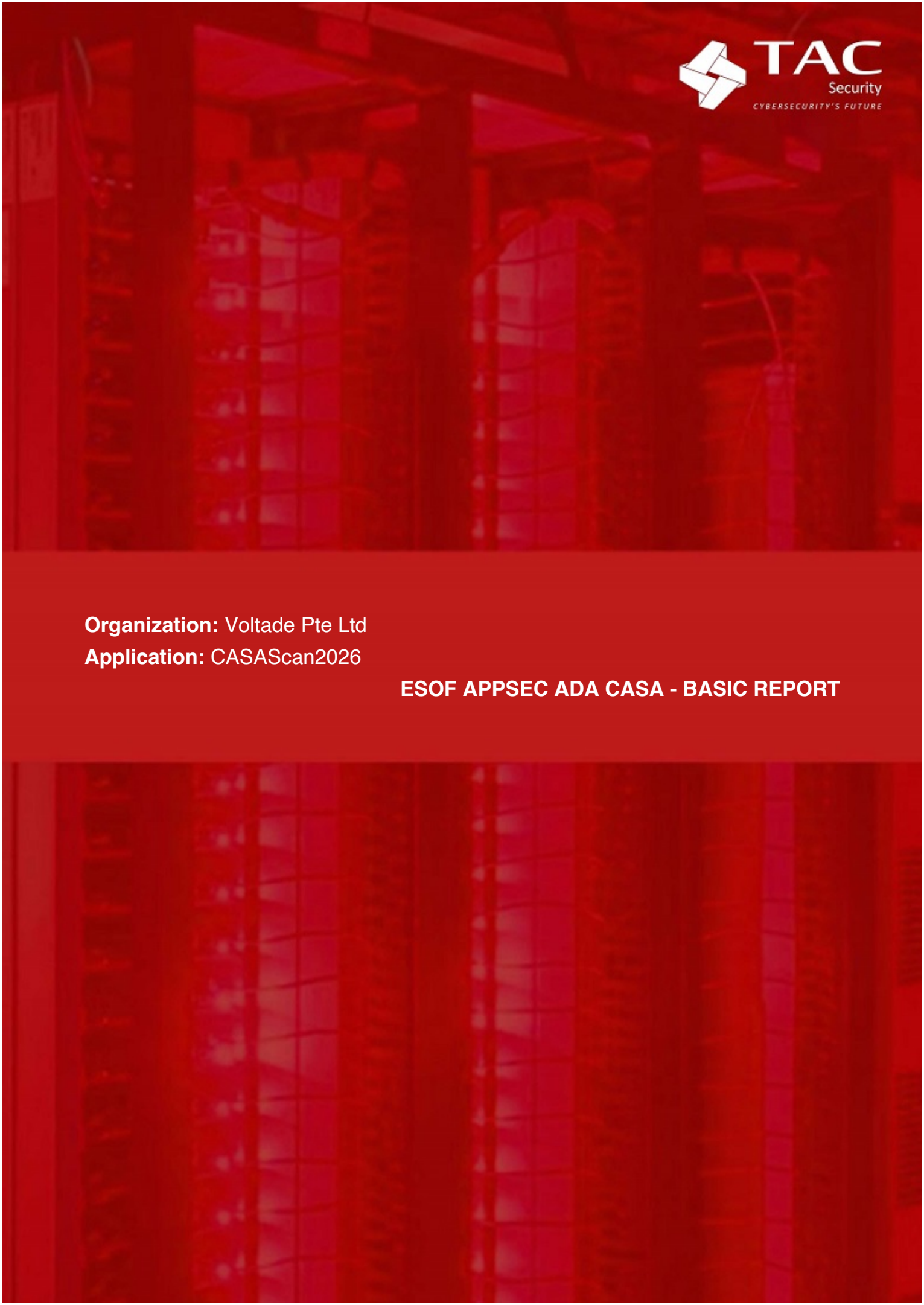


Organization: Voltade Pte Ltd

Application: CASAScan2026

ESOF APPSEC ADA CASA - BASIC REPORT



Security is in Our DNA

1st Largest Auditor

Market share (almost 100%) of UPI assessment.

2nd Largest Financial Institution

Of countries application assessor.

3rd Largest telecom Company's

End to end security assessor.

Fortune 500

Oil and Gas company is protected by us.

10 Billion Transactions

Assessed on more than 200+ banking applications.

Top Fortune 500

Companies vulnerabilities have been managed by ESOF AppSec ADA.

Executive Summary

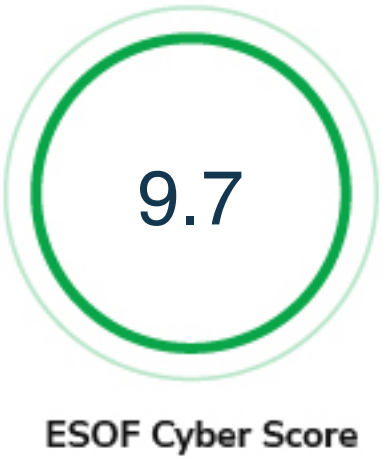
CASA has built upon the industry-recognized standards of the OWASP's Application Security Verification Standard (ASVS) to provide a consistent set of requirements to harden security for any application. Further, CASA provides a uniform way to perform trusted assurance assessments of these requirements when such assessments are required for applications with potential access to sensitive data.

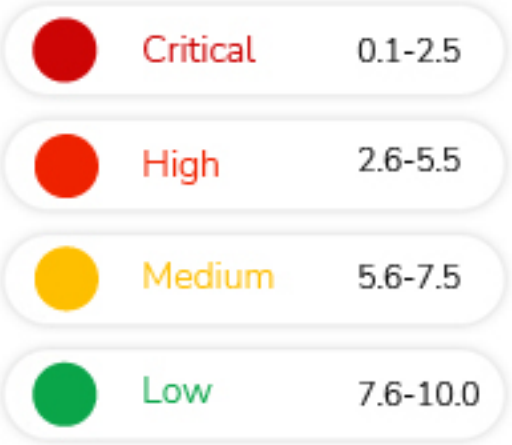
There is no "one size fits all solution" when it comes to evaluating application risk to securing user data. The CASA assessment acknowledges this reality and is adapted with a risk-based, multi-tier assessment approach to evaluate application risk based on user, scope, and other application specific items.

Risk Classification

Critical Risk	These vulnerabilities can allow attackers to take complete control of your web applications and web servers. In exploiting this type of vulnerability, attackers could carry out a range of malicious acts.
High Risk	A High severity vulnerability, which means that on exploiting such vulnerabilities, attackers, can view information about your system that helps them find or exploit other vulnerabilities that enable them to access sensitive user and administrator information.
Medium Risk	Potential weakness in controls, which could develop into an exposure. Or Issues that represent areas of concern and may impact controls. They should be addressed reasonably promptly.
Low Risk	Potential weaknesses in controls, which in combination with other weaknesses can develop into exposure. Suggested improvements not immediately/directly affecting controls.
Info Risk	Weaknesses mentioned under these sections are informational and are best practices. Either these weaknesses cannot be exploited directly or are very difficult to exploit due to multiple constrains.

ESOF AppSec ADA Cyber Score Classification





Target

- **Title:** CASAScan2026
- **Source:** https://envoy-crm.voltade.com

Testing Details

Start Date	Feb 2, 2026 05:25:51
Finish Date	Feb 20, 2026 07:17:49
Revalidation Date	Feb 20, 2026

Observation Summary

Sr. No.	Vulnerabilities	Severity	Status
1	Proxy Disclosure	Low	Patched
2	Permissions Policy Header Not Set	Info	Patched
3	Cookie Slack Detector	Info	Patched
4	Cookie Without Secure Flag	Info	Patched
5	HTTPS Content Available via HTTP	Info	Patched
6	Timestamp Disclosure - Unix	Info	Patched
7	Information Disclosure - Suspicious Comments	Info	Patched
8	Session Management Response Identified	Info	Patched
9	Storable but Non-Cacheable Content	Info	Patched
10	Re-examine Cache-control Directives	Info	Patched
11	User Agent Fuzzer	Info	Patched

Note: All the vulnerabilities need to be patched to pass the CASA Tier 2 & Tier 3 assessments.

1 Proxy Disclosure

Severity Level: Low

CWEID: 204

Status: Patched

Description:

1 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine

- A list of targets for an attack against the application.

- Potential vulnerabilities on the proxy servers that service the application.

- The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated.

Vulnerable URL

https://envoy-crm.voltade.com

Remedies:

Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server.
Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing).
Configure the web and application servers with custom error pages, to prevent 'fingerprintable' product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages.
Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers.

Evidence Url:

```
https://envoy-crm.voltade.com
```

Evidence Response:

```
Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - cloudflare The following web/application server has been identified: - cloudflare
https://envoy-crm.voltade.com/
Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - cloudflare The following web/application server has been identified: - cloudflare
https://envoy-crm.voltade.com/apple-icon-114x114.png
Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - cloudflare The following web/application server has been identified: - cloudflare
https://envoy-crm.voltade.com/apple-icon-120x120.png
Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - cloudflare The following web/application server has been identified: - cloudflare
https://envoy-crm.voltade.com/apple-icon-144x144.png
```

Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - cloudflare The following web/application server has been identified: - cloudflare

https://envoy-crm.voltade.com/

Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - cloudflare The following web/application server has been identified: - cloudflare

https://envoy-crm.voltade.com/android-icon-192x192.png

Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - cloudflare The following web/application server has been identified: - cloudflare

https://envoy-crm.voltade.com/apple-icon-114x114.png

Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - cloudflare The following web/application server has been identified: - cloudflare

https://envoy-crm.voltade.com/apple-icon-120x120.png

Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - cloudflare The following web/application server has been identified: - cloudflare

https://envoy-crm.voltade.com/apple-icon-144x144.png

Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - cloudflare The following web/application server has been identified: - cloudflare

Reference:
https://datatracker.ietf.org/doc/html/rfc7231#section-5.1.2

2 Permissions Policy Header Not Set

Severity Level: Info

CWEID: 693

Status: Patched

Description:

Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.

Vulnerable URL

https://envoy-crm.voltade.com

Remedies:

Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.

