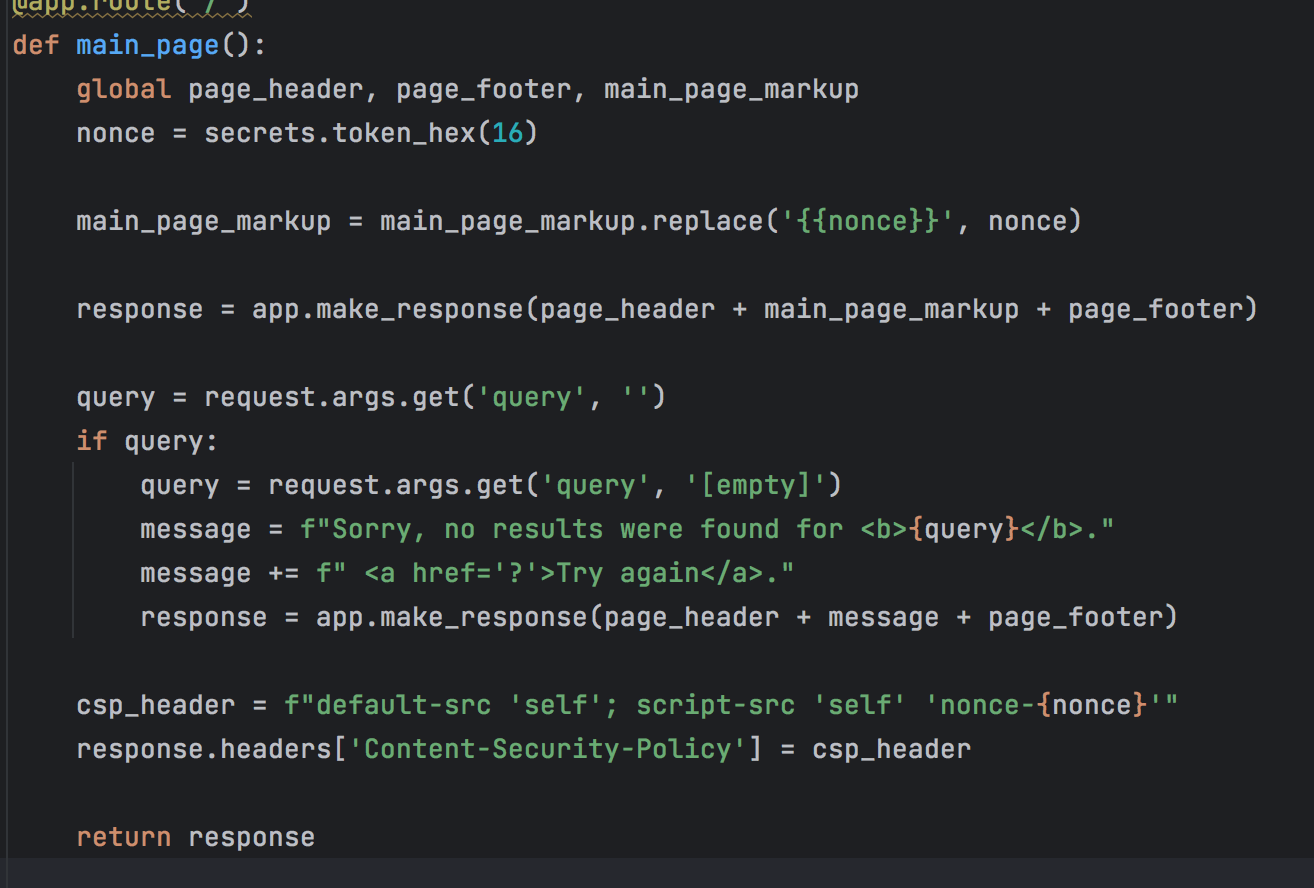
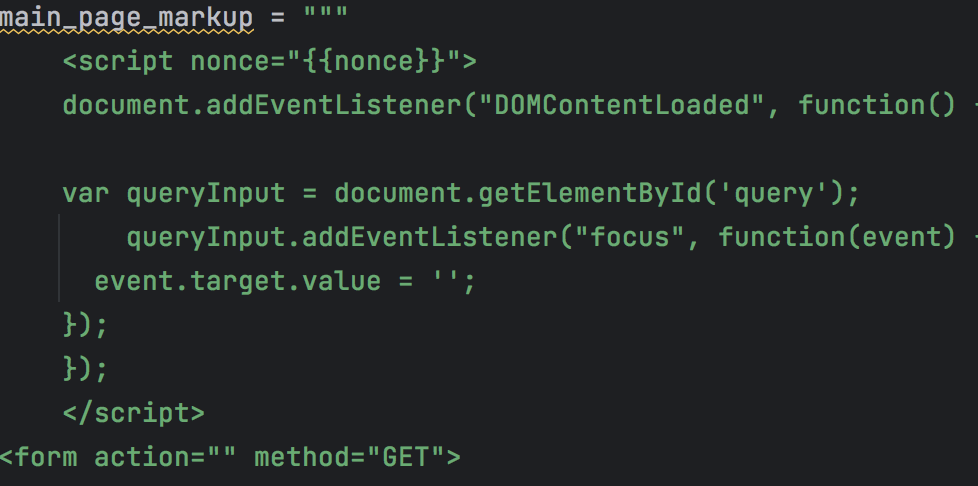
listen to DOMContentLoaded is to get the tag id after the tag is loaded completely

