

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

Privilege Separation

- Intended to impact of vulnerabilities exploited
- Divide client application into modules where each is limited to specific privileges required
- Helps to fine tune security controls and enforce boundaries
- E.g Admin area, authenticated area, guest/anonymous area etc