Adding hosts to your Content-Security-Policy (CSP) for Userlane

Last Modified on 03.07.2023

About Content Security Policies (CSP)

A Content Security Policy (CSP) is a security mechanism implemented by web applications to mitigate the risk of various types of attacks.

It allows to define a set of policies that specify which sources of content, such as scripts, stylesheets, images, and fonts, are allowed to be loaded and executed within their web application. By restricting the origins of content, CSP helps prevent the execution of malicious scripts or the loading of unauthorized resources, thereby enhancing the overall security of the application.

If you are using Content Security Policies (CSP) to protect your Application, you need to add some policies to make sure Userlane can work correctly and can be shown to your users.

Allowing the script execution for userlane.com

Add the following hostnames to your CSP `default-src` , `script-src` , `style-src` , `img-src` , `connect-src` , and `font-src` attribute:

```
https://*.userlane.com
https://*.sentry.io
```

This allows all userlane.com images, scripts, fonts, and styles to be loaded into your Application. This is necessary to make sure Userlane can function correctly.

ℹ We use Sentry for monitoring real-time our Application's code health.