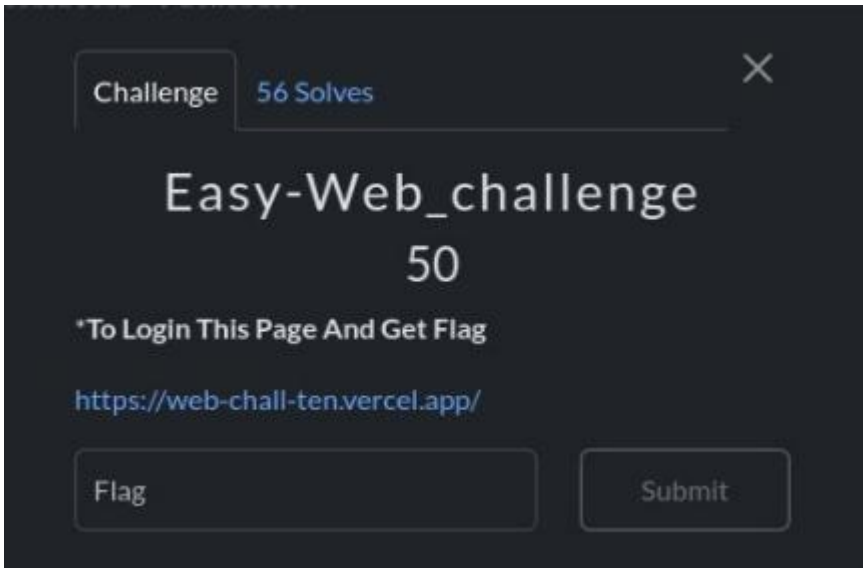
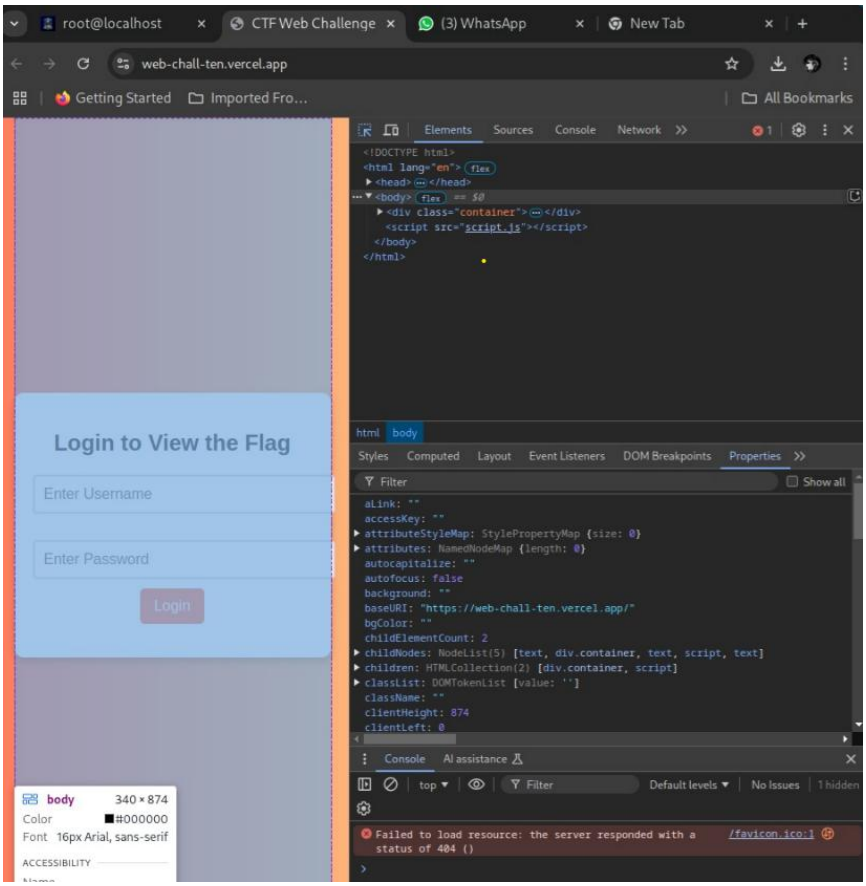
WEB

