WRITE-UP
SNI CTF 2024

Presented By:
Cina Gacor

[DAFTAR ISI]

[OSINT]

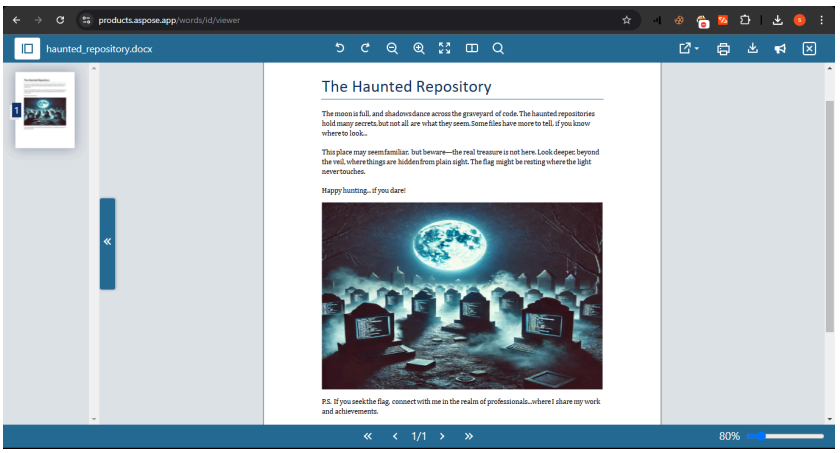
haunted-repository

Overview:

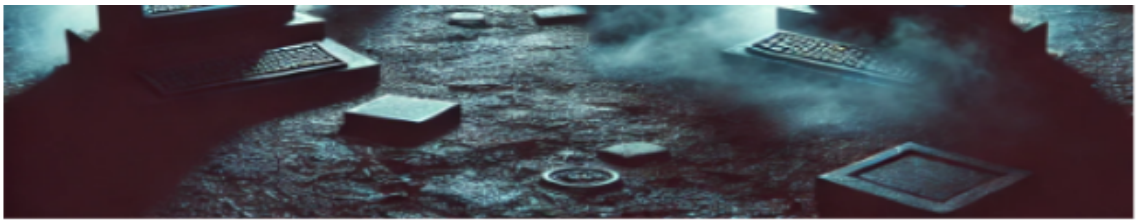
Pada tantangan ini saya dikasih sebuah file ms.word yang dimana merupakan petunjuk mengenai tantangan ini.

Solution:

1. Pertama yang saya lakukan adalah men-unduh dan melihat isi file ms.word tersebut.



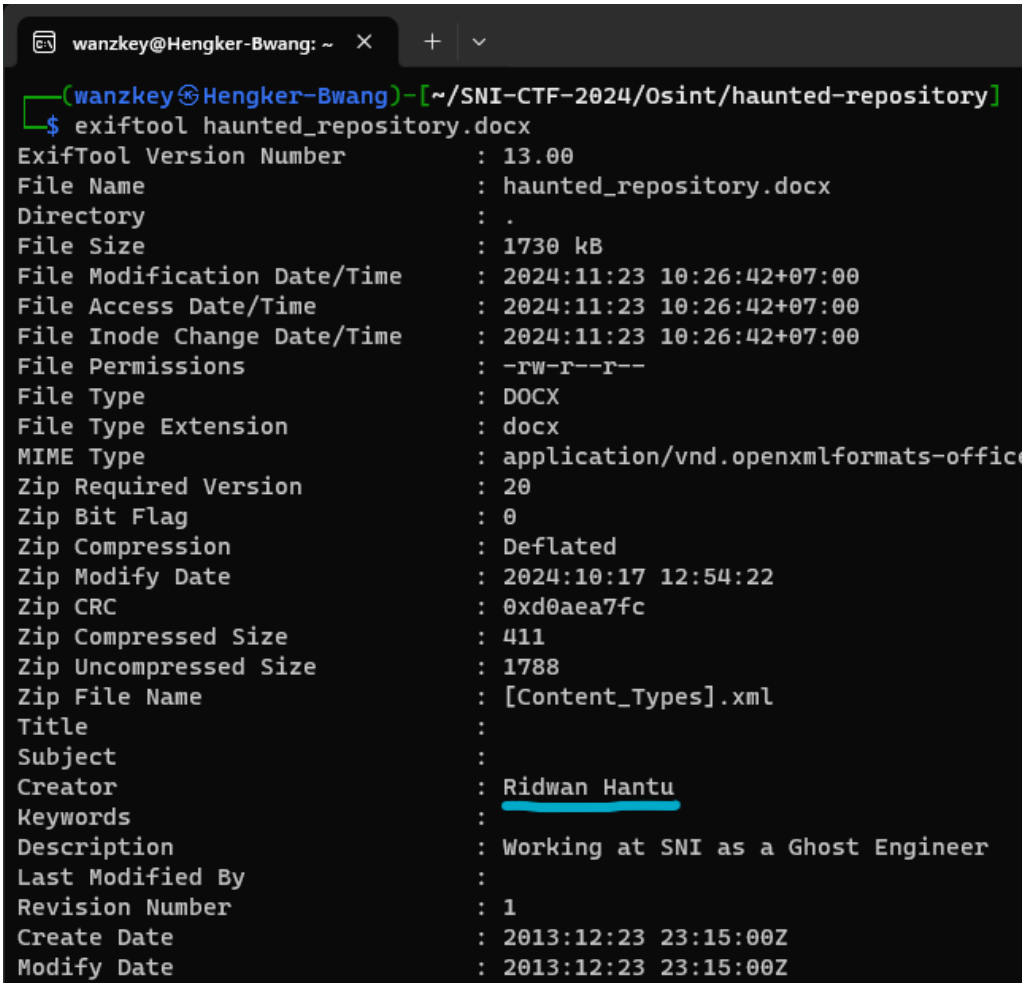
2. Berdasarkan Dalam file tersebut pada bawah gambar ada kalimat "connect with me in the realm of professionals... where I share my work and achievements."



