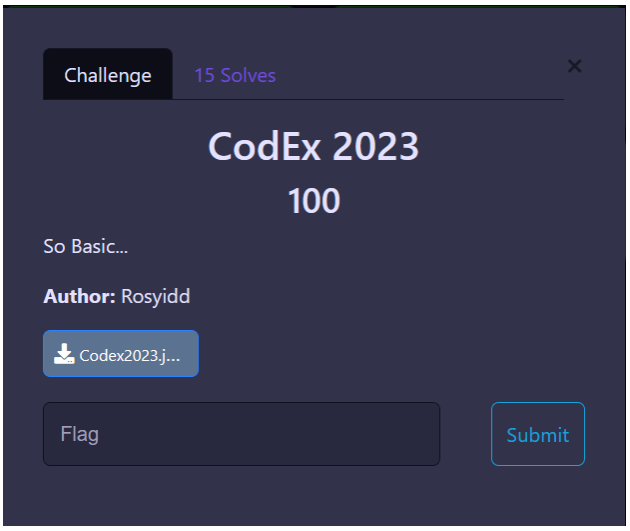
CTF CodEx 2023 WRITE UP

Steven Anthony
(235150201111035)

CodEx 2023
Warm Up

Deskripsi soal:



Link File :
https://codexploit.fun/files/c436823bf7d8bae318e95db39482b85c/Codex2023.jpeg?token=eyJ1c2VyX2lkIjo4LCJ0ZWFtX2lkIjpudWxsLCJmaWxlX2lkIjoxOH0.ZVfOkQ.dP4zXOkfl2j2OrYOx3SdULjQYrQ

Ketika di-open :

Solusi :
Ketika format file di-ubah menjadi .txt maka akan terlihat seperti berikut:

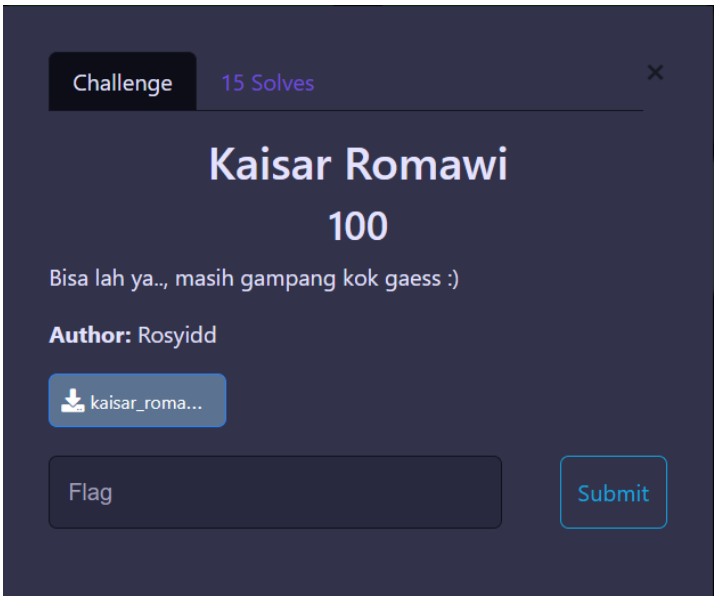
Flag:

```
title  ▯▯▯ ▯  ▯  ▯ª▯▯ ▯  ▯  ▯¼'' ▯  ▯80  '' ▯  ▯80  è▯  ▯

2023:10:19 15:08:58 2023:10:19 15:08:58  t i t l e  f l a g { t 3 r s 3 l 0 b 0 n g }  ÿþ <CREATOR: gd-jpeg v1.0

iHzreSzNTczkc9d'?>
w.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b"
19T15:08:58.795</xmp:CreateDate></rdf:Description><rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b"
:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc="http://purl.org/dc/elements/1.1/"><dc:title><rdf:Alt
ml:lang="x-default">title</rdf:li></rdf:Alt>
:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:li xml:lang="x-default">title</rdf:li></rdf:Alt>
RDF></x:xmpmeta>
```

flag{t3rs3l0b0ng}

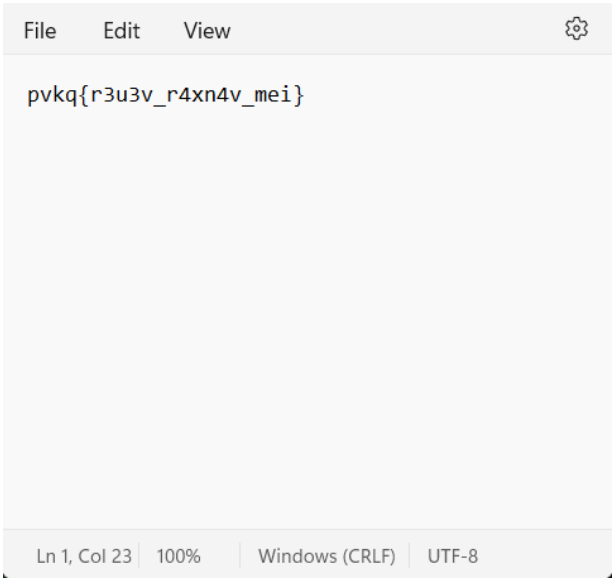
Kaisar Romawi
Warm Up

Diberikan file sebagai berikut :