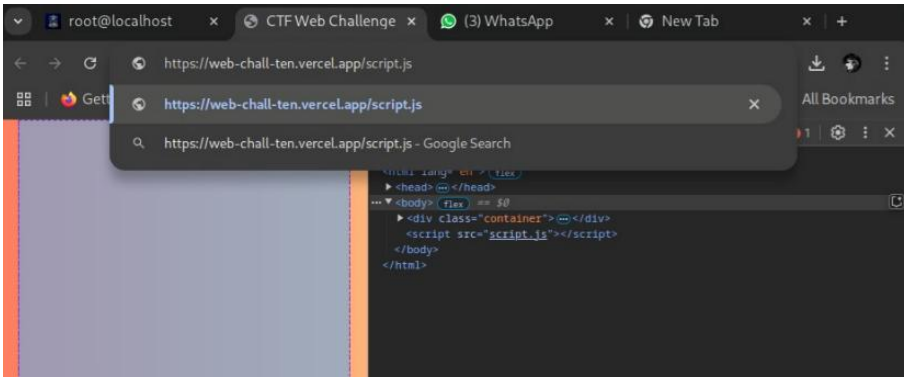
1. Easy-Web_Challenge



- Go to the given website
- Use the shortcut ctrl + shift + c
- We can see a javascript file



- In given url add /script.js

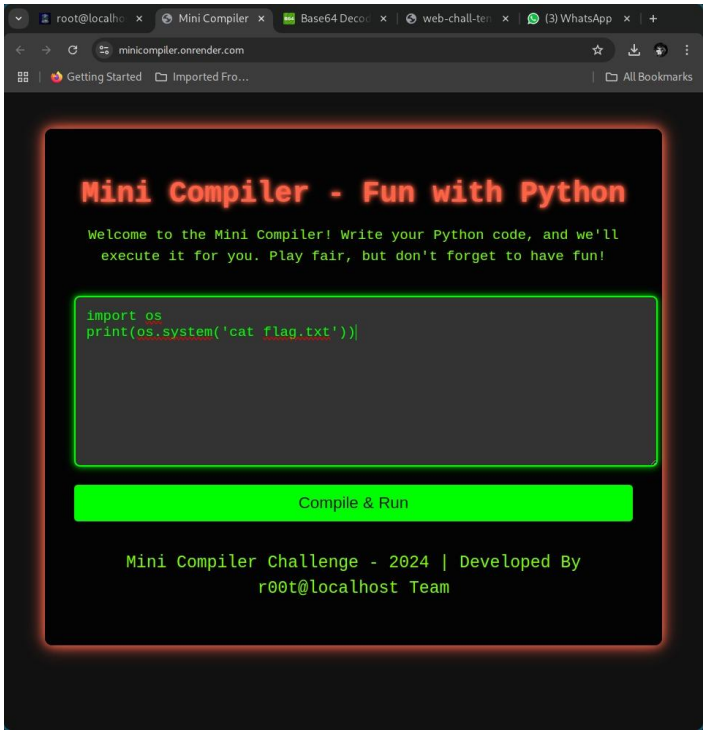


- We get an encoded flag
- Copy the encoded flag and decode using base64
- Displayed flag :
  root@localhost{The_web_chall_is_easy}

2. Mini vulnarable compiler

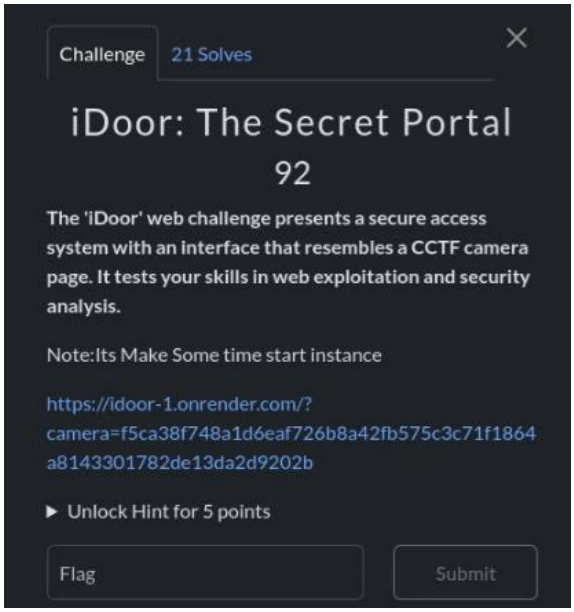
- Goto given url and paste below code in mini compiler

```
import os
print(os.system('cat flag.txt'))
```