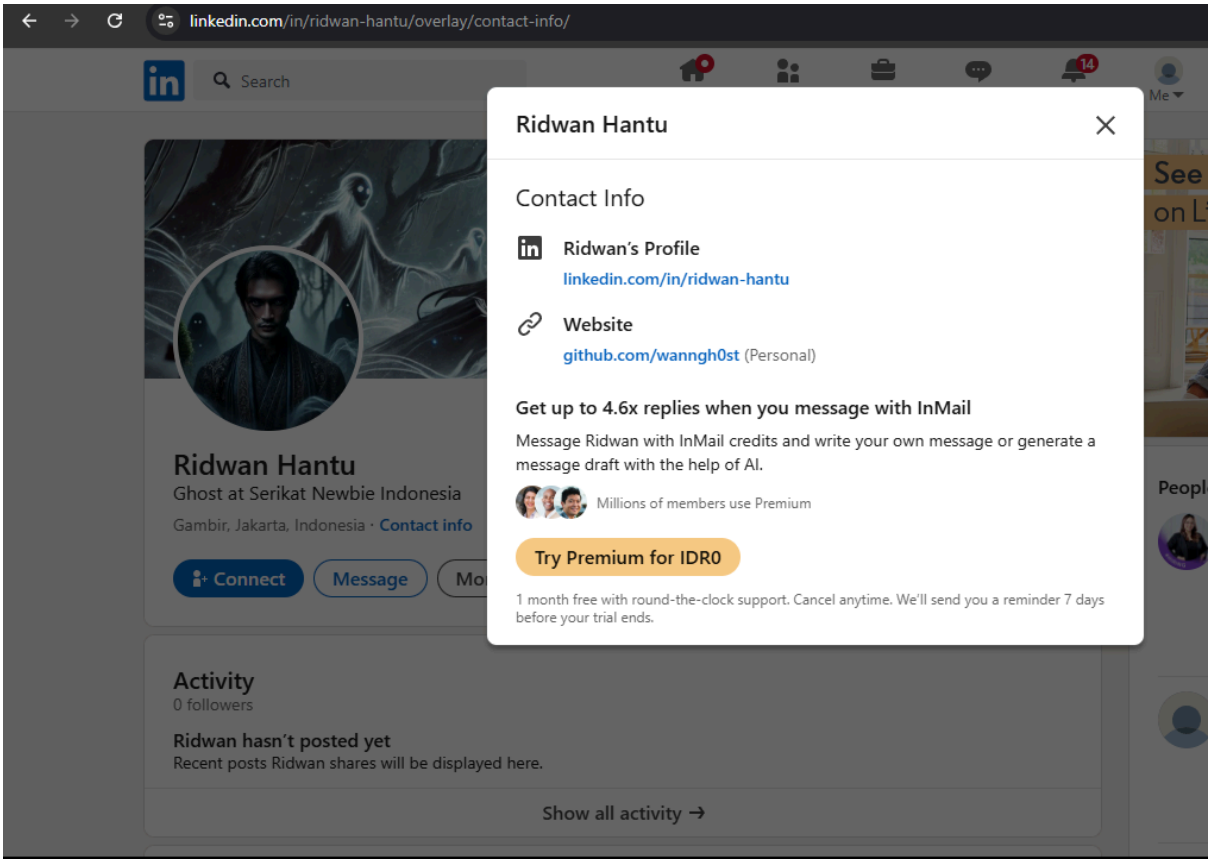
P.S. If you seek the flag, connect with me in the realm of professionals...where I share my work and achievements.

saya, langsung berasumsi klw petunjuk ini mengarahkan saya menuju platform profesional seperti LinkedIn, Github, atau Gitlab.

3. Karena saya tidak mengetahui nama author/pentunjuk tambahan saya mencoba melihat meta-data file ms.word tersebut, dan mendapatkan petunjuk baru mengenai tantangan ini.

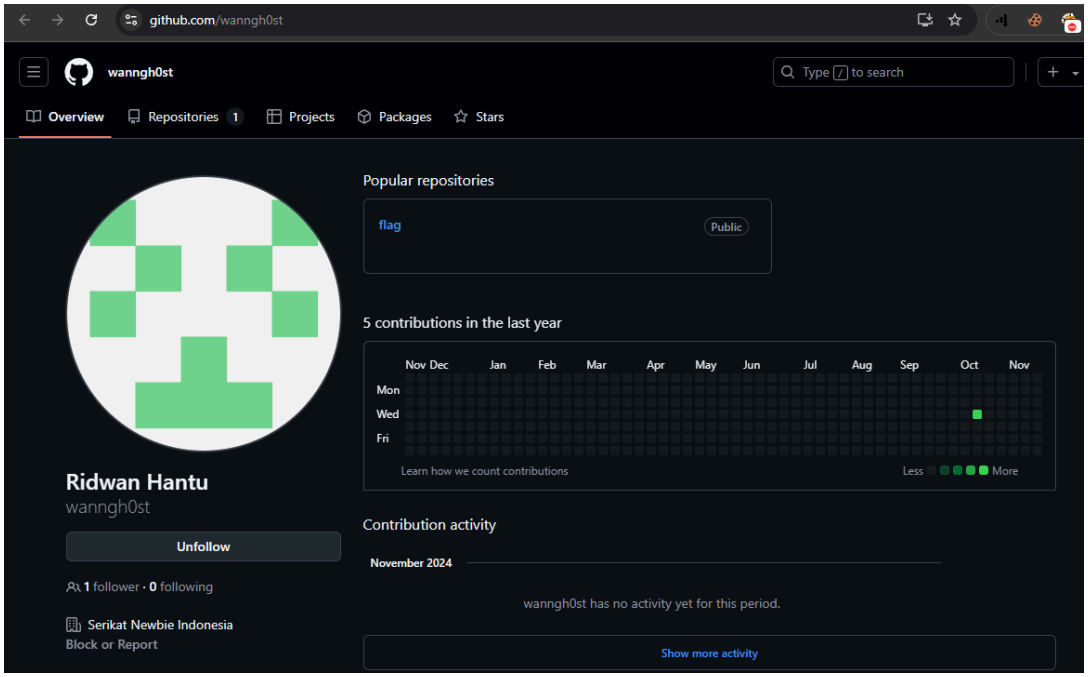


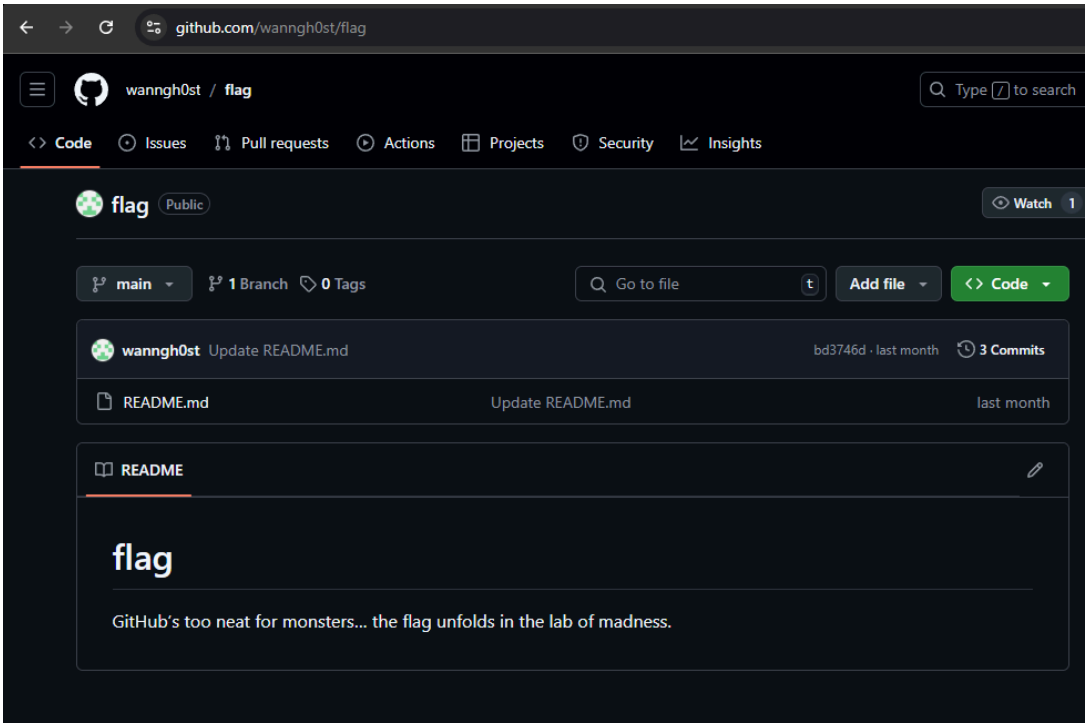
4. Setelah mendapatkan pentunjuk baru saya langsung ke platform LinkedIn dan mencari nama “Riduan Hantu” berdasarkan pentunjuk yang saya dapatkan.



