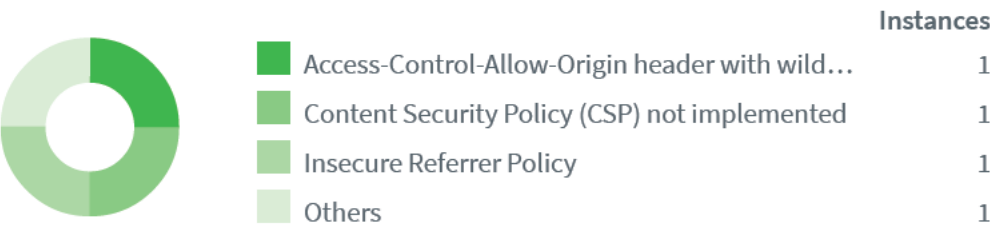
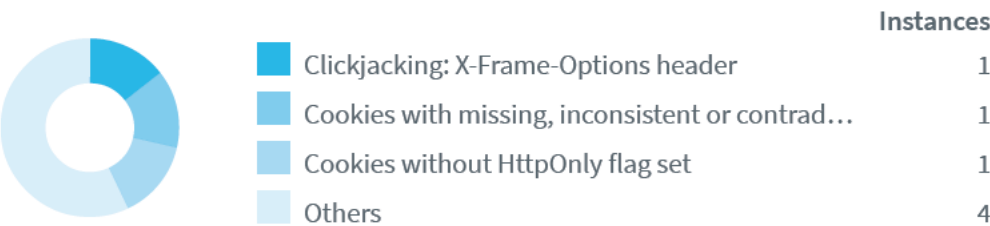













Informational



Low Severity



Impacts

SEVERITY	IMPACT	
 Low	1	Clickjacking: X-Frame-Options header
 Low	1	Cookies with missing, inconsistent or contradictory properties
 Low	1	Cookies without HttpOnly flag set
 Low	1	Cookies without Secure flag set
 Low	1	Documentation files
 Low	1	HTTP Strict Transport Security (HSTS) not implemented
 Low	1	Insecure Inline Frame (iframe)
 Informational	1	Access-Control-Allow-Origin header with wildcard (*) value
 Informational	1	Content Security Policy (CSP) not implemented
 Informational	1	Insecure Referrer Policy
 Informational	1	Subresource Integrity (SRI) not implemented

Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an X-Frame-Options header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

Impact

The impact depends on the affected web application.

<https://dcoderr-frontend-linux-dev.azurewebsites.net/>

Paths without secure XFO header:

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/complete>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/financeCompleted>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/:gig>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/:id>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/dashboard-seller/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/dashboard-user/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a9814617d09b8d4c3ff81>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/:id>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8bf9617d09b8d4c3fdc2>

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8aa0617d09b8d4c3fdb6>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8b55617d09b8d4c3fdb6>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a808e567bebd94c6b12be>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a7f6f567beb225e6b122e>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a79886d953ab473aa8530>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612967c2bd5d2d1ba1c75569>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612964a9bd5d2d19d7c75089>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/61295ba4bd5d2d707ac74bb0>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/61294b11c39b9a5bd6d16402>

Request

GET / HTTP/1.1
Referer: <https://dcderr-frontend-linux-dev.azurewebsites.net/>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4298.0 Safari/537.36
Host: dcderr-frontend-linux-dev.azurewebsites.net
Connection: Keep-alive

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

[The X-Frame-Options response header](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)

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

[Clickjacking](https://en.wikipedia.org/wiki/Clickjacking)

<https://en.wikipedia.org/wiki/Clickjacking>

[OWASP Clickjacking](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)

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

[Frame Buster Buster](https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

<https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed>

Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

<https://dcderr-frontend-linux-dev.azurewebsites.net/>

Verified

List of cookies with missing, inconsistent or contradictory properties:

