Findings

Medium

Finding 87: Content Security Policy (CSP) Header Not Set

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Medium	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	693

Vulnerable Endpoints / Systems (3)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/robots.txt	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

Description

Content Security Policy (CSP) is an added layer of security that helps to

detect and mitigate certain types of attacks, including Cross Site Scripting

(XSS) and data injection attacks. These attacks are used for everything from

data theft to site defacement or distribution of malware. CSP provides a set

of standard HTTP headers that allow website owners to declare approved sources

of content that browsers should be allowed to load on that page — covered

types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects

such as Java applets, ActiveX, audio and video files.

Mitigation

Ensure that your web server, application server, load balancer, etc. is

configured to set the Content-Security-Policy header.

Sample Request(s): Displaying 3 of 4

Request 1

```
Method:           GET
Param:
Attack:
EndpointQuery:    None
EndpointFragment: None
```

Request 2

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Request 3

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment: None
```

References

https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

https://www.w3.org/TR/CSP/

https://w3c.github.io/webappsec-csp/

https://web.dev/articles/csp

https://caniuse.com/#feat=contentsecuritypolicy

https://content-security-policy.com/

Finding 88: Hidden File Found

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Medium	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	538

Vulnerable Endpoints / Systems (4)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/._darcs	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/.bzr	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/.hg	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/BitKeeper	Active	Aug. 30, 2025	Aug. 30, 2025

Description

A sensitive file was identified as accessible or available. This may leak

administrative, configuration, or credential information which can be

leveraged by a malicious individual to further attack the system or conduct

social engineering efforts.

Mitigation

Consider whether or not the component is actually required in production, if

it isn't then disable it. If it is then ensure access to it requires

appropriate authentication and authorization, or limit exposure to internal

systems or specific source IPs, etc.

Sample Request(s): Displaying 3 of 4

Request 1

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Response 1

```
HTTP/1.1 200 OK
```

Request 2

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Response 2

```
HTTP/1.1 200 OK
```

Request 3

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Response 3

```
HTTP/1.1 200 OK
```

References

https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html

Finding 89: Missing Anti-Clickjacking Header

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Medium	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	1021

Vulnerable Endpoints / Systems (3)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/robots.txt	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

Description

The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

Mitigation

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Sample Request(s): Displaying 3 of 4

Request 1

```
Method:           GET
Param:            x-frame-options
Attack:
EndpointQuery:    None
EndpointFragment: None
```

Request 2

```
Method:           GET
Param:            x-frame-options
Attack:
EndpointQuery:    None
EndpointFragment: None
```

Request 3

```
Method:           GET
Param:            x-frame-options
Attack:
EndpointQuery:    None
EndpointFragment: None
```

References

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Finding 90: Sub Resource Integrity Attribute Missing

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Medium	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	345

Vulnerable Endpoints / Systems (3)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/robots.txt	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

Description

The integrity attribute is missing on a script or link tag served by an

external server. The integrity tag prevents an attacker who have gained access

to this server from injecting a malicious content.

Mitigation

Provide a valid integrity attribute to the tag.

Sample Request(s): Displaying 3 of 8

Request 1

```
Method:           GET
Param:
Attack:
```

```
EndpointQuery:     None
EndpointFragment:  None
```

Response 1

```
<link rel="stylesheet"
href="https://s3.chatteron.io/chatteron.io/public/bots/63885832a10c3574b3c295fb/animate.min.css"/>
```

Request 2

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Response 2

```
<script defer="" src="https://web.leena.ai/scripts/sdk.js"></script>
```

Request 3

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Response 3

```
<link rel="stylesheet"
href="https://s3.chatteron.io/chatteron.io/public/bots/63885832a10c3574b3c295fb/animate.min.css"/>
```

References

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Low

Finding 91: Cross-Domain JavaScript Source File Inclusion

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Low	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	829

Vulnerable Endpoints / Systems (3)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/robots.txt	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

Description

The page includes one or more script files from a third-party domain.

Mitigation

Ensure JavaScript source files are loaded from only trusted sources, and the

sources can't be controlled by end users of the application.

Sample Request(s): Displaying 3 of 4

Request 1

```
Method:            GET
Param:             https://web.leena.ai/scripts/sdk.js
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Response 1

```
<script defer="" src="https://web.leena.ai/scripts/sdk.js"></script>
```

Request 2

```
Method:            GET
Param:             https://web.leena.ai/scripts/sdk.js
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Response 2

```
<script defer="" src="https://web.leena.ai/scripts/sdk.js"></script>
```

Request 3

```
Method:            GET
Param:             https://web.leena.ai/scripts/sdk.js
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Response 3

```
<script defer="" src="https://web.leena.ai/scripts/sdk.js"></script>
```

References

Finding 92: Dangerous JS Functions

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Low	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	749

Vulnerable Endpoints / Systems (1)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/main.js	Active	Aug. 30, 2025	Aug. 30, 2025

Description

A dangerous JS function seems to be in use that would leave the site

vulnerable.

