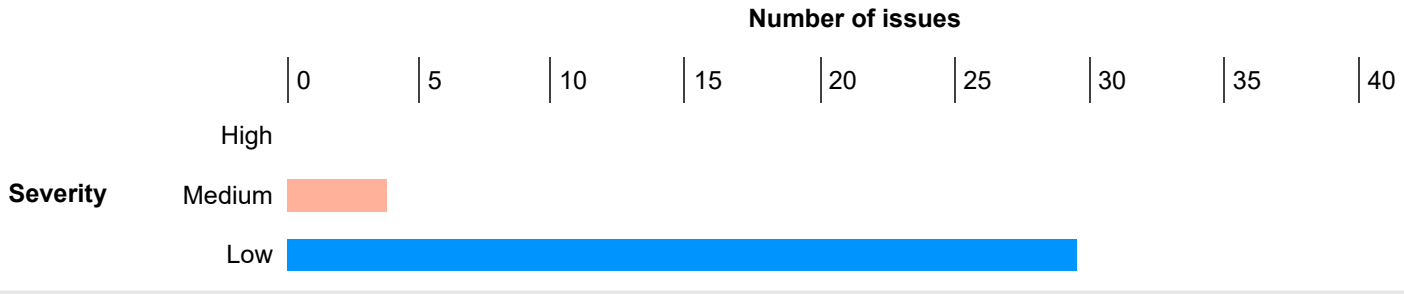
Burp Scanner Report

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	3	0	3
	Low	24	0	0	24
	Information	37	1	0	38
	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

2.5. https://firebase.googleapis.com/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig
2.6. https://firebaseinstallations.googleapis.com/v1/projects/shelterapp-1573928197721/installations
2.7. https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
2.8. https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmWUlfBBc4.woff2
2.9. https://fonts.gstatic.com/s/roboto/v32/KFOmCnqEu92Fr1Mu4mxK.woff2
2.10. https://maps.googleapis.com/
2.11. https://maps.googleapis.com/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo
2.12. https://maps.googleapis.com/maps-api-v3/api/js/59/1/common.js
2.13. https://maps.googleapis.com/maps-api-v3/api/js/59/1/map.js
2.14. https://maps.googleapis.com/maps-api-v3/api/js/59/1/marker.js
2.15. https://maps.googleapis.com/maps-api-v3/api/js/59/1/onion.js
2.16. https://maps.googleapis.com/maps-api-v3/api/js/59/1/util.js
2.17. https://maps.googleapis.com/maps/api/js
2.18. https://maps.googleapis.com/maps/api/js/StaticMapService.GetMapImage
2.19. https://maps.googleapis.com/maps/api/mapsjs/gen_204
2.20. https://maps.gstatic.com/mapfiles/api-3/images/cb_scout5_hdpi.png
2.21. https://maps.gstatic.com/mapfiles/api-3/images/drag-cross_hdpi.png
2.22. https://maps.gstatic.com/mapfiles/openhand_8_8.cur
2.23. https://maps.gstatic.com/mapfiles/transparent.png
2.24. https://www.google-analytics.com/g/collect

3. Content security policy: not enforced

4. Frameable response (potential Clickjacking)

5. Browser cross-site scripting filter disabled

5.1. https://firebase.googleapis.com/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig
5.2. https://firebaseinstallations.googleapis.com/v1/projects/shelterapp-1573928197721/installations
5.3. https://fonts.googleapis.com/css
5.4. https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
5.5. https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmWUlfBBc4.woff2
5.6. https://fonts.gstatic.com/s/roboto/v32/KFOmCnqEu92Fr1Mu4mxK.woff2
5.7. https://maps.googleapis.com/
5.8. https://maps.googleapis.com/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo
5.9. https://maps.googleapis.com/maps-api-v3/api/js/59/1/common.js
5.10. https://maps.googleapis.com/maps-api-v3/api/js/59/1/map.js
5.11. https://maps.googleapis.com/maps-api-v3/api/js/59/1/marker.js
5.12. https://maps.googleapis.com/maps-api-v3/api/js/59/1/onion.js
5.13. https://maps.googleapis.com/maps-api-v3/api/js/59/1/util.js
5.14. https://maps.googleapis.com/maps/api/js
5.15. https://maps.googleapis.com/maps/api/js/StaticMapService.GetMapImage
5.16. https://maps.googleapis.com/maps/api/mapsjs/gen_204
5.17. https://maps.gstatic.com/mapfiles/api-3/images/cb_scout5_hdpi.png
5.18. https://maps.gstatic.com/mapfiles/api-3/images/drag-cross_hdpi.png
5.19. https://maps.gstatic.com/mapfiles/openhand_8_8.cur
5.20. https://maps.gstatic.com/mapfiles/transparent.png
5.21. https://www.googletagmanager.com/gtag/js

6. Email addresses disclosed

6.1. https://maps.googleapis.com/maps/api/js
6.2. https://shelter.app/static/js/main.567d58aa.chunk.js
6.3. https://www.googletagmanager.com/gtag/js

7. Cacheable HTTPS response

7.1. https://api.shelter.app/bot/query
7.2. https://api.shelter.app/services/search-city-or-zip
7.3. https://firebase.googleapis.com/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig
7.4. https://firebaseinstallations.googleapis.com/v1/projects/shelterapp-1573928197721/installations
7.5. https://maps.googleapis.com/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo
7.6. https://maps.googleapis.com/maps/api/mapsjs/gen_204
7.7. https://shelter.app/introduce

---

1. Session token in URL

There are 3 instances of this issue:

- /maps/api/js/StaticMapService.GetMapImage
- /maps/vt
- /maps/vt

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://maps.googleapis.com/maps/api/js/StaticMapService.GetMapImage

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://maps.googleapis.com**
Path:	**/maps/api/js/StaticMapService.GetMapImage**

Issue detail

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

- https://maps.googleapis.com/maps/api/js/StaticMapService.GetMapImage?1m2&1i619736&2i749963&2e1&3u13&4m2&1u587&2u300&5m6&1e0&5sen-US&6sus&10b1&12b1&14i47083502&key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&token=75054

Request

```
GET /maps/api/js/StaticMapService.GetMapImage?1m2&1i619736&2i749963&2e1&3u13&4m2&1u587&2u300&5m6&1e0&5sen-US&6sus&10b1&12b1&14i47083502&key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&token=75054 HTTP/2
Host: maps.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: image/png
Date: Fri, 29 Nov 2024 00:40:45 GMT
Expires: Sat, 30 Nov 2024 00:40:45 GMT
Cache-Control: public, max-age=86400
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri https://csp.withgoogle.com/csp/scaffolding/msaispmnec:854:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/scaffolding/msaispmnec:854:0"}],}
Server: scaffolding on HTTPServer2
Content-Length: 69461
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Server-Timing: gfet4t7; dur=234
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

.PNG
.
...IHDR...K...,.....z.O...PLTE !$/04<=AIJMNRVVWZTnzcdgppt_w.z}..._'.i6.sC.|I.Cu.O  .[
..$..P..E..j..u..x..  ..k..n..q..t..z..}..a..i..q..y...B..N..Z..f..q..j..}...g..r.....................
...[SNIP]...
```

1.2. https://maps.googleapis.com/maps/vt

Summary

Severity: **Medium**

Confidence: **Firm**

Host: **https://maps.googleapis.com**

Path: **/maps/vt**

Issue detail

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

- https://maps.googleapis.com/maps/vt?pb=!1m5!1m4!1i13!2i2421!3i2930!4i256!2m3!1e0!2sm!3i714466695!3m12!2sen-US!3sUS!5e18!12m4!1e68!2m2!1sset!2sRoadmap!12m3!1e37!2m1!1ssmartmaps!4e0!5m2!1e3!5f2!23i47083502&key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&token=3481

Request

```
GET /maps/vt?pb=!1m5!1m4!1i13!2i2421!3i2930!4i256!2m3!1e0!2sm!3i714466695!3m12!2sen-
US!3sUS!5e18!12m4!1e68!2m2!1sset!2sRoadmap!12m3!1e37!2m1!1ssmartmaps!4e0!5m2!1e3!5f2!23i47083502&key=AIzaSy
C63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&token=3481 HTTP/2
Host: maps.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: image/webp
Date: Fri, 29 Nov 2024 00:41:15 GMT
Expires: Wed, 13 Aug 2025 05:31:37 GMT
Cache-Control: public, max-age=22222222
Access-Control-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Content-Security-Policy: script-src 'none'; object-src 'none'; base-uri 'none'
X-Content-Type-Options: nosniff
X-Server-Version-Bin: CgoIBBC3rvu5BhgB
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri
https://csp.withgoogle.com/csp/scaffolding/msptfdsghphc:130:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-
to/scaffolding/msptfdsghphc:130:0"}],}
Server: scaffolding on HTTPServer2
Content-Length: 50350
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Server-Timing: gfet4t7; dur=28
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

RIFF....WEBPVP8L..../..  ...6.mU...BZ.....B....?..<k.md.J..89C!tA..Cl.}...G..D.K".D.......6.......D...i    .dK$.....     ...$. .b.@A..$..
  .@"h. ..H..i.-.)27..wQ...M...Cd?....s}"dH
```

...Y.E3C._.lu.....Di...
...[SNIP]...