create a random secret key to encrypt session

create a random 16 byte nonce and save in session to front-end

1,

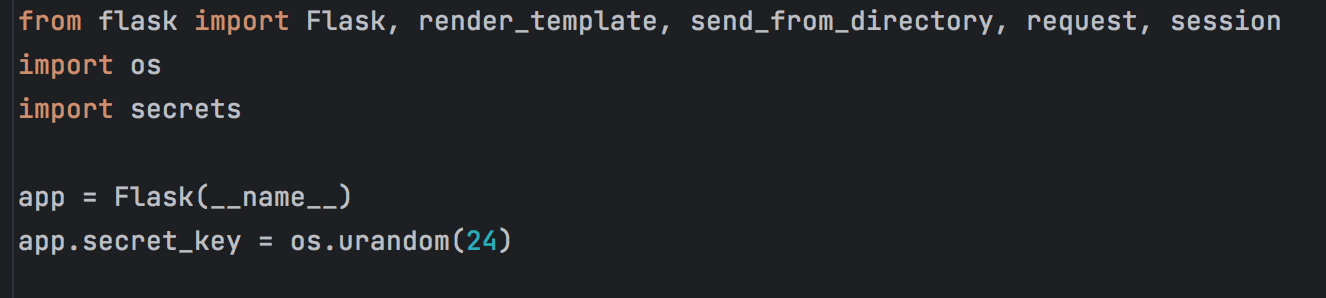


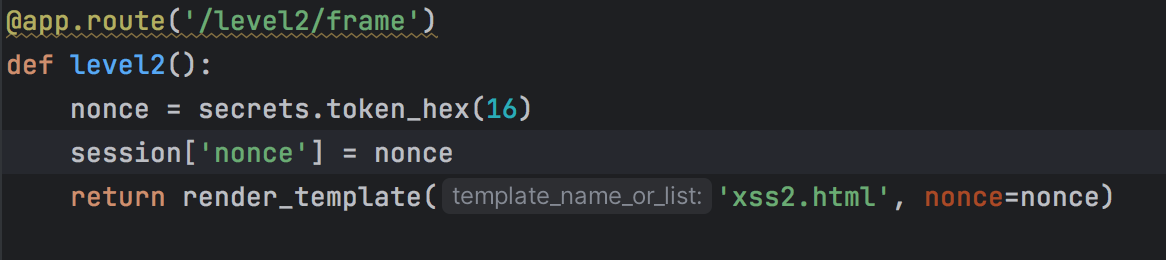


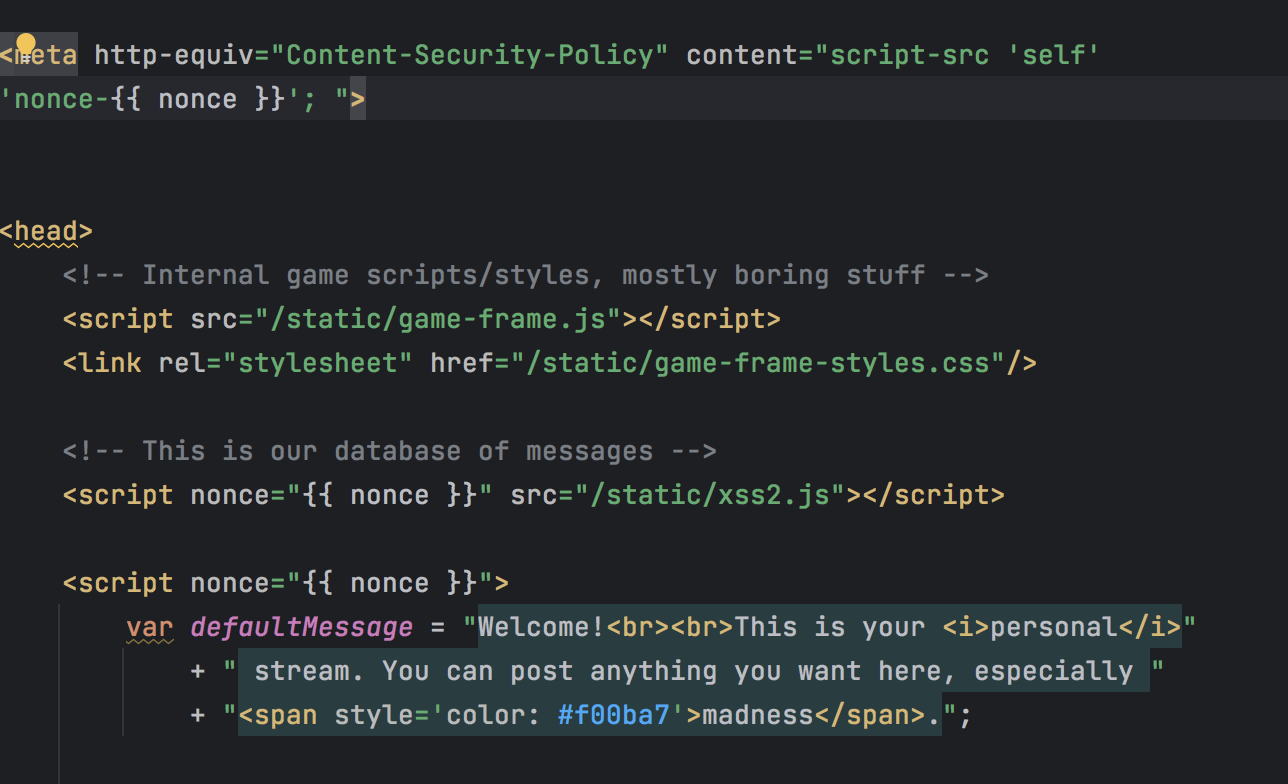
rewrite onfocus to listen and replace nonce value to global main-page-makeup to receive the nonce, it only run itself trust and same nonce value script to defend XSS attack