Evidence Url:

https://envoy-crm.voltade.com
https://envoy-crm.voltade.com/
https://envoy-crm.voltade.com/apple-icon-57x57.png
https://envoy-crm.voltade.com/apple-icon-72x72.png
https://envoy-crm.voltade.com/apple-icon-76x76.png
https://envoy-crm.voltade.com/robots.txt
https://envoy-crm.voltade.com/vite/assets/DashboardIcon-DOyOypg7.css
https://envoy-crm.voltade.com
https://envoy-crm.voltade.com/
https://envoy-crm.voltade.com
https://envoy-crm.voltade.com/
https://envoy-crm.voltade.com
https://envoy-crm.voltade.com/
https://envoy-crm.voltade.com/vite/assets/_commonjsHelpers-BosuxZz1.js
https://envoy-crm.voltade.com/vite/assets/index-saaBvr-j.js
https://envoy-crm.voltade.com/vite/assets/messages-Cv5GNJOJ.js
https://envoy-crm.voltade.com
https://envoy-crm.voltade.com/
https://envoy-crm.voltade.com
https://envoy-crm.voltade.com/
https://envoy-crm.voltade.com
https://envoy-crm.voltade.com/
https://envoy-crm.voltade.com
https://envoy-crm.voltade.com/
https://envoy-crm.voltade.com/apple-icon-60x60.png

`https://envoy-crm.voltade.com/robots.txt`
`https://envoy-crm.voltade.com/vite/assets/dashboard-i892xZS8.css`
`https://envoy-crm.voltade.com`
`https://envoy-crm.voltade.com/`
`https://envoy-crm.voltade.com/vite/assets/_plugin-vue_export-helper-DoIZy9Q9.js`
`https://envoy-crm.voltade.com/vite/assets/dashboard-CUhgxdwf.js`
`https://envoy-crm.voltade.com/vite/assets/index-BtuGy7By.js`

Reference:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Permissions-Policy
https://developer.chrome.com/blog/feature-policy/
https://scotthelme.co.uk/a-new-security-header-feature-policy/
https://w3c.github.io/webappsec-feature-policy/
https://www.smashingmagazine.com/2018/12/feature-policy/

3 Cookie Slack Detector

Severity Level: Info

CWEID: 205

Status: Patched

Description:

Repeated GET requests: drop a different cookie each time, followed by normal request with all cookies to stabilize session, compare responses against original baseline GET. This can reveal areas where cookie based authentication/attributes are not actually enforced.

Vulnerable URL

https://envoy-crm.voltade.com

Evidence Url:

```
https://envoy-crm.voltade.com/
```

Evidence Response:

```
NOTE: Because of its name this cookie may be important, but dropping it appears to have no
effect: [_chatwoot_session] Cookies that don't have expected effects can reveal flaws in
application logic. In the worst case, this can reveal where authentication via cookie
token(s) is not actually enforced. These cookies affected the response: These cookies did NOT
affect the response: _chatwoot_session
https://envoy-crm.voltade.com/android-icon-192x192.png
NOTE: Because of its name this cookie may be important, but dropping it appears to have no
effect: [_chatwoot_session] Cookies that don't have expected effects can reveal flaws in
application logic. In the worst case, this can reveal where authentication via cookie
token(s) is not actually enforced. These cookies affected the response: These cookies did NOT
affect the response: _chatwoot_session
https://envoy-crm.voltade.com/apple-icon-114x114.png
NOTE: Because of its name this cookie may be important, but dropping it appears to have no
effect: [_chatwoot_session] Cookies that don't have expected effects can reveal flaws in
application logic. In the worst case, this can reveal where authentication via cookie
token(s) is not actually enforced. These cookies affected the response: These cookies did NOT
affect the response: _chatwoot_session
https://envoy-crm.voltade.com/apple-icon-120x120.png
NOTE: Because of its name this cookie may be important, but dropping it appears to have no
effect: [_chatwoot_session] Cookies that don't have expected effects can reveal flaws in
application logic. In the worst case, this can reveal where authentication via cookie
token(s) is not actually enforced. These cookies affected the response: These cookies did NOT
affect the response: _chatwoot_session
https://envoy-crm.voltade.com/apple-icon-144x144.png
NOTE: Because of its name this cookie may be important, but dropping it appears to have no
effect: [_chatwoot_session] Cookies that don't have expected effects can reveal flaws in
application logic. In the worst case, this can reveal where authentication via cookie
token(s) is not actually enforced. These cookies affected the response: These cookies did NOT
affect the response: _chatwoot_session
```

https://envoy-crm.voltade.com
NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [_chatwoot_session] Cookies that don't have expected effects can reveal flaws in application logic. In the worst case, this can reveal where authentication via cookie token(s) is not actually enforced. These cookies affected the response: These cookies did NOT affect the response: _chatwoot_session
https://envoy-crm.voltade.com/android-icon-192x192.png
NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [_chatwoot_session] Cookies that don't have expected effects can reveal flaws in application logic. In the worst case, this can reveal where authentication via cookie token(s) is not actually enforced. These cookies affected the response: These cookies did NOT affect the response: _chatwoot_session
https://envoy-crm.voltade.com/apple-icon-114x114.png
NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [_chatwoot_session] Cookies that don't have expected effects can reveal flaws in application logic. In the worst case, this can reveal where authentication via cookie token(s) is not actually enforced. These cookies affected the response: These cookies did NOT affect the response: _chatwoot_session
https://envoy-crm.voltade.com/apple-icon-120x120.png
NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [_chatwoot_session] Cookies that don't have expected effects can reveal flaws in application logic. In the worst case, this can reveal where authentication via cookie token(s) is not actually enforced. These cookies affected the response: These cookies did NOT affect the response: _chatwoot_session
https://envoy-crm.voltade.com/apple-icon-144x144.png
NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [_chatwoot_session] Cookies that don't have expected effects can reveal flaws in application logic. In the worst case, this can reveal where authentication via cookie token(s) is not actually enforced. These cookies affected the response: These cookies did NOT affect the response: _chatwoot_session

Reference:
https://cwe.mitre.org/data/definitions/205.html

4 Cookie Without Secure Flag

Severity Level: Info

CWEID: 614

Status: Patched

Description:

A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Vulnerable URL

https://envoy-crm.voltade.com

Remedies:

Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Evidence Url:

```
https://envoy-crm.voltade.com
Set-Cookie: _chatwoot_session
https://envoy-crm.voltade.com/
Set-Cookie: _chatwoot_session
https://envoy-crm.voltade.com
Set-Cookie: _chatwoot_session
https://envoy-crm.voltade.com/
Set-Cookie: _chatwoot_session
```

Reference:

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

5 HTTPS Content Available via HTTP

Severity Level: Info

CWEID: 311

Status: Patched

Description:

Content which was initially accessed via HTTPS (i.e.: using SSL/TLS encryption) is also accessible via HTTP (without encryption).

Vulnerable URL

https://envoy-crm.voltade.com

Remedies:

Ensure that your web server, application server, load balancer, etc. is configured to only serve such content via HTTPS. Consider implementing HTTP Strict Transport Security.

Evidence Url:

`https://envoy-crm.voltade.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js`
`http://envoy-crm.voltade.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js`

Evidence Response:

`ZAP attempted to connect via:`
`http://envoy-crm.voltade.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js`
`https://envoy-crm.voltade.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js`
`http://envoy-crm.voltade.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js`
`ZAP attempted to connect via:`
`http://envoy-crm.voltade.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js`

Reference:

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

6 Timestamp Disclosure - Unix

Severity Level: Info

CWEID: 497

Status: Patched

Description:

A timestamp was disclosed by the application/web server. - Unix

Vulnerable URL

https://envoy-crm.voltade.com

Remedies:
Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Evidence Url:

```
https://envoy-crm.voltade.com/vite/assets/index-DVeFQc8H.js
1473231341
```

Evidence Response:

```
1473231341, which evaluates to: 2016-09-07 06:55:41.
https://envoy-crm.voltade.com/vite/assets/index-DVeFQc8H.js
1770035416
1770035416, which evaluates to: 2026-02-02 12:30:16.
https://envoy-crm.voltade.com/vite/assets/index-DVeFQc8H.js
1804603682
1804603682, which evaluates to: 2027-03-09 14:48:02.
https://envoy-crm.voltade.com/vite/assets/index-DVeFQc8H.js
1958414417
1958414417, which evaluates to: 2032-01-22 20:00:17.
https://envoy-crm.voltade.com/vite/assets/index-DVeFQc8H.js
1990404162
1990404162, which evaluates to: 2033-01-27 02:02:42.
https://envoy-crm.voltade.com/vite/assets/dashboard-CUhgxdwf.js
1712123232
1712123232, which evaluates to: 2024-04-03 05:47:12.
https://envoy-crm.voltade.com/vite/assets/dashboard-CUhgxdwf.js
1712123233
1712123233, which evaluates to: 2024-04-03 05:47:13.
https://envoy-crm.voltade.com/vite/assets/dashboard-CUhgxdwf.js
1729205669
1729205669, which evaluates to: 2024-10-17 22:54:29.
https://envoy-crm.voltade.com/vite/assets/dashboard-CUhgxdwf.js
1729732500
1729732500, which evaluates to: 2024-10-24 01:15:00.
https://envoy-crm.voltade.com/vite/assets/dashboard-CUhgxdwf.js
1729775588
```

```
1729775588, which evaluates to: 2024-10-24 13:13:08.
```

Reference:
https://cwe.mitre.org/data/definitions/200.html

7 Information Disclosure - Suspicious Comments

Severity Level: Info

CWEID: 615

Status: Patched

Description:

The response appears to contain suspicious comments which may help an attacker.

Vulnerable URL

https://envoy-crm.voltade.com

Remedies:
Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Evidence Url:

https://envoy-crm.voltade.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket -loader.min.js
from

Evidence Response:

The following pattern was used: \bFROM\b and was detected in likely comment: "//www.w3.org/2000/svg",E={"application/ecmascript":!0,"application/javascript":!0,"application/x-ecmascript":!0,"application/x-j", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/DashboardIcon-8ZzeG_Yc.js
query
The following pattern was used: \bQUERY\b and was detected in likely comment: "//www.w3.org/2000/svg",width:"24",height:"24",viewBox:"0 0 24 24",fill:"none",stroke:"currentColor","stroke-width":"2 ","stroke-l", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/MessageFormatter-Dgp1jRx5.js
xxx
The following pattern was used: \bXXX\b and was detected in likely comment: "//":{validate:function(t,n,r){var e=t.slice(n);return r.re.no_http||(r.re.no_http=new RegExp("^"+r.re.src_auth+"(?:localhost|(?:", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/_plugin-vue_export-helper-DoIZy9Q9.js
select
The following pattern was used: \bSELECT\b and was detected in likely comment: "//! #__NO_SIDE_EFFECTS__ */function Ze(e){const t=Object.create(null);for(const s of e.split(","))t[s]=1;return s=>s in t}const", see evidence field for the suspicious comment/snippet.*
https://envoy-crm.voltade.com/vite/assets/dashboard-BxHAGpM9.js
TODO
The following pattern was used: \bTODO\b and was detected in likely comment: "//;return e.binary&&(e.begin=Pr(t,/.\b/,e.binary,/\b.*/)),bi({scope:"meta",begin:t,end*