1.3. https://maps.googleapis.com/maps/vt

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://maps.googleapis.com**
Path:	**/maps/vt**

Issue detail

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

- https://maps.googleapis.com/maps/vt?pb=!1m4!1m3!1i13!2i2420!3i2929!1m4!1m3!1i13!2i2421!3i2929!1m4!1m3!1i13!2i2420!3i2930!1m4!1m3!1i13!2i2421!3i2930!1m4!1m3!1i13!2i2422!3i2929!1m4!1m3!1i13!2i2423!3i2929!1m4!1m3!1i13!2i2422!3i2930!1m4!1m3!1i13!2i2423!3i2930!2m3!1e0!2sm!3i714466707!3m12!2sen-US!3sUS!5e18!12m4!1e68!2m2!1sset!2sRoadmap!12m3!1e37!2m1!1ssmartmaps!4e3!12m1!5b1&callback=_xdc_._aoj2jw&key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&token=123221

Request

```
GET /maps/vt?pb=!1m4!1m3!1i13!2i2420!3i2929!1m4!1m3!1i13!2i2421!3i2929!1m4!1m3!1i13!2i2420!3i2930!1m4!1m3!1i13!2i2421!3i2930!1m4!1m3!1i13!2i2422!3i2929!1m4!1m3!1i13!2i2423!3i2929!1m4!1m3!1i13!2i2422!3i2930!1m4!1m3!1i13!2i2423!3i2930!2m3!1e0!2sm!3i714466707!3m12!2sen-US!3sUS!5e18!12m4!1e68!2m2!1sset!2sRoadmap!12m3!1e37!2m1!1ssmartmaps!4e3!12m1!5b1&callback=_xdc_._aoj2jw&key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&token=123221 HTTP/2
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4
```

Response

```
HTTP/2 200 OK
Content-Type: text/javascript
Date: Fri, 29 Nov 2024 00:41:16 GMT
Expires: Fri, 29 Nov 2024 00:41:16 GMT
Cache-Control: private, max-age=22222222
```

```
Access-Control-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Content-Security-Policy: script-src 'none'; object-src 'none'; base-uri 'none'
X-Content-Type-Options: nosniff
X-Server-Version-Bin: CgoIBBC3rvu5BhgB
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri
https://csp.withgoogle.com/csp/scaffolding/msptfdsghphc:130:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-
to/scaffolding/msptfdsghphc:130:0"}],}
Server: scaffolding on HTTPServer2
Content-Length: 9260
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Server-Timing: gfet4t7; dur=28
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

/* API Response */ _xdc_._aoj2jw && _xdc_._aoj2jw([{"id":"twtuwtwwtvtu","base":[634611712,767959040],"zrange":
[13,13],"layer":"m@714466707","features":[{"id":"6633970305550809473","a":[0,0,634611712,
...[SNIP]...
```

---

2. Strict transport security not enforced

There are 24 instances of this issue:

- https://api.shelter.app/
- https://api.shelter.app/services
- https://api.shelter.app/services/6052197226d8ce31cc4d48a7
- https://api.shelter.app/services/search-city-or-zip
- https://firebase.googleapis.com/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig
- https://firebaseinstallations.googleapis.com/v1/projects/shelterapp-1573928197721/installations
- https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
- https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmWUlfBBc4.woff2
- https://fonts.gstatic.com/s/roboto/v32/KFOmCnqEu92Fr1Mu4mxK.woff2
- https://maps.googleapis.com/
- https://maps.googleapis.com/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo
- https://maps.googleapis.com/maps-api-v3/api/js/59/1/common.js
- https://maps.googleapis.com/maps-api-v3/api/js/59/1/map.js
- https://maps.googleapis.com/maps-api-v3/api/js/59/1/marker.js
- https://maps.googleapis.com/maps-api-v3/api/js/59/1/onion.js
- https://maps.googleapis.com/maps-api-v3/api/js/59/1/util.js
- https://maps.googleapis.com/maps/api/js
- https://maps.googleapis.com/maps/api/js/StaticMapService.GetMapImage
- https://maps.googleapis.com/maps/api/mapsjs/gen_204
- https://maps.gstatic.com/mapfiles/api-3/images/cb_scout5_hdpi.png
- https://maps.gstatic.com/mapfiles/api-3/images/drag-cross_hdpi.png
- https://maps.gstatic.com/mapfiles/openhand_8_8.cur
- https://maps.gstatic.com/mapfiles/transparent.png
- https://www.google-analytics.com/g/collect

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

2.1. https://api.shelter.app/

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.shelter.app**
Path:	**/**

Issue detail

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

Request

```
OPTIONS /static-pages/FAQ HTTP/1.1
Host: api.shelter.app
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://shelter.app
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: same-site
Sec-Fetch-Dest: empty
```

```
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/1.1 204 No Content
Server: nginx
Date: Fri, 29 Nov 2024 00:42:10 GMT
Content-Length: 0
Connection: keep-alive
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
Vary: Access-Control-Request-Headers
Access-Control-Allow-Headers: authorization
```

2.2. https://api.shelter.app/services

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.shelter.app**
Path:	**/services**

Request

```
OPTIONS /services?
filter=type,isApproved&isApproved=true&limit=100&skip=0&search=name,+description,+serviceSummary,+address1,+address
2,+phone,+userEmail,+contactEmail&type=SHELTER HTTP/1.1
Host: api.shelter.app
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://shelter.app
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: same-site
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/1.1 204 No Content
Server: nginx
Date: Fri, 29 Nov 2024 00:39:34 GMT
Content-Length: 0
Connection: keep-alive
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
Vary: Access-Control-Request-Headers
Access-Control-Allow-Headers: authorization
```

2.3. https://api.shelter.app/services/6052197226d8ce31cc4d48a7

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://api.shelter.app**
Path:	**/services/6052197226d8ce31cc4d48a7**

Request

```
OPTIONS /services/6052197226d8ce31cc4d48a7 HTTP/1.1
Host: api.shelter.app
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: authorization
Origin: https://shelter.app
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: same-site
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/1.1 204 No Content
Server: nginx
Date: Fri, 29 Nov 2024 00:40:41 GMT
Content-Length: 0
Connection: keep-alive
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
Vary: Access-Control-Request-Headers
Access-Control-Allow-Headers: authorization
```

2.4. https://api.shelter.app/services/search-city-or-zip

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://api.shelter.app**

Path: **/services/search-city-or-zip**

Request

```
OPTIONS /services/search-city-or-zip HTTP/1.1
Host: api.shelter.app
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: authorization,content-type
Origin: https://shelter.app
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: same-site
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/1.1 204 No Content
Server: nginx
Date: Fri, 29 Nov 2024 00:39:42 GMT
Content-Length: 0
Connection: keep-alive
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
Vary: Access-Control-Request-Headers
Access-Control-Allow-Headers: authorization,content-type
```

2.5. https://firebase.googleapis.com/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://firebase.googleapis.com**

Path: **/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig**

Request

```
OPTIONS /v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig HTTP/1.1
Host: firebase.googleapis.com
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: x-goog-api-key
Origin: https://shelter.app
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://shelter.app/
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
Access-Control-Allow-Origin: https://shelter.app
Vary: origin
Vary: referer
Vary: x-origin
Access-Control-Allow-Methods: DELETE,GET,HEAD,OPTIONS,PATCH,POST,PUT
Access-Control-Allow-Headers: x-goog-api-key
Access-Control-Max-Age: 3600
Date: Fri, 29 Nov 2024 00:38:20 GMT
Content-Type: text/html
Server: ESF
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

2.6. https://firebaseinstallations.googleapis.com/v1/projects/shelterapp-1573928197721/installations

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://firebaseinstallations.googleapis.com**

Path: **/v1/projects/shelterapp-1573928197721/installations**

Request

```
OPTIONS /v1/projects/shelterapp-1573928197721/installations HTTP/1.1
Host: firebaseinstallations.googleapis.com
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type,x-goog-api-key
Origin: https://shelter.app
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://shelter.app/
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
Access-Control-Allow-Origin: https://shelter.app
Vary: origin
Vary: referer
Vary: x-origin
Access-Control-Allow-Methods: DELETE,GET,HEAD,OPTIONS,PATCH,POST,PUT
Access-Control-Allow-Headers: content-type,x-goog-api-key
Access-Control-Max-Age: 3600
Date: Fri, 29 Nov 2024 00:38:20 GMT
Content-Type: text/html
Server: ESF
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

2.7. https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmEU9fBBc4.woff2

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://fonts.gstatic.com**

Path: **/s/roboto/v32/KFOlCnqEu92Fr1MmEU9fBBc4.woff2**

Request

```
GET /s/roboto/v32/KFOlCnqEu92Fr1MmEU9fBBc4.woff2 HTTP/2
Host: fonts.gstatic.com
Origin: https://shelter.app
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
```

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: 18588
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Fri, 22 Nov 2024 01:46:32 GMT
Expires: Sat, 22 Nov 2025 01:46:32 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Thu, 01 Aug 2024 20:41:24 GMT
Content-Type: font/woff2
Age: 600893
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

wOF2......H..... ..H8.....................|.`..J.\    .<..
.....-..Z...x.6.$..0. .... ..S.7.5..K!.;..../.`..Sn.J.e.52P.(.....=9.....f.....$...*.fZ.p...N...t...
6.lfS.Ju.i.o.g..<...
.T"O    o..
...[SNIP]...
```

2.8. https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmWUlfBBc4.woff2

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://fonts.gstatic.com**

Path: **/s/roboto/v32/KFOlCnqEu92Fr1MmWUlfBBc4.woff2**

Request

```
GET /s/roboto/v32/KFOlCnqEu92Fr1MmWUlfBBc4.woff2 HTTP/2
Host: fonts.gstatic.com
Origin: https://shelter.app
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: CljcygE=
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
```

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: 18596
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 05:21:09 GMT
Expires: Fri, 28 Nov 2025 05:21:09 GMT
Cache-Control: public, max-age=31536000
Age: 69644
Last-Modified: Thu, 01 Aug 2024 20:41:21 GMT
Content-Type: font/woff2
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

wOF2......H.....H=.....|.`..J.H    .<..
.....>..Z...x.6.$..0. ..~. ..)...%.m..t.D<...U.c....D....@.....@e..a..R./<...p..q.q....S<.nm...X...(ER....e.....O.?Q_..FYH...
...[SNIP]...
```

2.9. https://fonts.gstatic.com/s/roboto/v32/KFOmCnqEu92Fr1Mu4mxK.woff2

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://fonts.gstatic.com**

Path: **/s/roboto/v32/KFOmCnqEu92Fr1Mu4mxK.woff2**

Request

```
GET /s/roboto/v32/KFOmCnqEu92Fr1Mu4mxK.woff2 HTTP/2
Host: fonts.gstatic.com
Origin: https://shelter.app
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
```

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: 18536
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 03:43:21 GMT
Expires: Fri, 28 Nov 2025 03:43:21 GMT
Cache-Control: public, max-age=31536000
Age: 75484
Last-Modified: Thu, 01 Aug 2024 20:41:24 GMT
Content-Type: font/woff2
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

wOF2......Hh.........H.............................Z..|.`..J.T    .<..
..H..U..Z...x.6.$..0. ..t. ..I....p..0.VU.......1....AQ...d..x...        R..4..-.c.
C$fUc.c..IX..@..~g.xs......%...O....eJ.w..U.|.......
...[SNIP]...
```

2.10. https://maps.googleapis.com/

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://maps.googleapis.com**

Path: **/**

Issue detail

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

Request

```
POST /$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo HTTP/2
Host: maps.googleapis.com
Content-Length: 241
X-Goog-Maps-Api-Signature: 41757
Sec-Ch-Ua-Platform: "Windows"
X-User-Agent: grpc-web-javascript/0.1
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
X-Goog-Maps-Channel-Id:
X-Goog-Maps-Client-Id:
Sec-Ch-Ua-Mobile: ?0
X-Goog-Api-Key: AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg
X-Goog-Maps-Api-Salt: xlYnQD7wE
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
Content-Type: application/json+protobuf
Accept: */*
Origin: https://shelter.app
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i

