Class Notes Monday

November 15th , 2021

**Content Security Policy:**

* XSS Protections
* Defined by the developers
* Enforced by the browser
* Doesn’t stop other vulnerabilities such as SQL Injections, Broken Access Control, Crypto F’s
* Relies on Fetch Directives, Navigation Directives and Page Directives
* Can define some **directives** in the HTTP headers, <meta> tag, or

Relies on something called “**Directives**” that tell the browser where they’re allowed to do

**Fetch Directives:**

* Self -> Origin of the CSP (Protocol, Host, Domain, Port) Ex: cs558.walls.ninja
* None
* Scheme
* Domains
* Paths
* Nonce/Hash

**Navigation Directives:**

* Can define what paths are allowed to be visited?

**Page Directives:**

* Can define what can happen on a particular page

**Form Action Directives:**

* Can define sources that are valid for actions

**UI Redress Attack:**

* Click Jacking (Can be avoided with X-Frame options: Deny, Same Origin)
* Display Fraud

Frame-Ancestors

* Check all frame children

URL example.com/apples

Frame-src ‘none’, frame-ancesters'self’

/oranges/

Frame-src self, frame-ancesters'none’