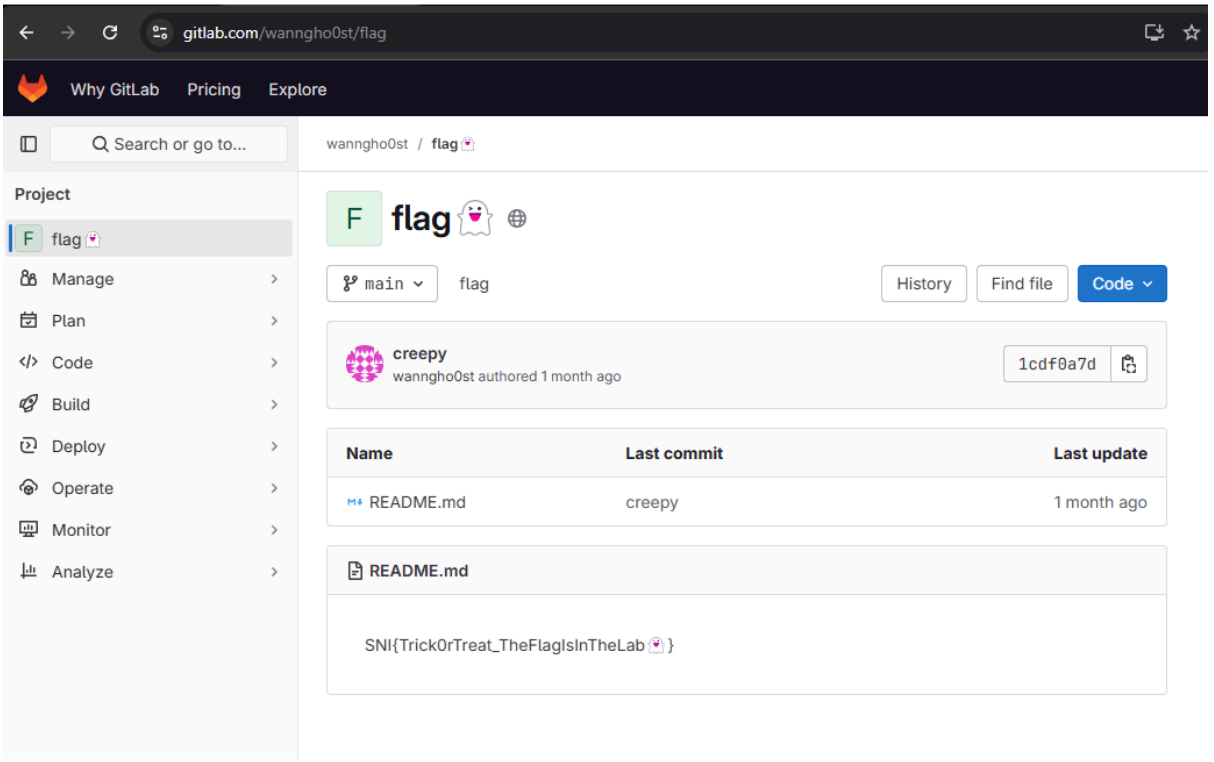
Disini saya mendapatkan pentunjuk baru yaitu akun github sang author, langsung saja saya menunju githubnya.

5. Setelah menuju akun github sang author disana terdapa sebuah repo bernama flag, awalnya saya mengira itu merupakan flagnya, namun ternyata merupakan pentunjuk baru mengenai cara mendapatkan flag tersebut.



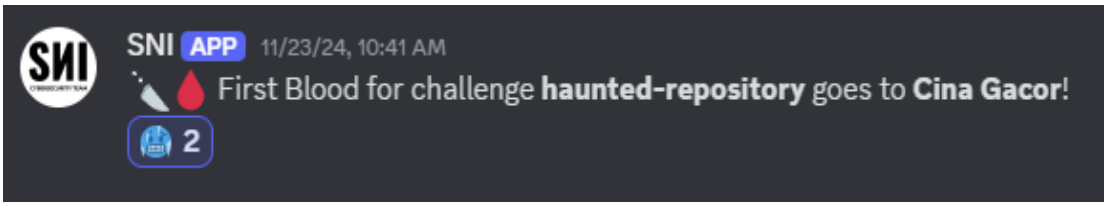


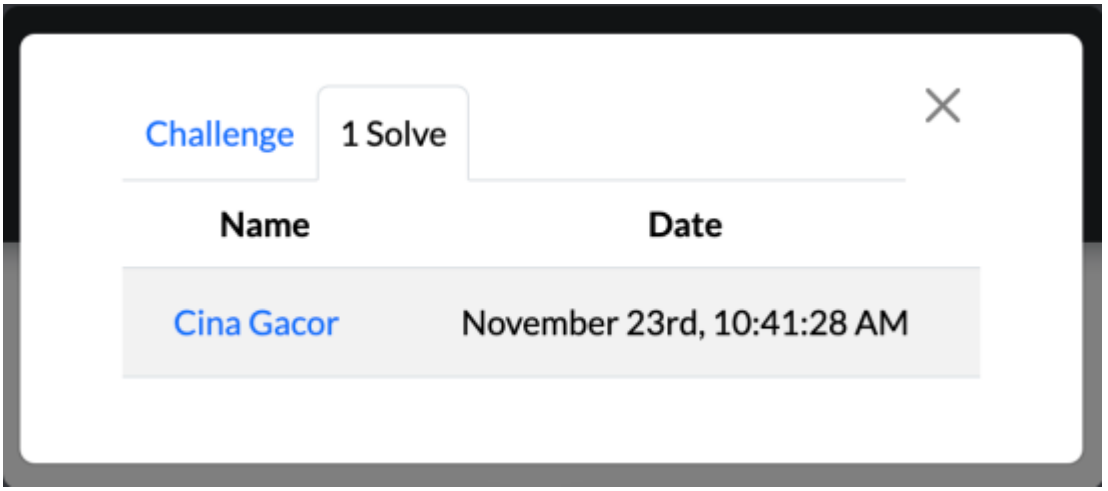
Bisa dilihat pada deskripsi pada gambar diatas “GitHub’s too neat for monsters… the flag unfolds in the lab of madness”, berdasarkan deskripsi tersebut saya berasumsi bahwa flagnya terdapat pada Gitlab bukan pada GitHub. saya langsung menuju gitlabnya dan voilaa dapat flagnya.



Flag: SNI{TrickOrTreat_TheFlagIsInTheLab👻}

***Pengen Pamer Pers blood:v**





eaaaaa aowkaowkw:v

[PROGRAMMING]

Hadiah Bengsky

Overview:

Pada tantangan ini saya dikasih sebuah file pdf bernama **“Hadiah_Bengsky”** yang dimana merupakan petunjuk mengenai tantangan ini dan sebuah file **“testcase.in”** file ini yang akan kita eksekusi untuk mendapatkan flagnya..

