Cross-Site Scripting (XSS) is a security vulnerability where an attacker places one or more malicious client-side scripts into an app's rendered content. A Content Security Policy (CSP) helps protect against XSS attacks by informing the browser of valid:

* Sources for loaded content, including scripts, stylesheets, and images.
* Actions taken by a page, specifying permitted URL targets of forms.
* Plugins that can be loaded.

To apply a CSP to an app, the developer specifies several CSP content security *directives* in one or more Content-Security-Policy headers or <meta> tags.

**Blazor WebAssembly**

In the <head> content of the wwwroot/index.html host page, apply the following code:

<meta http-equiv="Content-Security-Policy"

content="base-uri 'self';

block-all-mixed-content;

default-src 'self';

img-src data: https:;

object-src 'none';

script-src 'self'

'sha256-v8v3RKRPmN4odZ1CWM5gw80QKPCCWMcpNeOmimNL2AA='

'unsafe-eval'

https://code.jquery.com/

https://cdn.datatables.net/

https://cdn.datatables.net/;

style-src 'self'

'unsafe-inline'

https://cdn.datatables.net/;

upgrade-insecure-requests;">

Read More here: https://docs.microsoft.com/en-us/aspnet/core/blazor/security/content-security-policy?view=aspnetcore-5.0