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

2,



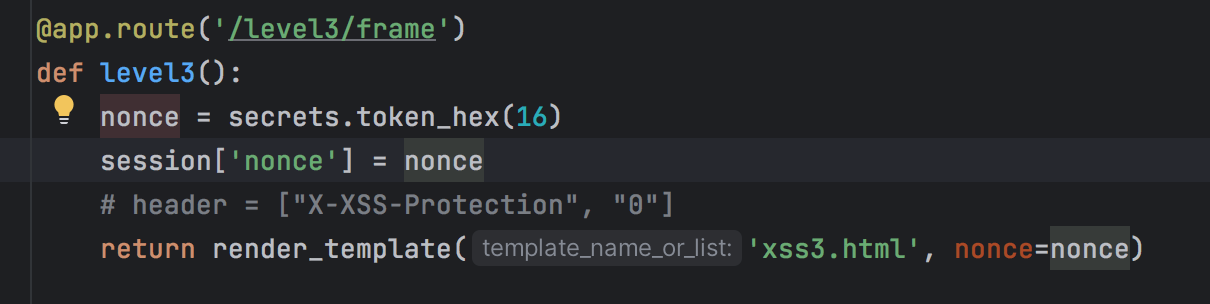




CSP to allow itself trust and same nonce value script, and use the nonce from back-end to trust the script

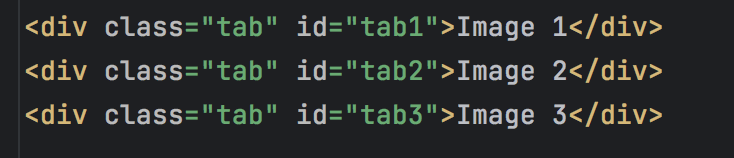
If use <img src='' onerror="alert('')" />, it will refuse