[[[45.46266733537652,-73.71671013528113],[45.57452880750897,-73.41360163014805]],13,null,"en-
US",0,"m@714000000",0,0,null,null,null,1,"https://shelter.app/services/6052197226d8ce31cc4d48a7",1,null,nul
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Cross-Origin-Resource-Policy: cross-origin
Content-Type: application/json+protobuf; charset=UTF-8
Vary: Origin
Vary: X-Origin
Vary: Referer
Date: Fri, 29 Nov 2024 00:41:15 GMT
Server: scaffolding on HTTPServer2
Content-Length: 25524
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: https://shelter.app
Access-Control-Expose-Headers: vary,vary,vary,content-encoding,date,server,content-length
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

["Map data ..2024 Google",[["obliques",[[45.567909609861289,-73.71826171875],[45.575600209478011,-73.41064453125]]],
```

["obliques",[[45.56021795715052,-73.71826171875],[45.567909609861289,-73.41064453125
...[SNIP]...

2.11. https://maps.googleapis.com/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo**

Request

```
OPTIONS /$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo HTTP/2
Host: maps.googleapis.com
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type,x-goog-api-key,x-goog-maps-api-salt,x-goog-maps-api-signature,x-goog-maps-channel-id,x-goog-maps-client-id,x-user-agent
Origin: https://shelter.app
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://shelter.app/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Access-Control-Allow-Origin: https://shelter.app
Vary: origin
Vary: referer
Vary: x-origin
Access-Control-Allow-Methods: DELETE,GET,HEAD,OPTIONS,PATCH,POST,PUT
Access-Control-Allow-Headers: content-type,x-goog-api-key,x-goog-maps-api-salt,x-goog-maps-api-signature,x-goog-maps-channel-id,x-goog-maps-client-id,x-user-agent
Access-Control-Max-Age: 3600
Date: Fri, 29 Nov 2024 00:41:10 GMT
Content-Type: text/html
Server: scaffolding on HTTPServer2
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

2.12. https://maps.googleapis.com/maps-api-v3/api/js/59/1/common.js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps-api-v3/api/js/59/1/common.js**

Request

```
GET /maps-api-v3/api/js/59/1/common.js HTTP/2
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/maps-api-js
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="maps-api-js"
Report-To: {"group":"maps-api-js","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/maps-api-
js"}]}
Timing-Allow-Origin: *
Content-Length: 274617
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 16:18:05 GMT
Expires: Fri, 28 Nov 2025 16:18:05 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Tue, 19 Nov 2024 01:42:57 GMT
Content-Type: text/javascript
Vary: Accept-Encoding, Origin
Age: 30020
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

google.maps.__gjsload__('common', function(_){var
Kia,Jia,Mia,Sia,Zia,$ia,cja,Cr,dja,Dr,eja,Er,fja,Fr,Ir,Kr,hja,ija,lja,mja,oja,us,qja,sja,tja,Fs,xja,jt,Fja,Hja,Gja,Lja,Mja,Pja,Qja,Rja,Ot,
Ut,Wja,Vt,Yt
...[SNIP]...
```

2.13. https://maps.googleapis.com/maps-api-v3/api/js/59/1/map.js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps-api-v3/api/js/59/1/map.js**

Request

```
GET /maps-api-v3/api/js/59/1/map.js HTTP/2
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/maps-api-js
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="maps-api-js"
Report-To: {"group":"maps-api-js","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/maps-api-
js"}]}
Timing-Allow-Origin: *
Content-Length: 81125
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 07:56:22 GMT
Expires: Fri, 28 Nov 2025 07:56:22 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Tue, 19 Nov 2024 01:42:57 GMT
Content-Type: text/javascript
Vary: Accept-Encoding, Origin
Age: 60262
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

google.maps.__gjsload__('map', function(_){var Dta=function(a){try{return _.ra.JSON.parse(a)}catch(b)
{}a=String(a);if(/^\s*$/.test(a)?0:/^[\],:{}\s\u2028\u2029]*$/.test(a.replace(/\\["\\\/bfnrtu]/g,"@
...[SNIP]...
```

2.14. https://maps.googleapis.com/maps-api-v3/api/js/59/1/marker.js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps-api-v3/api/js/59/1/marker.js**

Request

```
GET /maps-api-v3/api/js/59/1/marker.js HTTP/2
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/maps-api-js
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="maps-api-js"
Report-To: {"group":"maps-api-js","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/maps-api-
js"}]}
Timing-Allow-Origin: *
Content-Length: 74421
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Wed, 27 Nov 2024 20:26:25 GMT
Expires: Thu, 27 Nov 2025 20:26:25 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Tue, 19 Nov 2024 01:42:57 GMT
Content-Type: text/javascript
Vary: Accept-Encoding, Origin
Age: 101659
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

google.maps.__gjsload__('marker', function(_){var bWa=function(a,b){const
c=_.Ba(b);a.Eg.set(c,b);_.Om(a.Fg)},cWa=function(a,b){if(a.Fg.has(b))
{_.wk(b,"UPDATE_BASEMAP_COLLISION");_.wk(b,"UPDATE_MARKER
...[SNIP]...
```

2.15. https://maps.googleapis.com/maps-api-v3/api/js/59/1/onion.js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps-api-v3/api/js/59/1/onion.js**

Request

```
GET /maps-api-v3/api/js/59/1/onion.js HTTP/2
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/maps-api-js
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="maps-api-js"
Report-To: {"group":"maps-api-js","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/maps-api-
js"}]}
Timing-Allow-Origin: *
Content-Length: 30442
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Tue, 26 Nov 2024 17:23:16 GMT
Expires: Wed, 26 Nov 2025 17:23:16 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Tue, 19 Nov 2024 01:42:57 GMT
Content-Type: text/javascript
Vary: Accept-Encoding, Origin
Age: 199051
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

google.maps.__gjsload__('onion', function(_){var
tYa,uYa,XP,$P,ZP,xYa,yYa,zYa,wYa,AYa,bQ,BYa,CYa,DYa,FYa,HYa,IYa,KYa,LYa,OYa,QYa,SYa,UYa,WYa,XYa,VYa,hQ,iQ,gQ,j
Q,bZa,cZa,dZa,eZa,gZa,fZa,kQ,oZa,nZa,nQ,t
...[SNIP]...
```

2.16. https://maps.googleapis.com/maps-api-v3/api/js/59/1/util.js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps-api-v3/api/js/59/1/util.js**

Request

```
GET /maps-api-v3/api/js/59/1/util.js HTTP/2
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/maps-api-js
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="maps-api-js"
Report-To: {"group":"maps-api-js","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/maps-api-
js"}]}
Timing-Allow-Origin: *
Content-Length: 195339
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 13:04:23 GMT
Expires: Fri, 28 Nov 2025 13:04:23 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Tue, 19 Nov 2024 01:42:57 GMT
Content-Type: text/javascript
Vary: Accept-Encoding, Origin
Age: 41642
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

google.maps.__gjsload__('util', function(_){/*

Copyright 2024 Google, Inc
SPDX-License-Identifier: MIT
*/
```

var jxa,kxa,mxa,oxa,HB,pxa,qxa,sxa,JB,LB,txa,MB,NB,uxa,QB,wxa,UB,WB,XB,YB,ZB,$B,bC,cC,xxa,d
...[SNIP]...

2.17. https://maps.googleapis.com/maps/api/js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps/api/js**

Request

```
GET /maps/api/js?key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&v=weekly&callback=initMap HTTP/1.1
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Vary: Accept-Language
Vary: Origin
Vary: X-Origin
Vary: Referer
Etag: 0911f6db
Content-Type: text/javascript; charset=UTF-8
Cache-Control: public, max-age=1800, stale-while-revalidate=3600
Date: Fri, 29 Nov 2024 00:38:20 GMT
Server: scaffolding on HTTPServer2
Content-Length: 241793
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000


window.google = window.google || {};
google.maps = google.maps || {};
```

```
(function() {

var modules = google.maps.modules = {};
google.maps.__gjsload__ = function(name, text) {
modules[name]
...[SNIP]...
```

2.18. https://maps.googleapis.com/maps/api/js/StaticMapService.GetMapImage

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps/api/js/StaticMapService.GetMapImage**

Request

```
GET /maps/api/js/StaticMapService.GetMapImage?
1m2&1i619736&2i749963&2e1&3u13&4m2&1u587&2u300&5m6&1e0&5sen-
US&6sus&10b1&12b1&14i47083502&key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&token=75054 HTTP/2
Host: maps.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: image/png
Date: Fri, 29 Nov 2024 00:40:45 GMT
Expires: Sat, 30 Nov 2024 00:40:45 GMT
Cache-Control: public, max-age=86400
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri
https://csp.withgoogle.com/csp/scaffolding/msaispmnec:854:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-
to/scaffolding/msaispmnec:854:0"}],}
Server: scaffolding on HTTPServer2
Content-Length: 69461
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Server-Timing: gfet4t7; dur=234
```

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

.PNG
.
...IHDR...K...,.....z.O...PLTE !$/04<=AIJMNRVVWZTnzcdgppt_w.z}..._'.i6.sC.|l.Cu.O  .[
..$..P..E..j..u..x..  ..k..n..q..t..z..}..a..i..q..y...B..N..Z..f..q..j..}...g..r.....................
...[SNIP]...
```

2.19. https://maps.googleapis.com/maps/api/mapsjs/gen_204

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps/api/mapsjs/gen_204**

Request

```
GET /maps/api/mapsjs/gen_204?csp_test=true HTTP/2
Host: maps.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: */*
Origin: https://shelter.app
X-Client-Data: CljcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=UTF-8
Vary: Origin
Vary: X-Origin
Vary: Referer
Date: Fri, 29 Nov 2024 00:38:22 GMT
Server: scaffolding on HTTPServer2
Content-Length: 3
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: https://shelter.app
Access-Control-Expose-Headers: vary,vary,vary,content-encoding,date,server,content-length
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

```
{}
```

2.20. https://maps.gstatic.com/mapfiles/api-3/images/cb_scout5_hdpi.png

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.gstatic.com**
Path:	**/mapfiles/api-3/images/cb_scout5_hdpi.png**

Request

```
GET /mapfiles/api-3/images/cb_scout5_hdpi.png HTTP/2
Host: maps.gstatic.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: i
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: image/png
Access-Control-Allow-Origin: *
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/geo-tactile
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="geo-tactile"
Report-To: {"group":"geo-tactile","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/geo-tactile"}]}
Content-Length: 104139
Date: Fri, 29 Nov 2024 00:41:18 GMT
Expires: Fri, 29 Nov 2024 00:41:18 GMT
Cache-Control: private, max-age=31536000
Last-Modified: Tue, 18 May 2021 19:15:00 GMT
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

.PNG
.
...IHDR.............[O....IDATx....x.E....(...W.......z/H.E.. %=...C...H..t....z....:*X.^.......B.H~.........A...e.y>..m...e..;;;.......*O^.7....E.P.
```

<.^....A9PQR.O..^...g&-...IQ.2 QEIK..<9...
...[SNIP]...

