CSP & Cookies flags

CSP (Content Security Policy)

CSP is a feature that helps to prevent or minimize the risk of certain types of security threats. It consists of a series of instructions from a website to a browser, which instruct the browser to place restrictions on the things that the code comprising the site is allowed to do.

The primary use case for CSP is to control which resources, particularly JavaScript resources, are allowed to load. This is mainly used as a defense against XSS attacks, in which an attacker can inject malicious code into the victim's site.

A CSP can have other purposes as well, including defending against clickjacking and helping to ensure that a site's pages will be loaded over HTTPS.

Cookie flags

1. **Secure:**
   - This flag instructs the browser not to send this cookie over plain-text HTTP channels, cookie is sent only over TLS (HTTPS).
   - Only works if site is served over HTTPS, cookies set without Secure can leak on HTTP.

2. **HTTPOnly:**
   - This flag instructs the browser not to allow JavaScript to access the cookie value. This is an important mitigation step for XSS attacks.
   - Prevents cookie access but does not stop an attacker from causing requests that include the cookie (CSRF). Use **SameSite** and anti-CSRF tokens too.

3. **SameSite** (Strict, Lax, None)**:** This flag cookie was created as an attempt to reduce the exploitability of CSRF attacks.
   - **Strict:** cookie only sent for same-site navigation.

- **Lax:** allows some top-level cross-site GET navigations (default in many browsers).
- **None:** sent in all contexts but must be paired with **Secure**.

Example:

```
Set-Cookie: __Secure-MOZSESSIONID=7307d70a86bd4ab5a00499762; Max-Age=2592000;
Domain=example.org; Path=/; Secure; HttpOnly; SameSite=Lax
```