- <https://dcderr-frontend-linux-dev.azurewebsites.net/registration/complete>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/create-api/financeCompleted>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and

sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/:gig>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/:id>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/dashboard-seller/>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/registration/>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/edit-api/>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/dashboard-user/>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a9814617d09b8d4c3ff81>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/:id>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8bf9617d09b8d4c3fdc2>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8aa0617d09b8d4c3fdb6>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8b55617d09b8d4c3fdb6>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a808e567bebd94c6b12be>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a7f6f567beb225e6b122e>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a79886d953ab473aa8530>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612967c2bd5d2d1ba1c75569>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612964a9bd5d2d19d7c75089>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/61295ba4bd5d2d707ac74bb0>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/61294b11c39b9a5bd6d16402>

Cookie was set with:

```
Set-Cookie: auth.strategy=local; Path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

Request

```
GET / HTTP/1.1
```

```
Referer: https://dcoderr-frontend-linux-dev.azurewebsites.net/
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

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

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

[MDN | Set-Cookie](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie>

[Securing cookies with cookie prefixes](https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/)

<https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/>

[Cookies: HTTP State Management Mechanism](https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)

<https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05>

[SameSite Updates - The Chromium Projects](https://www.chromium.org/updates/same-site)

<https://www.chromium.org/updates/same-site>

[draft-west-first-party-cookies-07: Same-site Cookies](https://tools.ietf.org/html/draft-west-first-party-cookies-07)

<https://tools.ietf.org/html/draft-west-first-party-cookies-07>

Cookies without HttpOnly flag set

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

<https://dcoderr-frontend-linux-dev.azurewebsites.net/>

Verified

Cookies without HttpOnly flag set:

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/complete>

```
Set-Cookie: auth.strategy=local; Path=/
```

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/financeCompleted>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/:gig>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/:id>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/dashboard-seller/>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/dashboard-user/>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a9814617d09b8d4c3ff81>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/:id>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8bf9617d09b8d4c3fdc2>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8aa0617d09b8d4c3fdb6>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8b55617d09b8d4c3fdb6>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a808e567bebd94c6b12be>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a7f6f567beb225e6b122e>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a79886d953ab473aa8530>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612967c2bd5d2d1ba1c75569>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612964a9bd5d2d19d7c75089>

```
Set-Cookie: auth.strategy=local; Path=/
```

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/61295ba4bd5d2d707ac74bb0>

```
Set-Cookie: auth.strategy=local; Path=/
```

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/61294b11c39b9a5bd6d16402>

```
Set-Cookie: auth.strategy=local; Path=/
```

Request

```
GET / HTTP/1.1
Referer: https://dcderr-frontend-linux-dev.azurewebsites.net/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: dcderr-frontend-linux-dev.azurewebsites.net
Connection: Keep-alive
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Cookies without Secure flag set

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

Cookies without Secure flag set:

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/complete>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/financeCompleted>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/:gig>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/:id>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/dashboard-seller/>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/dashboard-user/>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a9814617d09b8d4c3ff81>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/:id>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8bf9617d09b8d4c3fdc2>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8aa0617d09b8d4c3fdb6>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8b55617d09b8d4c3fdbc>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a808e567bebd94c6b12be>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a7f6f567beb225e6b122e>

Set-Cookie: auth.strategy=local; Path=/

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a79886d953ab473aa8530>

```
Set-Cookie: auth.strategy=local; Path=/
```

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612967c2bd5d2d1ba1c75569>

```
Set-Cookie: auth.strategy=local; Path=/
```

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612964a9bd5d2d19d7c75089>

```
Set-Cookie: auth.strategy=local; Path=/
```

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/61295ba4bd5d2d707ac74bb0>

```
Set-Cookie: auth.strategy=local; Path=/
```

- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/61294b11c39b9a5bd6d16402>

```
Set-Cookie: auth.strategy=local; Path=/
```

Request

```
GET / HTTP/1.1
Referer: https://dcderr-frontend-linux-dev.azurewebsites.net/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: dcderr-frontend-linux-dev.azurewebsites.net
Connection: Keep-alive
```

Recommendation

If possible, you should set the Secure flag for these cookies.

Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

<https://dcoderr-frontend-linux-dev.azurewebsites.net/>

Documentation files:

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/README.md>

File contents (first 100 characters):

```
# STATIC

**This directory is not required, you can delete it if you don't want to use
it.**

This d ...
```

Request

```
GET /README.md HTTP/1.1
Cookie: auth.strategy=local
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: dcoderr-frontend-linux-dev.azurewebsites.net
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file accessible from internet.