:/$/,relevance:0,"on:begin":(n,s)=>{n.ind", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/globalConfig-BSmsGLII.js
debug
The following pattern was used: \bDEBUG\b and was detected in likely comment: "//next.vuex.vuejs.org/",logo:"https://vuejs.org/images/icons/favicon-96x96.png",packageName:"vuex",componentStateTypes:[Zu]},fun", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/index-BJHz0Nkb.js
XXX
The following pattern was used: \bXXX\b and was detected in likely comment: "//example.com");return n.hash=e,n.hash?n.hash.substring(1,n.hash.length):""}function KC(e,t){if(e=_n(e,"?"),t||e==="")return e;l", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/index-BtuGy7By.js
user
The following pattern was used: \bUSER\b and was detected in likely comment: "//localhost",Jt=Object.freeze(Object.defineProperty({__proto__:null,hasBrowserEnv:ue,hasStandardBrowserEnv:Mt,hasStandardBrowser", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/index-DVeFQc8H.js
todo
The following pattern was used: \bTODO\b and was detected in likely comment: "//".concat(this.host,"/m"),[2,dt(n,{headers:r,body:JSON.stringify(t),method:"POST"})]})})},e}(),je,Wt=function(e){J(t,e);functio", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/typing-BJhnH_67.js
from
The following pattern was used: \bFROM\b and was detected in likely comment: "//prosemirror.net/docs/guide/#generatable")}}function pu(t){let e=Object.create(null);for(let n in t){let i=t[n];if(!i.hasDefau", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/uuid-CEPYGtho.js
query
The following pattern was used: \bQUERY\b and was detected in likely comment: "//g,oi=/=/g,si=/\?/g,er=/\+/g,ci=/%5B/g,ui=/%5D/g,tr=/%5E/g,li=/%60/g,nr=/%7B/g,di=/%7C/g,rr=/%7D/g,fi=/%20/g;function zt(e){ret", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/vue-dompurify-html-DajrD5x3.js
from
The following pattern was used: \bFROM\b and was detected in likely comment: "//www.w3.org/1998/Math/MathML",re="http://www.w3.org/2000/svg",M="http://www.w3.org/1999/xhtml";let z=M,Le=!1,ye=null;const kt=l", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js
from
The following pattern was used: \bFROM\b and was detected in likely comment: "//www.w3.org/2000/svg",E={"application/ecmascript":!0,"application/javascript":!0,"application/x-ecmascript":!0,"application/x-j", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/DashboardIcon-nowfBrOY.js
query
The following pattern was used: \bQUERY\b and was detected in likely comment: "//www.w3.org/2000/svg",width:"24",height:"24",viewBox:"0 0 24

24",fill:"none",stroke:"currentColor","stroke-width":"2 ","stroke-l", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/MessageFormatter-Dgp1jRx5.js
xxx
The following pattern was used: \bXXX\b and was detected in likely comment: "//":{validate:function(t,n,r){var e=t.slice(n);return r.re.no_http||(r.re.no_http=new RegExp("^"+r.re.src_auth+"(?:localhost|(?:", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/_plugin-vue_export-helper-DoIZy9Q9.js
select
The following pattern was used: \bSELECT\b and was detected in likely comment: "//! #__NO_SIDE_EFFECTS__ */function Ze(e){const t=Object.create(null);for(const s of e.split(","))t[s]=1;return s=>s in t}const", see evidence field for the suspicious comment/snippet.*
https://envoy-crm.voltade.com/vite/assets/dashboard-CUhgxdwf.js
TODO
The following pattern was used: \bTODO\b and was detected in likely comment: "//;return e.binary&&(e.begin=Dr(t,/.\b/,e.binary,/\b.*/)),bi({scope:"meta",begin:t,end:/$/,relevance:0,"on:begin":(n,s)=>{n.ind", see evidence field for the suspicious comment/snippet.*
https://envoy-crm.voltade.com/vite/assets/globalConfig-BSmsGLII.js
debug
The following pattern was used: \bDEBUG\b and was detected in likely comment: "//next.vuex.vuejs.org/",logo:"https://vuejs.org/images/icons/favicon-96x96.png",packageName:"vuex",componentStateTypes:[Zu]},fun", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/index-BJHz0Nkb.js
XXX
The following pattern was used: \bXXX\b and was detected in likely comment: "//example.com");return n.hash=e,n.hash?n.hash.substring(1,n.hash.length):""}function KC(e,t){if(e=_n(e,"?"),t||e==="")return e;l", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/index-BtuGy7By.js
user
The following pattern was used: \bUSER\b and was detected in likely comment: "//localhost",Jt=Object.freeze(Object.defineProperty({__proto__:null,hasBrowserEnv:ue,hasStandardBrowserEnv:Mt,hasStandardBrowser", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/typing-BJhnH_67.js
from
The following pattern was used: \bFROM\b and was detected in likely comment: "//prosemirror.net/docs/guide/#generatable")}}function pu(t){let e=Object.create(null);for(let n in t){let i=t[n];if(!i.hasDefau", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/uuid-CEPYGtho.js
query
The following pattern was used: \bQUERY\b and was detected in likely comment: "//g,oi=/=/g,si=/\?/g,er=/\+/g,ci=/%5B/g,ui=/%5D/g,tr=/%5E/g,li=/%60/g,nr=/%7B/g,di=/%7C/g,rr=/%7D/g,fi=/%20/g;function zt(e){ret", see evidence field for the suspicious comment/snippet.
https://envoy-crm.voltade.com/vite/assets/vue-dompurify-html-DajrD5x3.js
from
The following pattern was used: \bFROM\b and was detected in likely comment: "//www.w3.org/1998/Math/MathML",re="http://www.w3.org/2000/svg",M="http://www.w3.org/1999/xhtml";let z=M,Le=!1,ye=null;const kt=l", see evidence field for the

`suspicious comment/snippet.`

8 Session Management Response Identified

Severity Level: Info

CWEID: -1

Status: Patched

Description:

The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Vulnerable URL

https://envoy-crm.voltade.com

Remedies:

This is an informational alert rather than a vulnerability and so there is nothing to fix.

Evidence Url:


```
https://envoy-crm.voltade.com
<script type="ec7a96a3be8056b75f6782b6-text/javascript"> window.chatwootConfig = { hostURL:
'https://envoy-crm.voltade.com', knowledgeBaseURL: '', fbAppId: '1064501834924073',
instagramAppId: '', googleOAuthClientId: '215202957494-
np384n1cef89j8ro528rb6qff1mtmku4.apps.googleusercontent.com', googleOAuthCallbackUrl:
'https://envoy-crm.voltade.com/omniauth/google_oauth2/callback', fbApiVersion: 'v22.0',
signupEnabled: 'true', isEnterprise: 'false', isMfaEnabled: 'true', whatsappConfigurationId:
'1533814824339124', vapidPublicKey: new Uint8Array([4, 244, 81, 216, 189, 227, 205, 206, 23,
85, 46, 49, 53, 250, 107, 33, 251, 106, 175, 82, 114, 163, 120, 67, 136, 4, 112, 161, 169,
95, 165, 61, 233, 185, 180, 114, 56, 21, 163, 157, 230, 18, 192, 195, 235, 202, 79, 8, 181,
228, 27, 242, 40, 9, 250, 3, 230, 29, 132, 70, 234, 172, 68, 160, 23]), enabledLanguages:
[{"name":"English (en)","iso_639_1_code":"en"},{"name":"Ø§Ù?Ø¹Ø±Ø¨Ù?Ø©
(ar)","iso_639_1_code":"ar"},{"name":"Nederlands (nl)
","iso_639_1_code":"nl"},{"name":"FranÃ§ais (fr)","iso_639_1_code":"fr"},{"name":"Deutsch
(de)","iso_639_1_code":"de"},{"name":"Italiano
(it)","iso_639_1_code":"it"},{"name":"æ?¥æ?¬èª? (ja)","iso_639_1_code":"ja"},{"name":"í??êµ-
ì?´ (ko)","iso_639_1_code":"ko"},{"name":"PortuguÃªs
(pt)","iso_639_1_code":"pt"},{"name":"Ñ?Ñ?Ñ•Ñ•ÐºÐ¸Ð¹
(ru)","iso_639_1_code":"ru"},{"name":"EspaÃ±ol
(es)","iso_639_1_code":"es"},{"name":"à´®à´²à´¯à´¾à´³à´ ?
(ml)","iso_639_1_code":"ml"},{"name":"CatalÃ
(ca)","iso_639_1_code":"ca"},{"name":"ÎµÎ»Î»Î·Î½Î¹ÎºÎ¬
(el)","iso_639_1_code":"el"},{"name":"PortuguÃªs Brasileiro (pt-
BR)","iso_639_1_code":"pt_BR"},{"name":"RomÃ¢nÄ?
(ro)","iso_639_1_code":"ro"},{"name":"à®€à®®à®¿à®´à¯•
(ta)","iso_639_1_code":"ta"},{"name":"Ù•Ø§Ø±Ø³Û? (fa)","iso_639_1_code":"fa"},{"name":"ä¸æ??
(å•°æ¹¾) (zh-TW)","iso_639_1_code":"zh_TW"},{"name":"Tiáº¿ng Viá»?t
```

(vi)","iso_639_1_code":"vi"},{"name":"dansk (da)","iso_639_1_code":"da"},{"name":"TÃ¼rkÃ§e
(tr)","iso_639_1_code":"tr"},{"name":"Ä•eÅ¡tina (cs)","iso_639_1_code":"cs"},{"name":"suomi,
suomen kieli (fi)","iso_639_1_code":"fi"},{"name":"Bahasa Indonesia
(id)","iso_639_1_code":"id"},{"name":"Svenska (sv)","iso_639_1_code":"sv"},{"name":"magyar
nyelv (hu)","iso_639_1_code":"hu"},{"name":"norsk (no)","iso_639_1_code":"no"},{"name":"ä¸æ??
(zh-CN)","iso_639_1_code":"zh_CN"},{"name":"jÄ?zyk polski
(pl)","iso_639_1_code":"pl"},{"name":"slovenÄ•ina
(sk)","iso_639_1_code":"sk"},{"name":"Ñ?ÐºÑ?Ð°Ñ?Ì•Ð½Ñ•Ñ ?ÐºÐ° Ð¼Ð¾Ì•Ð²Ð°
(uk)","iso_639_1_code":"uk"},{"name":"à¸ à¸²à¸©à¸²à¹?à¸ ?à¸¢
(th)","iso_639_1_code":"th"},{"name":"latvieÅ¡u valoda
(lv)","iso_639_1_code":"lv"},{"name":"Ãslenska
(is)","iso_639_1_code":"is"},{"name":"×¢Ö´×?×¨Ö´×?×ª
(he)","iso_639_1_code":"he"},{"name":"lietuviÅ³
(lt)","iso_639_1_code":"lt"},{"name":"Ð¡Ñ?Ð¿Ñ•ÐºÐ¸ (sr)","iso_639_1_code":"sr"}], helpUrls:
{"channel_email":"https://chwt.app/kb/email","channel_facebook":&
quot;https://chwt.app/kb/fb","knowledge_base":"https://chwt.app/kb/knowledg e-
base","agent_bots":"https://chwt.app/kb/agent-bots","team_manag
ement":"https://chwt.app/kb/teams","labels":"https://chwt.app/kb/
labels","custom_attributes":"https://chwt.app/kb/custom-attributes",&q
uot;canned_responses":"https://chwt.app/kb/canned","integrations":&quo
t;https://chwt.app/kb/integrations","campaigns":"https://chwt.app/kb/campai
gns","reports":"https://chwt.app/kb/reports","message_reply_to&qu
ot;:"https://chwt.app/kb/reply-to","sla":"https://chwt.app/kb/sla&quot ;}, selectedLocale:
'en' } window.globalConfig = {"LOGO":"/brand-assets/logo.svg","LOGO_DARK":"/brand-assets/
logo_dark.svg","LOGO_THUMBNAIL":"/brand-assets/logo_thumbnail.svg",&qu
ot;INSTALLATION_NAME":"Envoy
CRM","WIDGET_BRAND_URL":"https://www.chatwoot.com","TERMS_URL&quo
t;:"https://www.chatwoot.com/terms-of-service","BRAND_URL":"https://ww
w.chatwoot.com","BRAND_NAME":"Chatwoot","PRIVACY_URL":"
https://www.chatwoot.com/privacy-policy","DISPLAY_MANIFEST":true,"CREATE_NE
W_ACCOUNT_FROM_DASHBOARD":false,"CHATWOOT_INBOX_TOKEN":null,"API_CHANNEL_NA
ME":null,"API_CHANNEL_THUMBNAIL":null,"ANALYTICS_TOKEN":null,"DIR
ECT_UPLOADS_ENABLED":false,"HCAPTCHA_SITE_KEY":null,"LOGOUT_REDIRECT_LINK&q
uot;:"/app/login","DISABLE_USER_PROFILE_UPDATE":false,"DEPLOYMENT_ENV& quot;:"self-
hosted","INSTALLATION_PRICING_PLAN":"community",&quot
;APP_VERSION":"4.1.0","VAPID_PUBLIC_KEY":"BPRR2L3jzc4XVS4xNfprIft
qr1Jyo3hDiARwoalfpT3pubRyOBWjneYSwMPryk8IteQb8igJ-gPmHYRG6qxEoBc=","ENABLE_ACCOUNT_SI
GNUP":"true","FB_APP_ID":"1064501834924073","INSTAGRAM_
APP_ID":null,"FACEBOOK_API_VERSION":"v22.0","IS_ENTERPRISE":
false,"AZURE_APP_ID":"47e9fdaa-7c00-412f-ab48-d5c2ab187153","WHATSAPP_
CONFIGURATION_ID":"1533814824339124","GIT_SHA":"c2727e3",&qu
ot;IOS_APP_STORE_URL":"https://apps.apple.com/us/app/envoy-crm/id6754208045",&qu
ot;ANDROID_PLAY_STORE_URL":"https://play.google.com/store/apps/details?id=com.voltade
.envoy"} window.browserConfig = { browser_name: 'Chrome', } window.errorLoggingConfig =
'https://8cc8fb603ff7d79450bd92c83d873536@o4510242215231488.ingest.de.sentry.io/4510542981
955664' // window.errorLoggingConfig = undefined </script>