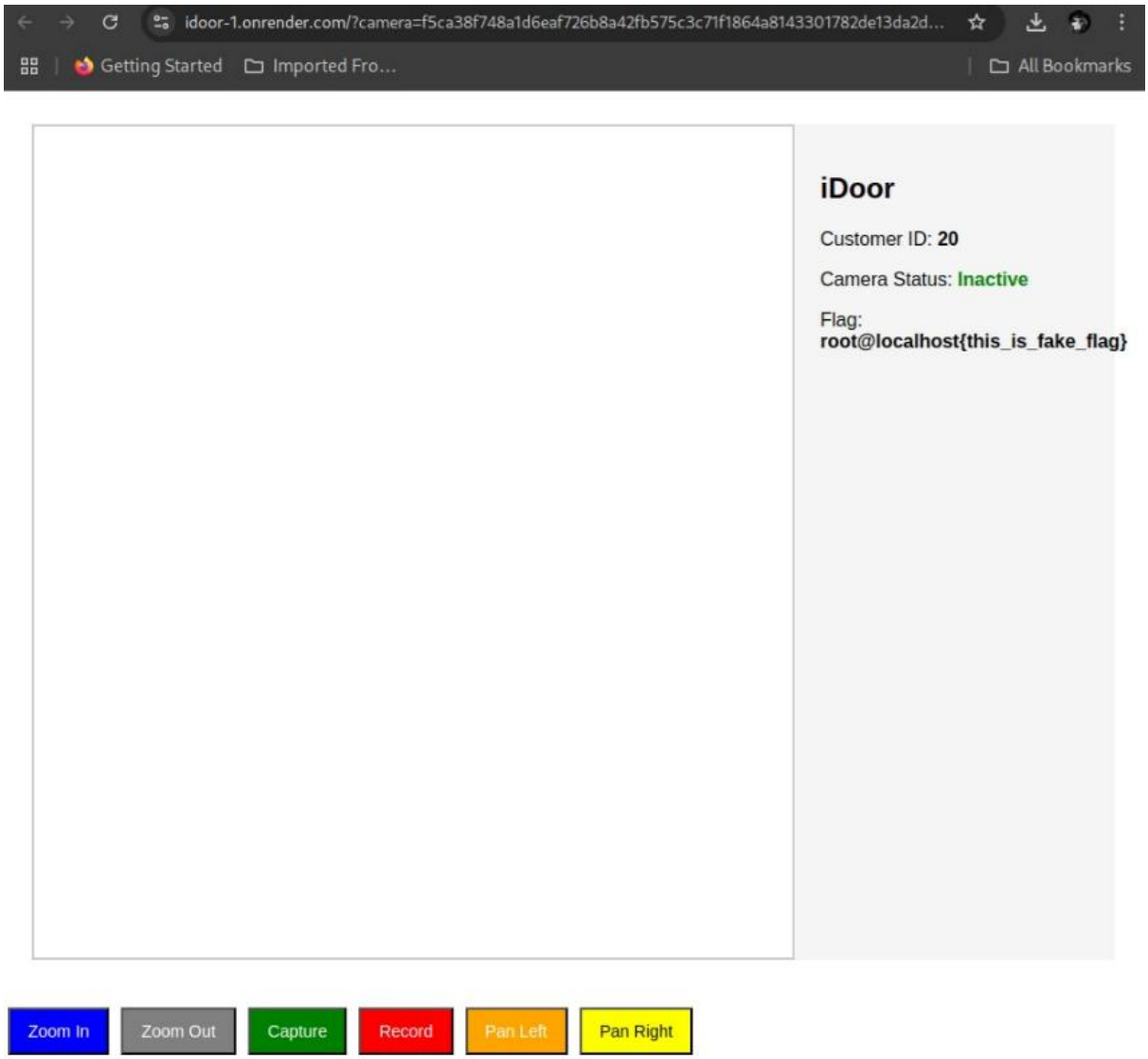


- Displayed flag : r00t@locahost{mini_compiler_pwn}

3. iDoor : The Secret Portal



navigate to given url



- observed camera value is hashed.
- Decoded hash value in crackstation site.
- For identifying customer id 20
- In linux terminal executed below command
  $ echo-n 20 | sha256sum