2.21. https://maps.gstatic.com/mapfiles/api-3/images/drag-cross_hdpi.png

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.gstatic.com**
Path:	**/mapfiles/api-3/images/drag-cross_hdpi.png**

Request

```
GET /mapfiles/api-3/images/drag-cross_hdpi.png HTTP/2
Host: maps.gstatic.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: i
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: image/png
Access-Control-Allow-Origin: *
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/geo-tactile
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="geo-tactile"
Report-To: {"group":"geo-tactile","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/geo-tactile"}]}
Content-Length: 419
Date: Fri, 29 Nov 2024 00:41:18 GMT
Expires: Fri, 29 Nov 2024 00:41:18 GMT
Cache-Control: private, max-age=31536000
Last-Modified: Tue, 18 May 2021 19:15:00 GMT
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

.PNG
.
...IHDR.....................jIDATx...%TEA..q..-8ww....{..W....uh.h.J.I.@%..p.p..:g....     ....]q..
```

```
!./4..#.......-...2.....6.w.uyw.:F..'.p.&h..&.x.'......Y.|..D0.L.....O:h..q..  ..p...khh...     X8p.
...[SNIP]...
```

2.22. https://maps.gstatic.com/mapfiles/openhand_8_8.cur

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.gstatic.com**
Path:	**/mapfiles/openhand_8_8.cur**

Request

```
GET /mapfiles/openhand_8_8.cur HTTP/1.1
Host: maps.gstatic.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: image/bmp
Access-Control-Allow-Origin: *
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/geo-tactile
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="geo-tactile"
Report-To: {"group":"geo-tactile","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/geo-tactile"}]}
Content-Length: 326
Date: Fri, 29 Nov 2024 00:41:10 GMT
Expires: Fri, 29 Nov 2024 00:41:10 GMT
Cache-Control: private, max-age=31536000
Last-Modified: Tue, 18 May 2021 19:15:00 GMT
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

..... .....0.......(...
```

...@.....?...w...g.....
...[SNIP]...

2.23. https://maps.gstatic.com/mapfiles/transparent.png

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://maps.gstatic.com**
Path:	**/mapfiles/transparent.png**

Request

```
GET /mapfiles/transparent.png HTTP/1.1
Host: maps.gstatic.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: image/png
Access-Control-Allow-Origin: *
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/geo-tactile
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="geo-tactile"
Report-To: {"group":"geo-tactile","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/geo-tactile"}]}
Content-Length: 68
Date: Fri, 29 Nov 2024 00:40:47 GMT
Expires: Fri, 29 Nov 2024 00:40:47 GMT
Cache-Control: private, max-age=31536000
Last-Modified: Tue, 18 May 2021 19:15:00 GMT
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

.PNG
```

.
...IHDR.....IDATx.c.....(.....IEND.B`.

2.24. https://www.google-analytics.com/g/collect

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://www.google-analytics.com**
Path:	**/g/collect**

Request

```
POST /g/collect?v=2&tid=G-WMS317DV0H&gtm=45je4bk0v885629536za200&_p=1732840702807&gcd=13l3l3l3l1l1&npa=0&dma=0&tag_exp=101925629~102067555~102067808~102077855~102081485&_fid=dYLHJ5swy2SUPshpv9gsSY&cid=230453292.1732840711&ul=en-us&sr=1280x800&uaa=&uab=&uafvl=&uamb=0&uam=&uap=Windows&uapv=&uaw=0&are=1&frm=0&pscdl=&_s=1&sid=1732840710&sct=1&seg=0&dl=https%3A%2F%2Fshelter.app%2Fintroduce&dt=Homeless%20Resources%20-%20Shelter%20App&en=page_view&_fv=1&_nsi=1&_ss=2&_ee=1&ep.origin=firebase&tfd=16169 HTTP/1.1
Host: www.google-analytics.com
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"
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://shelter.app
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
```

Response

```
HTTP/2 204 No Content
Access-Control-Allow-Origin: https://shelter.app
Date: Fri, 29 Nov 2024 00:39:24 GMT
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Cache-Control: no-cache, no-store, must-revalidate
Access-Control-Allow-Credentials: true
Content-Type: text/plain
Cross-Origin-Resource-Policy: cross-origin
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri https://csp.withgoogle.com/csp/scaffolding/ascnsrsggc:86:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/scaffolding/ascnsrsggc:86:0"}],}
```

```
Server: Golfe2
Content-Length: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

---

3. Content security policy: not enforced

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://www.google-analytics.com**
Path:	**/g/collect**

Issue detail

The content security policy is not currently enforced because the policy is served with the Content-Security-Policy-Report-Only header. This header will report any CSP violations but does not prevent any resources from being loaded.

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 transitioning from using the Content-Security-Policy-Report-Only header to the Content-Security-Policy header for CSP deployment, ensuring effective policy enforcement.

References

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

Request

```
POST /g/collect?v=2&tid=G-WMS317DV0H&gtm=45je4bk0v885629536za200&_p=1732840702807&gcd=13l3l3l3l1l1&npa=0&dma=0&tag_exp=101925629~102067555~102067808~102077855~102081485&_fid=dYLHJ5swy2SUPshpv9gsSY&cid=230453292.1732840711&ul=en-us&sr=1280x800&uaa=&uab=&uafvl=&uamb=0&uam=&uap=Windows&uapv=&uaw=0&are=1&frm=0&pscdl=&_s=1&sid=1732840710&sct=1&seg=0&dl=https%3A%2F%2Fshelter.app%2Fintroduce&dt=Homeless%20Resources%20-%20Shelter%20App&en=page_view&_fv=1&_nsi=1&_ss=2&_ee=1&ep.origin=firebase&tfd=16169 HTTP/1.1
Host: www.google-analytics.com
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"
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://shelter.app
Sec-Fetch-Site: cross-site
```

```
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
```

Response

```
HTTP/2 204 No Content
Access-Control-Allow-Origin: https://shelter.app
Date: Fri, 29 Nov 2024 00:39:24 GMT
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Cache-Control: no-cache, no-store, must-revalidate
Access-Control-Allow-Credentials: true
Content-Type: text/plain
Cross-Origin-Resource-Policy: cross-origin
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri
https://csp.withgoogle.com/csp/scaffolding/ascnsrsggc:86:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-
to/scaffolding/ascnsrsggc:86:0"}],}
Server: Golfe2
Content-Length: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

---

4. Frameable response (potential Clickjacking)

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://shelter.app**
Path:	**/introduce**

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 /introduce HTTP/1.1
Host: shelter.app
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
Cache-Control: max-age=3600
Content-Type: text/html; charset=utf-8
Etag: "e7282bd09cd4a8597655085b53c5b38e7867801b0d6023239e3e053d32df7345-br"
Last-Modified: Sun, 28 Apr 2024 19:54:20 GMT
Strict-Transport-Security: max-age=31556926
Accept-Ranges: bytes
Date: Fri, 29 Nov 2024 00:38:16 GMT
X-Served-By: cache-yul1970072-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732840697.630908,VS0,VE1
Vary: x-fh-requested-host, accept-encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 2650

<!doctype html><html lang="en"><head><meta charset="utf-8"/><meta content="https://shelter.app/favicon1.png"
name="og:image"/><meta content="https://shelter.app" name="og:url"/><link rel="shortcut ico
...[SNIP]...
```

---

5. Browser cross-site scripting filter disabled

There are 21 instances of this issue:

- https://firebase.googleapis.com/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig
- https://firebaseinstallations.googleapis.com/v1/projects/shelterapp-1573928197721/installations
- https://fonts.googleapis.com/css
- https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
- https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmWUlfBBc4.woff2
- https://fonts.gstatic.com/s/roboto/v32/KFOmCnqEu92Fr1Mu4mxK.woff2
- https://maps.googleapis.com/
- https://maps.googleapis.com/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo
- https://maps.googleapis.com/maps-api-v3/api/js/59/1/common.js
- https://maps.googleapis.com/maps-api-v3/api/js/59/1/map.js
- https://maps.googleapis.com/maps-api-v3/api/js/59/1/marker.js
- https://maps.googleapis.com/maps-api-v3/api/js/59/1/onion.js
- https://maps.googleapis.com/maps-api-v3/api/js/59/1/util.js
- https://maps.googleapis.com/maps/api/js
- https://maps.googleapis.com/maps/api/js/StaticMapService.GetMapImage
- https://maps.googleapis.com/maps/api/mapsjs/gen_204
- https://maps.gstatic.com/mapfiles/api-3/images/cb_scout5_hdpi.png
- https://maps.gstatic.com/mapfiles/api-3/images/drag-cross_hdpi.png
- https://maps.gstatic.com/mapfiles/openhand_8_8.cur
- https://maps.gstatic.com/mapfiles/transparent.png
- https://www.googletagmanager.com/gtag/js

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)

5.1. https://firebase.googleapis.com/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://firebase.googleapis.com**
Path:	**/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig**

Request

```
OPTIONS /v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig HTTP/1.1
Host: firebase.googleapis.com
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: x-goog-api-key
Origin: https://shelter.app
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://shelter.app/
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
Access-Control-Allow-Origin: https://shelter.app
Vary: origin
Vary: referer
Vary: x-origin
Access-Control-Allow-Methods: DELETE,GET,HEAD,OPTIONS,PATCH,POST,PUT
Access-Control-Allow-Headers: x-goog-api-key
Access-Control-Max-Age: 3600
Date: Fri, 29 Nov 2024 00:38:20 GMT
Content-Type: text/html
Server: ESF
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

5.2. https://firebaseinstallations.googleapis.com/v1/projects/shelterapp-1573928197721/installations

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://firebaseinstallations.googleapis.com**
Path:	**/v1/projects/shelterapp-1573928197721/installations**