3,









since use nonce, cannot handler event in html tag, so rewrite the onclick function in onload

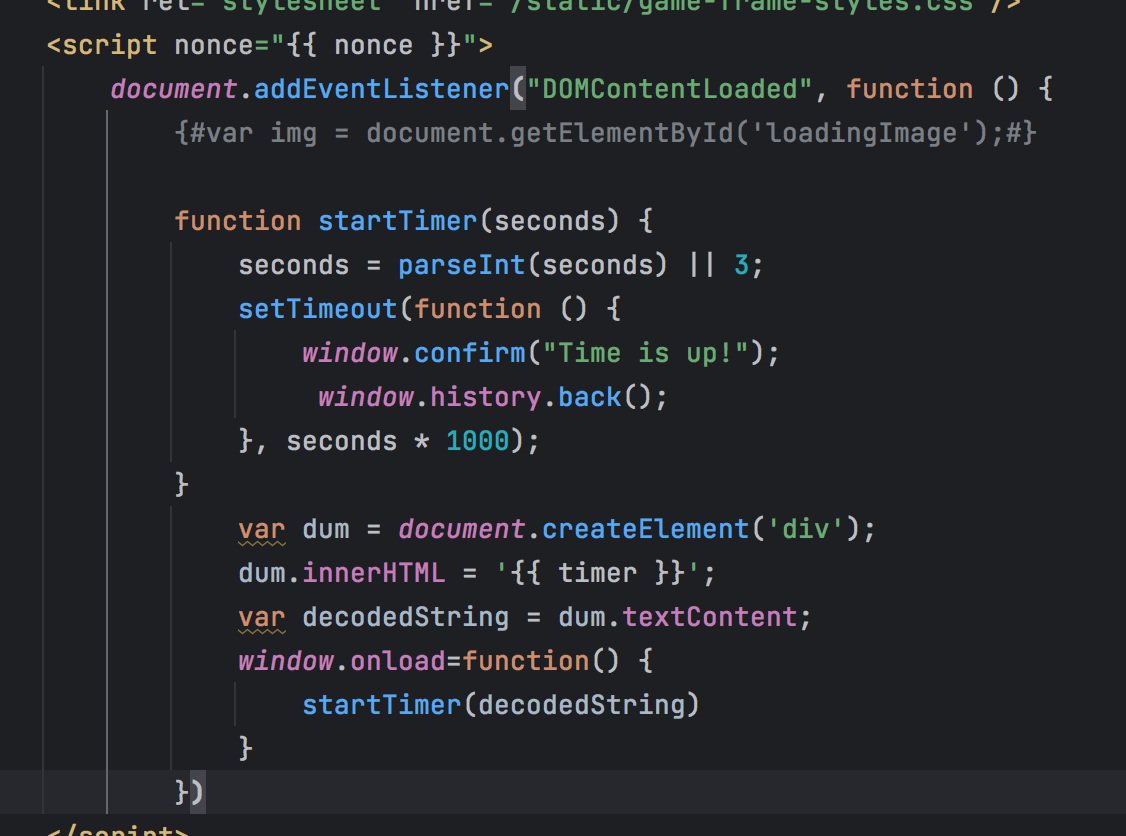
if use 127.0.0.1:5000/level3/frame#1' onerror="alert(1)", it will refuse and report img 404