Solution:

1. Hal pertama saya lakukan adalah mengecek petunjuk mengenai tantangan ini pada file pdf yang diberikan oleh author.

SNI CTF 2024 CTF 2024

Hadiah Bengsky

Bengsky sedang merencanakan acara ulang tahun sahabatnya dan ingin membeli beberapa hadiah dari sebuah toko. Toko tersebut menawarkan berbagai macam hadiah dengan harga yang tertera. Bengsky telah membuat daftar harga hadiah yang menarik perhatiannya. Bengsky ingin hadiahnya unik, yaitu setiap jenis hadiah maksimal hanya dibeli satu buah saja. Namun, Bengsky memiliki batasan uang yang dapat ia keluarkan karena ia hanya memiliki jumlah tertentu dalam anggarannya. Masalahnya, Bengsky ingin memastikan bahwa dia menggunakan seluruh anggarannya dengan efisien dan tidak ada sisa uang yang terbuang. Oleh karena itu, dia ingin mencari kombinasi dari daftar harga yang dapat dibelinya sehingga total harga hadiah tersebut tepat sama dengan jumlah uang yang ia miliki.

Toko menjual N jenis hadiah dengan harga yang sudah tertera dalam daftar harga. Bengsky memiliki anggaran sebesar M, dan dia ingin membeli hadiah-hadiah dengan total harga yang tepat sama dengan M. Setiap jenis hadiah hanya dapat dibeli satu kali. Tugas Anda adalah mencari kombinasi harga hadiah yang jumlahnya sama dengan M. Dipastikan input hanya memiliki tepat satu kombinasi.

Input

Baris pertama berisi d bilangan bulat, yaitu N ($1 \leq N \leq 40$) dan M ($1 \leq M \leq 10$) Baris berikutnya berisi N bilangan bulat $P,P,\ldots,P(0 \leq P \leq 10$)

Output

Kombinasi hadiah sedemikian sehingga total jumlah harga hadiah sama dengan M. Urutkan dari harga terkecil

Contoh Input #1

```
5 21
17 15 4 18 29
```

Contoh Output #1

```
4 17
```

Contoh Input #2

```
3 50
21 24 26
```

Contoh Output #2

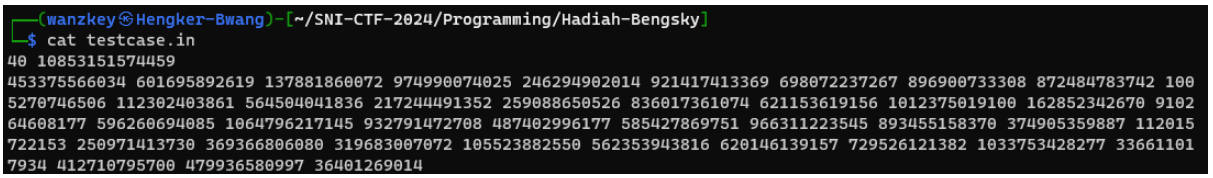
```
24 26
```

bisa dilihat pada gambar diatas merupakan mengenai cara menyelesaikan tantangan ctf ini. Setelah saya riset mengenai tantangan ini, rupanya merupakan tantangan **Subset Sum Problem** atau masalah pencarian kombinasi dari sejumlah elemen untuk mencapai jumlah tertentu. Dalam hal ini, saya diminta untuk mencari kombinasi harga hadiah yang totalnya sama dengan anggaran Bengsky (M), dengan syarat setiap hadiah hanya bisa dibeli sekali..

Disini saya menggunakan **backtracking** atau **dynamic programming** untuk menyelesaikan masalah ini. Namun, karena jumlah elemen yang terbatas (hanya 40 hadiah), saya membuat script solve yang akan mencoba setiap kombinasi harga satu per satu dan memeriksa apakah jumlahnya mencapai **M**.

2. Melihat File Testcase.in untuk membuat script solve menghitung menemukan kombinasi harga yang jumlahnya tepat sama dengan **M**, berikut hasilnya:

Melihat File Testcase.in



Ketika sudah melihat file tersebut saya langsung membuat script solve untuk menemukan kombinasi harga yang jumlahnya tepat sama dengan **M**.

Berikut Scriptnya:

```
from itertools import combinations

def find_combination_mitm(harga, M):
    N = len(harga)
    first_half = harga[:N//2]
    second_half = harga[N//2:]

    def get_subsets(arr):
        subsets = []
        for r in range(len(arr) + 1):
            for comb in combinations(arr, r):
                subsets.append(sum(comb))
        return subsets

    first_half_sums = get_subsets(first_half)
    second_half_sums = get_subsets(second_half)

    second_half_sums_set = set(second_half_sums)

    for first_sum in first_half_sums:
        if M - first_sum in second_half_sums_set:
            result = []

            for r in range(len(first_half) + 1):
                for comb in combinations(first_half, r):
                    if sum(comb) == first_sum:
                        result.extend(comb)
            for r in range(len(second_half) + 1):
                for comb in combinations(second_half, r):
                    if sum(comb) == (M - first_sum):
                        result.extend(comb)
            return sorted(result)
    return None

N, M = 40, 10853151574459
harga = [
    453375566034, 601695892619, 137881860072, 974990074025,
246294902014, 921417413369,
    698072237267, 896900733308, 872484783742, 1005270746506,
112302403861, 564504041836,
    217244491352, 259088650526, 836017361074, 621153619156,
1012375019100, 162852342670,
    910264608177, 596260694085, 1064796217145, 932791472708,
487402996177, 585427869751,
    966311223545, 893455158370, 374905359887, 112015722153,
250971413730, 369366806080,
    319683007072, 105523882550, 562353943816, 620146139157,
729526121382, 1033753428277,
    336611017934, 412710795700, 479936580997, 36401269014
]

kombinasi_hadiah = find_combination_mitm(harga, M)

if kombinasi_hadiah:
    print(" ".join(map(str, kombinasi_hadiah)))
else:
    print("Tidak ada kombinasi yang ditemukan.")
```

Hasil:

```
┌──(wanzkey㉿Hengker-Bwang)-[~/SNI-CTF-2024/Programming/Hadiah-Bengsky]
└─$ python3 nyari-kombinasi-harga.py
36401269014 112302403861 137881860072 162852342670 246294902014 250971413730 336611017934 369366806080 374905359887 4127
10795700 601695892619 620146139157 621153619156 729526121382 893455158370 910264608177 932791472708 1005270746506 103375
3428277 1064796217145
```

Terlihat bahwa script saya berhasil menemukan kombinasi harga yang jumlahnya tepat sama dengan **M**. karena untuk mendapatkan flag sesuai dengan format yang diminta berdasarkan deskripsi soal, yaitu **SNI{hex(sha256(output))}**, saya perlu membuat lagi script untuk **Menghitung SHA-256 Hash** dari output yang saya dapatkan dan **Mengonversi Hash ke Format Hexadecimal** baru sesuai dengan format flag yang diminta.