Request

```
OPTIONS /v1/projects/shelterapp-1573928197721/installations HTTP/1.1
Host: firebaseinstallations.googleapis.com
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type,x-goog-api-key
Origin: https://shelter.app
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://shelter.app/
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
Access-Control-Allow-Origin: https://shelter.app
Vary: origin
Vary: referer
Vary: x-origin
Access-Control-Allow-Methods: DELETE,GET,HEAD,OPTIONS,PATCH,POST,PUT
Access-Control-Allow-Headers: content-type,x-goog-api-key
Access-Control-Max-Age: 3600
Date: Fri, 29 Nov 2024 00:38:20 GMT
Content-Type: text/html
Server: ESF
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

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

Summary

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

Request

```
GET /css?family=Google+Sans+Text_old:400&text=%E2%86%90%E2%86%92%E2%86%91%E2%86%93&lang=en HTTP/2
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://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4
```

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 00:41:25 GMT
Date: Fri, 29 Nov 2024 00:41:25 GMT
Cache-Control: private, max-age=86400, stale-while-revalidate=604800
Last-Modified: Thu, 28 Nov 2024 23:34:23 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

/*
* See: https://fonts.google.com/license/googlerestricted
*/
@font-face {
font-family: 'Google Sans Text';
font-style: normal;
font-weight: 400;
src: url(https://fonts.gstatic.com/l/font?k
...[SNIP]...
```

5.4. https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmEU9fBBc4.woff2

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://fonts.gstatic.com**
Path:	**/s/roboto/v32/KFOlCnqEu92Fr1MmEU9fBBc4.woff2**

Request

```
GET /s/roboto/v32/KFOlCnqEu92Fr1MmEU9fBBc4.woff2 HTTP/2
Host: fonts.gstatic.com
Origin: https://shelter.app
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
```

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: 18588
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Fri, 22 Nov 2024 01:46:32 GMT
Expires: Sat, 22 Nov 2025 01:46:32 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Thu, 01 Aug 2024 20:41:24 GMT
Content-Type: font/woff2
Age: 600893
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

wOF2.....H..... ..H8.....|.`..J.\    .<..
.....-..Z...x.6.$..0. .... ..S.7.5..K!.;..../.`..Sn.J.e.52P.(.....=9.....f.....$...*.fZ.p...N...t...
```

6.IfS.Ju.i.o.g..<...
.T"O o..
...[SNIP]...

5.5. https://fonts.gstatic.com/s/roboto/v32/KFOlCnqEu92Fr1MmWUlfBBc4.woff2

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://fonts.gstatic.com**
Path:	**/s/roboto/v32/KFOlCnqEu92Fr1MmWUlfBBc4.woff2**

Request

```
GET /s/roboto/v32/KFOlCnqEu92Fr1MmWUlfBBc4.woff2 HTTP/2
Host: fonts.gstatic.com
Origin: https://shelter.app
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
```

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: 18596
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 05:21:09 GMT
Expires: Fri, 28 Nov 2025 05:21:09 GMT
Cache-Control: public, max-age=31536000
Age: 69644
Last-Modified: Thu, 01 Aug 2024 20:41:21 GMT
```

```
Content-Type: font/woff2
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

wOF2......H.....H=.....|.`..J.H    .<..
.....>..Z...x.6.$..0. ..~. ..)...%.m..t.D<...U.c....D....@.....@e..a..R./<...p..q.q....S<.nm...X...(ER....e.....O.?Q_..FYH...
...[SNIP]...
```

5.6. https://fonts.gstatic.com/s/roboto/v32/KFOmCnqEu92Fr1Mu4mxK.woff2

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://fonts.gstatic.com**
Path:	**/s/roboto/v32/KFOmCnqEu92Fr1Mu4mxK.woff2**

Request

```
GET /s/roboto/v32/KFOmCnqEu92Fr1Mu4mxK.woff2 HTTP/2
Host: fonts.gstatic.com
Origin: https://shelter.app
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
```

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: 18536
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 03:43:21 GMT
Expires: Fri, 28 Nov 2025 03:43:21 GMT
Cache-Control: public, max-age=31536000
```

```
Age: 75484
Last-Modified: Thu, 01 Aug 2024 20:41:24 GMT
Content-Type: font/woff2
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

wOF2......Hh.........H.............................Z..|.`..J.T    .<..
..H..U..Z...x.6.$..0. ..t. ..I....p..0.VU.......1....AQ...d..x...        R..4..-.c.
C$fUc.c..IX..@..~g.xs......%...O....eJ.w..U.|.......
...[SNIP]...
```

5.7. https://maps.googleapis.com/

Summary

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

Issue detail

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

Request

```
POST /$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo HTTP/2
Host: maps.googleapis.com
Content-Length: 241
X-Goog-Maps-Api-Signature: 41757
Sec-Ch-Ua-Platform: "Windows"
X-User-Agent: grpc-web-javascript/0.1
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
X-Goog-Maps-Channel-Id:
X-Goog-Maps-Client-Id:
Sec-Ch-Ua-Mobile: ?0
X-Goog-Api-Key: AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg
X-Goog-Maps-Api-Salt: xlYnQD7wE
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
Content-Type: application/json+protobuf
Accept: */*
Origin: https://shelter.app
X-Client-Data: CljcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i

[[[45.46266733537652,-73.71671013528113],[45.57452880750897,-73.41360163014805]],13,null,"en-
US",0,"m@714000000",0,0,null,null,null,1,"https://shelter.app/services/6052197226d8ce31cc4d48a7",1,null,nul
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Cross-Origin-Resource-Policy: cross-origin
Content-Type: application/json+protobuf; charset=UTF-8
Vary: Origin
Vary: X-Origin
Vary: Referer
Date: Fri, 29 Nov 2024 00:41:15 GMT
Server: scaffolding on HTTPServer2
Content-Length: 25524
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: https://shelter.app
Access-Control-Expose-Headers: vary,vary,vary,content-encoding,date,server,content-length
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

["Map data ..2024 Google",[["obliques",[[45.567909609861289,-73.71826171875],[45.575600209478011,-73.41064453125]]],
["obliques",[[45.56021795715052,-73.71826171875],[45.567909609861289,-73.41064453125
...[SNIP]...
```

5.8. https://maps.googleapis.com/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo**

Request

```
OPTIONS /$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo HTTP/2
Host: maps.googleapis.com
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type,x-goog-api-key,x-goog-maps-api-salt,x-goog-maps-api-signature,x-goog-maps-channel-id,x-goog-maps-client-id,x-user-agent
Origin: https://shelter.app
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://shelter.app/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Access-Control-Allow-Origin: https://shelter.app
Vary: origin
Vary: referer
Vary: x-origin
Access-Control-Allow-Methods: DELETE,GET,HEAD,OPTIONS,PATCH,POST,PUT
Access-Control-Allow-Headers: content-type,x-goog-api-key,x-goog-maps-api-salt,x-goog-maps-api-signature,x-goog-maps-channel-id,x-goog-maps-client-id,x-user-agent
Access-Control-Max-Age: 3600
Date: Fri, 29 Nov 2024 00:41:10 GMT
Content-Type: text/html
Server: scaffolding on HTTPServer2
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

5.9. https://maps.googleapis.com/maps-api-v3/api/js/59/1/common.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps-api-v3/api/js/59/1/common.js**

Request

```
GET /maps-api-v3/api/js/59/1/common.js HTTP/2
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/maps-api-js
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="maps-api-js"
Report-To: {"group":"maps-api-js","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/maps-api-
```

```
js"}]}
Timing-Allow-Origin: *
Content-Length: 274617
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 16:18:05 GMT
Expires: Fri, 28 Nov 2025 16:18:05 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Tue, 19 Nov 2024 01:42:57 GMT
Content-Type: text/javascript
Vary: Accept-Encoding, Origin
Age: 30020
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

google.maps.__gjsload__('common', function(_){var
Kia,Jia,Mia,Sia,Zia,$ia,cja,Cr,dja,Dr,eja,Er,fja,Fr,Ir,Kr,hja,ija,lja,mja,oja,us,qja,sja,tja,Fs,xja,jt,Fja,Hja,Gja,Lja,Mja,Pja,Qja,Rja,Ot,
Ut,Wja,Vt,Yt
...[SNIP]...
```

5.10. https://maps.googleapis.com/maps-api-v3/api/js/59/1/map.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps-api-v3/api/js/59/1/map.js**

Request

```
GET /maps-api-v3/api/js/59/1/map.js HTTP/2
Host: maps.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: */*
X-Client-Data: CljcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/maps-api-js
Cross-Origin-Resource-Policy: cross-origin
```

```
Cross-Origin-Opener-Policy: same-origin; report-to="maps-api-js"
Report-To: {"group":"maps-api-js","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/maps-api-
js"}]}
Timing-Allow-Origin: *
Content-Length: 81125
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 07:56:22 GMT
Expires: Fri, 28 Nov 2025 07:56:22 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Tue, 19 Nov 2024 01:42:57 GMT
Content-Type: text/javascript
Vary: Accept-Encoding, Origin
Age: 60262
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

google.maps.__gjsload__('map', function(_){var Dta=function(a){try{return _.ra.JSON.parse(a)}catch(b)
{}a=String(a);if(/^\s*$/.test(a)?0:/^[\],:{}\s\u2028\u2029]*$/.test(a.replace(/\\["\\\/bfnrtu]/g,"@
...[SNIP]...
```

5.11. https://maps.googleapis.com/maps-api-v3/api/js/59/1/marker.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps-api-v3/api/js/59/1/marker.js**

Request

```
GET /maps-api-v3/api/js/59/1/marker.js HTTP/2
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/maps-api-js
```

```
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="maps-api-js"
Report-To: {"group":"maps-api-js","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/maps-api-
js"}]}
Timing-Allow-Origin: *
Content-Length: 74421
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Wed, 27 Nov 2024 20:26:25 GMT
Expires: Thu, 27 Nov 2025 20:26:25 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Tue, 19 Nov 2024 01:42:57 GMT
Content-Type: text/javascript
Vary: Accept-Encoding, Origin
Age: 101659
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

google.maps.__gjsload__('marker', function(_){var bWa=function(a,b){const
c=_.Ba(b);a.Eg.set(c,b);_.Om(a.Fg)},cWa=function(a,b){if(a.Fg.has(b))
{_.wk(b,"UPDATE_BASEMAP_COLLISION");_.wk(b,"UPDATE_MARKER
...[SNIP]...
```

5.12. https://maps.googleapis.com/maps-api-v3/api/js/59/1/onion.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps-api-v3/api/js/59/1/onion.js**