Evidence Response:

No links have been found while there are scripts, which is an indication that this is a modern web application.
https://envoy-crm.voltade.com/
<script type="d8b46b5dd59c50411dd05115-text/javascript"> window.chatwootConfig = { hostURL:
'https://envoy-crm.voltade.com', knowledgeBaseURL: '', fbAppId: '1064501834924073',
instagramAppId: '', googleOAuthClientId: '215202957494-
np384n1cef89j8ro528rb6qff1mtmku4.apps.googleusercontent.com', googleOAuthCallbackUrl:
'https://envoy-crm.voltade.com/omniauth/google_oauth2/callback', fbApiVersion: 'v22.0',

signupEnabled: 'true', isEnterprise: 'false', isMfaEnabled: 'true', whatsappConfigurationId: '1533814824339124', vapidPublicKey: new Uint8Array([4, 244, 81, 216, 189, 227, 205, 206, 23, 85, 46, 49, 53, 250, 107, 33, 251, 106, 175, 82, 114, 163, 120, 67, 136, 4, 112, 161, 169, 95, 165, 61, 233, 185, 180, 114, 56, 21, 163, 157, 230, 18, 192, 195, 235, 202, 79, 8, 181, 228, 27, 242, 40, 9, 250, 3, 230, 29, 132, 70, 234, 172, 68, 160, 23]), enabledLanguages: [{"name":"English (en)","iso_639_1_code":"en"},{"name":"Ø§Ù?Ø¹Ø±Ø¨Ù?Ø©
(ar)","iso_639_1_code":"ar"},{"name":"Nederlands (nl)
","iso_639_1_code":"nl"},{"name":"FranÃ§ais (fr)","iso_639_1_code":"fr"},{"name":"Deutsch
(de)","iso_639_1_code":"de"},{"name":"Italiano
(it)","iso_639_1_code":"it"},{"name":"æ?¥æ?¬èª? (ja)","iso_639_1_code":"ja"},{"name":"í??êµ-
ì?´ (ko)","iso_639_1_code":"ko"},{"name":"PortuguÃªs
(pt)","iso_639_1_code":"pt"},{"name":"Ñ?Ñ?Ñ•Ñ•ÐºÐ¸Ð¹
(ru)","iso_639_1_code":"ru"},{"name":"EspaÃ±ol
(es)","iso_639_1_code":"es"},{"name":"à´®à´²à´¯à´¾à´³ ?
(ml)","iso_639_1_code":"ml"},{"name":"CatalÃ
(ca)","iso_639_1_code":"ca"},{"name":"ÎµÎ»Î»Î·Î½Î¹Îº
(el)","iso_639_1_code":"el"},{"name":"PortuguÃªs Brasileiro (pt-
BR)","iso_639_1_code":"pt_BR"},{"name":"RomÃ¢nÄ?
(ro)","iso_639_1_code":"ro"},{"name":"à®¤à®®à®¿à®´à¯•
(ta)","iso_639_1_code":"ta"},{"name":"Ù•Ø§Ø±Ø³Û? (fa)","iso_639_1_code":"fa"},{"name":"ä¸æ??
(å•æ¹¾) (zh-TW)","iso_639_1_code":"zh_TW"},{"name":"Tiáº¿ng Viá»?t
(vi)","iso_639_1_code":"vi"},{"name":"dansk (da)","iso_639_1_code":"da"},{"name":"TÃ¼rkÃ§e
(tr)","iso_639_1_code":"tr"},{"name":"Ä•eÅ¡tina (cs)","iso_639_1_code":"cs"},{"name":"suomi,
suomen kieli (fi)","iso_639_1_code":"fi"},{"name":"Bahasa Indonesia
(id)","iso_639_1_code":"id"},{"name":"Svenska (sv)","iso_639_1_code":"sv"},{"name":"magyar
nyelv (hu)","iso_639_1_code":"hu"},{"name":"norsk (no)","iso_639_1_code":"no"},{"name":"ä¸æ??
(zh-CN)","iso_639_1_code":"zh_CN"},{"name":"jÄ?zyk polski
(pl)","iso_639_1_code":"pl"},{"name":"slovenÄ•ina
(sk)","iso_639_1_code":"sk"},{"name":"Ñ?ÐºÑ?Ð°Ñ?Ì•Ð½Ñ•Ñ ?ÐºÐ° Ð¼Ð¾Ì•Ð²Ð°
(uk)","iso_639_1_code":"uk"},{"name":"à¸ à¸²à¸©à¸²à¹?à¸ ?à¸¢
(th)","iso_639_1_code":"th"},{"name":"latvieÅ¡u valoda
(lv)","iso_639_1_code":"lv"},{"name":"Ãslenska
(is)","iso_639_1_code":"is"},{"name":"×¢Ö´×?×¨Ö´×?×ª
(he)","iso_639_1_code":"he"},{"name":"lietuviÅ³
(lt)","iso_639_1_code":"lt"},{"name":"Ð¡Ñ?Ð¿Ñ•ÐºÐ¸ (sr)","iso_639_1_code":"sr"}], helpUrls:
{"channel_email":"https://chwt.app/kb/email","channel_facebook":&
quot;https://chwt.app/kb/fb","knowledge_base":"https://chwt.app/kb/knowledg e-
base","agent_bots":"https://chwt.app/kb/agent-bots","team_manag
ement":"https://chwt.app/kb/teams","labels":"https://chwt.app/kb/
labels","custom_attributes":"https://chwt.app/kb/custom-attributes",&q
uot;canned_responses":"https://chwt.app/kb/canned","integrations":&quo
t;https://chwt.app/kb/integrations","campaigns":"https://chwt.app/kb/campai
gns","reports":"https://chwt.app/kb/reports","message_reply_to&qu
ot;:"https://chwt.app/kb/reply-to","sla":"https://chwt.app/kb/sla&quot ;}, selectedLocale:
'en' } window.globalConfig = {"LOGO":"/brand-assets/logo.svg","LOGO_DARK":"/brand-assets/
logo_dark.svg","LOGO_THUMBNAIL":"/brand-assets/logo_thumbnail.svg",&qu
ot;INSTALLATION_NAME":"Envoy
CRM","WIDGET_BRAND_URL":"https://www.chatwoot.com","TERMS_URL&quo
t;:"https://www.chatwoot.com/terms-of-service","BRAND_URL":"https://ww
w.chatwoot.com","BRAND_NAME":"Chatwoot","PRIVACY_URL":"
https://www.chatwoot.com/privacy-policy","DISPLAY_MANIFEST":true,"CREATE_NE
W_ACCOUNT_FROM_DASHBOARD":false,"CHATWOOT_INBOX_TOKEN":null,"API_CHANNEL_NA
ME":null,"API_CHANNEL_THUMBNAIL":null,"ANALYTICS_TOKEN":null,"DIR
ECT_UPLOADS_ENABLED":false,"HCAPTCHA_SITE_KEY":null,"LOGOUT_REDIRECT_LINK&q
uot;:"/app/login","DISABLE_USER_PROFILE_UPDATE":false,"DEPLOYMENT_ENV& quot;:"self-