HTTP Strict Transport Security (HSTS) not implemented

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessible using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

<https://dcderr-frontend-linux-dev.azurewebsites.net/>

URLs where HSTS is not enabled:

- <https://dcderr-frontend-linux-dev.azurewebsites.net/registration/complete>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/create-api/financeCompleted>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/create-api/>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/registration/:gig>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/registration/>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/edit-api/:id>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/dashboard-seller/>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/edit-api/>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/dashboard-user/>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a9814617d09b8d4c3ff81>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/:id>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8bf9617d09b8d4c3fdc2>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8aa0617d09b8d4c3fdb6>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8b55617d09b8d4c3fdbc>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a808e567bebd94c6b12be>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a7f6f567beb225e6b122e>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612a79886d953ab473aa8530>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612967c2bd5d2d1ba1c75569>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/612964a9bd5d2d19d7c75089>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/61295ba4bd5d2d707ac74bb0>
- <https://dcderr-frontend-linux-dev.azurewebsites.net/api-profile/61294b11c39b9a5bd6d16402>

Request

```
GET / HTTP/1.1
Referer: https://dcderr-frontend-linux-dev.azurewebsites.net/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: dcderr-frontend-linux-dev.azurewebsites.net
Connection: Keep-alive
```

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org

<https://hstspreload.org/>

[Strict-Transport-Security](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

Insecure Inline Frame (iframe)

The web page was found to be using an Inline Frame ("iframe") to embed a resource, such as a different web page. The Inline Frame is either configured insecurely, or not as securely as expected. This vulnerability alert is based on the origin of the embedded resource and the iframe's sandbox attribute, which can be used to apply security restrictions as well as exceptions to these restrictions.

Impact

When a web page uses an insecurely configured iframe to embed another web page, the latter may manipulate the former, and trick its visitors into performing unwanted actions.

<https://dcoderr-frontend-linux-dev.azurewebsites.net/>

Verified

An iframe tag references an external resource, and no sandbox attribute is set.

Request

```
GET / HTTP/1.1
Referer: https://dcoderr-frontend-linux-dev.azurewebsites.net/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: dcoderr-frontend-linux-dev.azurewebsites.net
Connection: Keep-alive
```

Recommendation

Review the iframe's purpose and environment, and use the sandbox attribute to secure the iframe while applying sandbox directives to ease security restrictions if necessary.

References

[MDN | iframe: The Inline Frame Element](https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe)

<https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe>

[HTML Standard: iframe](https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element)

<https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element>

[HTML 5.2: 4.7. Embedded content](https://www.w3.org/TR/html52/semantics-embedded-content.html#element-attrdef-iframe-sandbox)

<https://www.w3.org/TR/html52/semantics-embedded-content.html#element-attrdef-iframe-sandbox>

Access-Control-Allow-Origin header with wildcard (*) value

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on the value of the Origin request header, "*", or "null" in the response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHttpRequest) requests to the site and access the responses.

Impact

Any website can make XHR requests to the site and access the responses.

<https://dcderr-frontend-linux-dev.azurewebsites.net/>

Affected paths (max. 25):

- /fonts/

Request

GET / HTTP/1.1

Origin: https://dcderr-frontend-linux-dev.azurewebsites.net

Cookie: auth.strategy=local

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/88.0.4298.0 Safari/537.36

Host: dcderr-frontend-linux-dev.azurewebsites.net

Recommendation

Check whether Access-Control-Allow-Origin: * is appropriate for the resource/response.