Mitigation

See the references for security advice on the use of these functions.

Sample Request(s): Displaying 1 of 1

Request 1

```
Method:           GET
Param:
Attack:
EndpointQuery:    None
EndpointFragment: None
```

Response 1

```
bypassSecurityTrustHtml(
```

References

https://angular.io/guide/security

Finding 93: Insufficient Site Isolation Against Spectre Vulnerability

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Low	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	693

Vulnerable Endpoints / Systems (5)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/assets/firebase-config.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/assets/images/login/beacon-favi-icon.svg	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/favicon.ico	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

Description

Cross-Origin-Resource-Policy header is an opt-in header designed to counter

side-channels attacks like Spectre. Resource should be specifically set as

shareable amongst different origins.

Mitigation

Ensure that the application/web server sets the Cross-Origin-Resource-Policy

header appropriately, and that it sets the Cross-Origin-Resource-Policy header

to 'same-origin' for all web pages.

'same-site' is considered as less secured and should be avoided.

If resources must be shared, set the header to 'cross-origin'.

If possible, ensure that the end user uses a standards-compliant and modern

web browser that supports the Cross-Origin-Resource-Policy header

(https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).

Sample Request(s): Displaying 3 of 12

Request 1

```
Method:           GET
Param:            Cross-Origin-Resource-Policy
Attack:
EndpointQuery:    None
EndpointFragment: None
```

Request 2

```
Method:           GET
Param:            Cross-Origin-Resource-Policy
Attack:
EndpointQuery:    None
EndpointFragment: None
```

Request 3

```
Method:           GET
Param:            Cross-Origin-Resource-Policy
Attack:
EndpointQuery:    None
EndpointFragment: None
```

References

https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy

Finding 94: Permissions Policy Header Not Set

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Low	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	693

Vulnerable Endpoints / Systems (8)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/assets/firebase-config.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/main.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/polyfills.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/robots.txt	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/runtime.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/scripts.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

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.

Mitigation

Ensure that your web server, application server, load balancer, etc. is

configured to set the Permissions-Policy header.

Sample Request(s): Displaying 3 of 9

Request 1

```
Method:           GET
Param:
Attack:
```

```
EndpointQuery:    None
EndpointFragment: None
```

Request 2

```
Method:           GET
Param:
Attack:
EndpointQuery:    None
EndpointFragment: None
```

Request 3

```
Method:           GET
Param:
Attack:
EndpointQuery:    None
EndpointFragment: None
```

References

https://developer.mozilla.org/en-US/docs/Web/HTTP/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/

Finding 95: Strict-Transport-Security Header Not Set

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Low	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	319

Vulnerable Endpoints / Systems (10)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/assets/firebase-config.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/assets/images/login/beacon-favi-icon.svg	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/favicon.ico	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/polyfills.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/robots.txt	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/runtime.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/scripts.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/styles.css	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

Description

HTTP Strict Transport Security (HSTS) is a web security policy mechanism

whereby a web server declares that complying user agents (such as a web

browser) are to interact with it using only secure HTTPS connections (i.e.

HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is

specified in RFC 6797.

Mitigation

Ensure that your web server, application server, load balancer, etc. is

configured to enforce Strict-Transport-Security.

Sample Request(s): Displaying 3 of 11

Request 1

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Request 2

```
Method:            GET
Param:
```

```
Attack:
EndpointQuery:    None
EndpointFragment: None
```

Request 3

```
Method:           GET
Param:
Attack:
EndpointQuery:    None
EndpointFragment: None
```

References

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

Finding 96: Timestamp Disclosure - Unix

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Low	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	497

Vulnerable Endpoints / Systems (2)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/main.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/styles.css	Active	Aug. 30, 2025	Aug. 30, 2025

Description

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

Mitigation

Manually confirm that the timestamp data is not sensitive, and that the data

cannot be aggregated to disclose exploitable patterns.

Sample Request(s): Displaying 2 of 2

Request 1

```
Method:           GET
Param:
Attack:
EndpointQuery:    None
EndpointFragment: None
```

Response 1

```
1490196078
```

Request 2

```
Method:           GET
Param:
Attack:
EndpointQuery:    None
EndpointFragment: None
```

Response 2

```
1490196078
```

References

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

Finding 97: X-Content-Type-Options Header Missing

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Low	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	693

Vulnerable Endpoints / Systems (11)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/assets/firebase-config.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/assets/images/login/beacon-favi-icon.svg	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/favicon.ico	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/main.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/polyfills.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/robots.txt	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/runtime.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/scripts.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/styles.css	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

Description

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.