since it only trust and same nonce value script

4,



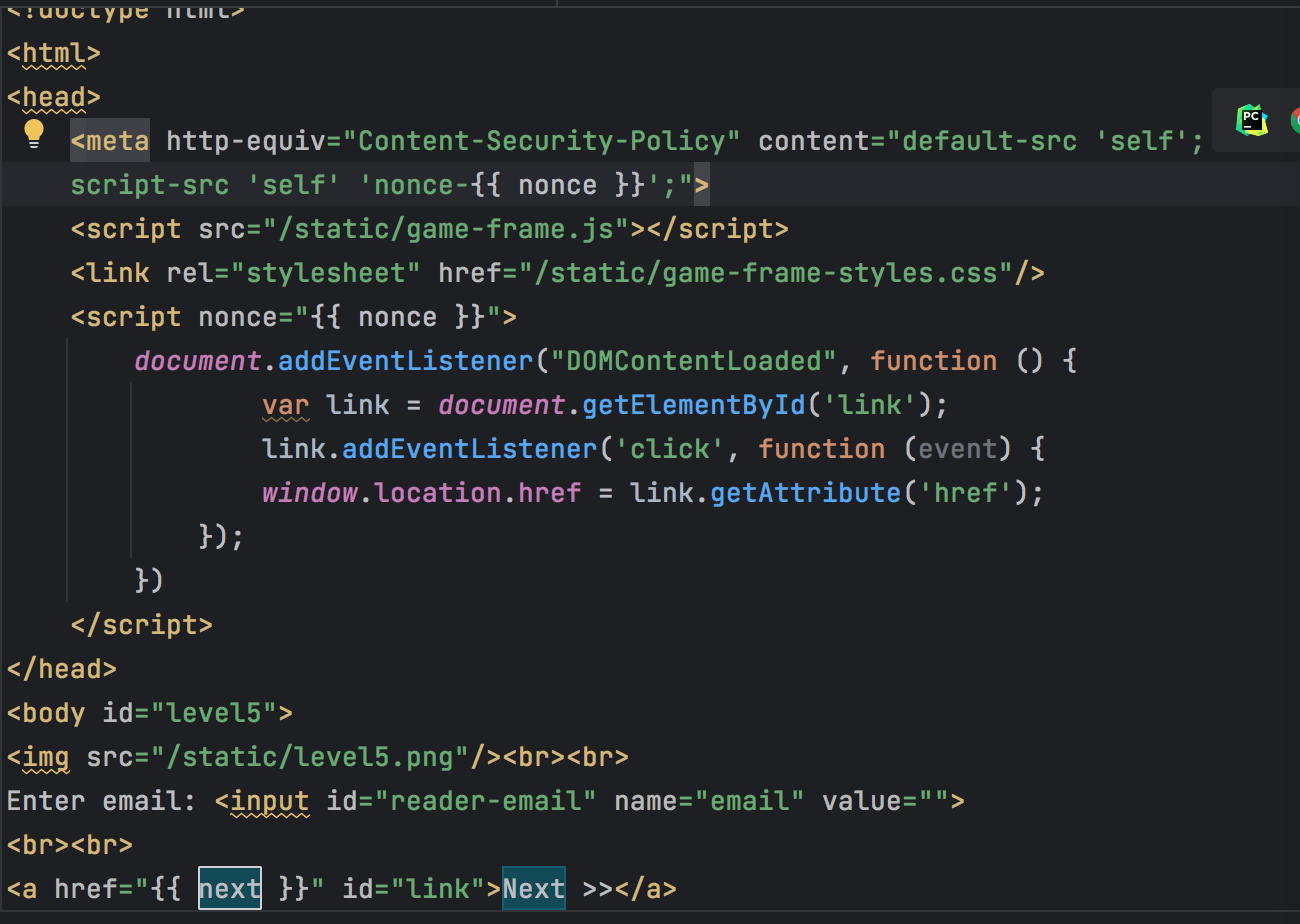
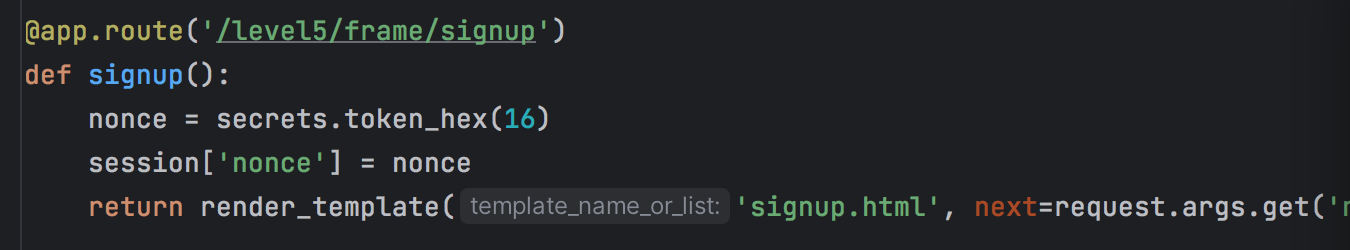




trust itself script and add the listener to dom, change html language to js

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

5,



use itself trust and same nonce value 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, enter and click the Next >>

6,



use itself trust and same nonce value 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