References

[Test Cross Origin Resource Sharing \(OTG-CLIENT-007\)](https://www.owasp.org/index.php/Test_Cross-Origin_Resource_Sharing_(OTG-CLIENT-007))

[https://www.owasp.org/index.php/Test_Cross-Origin_Resource_Sharing_\(OTG-CLIENT-007\)](https://www.owasp.org/index.php/Test_Cross-Origin_Resource_Sharing_(OTG-CLIENT-007))

[Cross-origin resource sharing](https://en.wikipedia.org/wiki/Cross-origin_resource_sharing)

https://en.wikipedia.org/wiki/Cross-origin_resource_sharing

[Cross-Origin Resource Sharing](http://www.w3.org/TR/cors/)

<http://www.w3.org/TR/cors/>

[CrossOriginRequestSecurity](https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity)

<https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity>

[Cross-Origin Resource Sharing \(CORS\) and the Access-Control-Allow-Origin Header](https://www.acunetix.com/blog/web-security-zone/cross-origin-resource-sharing-cors-access-control-allow-origin-header/)

<https://www.acunetix.com/blog/web-security-zone/cross-origin-resource-sharing-cors-access-control-allow-origin-header/>

[PortSwigger Research on CORS misconfiguration](https://portswigger.net/research/exploiting-cors-misconfigurations-for-bitcoins-and-bounties)

<https://portswigger.net/research/exploiting-cors-misconfigurations-for-bitcoins-and-bounties>

Content Security Policy (CSP) not implemented

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.

Content Security Policy (CSP) can be implemented by adding a Content-Security-Policy header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP

header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<https://dcoderr-frontend-linux-dev.azurewebsites.net/>

Paths without CSP header:

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/complete>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/financeCompleted>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/:gig>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/:id>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/dashboard-seller/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/dashboard-user/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a9814617d09b8d4c3ff81>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/:id>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8bf9617d09b8d4c3fdc2>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8aa0617d09b8d4c3fdb6>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8b55617d09b8d4c3fdbc>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a808e567bebd94c6b12be>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a7f6f567beb225e6b122e>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a79886d953ab473aa8530>

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612967c2bd5d2d1ba1c75569>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612964a9bd5d2d19d7c75089>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/61295ba4bd5d2d707ac74bb0>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/61294b11c39b9a5bd6d16402>

Request

```
GET / HTTP/1.1
Referer: https://dcoderr-frontend-linux-dev.azurewebsites.net/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: dcoderr-frontend-linux-dev.azurewebsites.net
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)

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

[Implementing Content Security Policy](https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Insecure Referrer Policy

Referrer Policy controls behaviour of the Referer header, which indicates the origin or web page URL the request was made from. The web application uses insecure Referrer Policy configuration that may leak user's information to third-party sites.

Impact

In some situations, an attacker may leak a user's private data

<https://dcoderr-frontend-linux-dev.azurewebsites.net/>

URLs where Referrer Policy configuration is insecure:

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/complete>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/financeCompleted>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/create-api/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/:gig>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/registration/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/:id>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/dashboard-seller/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/edit-api/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/dashboard-user/>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a9814617d09b8d4c3ff81>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/:id>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8bf9617d09b8d4c3fdc2>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8aa0617d09b8d4c3fdb6>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a8b55617d09b8d4c3fdbc>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a808e567bebd94c6b12be>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a7f6f567beb225e6b122e>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612a79886d953ab473aa8530>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612967c2bd5d2d1ba1c75569>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/612964a9bd5d2d19d7c75089>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/61295ba4bd5d2d707ac74bb0>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/api-profile/61294b11c39b9a5bd6d16402>

Request

```
GET / HTTP/1.1
Referer: https://dcoderr-frontend-linux-dev.azurewebsites.net/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: dcoderr-frontend-linux-dev.azurewebsites.net
Connection: Keep-alive
```

Recommendation

Consider setting Referrer-Policy header to 'strict-origin-when-cross-origin' or a stricter value

References

Referrer-Policy

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

Subresource Integrity (SRI) not implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

<https://dcoderr-frontend-linux-dev.azurewebsites.net/>

Pages where SRI is not implemented:

- <https://dcoderr-frontend-linux-dev.azurewebsites.net/>
Script SRC: <https://apis.google.com/js/platform.js?onload=onLoad>
- <https://dcoderr-frontend-linux-dev.azurewebsites.net/>
Script SRC: <https://js.stripe.com/v3/>

Request