hosted","INSTALLATION_PRICING_PLAN":"community",&quot
;APP_VERSION":"4.1.0","VAPID_PUBLIC_KEY":"BPRR2L3jzc4XVS4xNfprIft
qr1Jyo3hDiARwoalfpT3pubRyOBWjneYSwMPryk8IteQb8igJ-gPmHYRG6qxEoBc=","ENABLE_ACCOUNT_SI
GNUP":"true","FB_APP_ID":"1064501834924073","INSTAGRAM_
APP_ID":null,"FACEBOOK_API_VERSION":"v22.0","IS_ENTERPRISE":
false,"AZURE_APP_ID":"47e9fdaa-7c00-412f-ab48-d5c2ab187153","WHATSAPP_
CONFIGURATION_ID":"1533814824339124","GIT_SHA":"c2727e3",&qu
ot;IOS_APP_STORE_URL":"https://apps.apple.com/us/app/envoy-crm/id6754208045",&qu
ot;ANDROID_PLAY_STORE_URL":"https://play.google.com/store/apps/details?id=com.voltade
.envoy"} window.browserConfig = { browser_name: 'Chrome', } window.errorLoggingConfig =
'https://8cc8fb603ff7d79450bd92c83d873536@o4510242215231488.ingest.de.sentry.io/4510542981
955664' // window.errorLoggingConfig = undefined </script>
No links have been found while there are scripts, which is an indication that this is a
modern web application.
https://envoy-crm.voltade.com
_chatwoot_session
cookie:_chatwoot_session
https://envoy-crm.voltade.com/
_chatwoot_session
cookie:_chatwoot_session
https://envoy-crm.voltade.com
<script type="0e32a02d89eb7d9538a3c036-text/javascript"> window.chatwootConfig = { hostURL:
'https://envoy-crm.voltade.com', knowledgeBaseURL: '', fbAppId: '1064501834924073',
instagramAppId: '', googleOAuthClientId: '215202957494-
np384n1cef89j8ro528rb6qff1mtmku4.apps.googleusercontent.com', googleOAuthCallbackUrl:
'https://envoy-crm.voltade.com/omniauth/google_oauth2/callback', fbApiVersion: 'v22.0',
signupEnabled: 'true', isEnterprise: 'false', isMfaEnabled: 'true', whatsappConfigurationId:
'1533814824339124', vapidPublicKey: new Uint8Array([4, 244, 81, 216, 189, 227, 205, 206, 23,
85, 46, 49, 53, 250, 107, 33, 251, 106, 175, 82, 114, 163, 120, 67, 136, 4, 112, 161, 169,
95, 165, 61, 233, 185, 180, 114, 56, 21, 163, 157, 230, 18, 192, 195, 235, 202, 79, 8, 181,
228, 27, 242, 40, 9, 250, 3, 230, 29, 132, 70, 234, 172, 68, 160, 23]), enabledLanguages:
[{"name":"English (en)","iso_639_1_code":"en"},{"name":"Ø§Ù?Ø¹Ø±Ø¨Ù?Ø©
(ar)","iso_639_1_code":"ar"},{"name":"Nederlands (nl)
","iso_639_1_code":"nl"},{"name":"FranÃ§ais (fr)","iso_639_1_code":"fr"},{"name":"Deutsch
(de)","iso_639_1_code":"de"},{"name":"Italiano
(it)","iso_639_1_code":"it"},{"name":"æ?¥æ?¬èª? (ja)","iso_639_1_code":"ja"},{"name":"í??êµ-
ì?´ (ko)","iso_639_1_code":"ko"},{"name":"PortuguÃªs
(pt)","iso_639_1_code":"pt"},{"name":"Ñ?Ñ?Ñ•Ñ•ÐºÐ¸Ð¹
(ru)","iso_639_1_code":"ru"},{"name":"EspaÃ±ol
(es)","iso_639_1_code":"es"},{"name":"à´®à´²à´¯à´¾à´³ ?
(ml)","iso_639_1_code":"ml"},{"name":"CatalÃ
(ca)","iso_639_1_code":"ca"},{"name":"Î¼Î»Î»Î·Î½Î¹Îº¬
(el)","iso_639_1_code":"el"},{"name":"PortuguÃªs Brasileiro (pt-
BR)","iso_639_1_code":"pt_BR"},{"name":"RomÃ¢nÄ?
(ro)","iso_639_1_code":"ro"},{"name":"à®€à®®à®¿à®´à¯•
(ta)","iso_639_1_code":"ta"},{"name":"Ù•Ø§Ø±Ø³Û? (fa)","iso_639_1_code":"fa"},{"name":"ä¸æ??
(å•°æ¹¾) (zh-TW)","iso_639_1_code":"zh_TW"},{"name":"Tiáº¿ng Viá»?t
(vi)","iso_639_1_code":"vi"},{"name":"dansk (da)","iso_639_1_code":"da"},{"name":"TÃ¼rkÃ§e
(tr)","iso_639_1_code":"tr"},{"name":"Ä•eÅ¡tina (cs)","iso_639_1_code":"cs"},{"name":"suomi,
suomen kieli (fi)","iso_639_1_code":"fi"},{"name":"Bahasa Indonesia
(id)","iso_639_1_code":"id"},{"name":"Svenska (sv)","iso_639_1_code":"sv"},{"name":"magyar
nyelv (hu)","iso_639_1_code":"hu"},{"name":"norsk (no)","iso_639_1_code":"no"},{"name":"ä¸æ??
(zh-CN)","iso_639_1_code":"zh_CN"},{"name":"jÄ?zyk polski
(pl)","iso_639_1_code":"pl"},{"name":"slovenÄ•ina
(sk)","iso_639_1_code":"sk"},{"name":"Ñ?ÐºÑ?Ð°Ñ?Ì•Ð½Ñ•Ñ ?ÐºÐ° Ð¼Ð¾Ì•Ð²Ð°

(uk)","iso_639_1_code":"uk"},{"name":"à¸ à¸²à¸©à¸²à¹?à¸ ?à¸¢
(th)","iso_639_1_code":"th"},{"name":"latvieÅ¡u valoda
(lv)","iso_639_1_code":"lv"},{"name":"Ãslenska
(is)","iso_639_1_code":"is"},{"name":"×¢Ö´×?×¨Ö´×?×ª
(he)","iso_639_1_code":"he"},{"name":"lietuviÅ³
(lt)","iso_639_1_code":"lt"},{"name":"Ð¡Ñ?Ð¿Ñ•ÐºÐ¸ (sr)","iso_639_1_code":"sr"}], helpUrls:
{"channel_email":"https://chwt.app/kb/email","channel_facebook":&
quot;https://chwt.app/kb/fb","knowledge_base":"https://chwt.app/kb/knowledg e-
base","agent_bots":"https://chwt.app/kb/agent-bots","team_manag
ement":"https://chwt.app/kb/teams","labels":"https://chwt.app/kb/
labels","custom_attributes":"https://chwt.app/kb/custom-attributes",&q
uot;canned_responses":"https://chwt.app/kb/canned","integrations":&quo
t;https://chwt.app/kb/integrations","campaigns":"https://chwt.app/kb/campai
gns","reports":"https://chwt.app/kb/reports","message_reply_to&qu
ot;:"https://chwt.app/kb/reply-to","sla":"https://chwt.app/kb/sla&quot ;}, selectedLocale:
'en' } window.globalConfig = {"LOGO":"/brand-assets/logo.svg","LOGO_DARK":"/brand-assets/
logo_dark.svg","LOGO_THUMBNAIL":"/brand-assets/logo_thumbnail.svg",&qu
ot;INSTALLATION_NAME":"Envoy
CRM","WIDGET_BRAND_URL":"https://www.chatwoot.com","TERMS_URL&quo
t;:"https://www.chatwoot.com/terms-of-service","BRAND_URL":"https://ww
w.chatwoot.com","BRAND_NAME":"Chatwoot","PRIVACY_URL":"
https://www.chatwoot.com/privacy-policy","DISPLAY_MANIFEST":true,"CREATE_NE
W_ACCOUNT_FROM_DASHBOARD":false,"CHATWOOT_INBOX_TOKEN":null,"API_CHANNEL_NA
ME":null,"API_CHANNEL_THUMBNAIL":null,"ANALYTICS_TOKEN":null,"DIR
ECT_UPLOADS_ENABLED":false,"HCAPTCHA_SITE_KEY":null,"LOGOUT_REDIRECT_LINK&q
uot;:"/app/login","DISABLE_USER_PROFILE_UPDATE":false,"DEPLOYMENT_ENV& quot;:"self-
hosted","INSTALLATION_PRICING_PLAN":"community",&quot
;APP_VERSION":"4.1.0","VAPID_PUBLIC_KEY":"BPRR2L3jzc4XVS4xNfprIft
qr1Jyo3hDiARwoalfpT3pubRyOBWjneYSwMPryk8IteQb8igJ-gPmHYRG6qxEoBc=","ENABLE_ACCOUNT_SI
GNUP":"true","FB_APP_ID":"1064501834924073","INSTAGRAM_
APP_ID":null,"FACEBOOK_API_VERSION":"v22.0","IS_ENTERPRISE":
false,"AZURE_APP_ID":"47e9fdaa-7c00-412f-ab48-d5c2ab187153","WHATSAPP_
CONFIGURATION_ID":"1533814824339124","GIT_SHA":"af026ac",&qu
ot;IOS_APP_STORE_URL":"https://apps.apple.com/us/app/envoy-crm/id6754208045",&qu
ot;ANDROID_PLAY_STORE_URL":"https://play.google.com/store/apps/details?id=com.voltade
.envoy"} window.browserConfig = { browser_name: 'Chrome', } window.errorLoggingConfig =
'https://8cc8fb603ff7d79450bd92c83d873536@o4510242215231488.ingest.de.sentry.io/4510542981
955664' // window.errorLoggingConfig = undefined </script>
No links have been found while there are scripts, which is an indication that this is a
modern web application.
https://envoy-crm.voltade.com/
<script type="f75e7d5bb82ab0f8c22fa692-text/javascript"> window.chatwootConfig = { hostURL:
'https://envoy-crm.voltade.com', knowledgeBaseURL: '', fbAppId: '1064501834924073',
instagramAppId: '', googleOAuthClientId: '215202957494-
np384n1cef89j8ro528rb6qff1mtmku4.apps.googleusercontent.com', googleOAuthCallbackUrl:
'https://envoy-crm.voltade.com/omniauth/google_oauth2/callback', fbApiVersion: 'v22.0',
signupEnabled: 'true', isEnterprise: 'false', isMfaEnabled: 'true', whatsappConfigurationId:
'1533814824339124', vapidPublicKey: new Uint8Array([4, 244, 81, 216, 189, 227, 205, 206, 23,
85, 46, 49, 53, 250, 107, 33, 251, 106, 175, 82, 114, 163, 120, 67, 136, 4, 112, 161, 169,
95, 165, 61, 233, 185, 180, 114, 56, 21, 163, 157, 230, 18, 192, 195, 235, 202, 79, 8, 181,
228, 27, 242, 40, 9, 250, 3, 230, 29, 132, 70, 234, 172, 68, 160, 23]), enabledLanguages:
[{"name":"English (en)","iso_639_1_code":"en"},{"name":"Ø§Ù?Ø¹Ø±Ø¨Ù?Ø©
(ar)","iso_639_1_code":"ar"},{"name":"Nederlands (nl)
","iso_639_1_code":"nl"},{"name":"FranÃ§ais (fr)","iso_639_1_code":"fr"},{"name":"Deutsch
(de)","iso_639_1_code":"de"},{"name":"Italiano