Berikut Sciptnya:

Script Solve untuk dapat flag:

```python
import hashlib

output = [36401269014, 112302403861, 137881860072, 162852342670,
246294902014,
          250971413730, 336611017934, 369366806080, 374905359887,
412710795700,
          601695892619, 620146139157, 621153619156, 729526121382,
893455158370,
          910264608177, 932791472708, 1005270746506, 1033753428277,
1064796217145]

output_str = " ".join(map(str, output))

sha256_hash = hashlib.sha256(output_str.encode()).hexdigest()

flag = f"SNI{{{sha256_hash}}}"
print(flag)
```

Hasil:

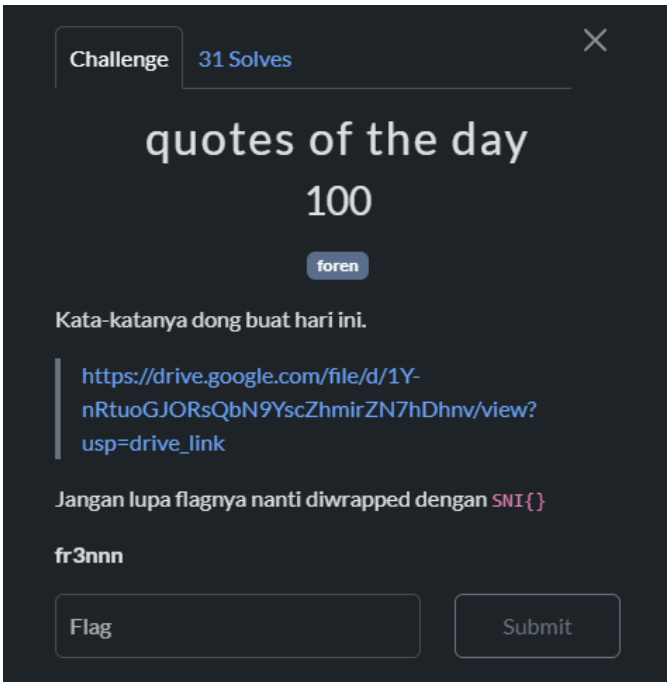
```
┌──(wanzkey㉿Hengker-Bwang)-[~/SNI-CTF-2024/Programming/Hadiah-Bengsky]
└─$ python3 solve.py
SNI{55e7e87ba720040b6ac8264ad340b61cf936b5e2f91f4651acd7cef752a3f3a6}
```

Voila berhasil kan……..

Flag: SNI{55e7e87ba720040b6ac8264ad340b61cf936b5e2f91f4651acd7cef752a3f3a6}

[FORENSIC]

Quotes Of The Day



Overview:

Pada tantangan kali ini saya suruh mendownload file yang berisi file png, yang dimana ternyata file tersebut rusak tidak dapat dibuka.

Solution:

1. identifikasi file png

```
┌──(wanzkey㉿Hengker-Bwang)-[~/SNI-CTF-2024/Forensic/quoute-Of-the-day]
└─$ file quotes_of_the_day.png
quotes_of_the_day.png: PNG image data, 808530225 x 808529968, 32-bit
```

hal pertama, yang saya lakukan melihat meta-data terkait file yang diberikan, disini saya melihat meta-data terkait filenya.

```
┌──(wanzkey㉿Hengker-Bwang)-[~/SNI-CTF-2024/Forensic/quoute-Of-the-day]
└─$ exiftool quotes_of_the_day.png
ExifTool Version Number         : 13.00
File Name                       : quotes_of_the_day.png
Directory                       : .
File Size                       : 74 kB
File Modification Date/Time     : 2024:11:23 11:30:50+07:00
File Access Date/Time           : 2024:11:25 10:04:31+07:00
File Inode Change Date/Time     : 2024:11:23 11:32:07+07:00
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 808530225
Image Height                    : 808529968
Bit Depth                       : 32
Color Type                      : Unknown (48)
Compression                     : Unknown (49)
Filter                          : Unknown (49)
Interlace                       : Unknown (49)
Warning                         : Corrupted PNG image
Image Size                      : 808530225x808529968
Megapixels                      : 653720916946.3
```

Bisa dilihat pada gambar diatas, saya menggunakan exiftool untuk melihat metadatanya, sudah jelas sekali bahwa file tersebut corrupt dan tidak dapat dibuka, bisa kita lihat bahwa image sizenya besar sekali, yang menyebabkan file tersebut corrupt.

2. Melakukan strings untuk melihat meta-data file tersebut

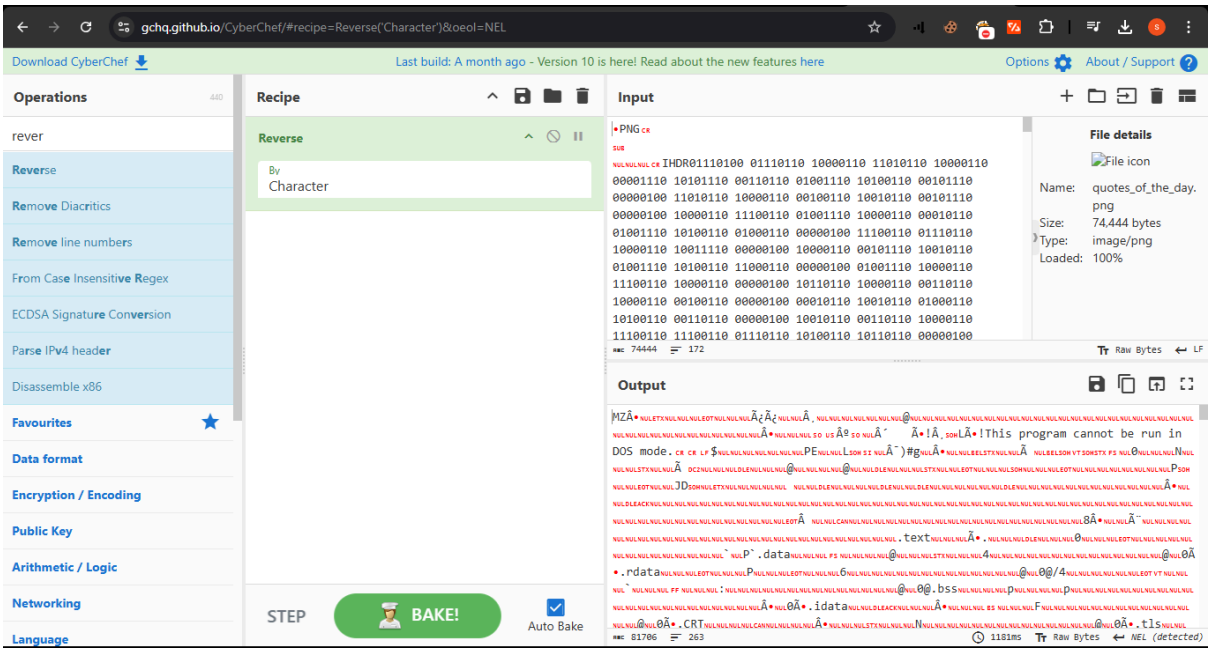
```
┌──(wanzkey㉿Hengker-Bwang)-[~/SNI-CTF-2024/Forensic/quoute-Of-the-day]
└─$ strings quotes_of_the_day.png
IHDR01110100 01110110 10000110 11010110 10000110 00001110 10101110 00110110 010
 10000110 00100110 10010110 00101110 00000100 10000110 11100110 01001110 100001
000100 11100110 01110110 10000110 10011110 00000100 10000110 00101110 10010110
```

