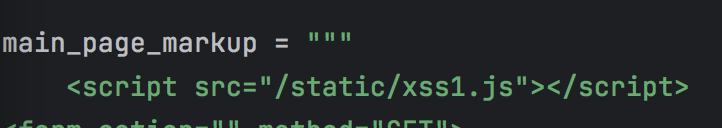
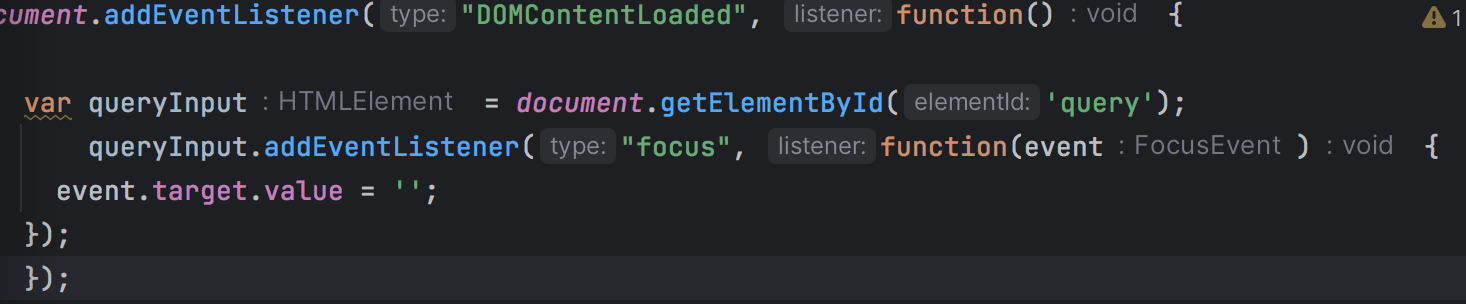
All the way is move inline script to outside and script-src itself

<meta http-equiv="Content-Security-Policy" content="default-src 'self';  
script-src 'self';">

