Content Security Policy

Se define en la aplicación web pero es el navegador el que la debe implementar. Se usa para evitar la ejecución de ciertas cosas, como por ejemplo, javaScript. Para ver que tan buena es una CSP podemos ir a csp-evaluator.withgoogle.com.

Es un mecanismo que permite restringir los contenidos que el navegador puede cargar en un sitio web. Se usa para detener ataques de inyección de código y XSS

```
content-security-policy: <policy-directive>; <policy-directive>
```

Principales directivas

- Directiva por defecto: Restringe el origen de los datos al propio sitio web

```
content-security-policy: default-src 'self'
```

- Directiva script: Controla el origen de todos los scripts

```
content-security-policy: default-src 'self'
```

- frame ancestor: permite definir cuando es posible incluir una web dentro de un iframe

```
content-security-policy: frame-ancestors 'none';
content-security-policy: frame-ancestors 'self' https://WWW.patata.porg;
```

Inyección de entidades externas en XML