pada saat pertama kali melihat menggunakan strings banyak sekali bilangan biner mirip dengan file executable, saya lanjut melihat kebawah siapa tahu ada petunjuk tambahan.

```
.d% ezis tib noitacoler oduesp nwonknU
.d% noisrev locotorp noitacoler oduesp nwonknU
p% sserdda ta setyb d% rof deliaf yreuQlautriV
:eruliaf emitnur wgniM
uka_irabak_ukirid_aynkurub_gnatnet_atirecreb_gnaroeses_akij :)3/1(
!ini irah taub gnod aynatak-ataK
}?nareneb_sam_nikay_ipat_nerof_ze{INS .ulud apatreb gnidneM ?ag ini timbus aboc uaM
e8375a38953e_ 3/3 sam aynkayak gnitnep ini
%%d% ]
sessalCretsigeR_vJ_
lld.61-jcgbil
ofni_emarf_retsigered__
ofni_emarf_retsiger__
lld.1-2wd_s_ccgbil
```

```
atad.`P
txet.
.edom SOD ni nur eb tonnac margorp sihT!
```

saya menemukan info yang menarik, ternyata file ini metadata-nya terbaik, langsung saja saya menggunakan tools cyberchef untuk melakukan reverse pada file tersebut.



setelah reverse file pngnya, saya save file yang telah direverse dan mengecek kembali dengan strings pada file yang telah direverse.

```
┌──(wanzkey㉿Hengker-Bwang)-[~/SNI-CTF-2024/Forensic/quoute-Of-the-day]
└─$ strings reverse.dat
!This program cannot be run in DOS mode.
.text
P`.data
.rdata
0@/4
0@.bss
```

Bisa dilihat pada gambar diatas bahwa saya berhasil telah mereverse filenya, akan tetapi saya mengubah ekstensi file tersebut menjadi “.dat” yang sebelumnya adalah “.png”.

saya kembali mengecek kebawah untuk melihat data file tersebut ternyata voila saya mendapatkan potongan flag 1 & 3.

```
ini penting kayaknya mas 3/3 _e35983a5738e
Mau coba submit ini ga? Mending bertapa dulu. SNI{ez_foren_tapi_yakin_mas_beneran?}
Kata-katanya dong buat hari ini!
(1/3): jika_seseorang_bercerita_tentang_buruknya_diriku_kabari_aku
Mingw runtime failure:
  VirtualQuery failed for %d bytes at address %p
  Unknown pseudo relocation protocol version %d.
  Unknown pseudo relocation bit size %d.
glob-1.0-mingw32
GCC: (GNU) 6.3.0
```

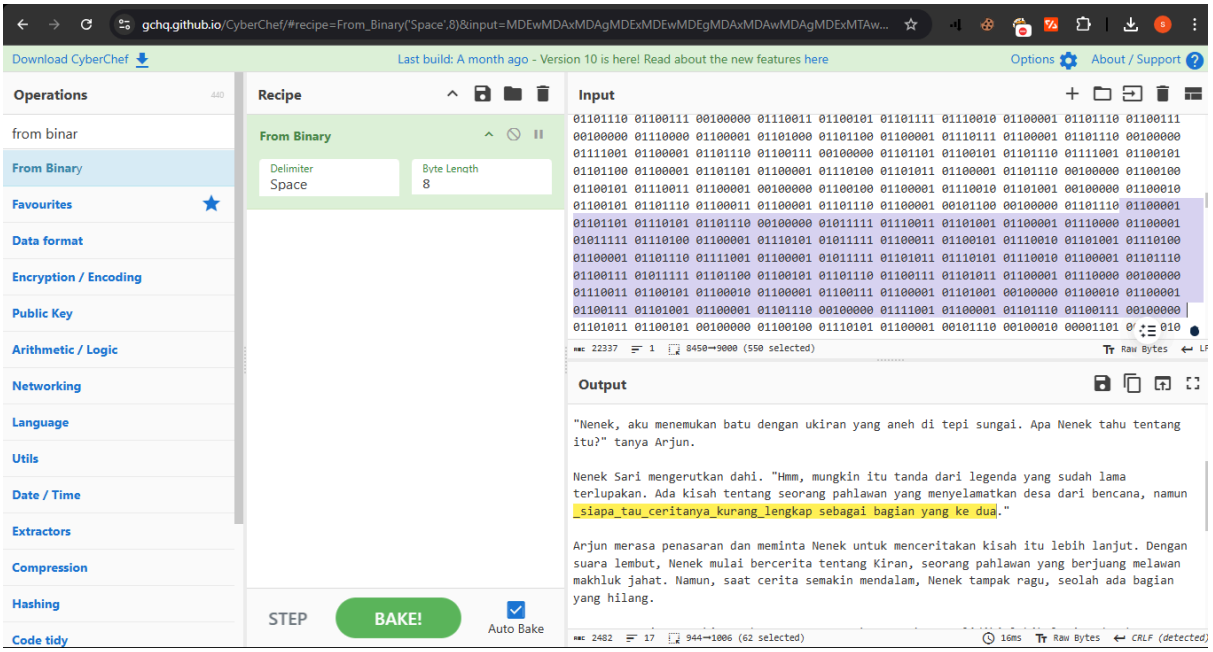
“(1/3): jika_seseorang_bercerita_tentang_buruknya_diriku_kabari_aku”

“(3/3) _e35983a5738e”

saya kembali kebawah untuk melihat bilangan biner tadi, saya berasumsi bahwa pada bilangan tersebut terdapat potongan flag keduanya.

```
_vfprintf
__imp__EnterCriticalSection@4
__imp__fwrite
01000100 01101001 00100000 01110011 01100101 01100010 01110101 01100001
00001 00100000 01101011 01100101 01100011 01101001 01101100 00100000 011
00 01101001 01101011 01100101 01101100 01101001 01101100 01101001 011011
01100101 01101000 00100000 01101000 01110101 01110100 01100001 01101110
```

Disini saya menyalin semua kode biner, lalu mendecodenya menggunakan cyberchef.



nah voila berhasil mendapatkan potongan keduanya.

