Document Object Model XSS

Refer to this link for basic explanation and common sources/ sinks:

<https://portswigger.net/web-security/dom-based>

Refer to this link for DOM invader docs:

<https://portswigger.net/burp/documentation/desktop/tools/dom-invader/enabling>

We can use DOM Invader to help us locate DOM XSS.

Open dev tools and navigate to the DOM invader tab (only works in Burp Browser)

* Make sure all Misc settings are selected.

Copy the canary value and inject it everywhere you can.

You will see the alerts populate the DOM section within dev tools.

The “value” part will update as you change your payload making it really easy to see how the app is manipulating your payload (what values are escaped, encoded …….)

Clicking the Stack Trace link on the right will allow you to see the client-side code and highlight the line your input was passed into.

* Press the link then navigate to the console tab of dev tools. Once there select the topmost link within the console tab. From here you will be brought to the code and the line where you input was seen is highlighted.

Graphical user interface, text, application, email

Description automatically generatedBasics:

Text, Word

Description automatically generatedText

Description automatically generated