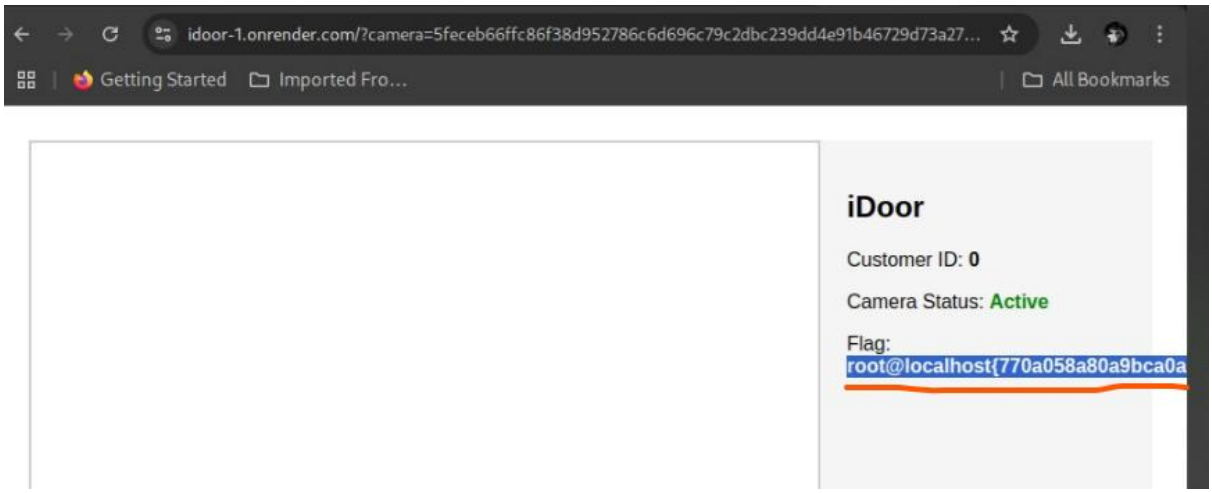
```
HotWater% echo -n 20 | sha256sum
f5ca38f748a1d6eaf726b8a42fb575c3c71f1864a8143301782de13da2d9202b
```

- As the above hash value matched the given camera hashed value. Substituted root 0 instead 20

- In linux terminal executed below command
  $ echo-n 0 | sha256sum

```
HotWater% echo -n 0 | sha256sum
5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9
```

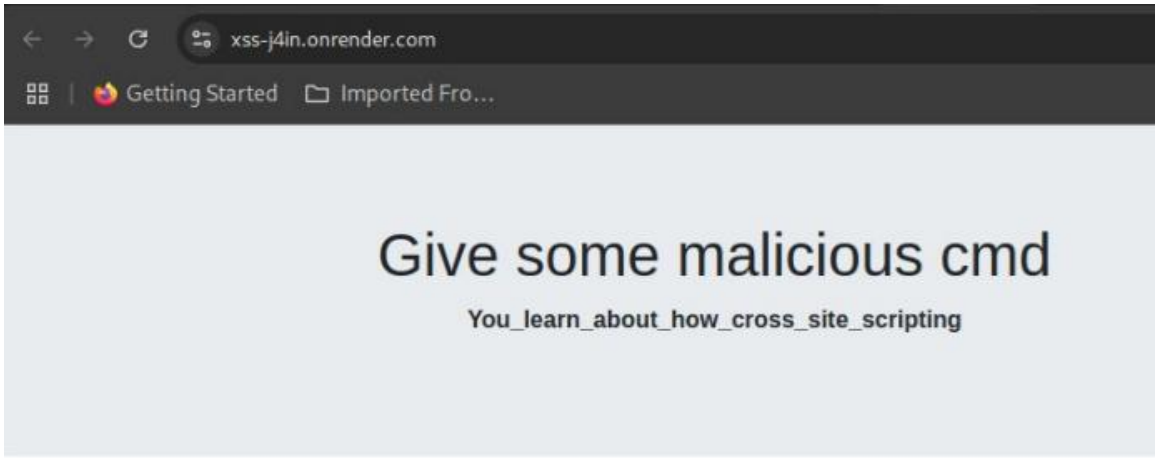
- Substitute the hash value in url and we get the flag



Flag displayed :
root@localhost{770a058a80a9bca0a87c3e2ebe1ee9b2}

4. XSS Vulnerability

- Navigate to given url



Give me something:

Thing to lower case

Submit

- Type the command
  <img src=x onerror=alert('test')>
- Flag will be displayed in alert popup message.
  root@localhost{Byp4ss_Sanitiz3r_123}