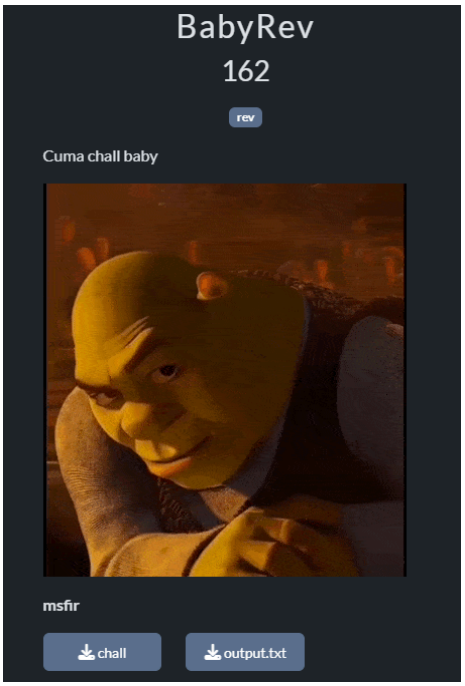
“(2/3) _siapa_tau_ceritanya_kurang_lengkap”

Flag:

SNI{jika_seseorang_bercerita_tentang_buruknya_diriku_kabari_aku_siapa_tau_ceritanya_kurang_lengkap_e35983a5738e}

[REVERSE ENGINEERING]

Quote Of The Day



Overview:

Pada tantangan kali ini saya dikasih sebuah file “chall & output.txt”

Solution:

1. Hal yang pertama saya lakukan adalah mengidentifikasi jenis file chall ini.

```
┌──(wanzkey㉿Hengker-Bwang)-[~/SNI-CTF-2024/Reverse-Engineering/BabyRev]
└─$ file chall
chall: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.s
o.2, BuildID[sha1]=a77d3f5b30f3acbb4f5bf810e551785839abdc06, for GNU/Linux 3.2.0, not stripped
```

ternyata tipe file ini adalah ELF 64bit.

2. Melihat isi file output.txt

```
┌──(wanzkey㉿Hengker-Bwang)-[~/SNI-CTF-2024/Reverse-Engineering/BabyRev]
└─$ cat output.txt
0 24 59 86 2 14 43 17 17 24 0 54 7 46 49 11 1 11 16 10 1 0 53 58 0 0 18 18 1 53 90 57
```

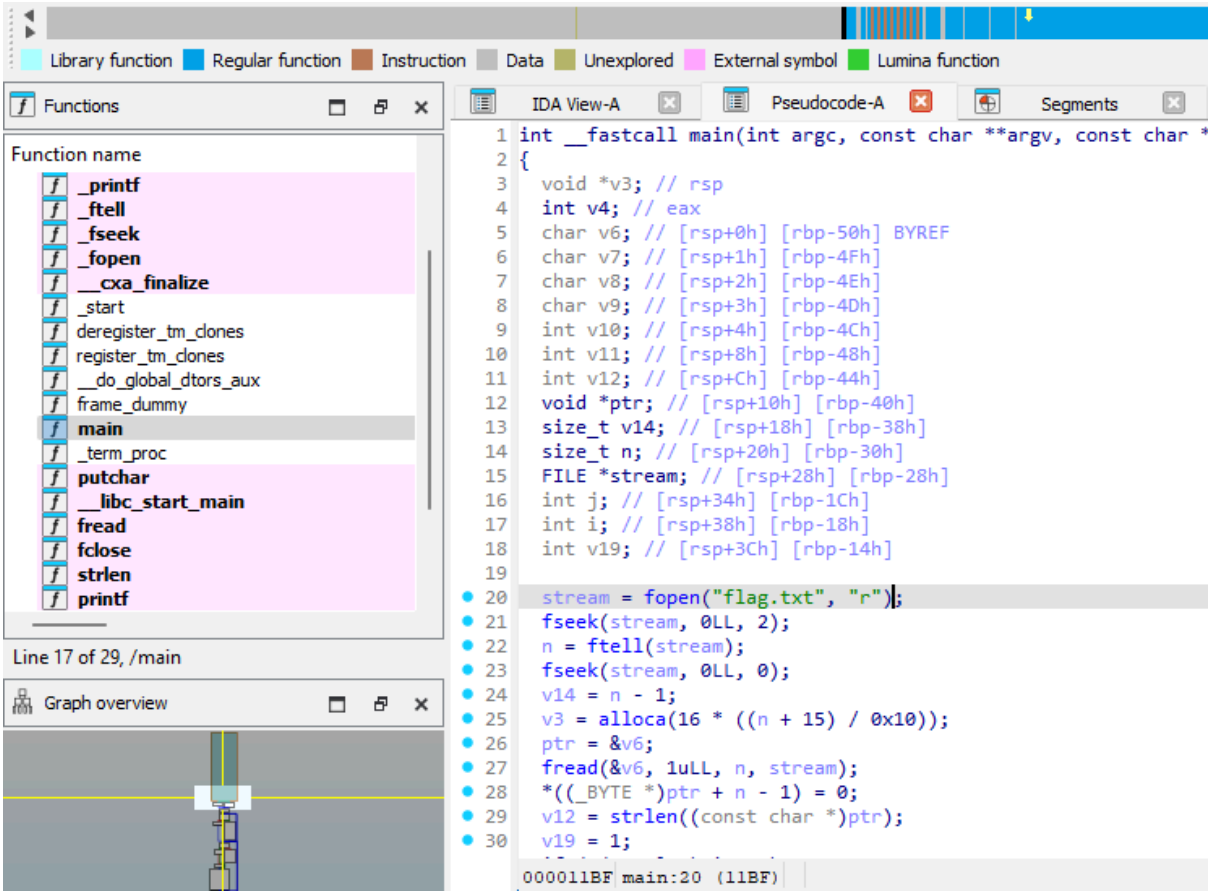
Setelah melihat isi file tersebut, jelas sekali tujuan tantangan ini adalah mencari cara agar output ini keluar menjadi flag yang asli.

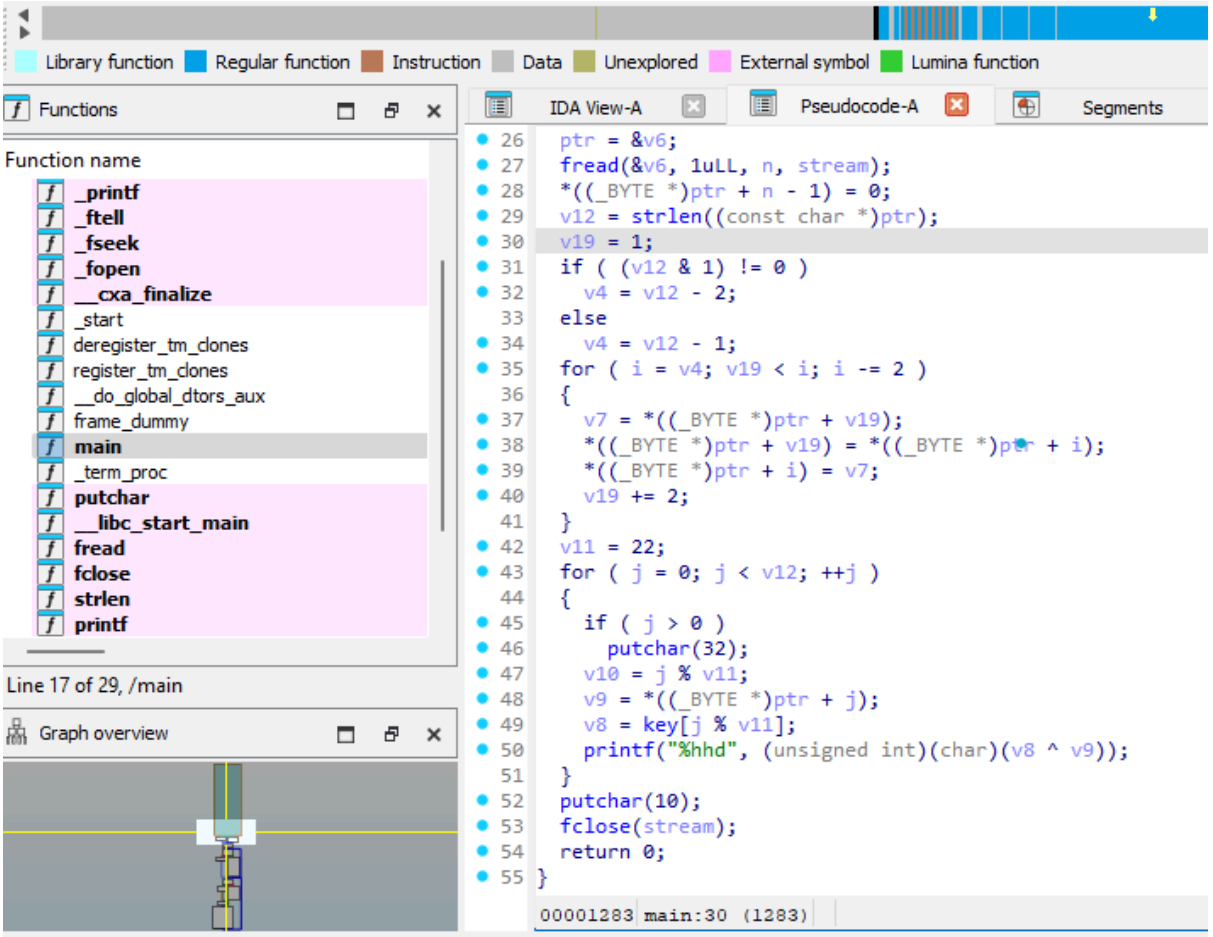
Setelah mengindentifikasi dan melihat isi file output tersebut, langsung saja saya menggunakan IDA untuk menganalisis lebih lanjut mengenai file chall ini.

