Same-Origin Policy - CORS

- Very strict - often relaxed with Cross Origin Resource Sharing (CORS)
- Additional HTTP headers that specify permitted/trusted origins and access control e.g **Access-Control-Allow-Origin**

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

Content Security Policy (CSP)

- Intended to mitigate XSS and other injection attacks
- Server returns **Content-Security-Policy** HTTP header or <meta> tag
- Controls what resources can be loaded, how they must be loaded and what can be executed.

```
<meta
  http-equiv="Content-Security-Policy"
  content="default-src 'self'; img-src https://*; child-src 'none';" />
```

All content must come from origin, can include images from https origins, no inline scripts, no nested contexts like iframes are permitted

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