapbox.com http://api.particle.io
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; script-src 'self' 'unsafe-inline' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: 'unsafe-eval'; connect-src * 'self' http://api.mapbox.com https://api.mapbox.com
http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data:; img-src data: 'self' http://accessibility-cloud-uploads.s3.amazonaws.com
https://accessibility-cloud-uploads.s3.amazonaws.com http://api.mapbox.com https://api.mapbox.com http://api.particle.io
```

```
https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-v2.freetls.fastly.net https://osm-
api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com http://npmcdn.com https://npmcdn.com
https://metabase.i.wheelmap.tech blob: data: http://* blob: https://* blob:; style-src 'self' 'unsafe-inline' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data:; media-src 'self' http://api.mapbox.com
https://api.mapbox.com http://api.particle.io https://api.particle.io https://v2.accessibility.cloud https://accessibility-cloud-
v2.freetls.fastly.net https://osm-api.wheelmap.tech/api/v1 http://api.tiles.mapbox.com https://api.tiles.mapbox.com
http://npmcdn.com https://npmcdn.com https://metabase.i.wheelmap.tech blob: data: blob:;
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cf-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=hGcQWMAHHWbkatPS8gmcAbpJObfX3pu5LUSMMC4jzUiR7YBJh0T%2FuUyKNCkw7%2FUTIi556lJJbms6Egld%2BWxX
wnIUHgcFxr3fHMJ4zOX2vhcBCd51nUjZE9y%2FFdy0jLA%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8e9e733d6e8ba269-YUL
Alt-Svc: h3=":443"; ma=86400
Server-Timing: cfL4;desc="?
proto=TCP&rtt=15371&min_rtt=9222&rtt_var=12754&sent=11&recv=12&lost=0&retrans=0&sent_bytes=3698&recv_bytes=145
2&delivery_rate=218641&cwnd=248&unsent_bytes=0&cid=13492432fa2054cf&ts=446&x=0"

<!DOCTYPE html>
<html lang="en">
<head>


</head>
<body><noscript
>...... Sorry, this app needs JavaScript to work. Please enable JavaScript in your
browser.</noscript
>
<div id="react-ap
...[SNIP]...
```

Report generated by Burp Suite web vulnerability scanner v2024.9.5, at Thu Nov 28 19:25:42 EST 2024.