3. Analisis Lebih Lanjut Menggunakan tools IDA.

Ketika membuka IDA, saya langsung mengecek function main yang mungkin cara kerja untuk mendapatkan flag pada tantangan kali ini.

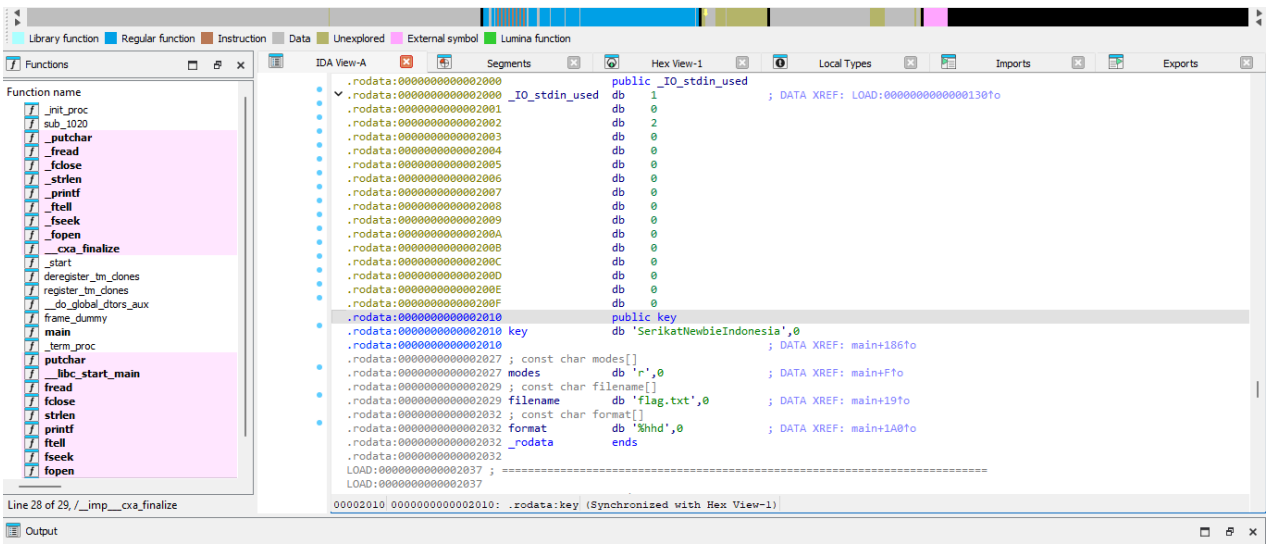
1. Cek Function Main.





Setelah memeriksa function main, saya langsung mengecek Segment pada chall tersebut, yaitu .rodata

.rodata



Disana terdapat sebuah key

Key

```
.rodata:000000000000200D                db    0
.rodata:000000000000200E                db    0
.rodata:000000000000200F                db    0
.rodata:0000000000002010                public key
.rodata:0000000000002010 key            db 'SerikatNewbieIndonesia',0
.rodata:0000000000002010                                        ; DATA XREF: main+186↑o
.rodata:0000000000002027 ; const char modes[]
.rodata:0000000000002027 modes          db 'r',0                ; DATA XREF: main+F↑o
.rodata:0000000000002029 ; const char filename[]
.rodata:0000000000002029 filename       db 'flag.txt',0         ; DATA XREF: main+19↑o
.rodata:0000000000002032 ; const char format[]
.rodata:0000000000002032 format         db '%hhd',0             ; DATA XREF: main+1A0↑o
.rodata:0000000000002032 _rodata        ends
.rodata:0000000000002032
```

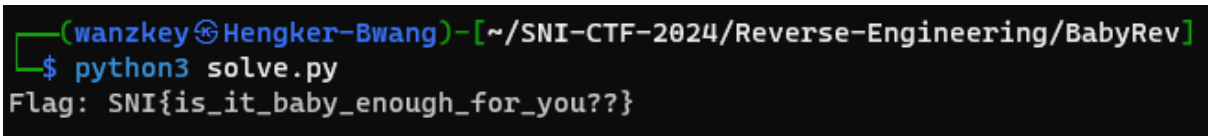
Singkat saja inti pada tantangan ini kurang lebih yg harus kita lakukan adalah memecahkan kode xor menggunakan key yang terdapat pada diatas yaitu **“SerikatNewbieIndoensia”**, disini saya menggunakan **ChatGPT** untuk membantu saya membuat script untuk menyelesaikannya, maklum keterbataasan ilmu mengenai reverse:v.

Berikut Script Solvenya:

Script Solve:

```python
output = [0, 24, 59, 86, 2, 14, 43, 17, 17, 24, 0, 54, 7, 46, 49, 11,
1, 11, 16, 10, 1, 0, 53, 58, 0, 0, 18, 18, 1, 53, 90, 57]

key = "SerikatNewbieIndonesia"
key_len = len(key)
decoded = []
for i, value in enumerate(output):
    decoded_char = value ^ ord(key[i % key_len])
    decoded.append(chr(decoded_char))

decoded_str = ''.join(decoded)
length = len(decoded_str)
restored = list(decoded_str)

mid = length // 2
left = 1 if length % 2 == 0 else 2

for i in range(1, mid, 2):
    restored[i], restored[length - left] = restored[length - left],
restored[i]
    left += 2
original = ''.join(restored)

print("Flag:", original)
```

Hasil Script Solve:



Flag: SNI{is_it_baby_enough_for_you??