(it)","iso_639_1_code":"it"},{"name":"æ?¥æ?¬èª? (ja)","iso_639_1_code":"ja"},{"name":"í??êµ-
ì?´ (ko)","iso_639_1_code":"ko"},{"name":"PortuguÃªs
(pt)","iso_639_1_code":"pt"},{"name":"Ñ?Ñ?Ñ•Ñ•ÐºÐ¸Ð¹
(ru)","iso_639_1_code":"ru"},{"name":"EspaÃ±ol
(es)","iso_639_1_code":"es"},{"name":"à´®à´²à´¯à´¾à´³à´ ?
(ml)","iso_639_1_code":"ml"},{"name":"CatalÃ
(ca)","iso_639_1_code":"ca"},{"name":"ÎµÎ»Î·Î½Î¹ÎºÎ¬
(el)","iso_639_1_code":"el"},{"name":"PortuguÃªs Brasileiro (pt-
BR)","iso_639_1_code":"pt_BR"},{"name":"RomÃ¢nÄ?
(ro)","iso_639_1_code":"ro"},{"name":"à®€à®®à®¿à®´à¯•
(ta)","iso_639_1_code":"ta"},{"name":"Ù•Ø§Ø±Ø³Û? (fa)","iso_639_1_code":"fa"},{"name":"ä¸æ??
(å•°æ¹¾) (zh-TW)","iso_639_1_code":"zh_TW"},{"name":"Tiáº¿ng Viá»?t
(vi)","iso_639_1_code":"vi"},{"name":"dansk (da)","iso_639_1_code":"da"},{"name":"TÃ¼rkÃ§e
(tr)","iso_639_1_code":"tr"},{"name":"Ä•eÅ¡tina (cs)","iso_639_1_code":"cs"},{"name":"suomi,
suomen kieli (fi)","iso_639_1_code":"fi"},{"name":"Bahasa Indonesia
(id)","iso_639_1_code":"id"},{"name":"Svenska (sv)","iso_639_1_code":"sv"},{"name":"magyar
nyelv (hu)","iso_639_1_code":"hu"},{"name":"norsk (no)","iso_639_1_code":"no"},{"name":"ä¸æ??
(zh-CN)","iso_639_1_code":"zh_CN"},{"name":"jÄ?zyk polski
(pl)","iso_639_1_code":"pl"},{"name":"slovenÄ•ina
(sk)","iso_639_1_code":"sk"},{"name":"Ñ?ÐºÑ?Ð°Ñ?Ì•Ð½Ñ•Ñ ?ÐºÐ° Ð¼Ð¾Ì•Ð²Ð°
(uk)","iso_639_1_code":"uk"},{"name":"à¸ à¸²à¸©à¸²à¹?à¸ ?à¸¢
(th)","iso_639_1_code":"th"},{"name":"latvieÅ¡u valoda
(lv)","iso_639_1_code":"lv"},{"name":"Ãslenska
(is)","iso_639_1_code":"is"},{"name":"×¢Ö´×?×¨Ö´×?×ª
(he)","iso_639_1_code":"he"},{"name":"lietuviÅ³
(lt)","iso_639_1_code":"lt"},{"name":"Ð¡Ñ?Ð¿Ñ•ÐºÐ¸ (sr)","iso_639_1_code":"sr"}], helpUrls:
{"channel_email":"https://chwt.app/kb/email","channel_facebook":&
quot;https://chwt.app/kb/fb","knowledge_base":"https://chwt.app/kb/knowledg e-
base","agent_bots":"https://chwt.app/kb/agent-bots","team_manag
ement":"https://chwt.app/kb/teams","labels":"https://chwt.app/kb/
labels","custom_attributes":"https://chwt.app/kb/custom-attributes",&q
uot;canned_responses":"https://chwt.app/kb/canned","integrations":&quo
t;https://chwt.app/kb/integrations","campaigns":"https://chwt.app/kb/campai
gns","reports":"https://chwt.app/kb/reports","message_reply_to&qu
ot;:"https://chwt.app/kb/reply-to","sla":"https://chwt.app/kb/sla&quot ;}, selectedLocale:
'en' } window.globalConfig = {"LOGO":"/brand-assets/logo.svg","LOGO_DARK":"/brand-assets/
logo_dark.svg","LOGO_THUMBNAIL":"/brand-assets/logo_thumbnail.svg",&qu
ot;INSTALLATION_NAME":"Envoy
CRM","WIDGET_BRAND_URL":"https://www.chatwoot.com","TERMS_URL&quo
t;:"https://www.chatwoot.com/terms-of-service","BRAND_URL":"https://ww
w.chatwoot.com","BRAND_NAME":"Chatwoot","PRIVACY_URL":"
https://www.chatwoot.com/privacy-policy","DISPLAY_MANIFEST":true,"CREATE_NE
W_ACCOUNT_FROM_DASHBOARD":false,"CHATWOOT_INBOX_TOKEN":null,"API_CHANNEL_NA
ME":null,"API_CHANNEL_THUMBNAIL":null,"ANALYTICS_TOKEN":null,"DIR
ECT_UPLOADS_ENABLED":false,"HCAPTCHA_SITE_KEY":null,"LOGOUT_REDIRECT_LINK&q
uot;:"/app/login","DISABLE_USER_PROFILE_UPDATE":false,"DEPLOYMENT_ENV& quot;:"self-
hosted","INSTALLATION_PRICING_PLAN":"community",&quot
;APP_VERSION":"4.1.0","VAPID_PUBLIC_KEY":"BPRR2L3jzc4XVS4xNfprIft
qr1Jyo3hDiARwoalfpT3pubRyOBWjneYSwMPryk8IteQb8igJ-gPmHYRG6qxEoBc=","ENABLE_ACCOUNT_SI
GNUP":"true","FB_APP_ID":"1064501834924073","INSTAGRAM_
APP_ID":null,"FACEBOOK_API_VERSION":"v22.0","IS_ENTERPRISE":
false,"AZURE_APP_ID":"47e9fdaa-7c00-412f-ab48-d5c2ab187153","WHATSAPP_
CONFIGURATION_ID":"1533814824339124","GIT_SHA":"af026ac",&qu
ot;IOS_APP_STORE_URL":"https://apps.apple.com/us/app/envoy-crm/id6754208045",&qu
ot;ANDROID_PLAY_STORE_URL":"https://play.google.com/store/apps/details?id=com.voltade

```
.envoy"} window.browserConfig = { browser_name: 'Chrome', } window.errorLoggingConfig =
'https://8cc8fb603ff7d79450bd92c83d873536@o4510242215231488.ingest.de.sentry.io/4510542981
955664' // window.errorLoggingConfig = undefined </script>
No links have been found while there are scripts, which is an indication that this is a
modern web application.
https://envoy-crm.voltade.com
_chatwoot_session
cookie:_chatwoot_session
https://envoy-crm.voltade.com/
_chatwoot_session
cookie:_chatwoot_session
```

Reference:
https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/

9 Storable but Non-Cacheable Content

Severity Level: Info

CWEID: 524

Status: Patched

Description:

The response contents are storable by caching components such as proxy servers, but will not be retrieved directly from the cache, without validating the request upstream, in response to similar requests from other users.

Vulnerable URL

https://envoy-crm.voltade.com

Evidence Url:

```
https://envoy-crm.voltade.com
private
https://envoy-crm.voltade.com/
406
https://envoy-crm.voltade.com/
private
https://envoy-crm.voltade.com/apple-icon-57x57.png
max-age=31556952
https://envoy-crm.voltade.com/apple-icon-72x72.png
max-age=31556952
https://envoy-crm.voltade.com/robots.txt
max-age=31556952
https://envoy-crm.voltade.com/sitemap.xml
```

Evidence Response:

```
In the absence of an explicitly specified caching lifetime directive in the response, a
liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
https://envoy-crm.voltade.com/vite/assets/DashboardIcon-DOyOypg7.css
max-age=31556952
https://envoy-crm.voltade.com/widget
no-cache
https://envoy-crm.voltade.com
private
https://envoy-crm.voltade.com/
406
https://envoy-crm.voltade.com/
private
https://envoy-crm.voltade.com/apple-icon-57x57.png
max-age=31556952
https://envoy-crm.voltade.com/apple-icon-60x60.png
max-age=31556952
https://envoy-crm.voltade.com/robots.txt
max-age=31556952
```

`https://envoy-crm.voltade.com/sitemap.xml`

`In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.`

`https://envoy-crm.voltade.com/vite/assets/dashboard-i892xZS8.css`

`max-age=31556952`

`https://envoy-crm.voltade.com/widget`

`no-cache`

Reference:

https://datatracker.ietf.org/doc/html/rfc7234
https://datatracker.ietf.org/doc/html/rfc7231
https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html

10 Re-examine Cache-control Directives

Severity Level: Info

CWEID: 525

Status: Patched

Description:

The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Vulnerable URL

https://envoy-crm.voltade.com

Remedies:

For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

Evidence Url:

```
https://envoy-crm.voltade.com
max-age=0, private, must-revalidate
https://envoy-crm.voltade.com/
max-age=0, private, must-revalidate
https://envoy-crm.voltade.com/manifest.json?v=1.0.0
public, max-age=31556952
https://envoy-crm.voltade.com/robots.txt
public, max-age=31556952
https://envoy-crm.voltade.com
max-age=0, private, must-revalidate
https://envoy-crm.voltade.com/
max-age=0, private, must-revalidate
https://envoy-crm.voltade.com/manifest.json?v=1.0.0
public, max-age=31556952
https://envoy-crm.voltade.com/robots.txt
public, max-age=31556952
```

Reference:

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

11 User Agent Fuzzer

Severity Level: Info

Status: Patched

Description:

Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

Vulnerable URL

https://envoy-crm.voltade.com

Evidence Url:

`https://envoy-crm.voltade.com`
`https://envoy-crm.voltade.com`
`https://envoy-crm.voltade.com`
`https://envoy-crm.voltade.com/`
`https://envoy-crm.voltade.com/`
`https://envoy-crm.voltade.com`
`https://envoy-crm.voltade.com`
`https://envoy-crm.voltade.com/`
`https://envoy-crm.voltade.com/`
`https://envoy-crm.voltade.com/`

Reference:

https://owasp.org/wstg

SAQ

Sr. No.	Requirements	Applicable	Comments
1	Verify documentation and justification of all the application's trust boundaries, components, and significant data flows.	No	NIL
2	Verify the application does not use unsupported, insecure, or deprecated client-side technologies such as NSAPI plugins, Flash, Shockwave, ActiveX, Silverlight, NACL, or client-side Java applets.	No	NIL
3	Verify that trusted enforcement points, such as access control gateways, servers, and serverless functions, enforce access controls. Never enforce access controls on the client.	No	NIL
4	Verify that all sensitive data is identified and classified into protection levels.	No	NIL
5	Verify that all protection levels have an associated set of protection requirements, such as encryption requirements, integrity requirements, retention, privacy and other confidentiality requirements, and that these are applied in the architecture.	No	NIL
6	Verify that the application employs integrity protections, such as code signing or subresource integrity. The application must not load or execute code from untrusted sources, such as loading includes, modules, plugins, code, or libraries from untrusted sources or the Internet.	No	NIL
7	Verify that the application has protection from subdomain takeovers if the application relies upon DNS entries or DNS subdomains, such as expired domain names, out of date DNS pointers or CNAMEs, expired projects at public source code repos, or transient cloud APIs, serverless functions, or storage buckets (*autogen-bucket-id*.cloud.example.com) or similar. Protections can include ensuring that DNS names used by applications are regularly checked for expiry or change.	No	NIL
8	Verify documentation and justification of all the application's trust boundaries, components, and significant data flows.	Yes	We maintain comprehensive documentation of all application trust boundaries, components, and data flows. Architecture diagrams and data flow documentation are reviewed and updated regularly.
9	Verify that the application has anti-automation controls to protect against excessive calls such as mass data exfiltration, business logic requests, file uploads or denial of service attacks.	No	NIL
10	Verify the application does not use unsupported, insecure, or deprecated client-side technologies such as NSAPI plugins, Flash, Shockwave, ActiveX, Silverlight, NACL, or client-side Java applets.	Yes	Our application does not use any unsupported, insecure, or deprecated client-side technologies such as Flash, Shockwave, ActiveX, Silverlight, NACL, or NSAPI plugins. We use modern, supported frameworks and libraries only.