```
GET / HTTP/1.1
Referer: https://dcoderr-frontend-linux-dev.azurewebsites.net/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: dcoderr-frontend-linux-dev.azurewebsites.net
Connection: Keep-alive
```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a `<script>` element that implements Subresource Integrity (SRI).

For example, you can use the following `<script>` element to tell a browser that before executing the `https://example.com/example-framework.js` script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQholwx4JwY8wC"
crossorigin="anonymous"></script>
```

References


[Subresource Integrity](https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)

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

[SRI Hash Generator](https://www.srihash.org/)

<https://www.srihash.org/>

Coverage

 <https://dcoderr-frontend-linux-dev.azurewebsites.net>

 _nuxt

 001cdab.js

 0199ec6.js


 0a71a55.js

 1817eca.js

 18b688f.js

 201def4.js


 2a6c4d0.js

 47aac45.js

 4ef8d7d.js

 58676b4.js

 6392bbd.js

 8c66260.js

 8ec30b1.js

 9861fe3.js

 abe7c22.js

 b6c5e65.js

 bbb4225.js

 bec1b07.js

 c585a16.js

 d0b3ec9.js

 d35cdfa.js

 d6898de.js

 d847512.js

 d86d147.js

 dfb1335.js

 e85750e.js

 f53ce68.js

 fb0859c.js

 manifest.70589522.json

📁 api-profile

📄 :id

📄 60318b5574f86513b7181aaa

📄 60765f2f13f921df10527f8e

📄 609ec87aed355b9f271f5764

📄 60aabe02a410e0a8192542f7

📄 60ab2419787fe847c37cec43

📄 60c39e49112a1e821236689f

📄 60ce2f5cf2ddd4621ec88748

📄 60d4ccdb228198518057558b

📄 60db905215fde56c612c6f61

📄 60de36fa02cdb5f1a37af5f3

📄 60df3af644b383ad3821328c

📄 60df3fb544b3831227213298

📄 60df44d944b3839c5621329b

📄 60df499044b38319422132b0

📄 60df4e6d44b383c6b32132b8

📄 60e652b7438025e0af74759f

📄 60e8bc88b27a662cd0dd9a61

📄 60e8c7c1438025e0af7479b2

📄 60fcb131abceecac8bc210e6

📄 60fcb3b1abceecac8bc210ea

📄 6106ba2a6920cc58f13ee10f

📄 6106bcd4e8262d597d47c6b3

📄 610b349228e373192151ab0f

📄 610dde7e92470943cd104921

📄 61101c84fd126d6255901b9a

📄 6116bd4726ff0f35a2880446


































📄 61227ab66747c229ccea0def

📄 612299609b130b2f30f02dda

📄 6125a426c39b9a64d0d15a0a

📄 6125a4bcc39b9a66f4d15a0d

📄 61279847c39b9afdbfd15ea8

 61294b11c39b9a5bd6d16402
 61295ba4bd5d2d707ac74bb0
 612964a9bd5d2d19d7c75089
 612967c2bd5d2d1ba1c75569
 612a79886d953ab473aa8530
 612a7f6f567beb225e6b122e
 612a808e567bebd94c6b12be
 612a8aa0617d09b8d4c3fdb6
 612a8b55617d09b8d4c3fdb6
 612a8bf9617d09b8d4c3fdc2
 612a9814617d09b8d4c3ff81
 create-api
 completed
 :id
 financeCompleted
 dashboard-seller
 customers
 :id
 dashboard-user
 billing
 :id
 usage
 :id
 data
 edit-api
 :id
 completed
 fonts
 images
 registration
 :gig
 complete
 create-api

 dashboard-seller

 dashboard-user

 privacy

 README.md

 settings

 sw.js

 terms