Request

```
GET /maps-api-v3/api/js/59/1/onion.js HTTP/2
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
```

```
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/maps-api-js
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="maps-api-js"
Report-To: {"group":"maps-api-js","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/maps-api-
js"}]}
Timing-Allow-Origin: *
Content-Length: 30442
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Tue, 26 Nov 2024 17:23:16 GMT
Expires: Wed, 26 Nov 2025 17:23:16 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Tue, 19 Nov 2024 01:42:57 GMT
Content-Type: text/javascript
Vary: Accept-Encoding, Origin
Age: 199051
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

google.maps.__gjsload__('onion', function(_){var
tYa,uYa,XP,$P,ZP,xYa,yYa,zYa,wYa,AYa,bQ,BYa,CYa,DYa,FYa,HYa,IYa,KYa,LYa,OYa,QYa,SYa,UYa,WYa,XYa,VYa,hQ,iQ,gQ,j
Q,bZa,cZa,dZa,eZa,gZa,fZa,kQ,oZa,nZa,nQ,t
...[SNIP]...
```

5.13. https://maps.googleapis.com/maps-api-v3/api/js/59/1/util.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps-api-v3/api/js/59/1/util.js**

Request

```
GET /maps-api-v3/api/js/59/1/util.js HTTP/2
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/maps-api-js
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin; report-to="maps-api-js"
Report-To: {"group":"maps-api-js","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/maps-api-
js"}]}
Timing-Allow-Origin: *
Content-Length: 195339
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 13:04:23 GMT
Expires: Fri, 28 Nov 2025 13:04:23 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Tue, 19 Nov 2024 01:42:57 GMT
Content-Type: text/javascript
Vary: Accept-Encoding, Origin
Age: 41642
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

google.maps.__gjsload__('util', function(_){/*

Copyright 2024 Google, Inc
SPDX-License-Identifier: MIT
*/
var jxa,kxa,mxa,oxa,HB,pxa,qxa,sxa,JB,LB,txa,MB,NB,uxa,QB,wxa,UB,WB,XB,YB,ZB,$B,bC,cC,xxa,d
...[SNIP]...
```

5.14. https://maps.googleapis.com/maps/api/js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps/api/js**

Request

```
GET /maps/api/js?key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&v=weekly&callback=initMap HTTP/1.1
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
```

```
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Vary: Accept-Language
Vary: Origin
Vary: X-Origin
Vary: Referer
Etag: 0911f6db
Content-Type: text/javascript; charset=UTF-8
Cache-Control: public, max-age=1800, stale-while-revalidate=3600
Date: Fri, 29 Nov 2024 00:38:20 GMT
Server: scaffolding on HTTPServer2
Content-Length: 241793
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000


window.google = window.google || {};
google.maps = google.maps || {};
(function() {

var modules = google.maps.modules = {};
google.maps.__gjsload__ = function(name, text) {
modules[name]
...[SNIP]...
```

5.15. https://maps.googleapis.com/maps/api/js/StaticMapService.GetMapImage

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps/api/js/StaticMapService.GetMapImage**

Request

```
GET /maps/api/js/StaticMapService.GetMapImage?
1m2&1i619736&2i749963&2e1&3u13&4m2&1u587&2u300&5m6&1e0&5sen-
US&6sus&10b1&12b1&14i47083502&key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&token=75054 HTTP/2
Host: maps.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
```

```
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: image/png
Date: Fri, 29 Nov 2024 00:40:45 GMT
Expires: Sat, 30 Nov 2024 00:40:45 GMT
Cache-Control: public, max-age=86400
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri
https://csp.withgoogle.com/csp/scaffolding/msaispmnec:854:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-
to/scaffolding/msaispmnec:854:0"}],}
Server: scaffolding on HTTPServer2
Content-Length: 69461
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Server-Timing: gfet4t7; dur=234
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

.PNG
.
...IHDR...K...,.....z.O...PLTE !$/04<=AIJMNRVVWZTnzcdgppt_w.z}..._'.i6.sC.|I.Cu.O  .[
..$..P..E..j..u..x..  ..k..n..q..t..z..}..a..i..q..y...B..N..Z..f..q..j..}...g..r.....................
...[SNIP]...
```

5.16. https://maps.googleapis.com/maps/api/mapsjs/gen_204

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps/api/mapsjs/gen_204**

Request

```
GET /maps/api/mapsjs/gen_204?csp_test=true HTTP/2
Host: maps.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: */*
Origin: https://shelter.app
```

```
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=UTF-8
Vary: Origin
Vary: X-Origin
Vary: Referer
Date: Fri, 29 Nov 2024 00:38:22 GMT
Server: scaffolding on HTTPServer2
Content-Length: 3
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: https://shelter.app
Access-Control-Expose-Headers: vary,vary,vary,content-encoding,date,server,content-length
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{}
```

5.17. https://maps.gstatic.com/mapfiles/api-3/images/cb_scout5_hdpi.png

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.gstatic.com**
Path:	**/mapfiles/api-3/images/cb_scout5_hdpi.png**

Request

```
GET /mapfiles/api-3/images/cb_scout5_hdpi.png HTTP/2
Host: maps.gstatic.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
```

Priority: i

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: image/png
Access-Control-Allow-Origin: *
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/geo-tactile
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="geo-tactile"
Report-To: {"group":"geo-tactile","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/geo-tactile"}]}
Content-Length: 104139
Date: Fri, 29 Nov 2024 00:41:18 GMT
Expires: Fri, 29 Nov 2024 00:41:18 GMT
Cache-Control: private, max-age=31536000
Last-Modified: Tue, 18 May 2021 19:15:00 GMT
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

.PNG
.
...IHDR.............[O....IDATx....x.E....(...W.......z/H.E.. %=...C...H..t....z....:*X.^.......B.H~.........A...e.y>..m...e..;;;.......*O^.7....E.P.
<.^....A9PQR.O..^...g&-...IQ.2  QEIK..<9...
...[SNIP]...
```

5.18. https://maps.gstatic.com/mapfiles/api-3/images/drag-cross_hdpi.png

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.gstatic.com**
Path:	**/mapfiles/api-3/images/drag-cross_hdpi.png**

Request

```
GET /mapfiles/api-3/images/drag-cross_hdpi.png HTTP/2
Host: maps.gstatic.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
```

Priority: i

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: image/png
Access-Control-Allow-Origin: *
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/geo-tactile
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="geo-tactile"
Report-To: {"group":"geo-tactile","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/geo-tactile"}]}
Content-Length: 419
Date: Fri, 29 Nov 2024 00:41:18 GMT
Expires: Fri, 29 Nov 2024 00:41:18 GMT
Cache-Control: private, max-age=31536000
Last-Modified: Tue, 18 May 2021 19:15:00 GMT
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

.PNG
.
...IHDR.....................jIDATx...%TEA..q..-8ww....{..W....uh.h.J.I.@%..p.p..:g....     ....]q..
!./4..#.......-...2.....6.w.uyw.:F..'.p.&h..&.x.'......Y.|..D0.L.....O:h..q..  ..p...khh...     X8p.
...[SNIP]...
```

5.19. https://maps.gstatic.com/mapfiles/openhand_8_8.cur

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.gstatic.com**
Path:	**/mapfiles/openhand_8_8.cur**

Request

```
GET /mapfiles/openhand_8_8.cur HTTP/1.1
Host: maps.gstatic.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
```

```
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: image/bmp
Access-Control-Allow-Origin: *
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/geo-tactile
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="geo-tactile"
Report-To: {"group":"geo-tactile","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/geo-tactile"}]}
Content-Length: 326
Date: Fri, 29 Nov 2024 00:41:10 GMT
Expires: Fri, 29 Nov 2024 00:41:10 GMT
Cache-Control: private, max-age=31536000
Last-Modified: Tue, 18 May 2021 19:15:00 GMT
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

...... ......0.......(...
...@.....?...w...g.....
...[SNIP]...
```

5.20. https://maps.gstatic.com/mapfiles/transparent.png

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.gstatic.com**
Path:	**/mapfiles/transparent.png**

Request

```
GET /mapfiles/transparent.png HTTP/1.1
Host: maps.gstatic.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: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

```
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: image/png
Access-Control-Allow-Origin: *
Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/geo-tactile
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="geo-tactile"
Report-To: {"group":"geo-tactile","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/geo-tactile"}]}
Content-Length: 68
Date: Fri, 29 Nov 2024 00:40:47 GMT
Expires: Fri, 29 Nov 2024 00:40:47 GMT
Cache-Control: private, max-age=31536000
Last-Modified: Tue, 18 May 2021 19:15:00 GMT
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

.PNG
.
...IHDR.....IDATx.c.....(.....IEND.B`.
```

5.21. https://www.googletagmanager.com/gtag/js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://www.googletagmanager.com**
Path:	**/gtag/js**

Request

```
GET /gtag/js?l=dataLayer&id=G-WMS317DV0H HTTP/1.1
Host: www.googletagmanager.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: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: application/javascript; charset=UTF-8
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Cache-Control
Vary: Accept-Encoding
Date: Fri, 29 Nov 2024 00:38:30 GMT
Expires: Fri, 29 Nov 2024 00:38:30 GMT
Cache-Control: private, max-age=900
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cross-Origin-Resource-Policy: cross-origin
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri
https://csp.withgoogle.com/csp/scaffolding/ascgcycc:838:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-
to/scaffolding/ascgcycc:838:0"}],}
Server: Google Tag Manager
Content-Length: 361509
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000


// Copyright 2012 Google Inc. All rights reserved.