Sr. No.	Requirements	Applicable	Comments
11	Verify that files obtained from untrusted sources are stored outside the web root, with limited permissions.	No	NIL
12	Verify that trusted enforcement points, such as access control gateways, servers, and serverless functions, enforce access controls. Never enforce access controls on the client.	Yes	Access controls are enforced on trusted server-side components including access control gateways, servers, and serverless functions. No access control decisions are made on the client side.
13	Verify that files obtained from untrusted sources are scanned by antivirus scanners to prevent upload and serving of known malicious content.	No	NIL
14	Verify that all sensitive data is identified and classified into protection levels.	No	No
15	Verify API URLs do not expose sensitive information, such as the API key, session tokens etc.	No	NIL
16	Verify that all protection levels have an associated set of protection requirements, such as encryption requirements, integrity requirements, retention, privacy and other confidentiality requirements, and that these are applied in the architecture.	Yes	All protection levels have associated protection requirements including encryption, integrity, retention, privacy, and confidentiality requirements. These are applied consistently across the architecture.
17	Verify that authorization decisions are made at both the URI, enforced by programmatic or declarative security at the controller or router, and at the resource level, enforced by model-based permissions.	No	NIL
18	Verify that the application employs integrity protections, such as code signing or subresource integrity. The application must not load or execute code from untrusted sources, such as loading includes, modules, plugins, code, or libraries from untrusted sources or the Internet.	Yes	The application employs integrity protections including code signing and subresource integrity (SRI). We do not load or execute code from untrusted sources, and all third-party libraries are verified.
19	Verify that enabled RESTful HTTP methods are a valid choice for the user or action, such as preventing normal users using DELETE or PUT on protected API or resources.	No	NIL

Sr. No.	Requirements	Applicable	Comments
20	Verify that the application has protection from subdomain takeovers if the application relies upon DNS entries or DNS subdomains, such as expired domain names, out of date DNS pointers or CNAMEs, expired projects at public source code repos, or transient cloud APIs, serverless functions, or storage buckets (*autogen-bucket-id*.cloud.example.com) or similar. Protections can include ensuring that DNS names used by applications are regularly checked for expiry or change.	Yes	The application has protection from subdomain takeovers. DNS entries and subdomains are regularly monitored and verified to prevent unauthorized takeover attempts.
21	Verify that the application build and deployment processes are performed in a secure and repeatable way, such as CI / CD automation, automated configuration management, and automated deployment scripts.	No	NIL
22	Verify that the application has anti-automation controls to protect against excessive calls such as mass data exfiltration, business logic requests, file uploads or denial of service attacks.	Yes	The application has anti-automation controls in place including rate limiting, CAPTCHA, and throttling mechanisms to protect against excessive calls and automated attacks.
23	Verify that the application, configuration, and all dependencies can be re-deployed using automated deployment scripts, built from a documented and tested runbook in a reasonable time, or restored from backups in a timely fashion.	No	NIL
24	Verify that files obtained from untrusted sources are stored outside the web root, with limited permissions.	Yes	Files obtained from untrusted sources are stored outside the web root with limited permissions. Access to these files is restricted and they are not directly accessible via web requests.
25	Verify that authorized administrators can verify the integrity of all security-relevant configurations to detect tampering.	No	NIL
26	Verify that files obtained from untrusted sources are scanned by antivirus scanners to prevent upload and serving of known malicious content.	Yes	All files obtained from untrusted sources are scanned by antivirus scanners before processing. This prevents upload of known malicious content to the application.
27	Verify that web or application server and application framework debug modes are disabled in production to eliminate debug features, developer consoles, and unintended security disclosures.	No	NIL

Sr. No.	Requirements	Applicable	Comments
28	Verify API URLs do not expose sensitive information, such as the API key, session tokens etc.	Yes	API URLs do not expose sensitive information such as API keys, session tokens, or credentials. All sensitive data is transmitted via request headers or body, never in URL parameters.
29	Verify that the supplied Origin header is not used for authentication or access control decisions, as the Origin header can easily be changed by an attacker.	No	NIL
30	Verify that authorization decisions are made at both the URI, enforced by programmatic or declarative security at the controller or router, and at the resource level, enforced by model-based permissions.	Yes	Authorization decisions are made at both the URI level and resource level, enforced by programmatic or declarative security in the controller or router. Access control is applied consistently across all layers.
31	Verify that user set passwords are at least 12 characters in length	No	NIL
32	Verify that enabled RESTful HTTP methods are a valid choice for the user or action, such as preventing normal users using DELETE or PUT on protected API or resources.	Yes	Enabled RESTful HTTP methods are validated to ensure they are appropriate for the user and action. Unauthorized methods such as DELETE or PUT are restricted and prevented for non-privileged users.
33	Verify system generated initial passwords or activation codes SHOULD be securely randomly generated, SHOULD be at least 6 characters long, and MAY contain letters and numbers, and expire after a short period of time. These initial secrets must not be permitted to become the long term password.	No	NIL
34	Verify that the application build and deployment processes are performed in a secure and repeatable way, such as CI / CD automation, automated configuration management, and automated deployment scripts.	Yes	The application build and deployment processes are performed in a secure and repeatable manner using CI/CD pipelines with security checks, code reviews, and automated testing at each stage.

Sr. No.	Requirements	Applicable	Comments
35	Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))	No	NIL
36	Verify that the application, configuration, and all dependencies can be re-deployed using automated deployment scripts, built from a documented and tested runbook in a reasonable time, or restored from backups in a timely fashion.	No	No
37	Verify shared or default accounts are not present (e.g. "root", "admin", or "sa").	No	NIL
38	Verify that authorized administrators can verify the integrity of all security-relevant configurations to detect tampering.	Yes	Authorized administrators can verify the integrity of all security-relevant configurations through configuration management tools, audit logs, and integrity checking mechanisms.
39	Verify that lookup secrets can be used only once.	No	NIL
40	Verify that web or application server and application framework debug modes are disabled in production to eliminate debug features, developer consoles, and unintended security disclosures.	Yes	Web and application server debug modes are disabled in production to prevent exposure of sensitive security information such as stack traces, debug logs, or error details.
41	Verify that the out of band verifier expires out of band authentication requests, codes, or tokens after 10 minutes.	No	NIL
42	Verify that the supplied Origin header is not used for authentication or access control decisions, as the Origin header can easily be changed by an attacker.	Yes	The supplied Origin header is not used for authentication or access control decisions. We use secure token-based authentication and do not rely on Origin headers for security enforcement.
43	Verify that the initial authentication code is generated by a secure random number generator, containing at least 20 bits of entropy (typically a six digital random number is sufficient).	No	NIL

Sr. No.	Requirements	Applicable	Comments
44	Verify that user set passwords are at least 12 characters in length	Yes	User-set passwords are required to be at least 12 characters in length. Our password policy enforces minimum length, complexity, and checks against known breached password lists.
45	Verify that logout and expiration invalidate the session token, such that the back button or a downstream relying party does not resume an authenticated session, including across relying parties. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))	No	NIL
46	Verify system generated initial passwords or activation codes SHOULD be securely randomly generated, SHOULD be at least 6 characters long, and MAY contain letters and numbers, and expire after a short period of time. These initial secrets must not be permitted to become the long term password.	No	No
47	Verify that the application gives the option to terminate all other active sessions after a successful password change (including change via password reset/recovery), and that this is effective across the application, federated login (if present), and any relying parties.	No	NIL
48	Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))	Yes	Passwords are stored using a strong, salted, one-way hashing algorithm resistant to offline attacks. We use bcrypt/argon2 with appropriate work factors for password hashing.
49	Verify the application uses session tokens rather than static API secrets and keys, except with legacy implementations.	No	NIL
50	Verify shared or default accounts are not present (e.g. "root", "admin", or "sa").	Yes	No shared or default accounts are present in the application. Default accounts such as root, admin, or sa are removed or disabled before deployment. Each user has a unique account.
51	Verify the application ensures a full, valid login session or requires re-authentication or secondary verification before allowing any sensitive transactions or account modifications.	No	NIL

Sr. No.	Requirements	Applicable	Comments
52	Verify that lookup secrets can be used only once.	Yes	Lookup secrets are single-use and can only be used once. After a lookup secret is consumed, it is invalidated and cannot be reused for subsequent authentication attempts.
53	Verify that the application enforces access control rules on a trusted service layer, especially if client-side access control is present and could be bypassed.	No	NIL
54	Verify that the out of band verifier expires out of band authentication requests, codes, or tokens after 10 minutes.	Yes	Out-of-band authentication requests, codes, and tokens expire after a short configurable period. Expired tokens are invalidated and cannot be reused for verification.
55	Verify that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.	No	NIL
56	Verify that the initial authentication code is generated by a secure random number generator, containing at least 20 bits of entropy (typically a six digital random number is sufficient).	Yes	Initial authentication codes are generated using a cryptographically secure pseudo-random number generator (CSPRNG), contain at least 20 bits of entropy, and are sufficiently random to resist guessing attacks.
57	Verify that the principle of least privilege exists - users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege. ([C7](https://owasp.org/www-project-proactive-controls/#div-numbering))	No	NIL
58	Verify that logout and expiration invalidate the session token, such that the back button or a downstream relying party does not resume an authenticated session, including across relying parties. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))	Yes	Logout and session expiration properly invalidate the session token. The back button or downstream relying party does not resume an authenticated session after logout.
59	Verify that access controls fail securely including when an exception occurs. ([C10](https://owasp.org/www-project-proactive-controls/#div-numbering))	No	NIL

Sr. No.	Requirements	Applicable	Comments
60	Verify that the application gives the option to terminate all other active sessions after a successful password change (including change via password reset/recovery), and that this is effective across the application, federated login (if present), and any relying parties.	Yes	The application provides users with the option to terminate all other active sessions after a successful password change, ensuring no unauthorized sessions remain active.
61	Verify that sensitive data and APIs are protected against Insecure Direct Object Reference (IDOR) attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.	No	NIL
62	Verify the application uses session tokens rather than static API secrets and keys, except with legacy implementations.	Yes	The application uses dynamic session tokens rather than static API secrets and keys for authentication. Stateless session tokens are securely generated and managed per session.
63	Verify administrative interfaces use appropriate multi-factor authentication to prevent unauthorized use.	No	NIL
64	Verify the application ensures a full, valid login session or requires re-authentication or secondary verification before allowing any sensitive transactions or account modifications.	Yes	The application ensures a full, valid login session or requires re-authentication or secondary verification before allowing sensitive transactions or account modifications.
65	Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).	No	NIL
66	Verify that the application enforces access control rules on a trusted service layer, especially if client-side access control is present and could be bypassed.	Yes	The application enforces access control rules on a trusted service layer. Client-side access control checks are only used for UI purposes and are always backed by server-side enforcement.
67	Verify that the application sanitizes user input before passing to mail systems to protect against SMTP or IMAP injection.	No	NIL