This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Mitigation

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Sample Request(s): Displaying 3 of 12

Request 1

```
Method:            GET
Param:             x-content-type-options
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Request 2

```
Method:            GET
Param:             x-content-type-options
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Request 3

```
Method:            GET
Param:             x-content-type-options
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

References

https://learn.microsoft.com/en-us/previous-versions/windows/internet-

explorer/ie-developer/compatibility/gg622941(v=vs.85)

https://owasp.org/www-community/Security_Headers

Info

Finding 98: Information Disclosure - Suspicious Comments

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Info	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	615

Vulnerable Endpoints / Systems (4)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/main.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/polyfills.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/runtime.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/scripts.js	Active	Aug. 30, 2025	Aug. 30, 2025

Description

The response appears to contain suspicious comments which may help an

attacker.

Mitigation

Remove all comments that return information that may help an attacker and fix

any underlying problems they refer to.

Sample Request(s): Displaying 3 of 4

Request 1

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Response 1

```
from
```

Request 2

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Response 2

```
user
```

Request 3

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Response 3

```
later
```

References

Finding 99: Modern Web Application

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter
Info	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)

Vulnerable Endpoints / Systems (3)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/robots.txt	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

Description

The application appears to be a modern web application. If you need to explore

it automatically then the Ajax Spider may well be more effective than the

standard one.

Mitigation

This is an informational alert and so no changes are required.

Sample Request(s): Displaying 3 of 4

Request 1

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Response 1

```
<script defer="" src="https://web.leena.ai/scripts/sdk.js"></script>
```

Request 2

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Response 2

```
<script defer="" src="https://web.leena.ai/scripts/sdk.js"></script>
```

Request 3

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Response 3

```
<script defer="" src="https://web.leena.ai/scripts/sdk.js"></script>
```

References

Finding 100: Non-Storable Content

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Info	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	524

Vulnerable Endpoints / Systems (1)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

Description

The response contents are not storable by caching components such as proxy

servers. If the response does not contain sensitive, personal or user-specific

information, it may benefit from being stored and cached, to improve performance.

Mitigation

The content may be marked as storable by ensuring that the following conditions are satisfied:

The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable)

The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood)

The "no-store" cache directive must not appear in the request or response header fields

For caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the response

For caching by "shared" caches such as "proxy" caches, the "Authorization" header field must not appear in the request, unless the response explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control response directives)

In addition to the conditions above, at least one of the following conditions must also be satisfied by the response:

It must contain an "Expires" header field

It must contain a "max-age" response directive

For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive

It must contain a "Cache Control Extension" that allows it to be cached

It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).

Sample Request(s): Displaying 1 of 1

Request 1

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Response 1

```
403
```

References

https://datatracker.ietf.org/doc/html/rfc7234

https://datatracker.ietf.org/doc/html/rfc7231

https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html

Finding 101: Re-Examine Cache-Control Directives

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Info	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	525

Vulnerable Endpoints / Systems (3)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/robots.txt	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

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.

Mitigation

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".

Sample Request(s): Displaying 3 of 4

Request 1

```
Method:            GET
Param:             cache-control
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Request 2

```
Method:            GET
Param:             cache-control
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

Request 3

```
Method:            GET
Param:             cache-control
Attack:
EndpointQuery:     None
EndpointFragment:  None
```

References

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding 102: Storable and Cacheable Content

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE
Info	N.A. / N.A.	Active, Verified	Aug. 30, 2025	0 days	Admin User (admin)	524

Vulnerable Endpoints / Systems (10)

Endpoint	Status	Date Discovered	Last Modified
https://admin.dev.beaconconnect.app/assets/firebase-config.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/assets/images/login/beacon-favi-icon.svg	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/favicon.ico	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/polyfills.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/robots.txt	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/runtime.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/scripts.js	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/sitemap.xml	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app/styles.css	Active	Aug. 30, 2025	Aug. 30, 2025
https://admin.dev.beaconconnect.app	Active	Aug. 30, 2025	Aug. 30, 2025

Description

The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Mitigation

Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:

Cache-Control: no-cache, no-store, must-revalidate, private

Pragma: no-cache

Expires: 0

This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching

servers to not store the response, and to not retrieve the response (without

validation) from the cache, in response to a similar request.

Sample Request(s): Displaying 3 of 11

Request 1

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Request 2

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment: None
```

Request 3

```
Method:            GET
Param:
Attack:
EndpointQuery:     None
EndpointFragment: None
```

References

https://datatracker.ietf.org/doc/html/rfc7234

https://datatracker.ietf.org/doc/html/rfc7231

https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html