(function(){

var data = {
"resource": {
"version":"1",

"macros":[{"function":"__e"},{"function":"__c","vtp_value":"google.ca"},{"function"
...[SNIP]...
```

---

6. Email addresses disclosed

There are 3 instances of this issue:

- https://maps.googleapis.com/maps/api/js
- https://shelter.app/static/js/main.567d58aa.chunk.js
- https://www.googletagmanager.com/gtag/js

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

6.1. https://maps.googleapis.com/maps/api/js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps/api/js**

Issue detail

The following email address was disclosed in the response:

- robert@broofa.com

Request

```
GET /maps/api/js?key=AIzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg&v=weekly&callback=initMap HTTP/1.1
Host: maps.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: */*
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Timing-Allow-Origin: *
```

```
Cross-Origin-Resource-Policy: cross-origin
Vary: Accept-Language
Vary: Origin
Vary: X-Origin
Vary: Referer
Etag: 0911f6db
Content-Type: text/javascript; charset=UTF-8
Cache-Control: public, max-age=1800, stale-while-revalidate=3600
Date: Fri, 29 Nov 2024 00:38:20 GMT
Server: scaffolding on HTTPServer2
Content-Length: 241793
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000


window.google = window.google || {};
google.maps = google.maps || {};
(function() {

var modules = google.maps.modules = {};
google.maps.__gjsload__ = function(name, text) {
modules[name]
...[SNIP]...
/
/*

Copyright 2019 Google LLC
SPDX-License-Identifier: BSD-3-Clause
*/
/*

Copyright 2017 Google LLC
SPDX-License-Identifier: BSD-3-Clause
*/
/*

Math.uuid.js (v1.4)
http://www.broofa.com
mailto:robert@broofa.com
Copyright (c) 2010 Robert Kieffer
Dual licensed under the MIT and GPL licenses.
*/
var aaa,ma,pa,oa,ta,caa,daa,Na,Ab,Eb,eaa,xc,yc,faa,Hc,Ic,Nc,od,kaa,Od,Fd,Gd,Kd,ce,maa,naa,$d,laa,oaa,le,paa,oe,ne,pe,
...[SNIP]...
```

6.2. https://shelter.app/static/js/main.567d58aa.chunk.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://shelter.app**
Path:	**/static/js/main.567d58aa.chunk.js**

Issue detail

The following email addresses were disclosed in the response:

- mark@gmail.com
- shelterappinfo@gmail.com
- abc@gmail.com
- name@your-nonprofit.org
- ecyehappinfo@gmail.com

Request

```
GET /static/js/main.567d58aa.chunk.js HTTP/2
Host: shelter.app
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://shelter.app/introduce
Accept-Encoding: gzip, deflate, br
Priority: u=1
```

Response

```
HTTP/2 200 OK
Cache-Control: max-age=3600
Content-Type: text/javascript; charset=utf-8
Etag: "7429dabc8c880321875359b92c8a6672e514ac25b169f509b0e565fbdcf2064e-br"
Last-Modified: Sun, 28 Apr 2024 19:54:20 GMT
Strict-Transport-Security: max-age=31556926
Accept-Ranges: bytes
Date: Fri, 29 Nov 2024 00:38:16 GMT
X-Served-By: cache-yul1970072-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732840697.896654,VS0,VE1
Vary: x-fh-requested-host, accept-encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 302654

(this["webpackJsonpshelter-web"]=this["webpackJsonpshelter-web"]||[]).push([[0],{223:function(e,t,a)
{e.exports=a.p+"static/media/loading.71055614.svg"},24:function(e,t,a){"use strict";a.r(t);var n,r=a
...[SNIP]...
red:!0}),error:b.name}),b.name&&"required"===b.name.type&&r.a.createElement(Gr,null,E("REQUIRED_INPUT_CTA",
{value:E("NAME")})),r.a.createElement(Tc,
{name:"email",type:"email",fullWidth:!0,placeholder:"mark@gmail.com",label:E("EMAIL"),validate:f({required:!0,pattern:/^(([^<>
...[SNIP]...
PORT_TITLE")),r.a.createElement("form",{className:t.root,name:"feedback",onSubmit:u((function(e,t)
{t.preventDefault(),c(e)}))},r.a.createElement(Tc,
{name:"email",type:"email",fullWidth:!0,placeholder:"mark@gmail.com",label:o("EMAIL"),validate:l({required:!0,pattern:/^(([^<>
...[SNIP]...
e:"CREATE_FEEDBACK_REQUEST",form:e,message:t("SENT_FEEDBACK_SUCCESSFULLY")}),l("email",""),l("subject",""),l(
"message",""))})),r.a.createElement(Tc,
{name:"email",type:"email",fullWidth:!0,placeholder:"mark@gmail.com",label:t("EMAIL"),validate:c({required:!0,pattern:/^(([^<>
...[SNIP]...
!1),t.preventDefault(),Ol(e.email).then((function(e){404===e.code?f(!0):200===e.code&&
(m("email",""),f(!1),i(!0)),h(!1)}))}))},r.a.createElement(Tc,
{name:"email",type:"email",fullWidth:!0,placeholder:"mark@gmail.com",label:t("EMAIL"),validate:s({required:!0,pattern:/^(([^<>
```

```
...[SNIP]...
otalServices}),p.totalServices&&"min"===p.totalServices.type&&r.a.createElement(Gr,null,t("MINIMUM_TOTAL_SERVICE",
{value:1}))),r.a.createElement(Tc,
{name:"email",type:"email",fullWidth:!0,placeholder:"mark@gmail.com",label:t("EMAIL"),validate:E,error:p.email,disabled:!0}),r.
a.createElement(Tc,{name:"createdAt",type:"string",fullWidth:!0,placeholder:"",label:t("CREATED_AT"),value:_()
(c.createdAt).format("MM/DD/YYY
...[SNIP]...
playName&&"required"===u.displayName.type&&r.a.createElement(Gr,null,t("REQUIRED_INPUT_CTA",
{value:t("DISPLAY_NAME_SIGNUP")})),r.a.createElement(Tc,
{name:"email",type:"email",fullWidth:!0,placeholder:"mark@gmail.com",label:t("EMAIL"),validate:s,error:u.email,disabled:!0}),r.a
.createElement(Tc,{name:"phone",type:"phonenumber",fullWidth:!0,placeholder:"(303) 555-
0100",label:t("PHONE"),validate:s({required:!1}),erro
...[SNIP]...
```

6.3. https://www.googletagmanager.com/gtag/js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://www.googletagmanager.com**
Path:	**/gtag/js**

Issue detail

The following email addresses were disclosed in the response:

- em.test@example.com
- test@example.com

Request

```
GET /gtag/js?l=dataLayer&id=G-WMS317DV0H HTTP/1.1
Host: www.googletagmanager.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: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: application/javascript; charset=UTF-8
Access-Control-Allow-Origin: *
```

Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Cache-Control
Vary: Accept-Encoding
Date: Fri, 29 Nov 2024 00:38:30 GMT
Expires: Fri, 29 Nov 2024 00:38:30 GMT
Cache-Control: private, max-age=900
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cross-Origin-Resource-Policy: cross-origin
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri https://csp.withgoogle.com/csp/scaffolding/ascgcycc:838:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/scaffolding/ascgcycc:838:0"}],}
Server: Google Tag Manager
Content-Length: 361509
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

// Copyright 2012 Google Inc. All rights reserved.

(function(){

var data = {
"resource": {
"version":"1",

"macros":[{"function":"__e"},{"function":"__c","vtp_value":"google.ca"},{"function"
...[SNIP]...
,g),!0)}else f===5?a==="conversion"?d():a==="user_data_web"&&d():f!==6&&f!==7||a!=="conversion"||d()},Ow=function(a,b){if(a===0)return ni(b,!1);if(a===1)return ni(b,!0,!0);if(a===2)return li({Gb:"tv.1~em.test@example.com~fn.Fake~ln.Name~co.US~sa.123 Fake St~ct.Non-Applicable~pn.+1234567890~pc.12345~rg.ca",
Ld:9,mg:!1},!0)},Qw=function(a,b){var c,d;if(a==="user_data_web"){var e=b.metadata.split_experiment_arm;if(e===6|
...[SNIP]...

---

7. Cacheable HTTPS response

There are 12 instances of this issue:

- https://api.shelter.app/bot/query
- https://api.shelter.app/services/search-city-or-zip
- https://firebase.googleapis.com/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig
- https://firebaseinstallations.googleapis.com/v1/projects/shelterapp-1573928197721/installations
- https://maps.googleapis.com/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo
- https://maps.googleapis.com/maps/api/mapsjs/gen_204
- https://shelter.app/introduce
- https://shelter.app/static/js/2.d1660a62.chunk.js
- https://shelter.app/static/js/main.567d58aa.chunk.js
- https://shelter.app/static/media/Harabara.4f6ec3a7.otf
- https://shelter.app/static/media/loading.71055614.svg
- https://shelter.app/static/media/pinBRed.20bf45a0.svg

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

7.1. https://api.shelter.app/bot/query

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.shelter.app**
Path:	**/bot/query**

Request

```
POST /bot/query HTTP/1.1
Host: api.shelter.app
Content-Length: 84
Sec-Ch-Ua-Platform: "Windows"
Authorization: Bearer undefined
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
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: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Origin: https://shelter.app
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
```

```
{"query":"Hi","chatToken":"0.2pck29o1geo","location":"Montr..al","userTimezone":300}
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 29 Nov 2024 00:42:23 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 1292
Connection: keep-alive
X-Powered-By: Express
Access-Control-Allow-Origin: *
ETag: W/"50c-iAa5TqsKyWU0AD5P+oWUzMKCB58"

[{"platform":"PLATFORM_UNSPECIFIED","text":{"text":["Hi there! I'm Mandy, ShelterApp chatbot. How can I help you today?"]},"message":"text"},{"platform":"PLATFORM_UNSPECIFIED","payload":{"fields":{"qu
...[SNIP]...
```

7.2. https://api.shelter.app/services/search-city-or-zip

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api.shelter.app**
Path:	**/services/search-city-or-zip**

Request

```
POST /services/search-city-or-zip HTTP/1.1
Host: api.shelter.app
Content-Length: 22
Sec-Ch-Ua-Platform: "Windows"
Authorization: Bearer undefined
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
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: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Origin: https://shelter.app
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive

{"keyword":"montreal"}
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 29 Nov 2024 00:40:04 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 263
Connection: keep-alive
X-Powered-By: Express
Access-Control-Allow-Origin: *
ETag: W/"107-crUmDu8ljiKDN4oRHFz4O27AAQk"

{"cities":[{"location":{"type":"Point","coordinates":[-73.5649053,45.5177314]},"name":"Montr..al","state":"QC","search":"Montr..al
QC","createdAt":"2020-01-22T04:09:50.005Z","notes":"Migrated from Str
...[SNIP]...
```

7.3. https://firebase.googleapis.com/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://firebase.googleapis.com**
Path:	**/v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig**

Request

```
OPTIONS /v1alpha/projects/-/apps/1:972668199767:web:5a26a58131cd21925b1412/webConfig HTTP/1.1
Host: firebase.googleapis.com
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: x-goog-api-key
Origin: https://shelter.app
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://shelter.app/
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
Access-Control-Allow-Origin: https://shelter.app
Vary: origin
Vary: referer
Vary: x-origin
Access-Control-Allow-Methods: DELETE,GET,HEAD,OPTIONS,PATCH,POST,PUT
Access-Control-Allow-Headers: x-goog-api-key
Access-Control-Max-Age: 3600
```

```
Date: Fri, 29 Nov 2024 00:38:20 GMT
Content-Type: text/html
Server: ESF
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