1,

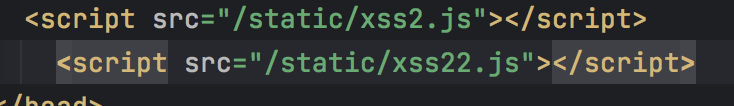




rewrite onfocus to listen. it only run it outside script to defend XSS attack

if use <script> alert("") </script>, it will refuse

2,

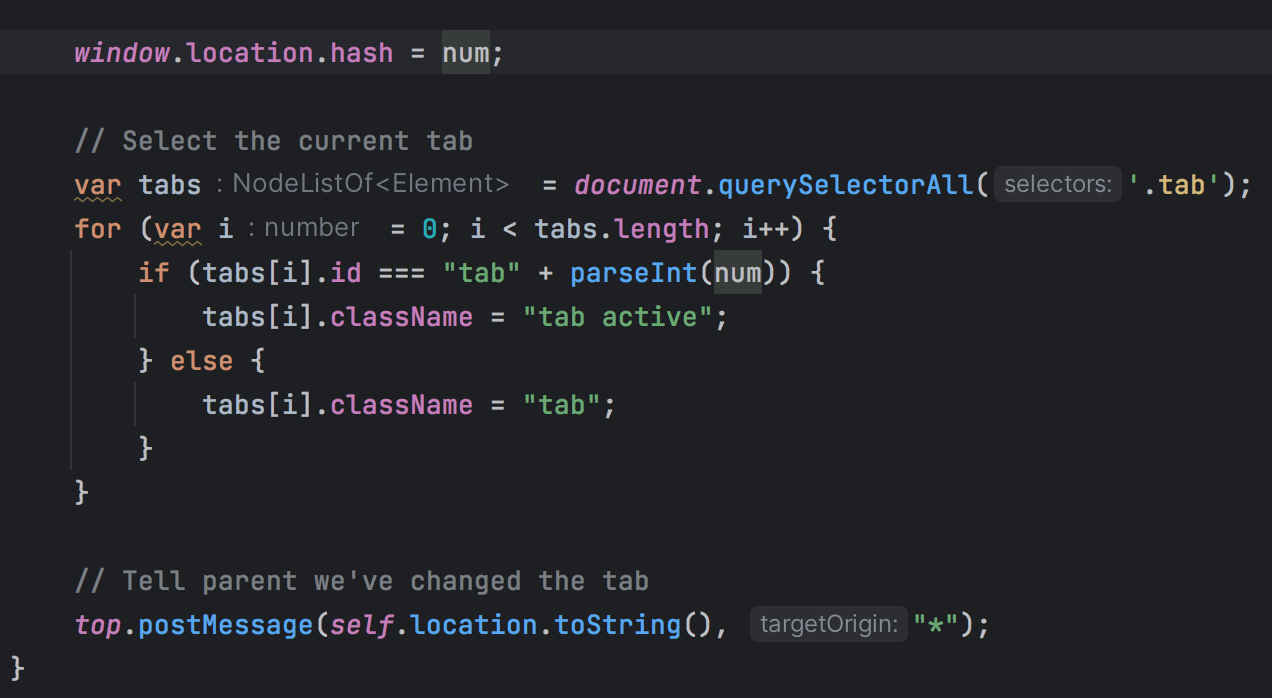


CSP to allow it outside script, and use the nonce from back-end to trust the script

If use <img src='' onerror="alert('')" />, it will refuse

3,





rewrite the onclick function in onload

if use 127.0.0.1:5000/level3/frame#1' onerror="alert(1)", it will refuse and report img 404

since it only trust outside script

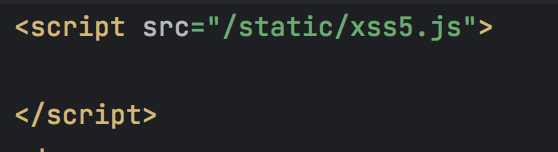
4,

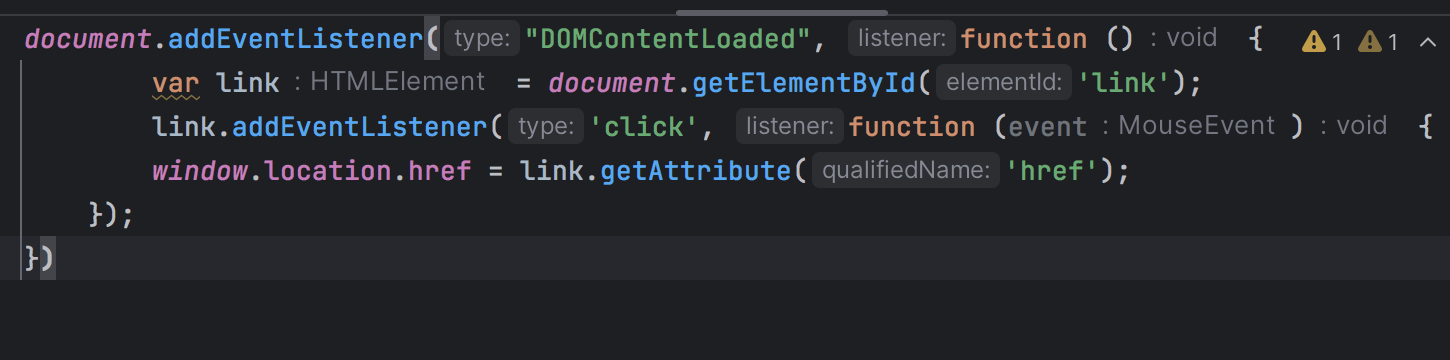


trust itself outside script and add the listener to dom, change html language to js

If use 3'); alert('1, it will refuse and count down after 3 seconds

5,





use it outside script to defend the xss by <a> tag

<http://127.0.0.1:5000/level5/frame/signup?next=javascript:alert(1)>

it will refuse when change the url and click the Next >>

6,



use it outside script.

if use 127.0.0.1:5000/last/frame#HTTPS://www.google.com/jsapi?callback=alert

127.0.0.1:5000/last/frame#//www.google.com/jsapi?callback=alert

127.0.0.1:5000/last/frame#data:text(),alert()

it will refuse