Identifying JS files

1. App relevant stuff
    a. Lazy loaded JS
    b. Vendor libraries
2. Third party
    a. Can pivot to XSS?
    b. Steal relevant info?
3. Tracking
    a. Window.location.href leak
4. HTML <script> tags

Analysis

1. Beautification
    a. pprettier
        i. https://github.com/microsoft/parallel-prettier
    b. VSCode
2. Identifying client-side paths
    a. Hash changes
3. Identifying server-side paths
    a. API endpoints
    b. HTTP Verbs
4. Sources & Sinks
    a. Sources
        i. URLSearchParams
        ii. location.* / Hash
            1. location.assign
            2. location.replace
        iii. Window.open
        iv. Cookies
        v. Localstorage/sessionstorage
    b. Sinks
        i. Location.href (always check CSP)
        ii. innerhtml
        iii. .html
        iv. unsafe templating
        v. dangerouslysethtml
        vi. createElement (iframe, a, script, etc)

~~5. Dynamic analysis (devtools 101)~~

6. JS Adjacents
    a. Feature Flags
    b. function isFeatureFlagEnabled(){...}
    c. M&R rule:
        i. Response Body
        ii. isFeatureFlagEnabled(){
        iii. isFeatureFlagEnabled(){return true;

iv.

Additional Topics

1. Dynamic Wordlist Generation
2. Longterm monitoring via regex & crontab