7.4. https://firebaseinstallations.googleapis.com/v1/projects/shelterapp-1573928197721/installations

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://firebaseinstallations.googleapis.com**
Path:	**/v1/projects/shelterapp-1573928197721/installations**

Request

```
OPTIONS /v1/projects/shelterapp-1573928197721/installations HTTP/1.1
Host: firebaseinstallations.googleapis.com
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type,x-goog-api-key
Origin: https://shelter.app
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://shelter.app/
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
Access-Control-Allow-Origin: https://shelter.app
Vary: origin
Vary: referer
Vary: x-origin
Access-Control-Allow-Methods: DELETE,GET,HEAD,OPTIONS,PATCH,POST,PUT
Access-Control-Allow-Headers: content-type,x-goog-api-key
Access-Control-Max-Age: 3600
Date: Fri, 29 Nov 2024 00:38:20 GMT
Content-Type: text/html
Server: ESF
Content-Length: 0
X-Xss-Protection: 0
```

```
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

7.5. https://maps.googleapis.com/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo**

Request

```
OPTIONS /$rpc/google.internal.maps.mapsjs.v1.MapsJsInternalService/GetViewportInfo HTTP/2
Host: maps.googleapis.com
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type,x-goog-api-key,x-goog-maps-api-salt,x-goog-maps-api-signature,x-goog-maps-channel-id,x-goog-maps-client-id,x-user-agent
Origin: https://shelter.app
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://shelter.app/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Access-Control-Allow-Origin: https://shelter.app
Vary: origin
Vary: referer
Vary: x-origin
Access-Control-Allow-Methods: DELETE,GET,HEAD,OPTIONS,PATCH,POST,PUT
Access-Control-Allow-Headers: content-type,x-goog-api-key,x-goog-maps-api-salt,x-goog-maps-api-signature,x-goog-maps-channel-id,x-goog-maps-client-id,x-user-agent
Access-Control-Max-Age: 3600
Date: Fri, 29 Nov 2024 00:41:10 GMT
Content-Type: text/html
Server: scaffolding on HTTPServer2
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
```

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

7.6. https://maps.googleapis.com/maps/api/mapsjs/gen_204

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://maps.googleapis.com**
Path:	**/maps/api/mapsjs/gen_204**

Request

```
GET /maps/api/mapsjs/gen_204?csp_test=true HTTP/2
Host: maps.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: */*
Origin: https://shelter.app
X-Client-Data: CIjcygE=
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shelter.app/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=UTF-8
Vary: Origin
Vary: X-Origin
Vary: Referer
Date: Fri, 29 Nov 2024 00:38:22 GMT
Server: scaffolding on HTTPServer2
Content-Length: 3
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: https://shelter.app
Access-Control-Expose-Headers: vary,vary,vary,content-encoding,date,server,content-length
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{}
```

7.7. https://shelter.app/introduce

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://shelter.app**
Path:	**/introduce**

Request

```
GET /introduce HTTP/1.1
Host: shelter.app
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
Cache-Control: max-age=3600
Content-Type: text/html; charset=utf-8
Etag: "e7282bd09cd4a8597655085b53c5b38e7867801b0d6023239e3e053d32df7345-br"
Last-Modified: Sun, 28 Apr 2024 19:54:20 GMT
Strict-Transport-Security: max-age=31556926
Accept-Ranges: bytes
Date: Fri, 29 Nov 2024 00:38:16 GMT
X-Served-By: cache-yul1970072-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732840697.630908,VS0,VE1
Vary: x-fh-requested-host, accept-encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 2650

<!doctype html><html lang="en"><head><meta charset="utf-8"/><meta content="https://shelter.app/favicon1.png"
name="og:image"/><meta content="https://shelter.app" name="og:url"/><link rel="shortcut ico
...[SNIP]...
```

7.8. https://shelter.app/static/js/2.d1660a62.chunk.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://shelter.app**
Path:	**/static/js/2.d1660a62.chunk.js**

Request

```
GET /static/js/2.d1660a62.chunk.js HTTP/2
Host: shelter.app
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://shelter.app/introduce
Accept-Encoding: gzip, deflate, br
Priority: u=1
```

Response

```
HTTP/2 200 OK
Cache-Control: max-age=3600
Content-Type: text/javascript; charset=utf-8
Etag: "d170eebf68aacc7c222f492e175855ccc0d25c6b1363d6cec0911136b4963840-br"
Last-Modified: Sun, 28 Apr 2024 19:54:20 GMT
Strict-Transport-Security: max-age=31556926
Accept-Ranges: bytes
Date: Fri, 29 Nov 2024 00:38:16 GMT
X-Served-By: cache-yul1970072-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732840697.894979,VS0,VE1
Vary: x-fh-requested-host, accept-encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 2184142

/*! For license information please see 2.d1660a62.chunk.js.LICENSE.txt */
(this["webpackJsonpshelter-web"]=this["webpackJsonpshelter-web"]||[]).push([[2],[function(e,t,n){"use strict";e.exports=n(502)
...[SNIP]...
```

7.9. https://shelter.app/static/js/main.567d58aa.chunk.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://shelter.app**

Path: **/static/js/main.567d58aa.chunk.js**

Request

```
GET /static/js/main.567d58aa.chunk.js HTTP/2
Host: shelter.app
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://shelter.app/introduce
Accept-Encoding: gzip, deflate, br
Priority: u=1
```

Response

```
HTTP/2 200 OK
Cache-Control: max-age=3600
Content-Type: text/javascript; charset=utf-8
Etag: "7429dabc8c880321875359b92c8a6672e514ac25b169f509b0e565fbdcf2064e-br"
Last-Modified: Sun, 28 Apr 2024 19:54:20 GMT
Strict-Transport-Security: max-age=31556926
Accept-Ranges: bytes
Date: Fri, 29 Nov 2024 00:38:16 GMT
X-Served-By: cache-yul1970072-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732840697.896654,VS0,VE1
Vary: x-fh-requested-host, accept-encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 302654

(this["webpackJsonpshelter-web"]=this["webpackJsonpshelter-web"]||[]).push([[0],{223:function(e,t,a)
{e.exports=a.p+"static/media/loading.71055614.svg"},24:function(e,t,a){"use strict";a.r(t);var n,r=a
...[SNIP]...
```

7.10. https://shelter.app/static/media/Harabara.4f6ec3a7.otf

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://shelter.app**

Path: **/static/media/Harabara.4f6ec3a7.otf**

Request

```
GET /static/media/Harabara.4f6ec3a7.otf HTTP/2
Host: shelter.app
Cookie: _ga_WMS317DV0H=GS1.1.1732840710.1.0.1732840710.0.0.0; _ga=GA1.1.230453292.1732840711;
%40shelter_alreadyaccess=true
Origin: https://shelter.app
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: cors
Sec-Fetch-Dest: font
Referer: https://shelter.app/static/css/main.b98a6694.chunk.css
Accept-Encoding: gzip, deflate, br
Priority: u=0
```

Response

```
HTTP/2 200 OK
Cache-Control: max-age=3600
Content-Type: font/otf
Etag: "0b3efb4561f866e36dea29357c5fd90d037655f97d3d076c3471003d45bfaa2c-br"
Last-Modified: Sun, 28 Apr 2024 19:54:20 GMT
Strict-Transport-Security: max-age=31556926
Accept-Ranges: bytes
Date: Fri, 29 Nov 2024 00:39:33 GMT
X-Served-By: cache-yul1970071-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732840774.808070,VS0,VE1
Vary: x-fh-requested-host, accept-encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 66748

OTTO......PCFF w..K........FFTM.......L....GDEF..... GPOS...m.....
  nGSUB.....0OS/2...W...@...`cmap%D.T...X....head..4........6hhea.5.........$hmtx.@ ...h...Rmaxp..P....8....name.....
...[SNIP]...
```

7.11. https://shelter.app/static/media/loading.71055614.svg

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://shelter.app**

Path: **/static/media/loading.71055614.svg**

Request

```
GET /static/media/loading.71055614.svg HTTP/2
Host: shelter.app
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://shelter.app/introduce
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
```

Response

```
HTTP/2 200 OK
Cache-Control: max-age=3600
Content-Type: image/svg+xml
Etag: "49bc8fa3285b11e344877a0a579ad54e99fae36287348d88502e76a9738caa81-br"
Last-Modified: Sun, 28 Apr 2024 19:54:20 GMT
Strict-Transport-Security: max-age=31556926
Accept-Ranges: bytes
Date: Fri, 29 Nov 2024 00:38:20 GMT
X-Served-By: cache-yul1970072-YUL
X-Cache: HIT
X-Cache-Hits: 0
X-Timer: S1732840701.877265,VS0,VE1
Vary: x-fh-requested-host, accept-encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 3062

<svg width='118px' height='118px' xmlns="http://www.w3.org/2000/svg" viewBox="0 0 100 100"
preserveAspectRatio="xMidYMid" class="uil-default"><rect x="0" y="0" width="100" height="100" fill="none" cla
...[SNIP]...
```

7.12. https://shelter.app/static/media/pinBRed.20bf45a0.svg

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://shelter.app**

Path: **/static/media/pinBRed.20bf45a0.svg**

Request

```
GET /static/media/pinBRed.20bf45a0.svg HTTP/2
Host: shelter.app
Cookie: _ga_WMS317DV0H=GS1.1.1732840710.1.0.1732840710.0.0.0; _ga=GA1.1.230453292.1732840711;
%40shelter_alreadyaccess=true
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://shelter.app/services/6052197226d8ce31cc4d48a7
Accept-Encoding: gzip, deflate, br
Priority: i
```

Response

```
HTTP/2 200 OK
Cache-Control: max-age=3600
Content-Type: image/svg+xml
Etag: "217bdb7129e941426384e92a27011cd51d6509c078f4f4b9bca8c2bd58e10707-br"
Last-Modified: Sun, 28 Apr 2024 19:54:20 GMT
Strict-Transport-Security: max-age=31556926
Accept-Ranges: bytes
Date: Fri, 29 Nov 2024 00:40:47 GMT
X-Served-By: cache-yul1970056-YUL
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1732840848.520067,VS0,VE125
Vary: x-fh-requested-host, accept-encoding
Alt-Svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Length: 1363

<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 20010904//EN"
"http://www.w3.org/TR/2001/REC-SVG-20010904/DTD/svg10.dtd">
<svg version="1.0" xmlns="http://www.w3.org/2000/
...[SNIP]...
```

Report generated by Burp Suite web vulnerability scanner v2024.9.5, at Thu Nov 28 19:50:10 EST 2024.