Sr. No.	Requirements	Applicable	Comments
68	Verify that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.	Yes	All user and data attributes and policy information used by access controls cannot be manipulated by end users. Access control attributes are managed server-side and protected from tampering.
69	Verify that the application avoids the use of eval() or other dynamic code execution features. Where there is no alternative, any user input being included must be sanitized or sandboxed before being executed.	No	NIL
70	Verify that the principle of least privilege exists - users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege. ([C7](https://owasp.org/www-project-proactive-controls/#div-numbering))	Yes	The principle of least privilege is enforced. Users can only access functions, data files, URLs, controllers, services, and other resources for which they have specific authorization.
71	Verify that access controls fail securely including when an exception occurs. ([C10](https://owasp.org/www-project-proactive-controls/#div-numbering))	Yes	Access controls fail securely including when an exception occurs. In the event of a failure, access is denied by default rather than granted, ensuring no unauthorized access during error conditions.
72	Verify that the application protects against SSRF attacks, by validating or sanitizing untrusted data or HTTP file metadata, such as filenames and URL input fields, and uses allow lists of protocols, domains, paths and ports.	No	NIL
73	Verify that the application sanitizes, disables, or sandboxes user-supplied Scalable Vector Graphics (SVG) scriptable content, especially as they relate to XSS resulting from inline scripts, and foreignObject.	No	NIL
74	Verify that sensitive data and APIs are protected against Insecure Direct Object Reference (IDOR) attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.	Yes	Sensitive data and APIs are protected against Insecure Direct Object Reference (IDOR) attacks. We use indirect references, authorization checks, and access control validation for all object access.
75	Verify that output encoding is relevant for the interpreter and context required. For example, use encoders specifically for HTML values, HTML attributes, JavaScript, URL parameters, HTTP headers, SMTP, and others as the context requires, especially from untrusted inputs (e.g. names with Unicode or apostrophes, such as ã•ã•? or O'Hara). ([C4](https://owasp.org/www-project-proactive-controls/#div-numbering))	No	NIL

Sr. No.	Requirements	Applicable	Comments
76	Verify administrative interfaces use appropriate multi-factor authentication to prevent unauthorized use.	Yes	Administrative interfaces use multi-factor authentication (MFA) to prevent unauthorized use. Admin access requires additional verification beyond standard username/password credentials.
77	Verify that the application protects against JSON injection attacks, JSON eval attacks, and JavaScript expression evaluation. ([C4](https://owasp.org/www-project-proactive-controls/#div-numbering))	No	NIL
78	Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).	Yes	The application has defenses against HTTP parameter pollution attacks. Input parsing is handled consistently and duplicate or conflicting parameters are properly managed to prevent exploitation.
79	Verify that the application protects against LDAP injection vulnerabilities, or that specific security controls to prevent LDAP injection have been implemented. ([C4](https://owasp.org/www-project-proactive-controls/#div-numbering))	No	NIL
80	Verify that the application sanitizes user input before passing to mail systems to protect against SMTP or IMAP injection.	Yes	The application sanitizes all user input before passing it to mail systems. This protects against SMTP/IMAP injection and ensures no malicious commands can be injected via email-related functionality.
81	Verify that regulated private data is stored encrypted while at rest, such as Personally Identifiable Information (PII), sensitive personal information, or data assessed likely to be subject to EU's GDPR.	No	NIL
82	Verify that the application avoids the use of eval() or other dynamic code execution features. Where there is no alternative, any user input being included must be sanitized or sandboxed before being executed.	Yes	The application avoids the use of eval() and other dynamic code execution features. Where alternatives do not exist, user input is sanitized and sandboxed before inclusion in dynamic execution.

Sr. No.	Requirements	Applicable	Comments
83	Verify that all cryptographic operations are constant-time, with no 'short-circuit' operations in comparisons, calculations, or returns, to avoid leaking information.	No	NIL
84	Verify that the application protects against SSRF attacks, by validating or sanitizing untrusted data or HTTP file metadata, such as filenames and URL input fields, and uses allow lists of protocols, domains, paths and ports.	Yes	The application protects against SSRF attacks by validating and sanitizing all untrusted data used in HTTP requests. Allowlists and URL validation are implemented to restrict outbound requests.
85	Verify that random GUIDs are created using the GUID v4 algorithm, and a Cryptographically-secure Pseudo-random Number Generator (CSPRNG). GUIDs created using other pseudo-random number generators may be predictable.	No	NIL
86	Verify that the application sanitizes, disables, or sandboxes user-supplied Scalable Vector Graphics (SVG) scriptable content, especially as they relate to XSS resulting from inline scripts, and foreignObject.	Yes	The application sanitizes, disables, or sandboxes user-supplied SVG scriptable content, especially inline scripts and foreignObject elements, to prevent XSS attacks through SVG files.
87	Verify that key material is not exposed to the application but instead uses an isolated security module like a vault for cryptographic operations. ([C8](https://owasp.org/www-project-proactive-controls/#div-numbering))	No	NIL
88	Verify that output encoding is relevant for the interpreter and context required. For example, use encoders specifically for HTML values, HTML attributes, JavaScript, URL parameters, HTTP headers, SMTP, and others as the context requires, especially from untrusted inputs (e.g. names with Unicode or apostrophes, such as ã•ã•? or O'Hara). ([C4](https://owasp.org/www-project-proactive-controls/#div-numbering))	Yes	Output encoding is applied appropriately for the interpreter and context required. HTML entity encoding, JavaScript encoding, URL encoding, and CSS encoding are used in their respective contexts.
89	Verify that the application does not log credentials or payment details. Session tokens should only be stored in logs in an irreversible, hashed form. ([C9, C10](https://owasp.org/www-project-proactive-controls/#div-numbering))	No	NIL

Sr. No.	Requirements	Applicable	Comments
90	Verify that the application protects against JSON injection attacks, JSON eval attacks, and JavaScript expression evaluation. ([C4](https://owasp.org/www-project-proactive-controls/#div-numbering))	Yes	The application protects against JSON injection attacks, JSON eval attacks, and JavaScript expression injection. All JSON parsing uses safe methods and user input is properly escaped.
91	Verify the application protects sensitive data from being cached in server components such as load balancers and application caches.	No	NIL
92	Verify that the application protects against LDAP injection vulnerabilities, or that specific security controls to prevent LDAP injection have been implemented. ([C4](https://owasp.org/www-project-proactive-controls/#div-numbering))	Yes	The application protects against LDAP injection vulnerabilities. Specific security controls are in place to prevent injection through proper input validation, parameterized queries, and escaping.
93	Verify that data stored in browser storage (such as localStorage, sessionStorage, IndexedDB, or cookies) does not contain sensitive data.	No	NIL
94	Verify that regulated private data is stored encrypted while at rest, such as Personally Identifiable Information (PII), sensitive personal information, or data assessed likely to be subject to EU's GDPR.	Yes	Regulated private data including PII and sensitive personal information is stored encrypted at rest using industry-standard encryption algorithms (AES-256). Encryption keys are managed securely.
95	Verify that sensitive data is sent to the server in the HTTP message body or headers, and that query string parameters from any HTTP verb do not contain sensitive data.	No	NIL
96	Verify that all cryptographic operations are constant-time, with no 'short-circuit' operations in comparisons, calculations, or returns, to avoid leaking information.	Yes	All cryptographic operations are implemented as constant-time operations with no short-circuit logic. This prevents timing-based side-channel attacks that could leak sensitive information.
97	Verify accessing sensitive data is audited (without logging the sensitive data itself), if the data is collected under relevant data protection directives or where logging of access is required.	No	NIL

Sr. No.	Requirements	Applicable	Comments
98	Verify that random GUIDs are created using the GUID v4 algorithm, and a Cryptographically-secure Pseudo-random Number Generator (CSPRNG). GUIDs created using other pseudo-random number generators may be predictable.	Yes	Random GUIDs are created using the GUID v4 algorithm with a cryptographically secure pseudo-random number generator (CSPRNG), ensuring sufficient randomness and uniqueness.
99	Verify that connections to and from the server use trusted TLS certificates. Where locally generated or self-signed certificates are used, the server must be configured to only trust specific local CAs and specific self-signed certificates. All others should be rejected.	No	NIL
100	Verify that key material is not exposed to the application but instead uses an isolated security module like a vault for cryptographic operations. ([C8](https://owasp.org/www-project-proactive-controls/#div-numbering))	Yes	Key material is not directly exposed to the application. Keys are managed using an isolated security module or key management service (KMS) to protect cryptographic keys from unauthorized access.
101	Verify that proper certification revocation, such as Online Certificate Status Protocol (OCSP) Stapling, is enabled and configured.	No	NIL
102	Verify that the application does not log credentials or payment details. Session tokens should only be stored in logs in an irreversible, hashed form. ([C9, C10](https://owasp.org/www-project-proactive-controls/#div-numbering))	Yes	The application does not log credentials or payment details. Session tokens are stored only in hashed form in logs, and all sensitive data is masked or excluded from logging output.
103	Verify the application protects sensitive data from being cached in server components such as load balancers and application caches.	Yes	The application protects sensitive data from being cached in server components such as load balancers and application caches. Cache-Control headers and no-store directives are applied to sensitive responses.

Sr. No.	Requirements	Applicable	Comments
104	Verify that data stored in browser storage (such as localStorage, sessionStorage, IndexedDB, or cookies) does not contain sensitive data.	Yes	Data stored in browser storage (localStorage, sessionStorage, IndexedDB, or cookies) does not contain sensitive data. Sensitive information is only stored server-side with secure session management.
105	Verify that sensitive data is sent to the server in the HTTP message body or headers, and that query string parameters from any HTTP verb do not contain sensitive data.	Yes	Sensitive data is sent to the server in the HTTP message body or headers only. Query string parameters of any HTTP method do not contain sensitive data to prevent exposure in server logs and referrer headers.
106	Verify accessing sensitive data is audited (without logging the sensitive data itself), if the data is collected under relevant data protection directives or where logging of access is required.	Yes	Access to sensitive data is audited without logging the sensitive data itself. Audit trails capture who accessed what data, when, and from where, while ensuring the actual sensitive data is not recorded.
107	Verify that connections to and from the server use trusted TLS certificates. Where locally generated or self-signed certificates are used, the server must be configured to only trust specific local CAs and specific self-signed certificates. All others should be rejected.	Yes	Connections to and from the server use trusted TLS certificates from recognized certificate authorities. TLS 1.2 or higher is enforced for all connections, and certificate validity is verified.
108	Verify that proper certification revocation, such as Online Certificate Status Protocol (OCSP) Stapling, is enabled and configured.	Yes	Proper certificate revocation mechanisms including OCSP Stapling are configured and enabled. Certificate revocation status is checked to ensure compromised certificates are not trusted.



mail@tacsecurity.com I tacsecurity.com

© 2026 TAC Security. All rights reserved. This document is copyright protected. No information contained herein, shall, for any purpose other than its intended purpose, be disclosed, transmitted, duplicated, and used in whole and/or in part without prior written permission of TAC Security. Any redistribution or reproduction of part or all of the contents in any form in prohibited and will tantamount to a breach. TAC Security Solutions does not claim this report to be error free, even though every care has been taken to prepare the same.

Copyright © TAC Security - 2026-2027 All Rights Reserved.