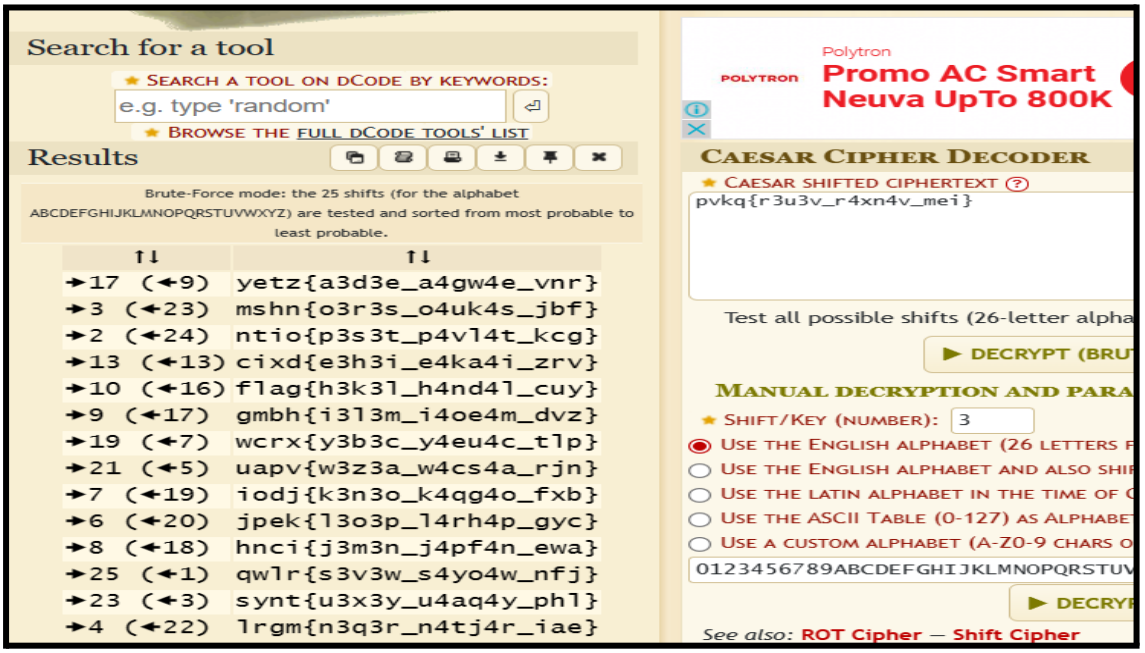


Link File:
https://codexploit.fun/files/14859f1432a072403dfd096f5183fda3/kaisar_romawi.txt?token=eyJ1c2VyX2lkIjo4LCJ0ZWFtX2lkIjpudWxsLCJmaWxlX2lkIjoxOX0.ZVfOzg.aiCqC9hOOjmUDpNULGfW6nzZ5Ns

Ketika dibuka :



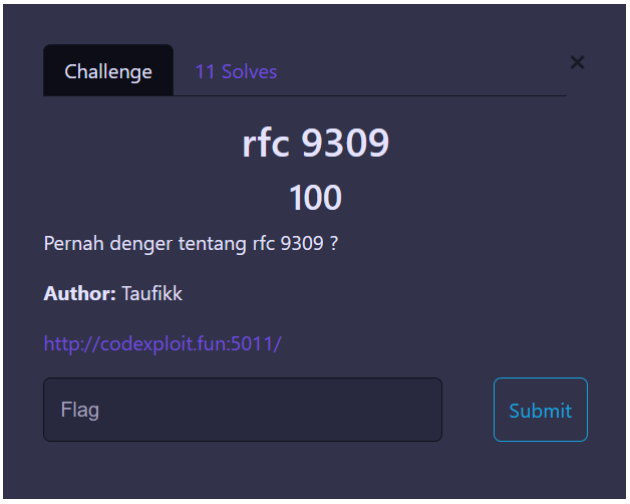
Solusi :
Dari Judul soal dapat kita simpulkan bahwa “Kaisar” > Caesar, maka dapat kita decode menggunakan Caesar Cipher



Dapat kita lihat bahwa Flag : `flag{h3k3l_h4nd4l_cuy}`

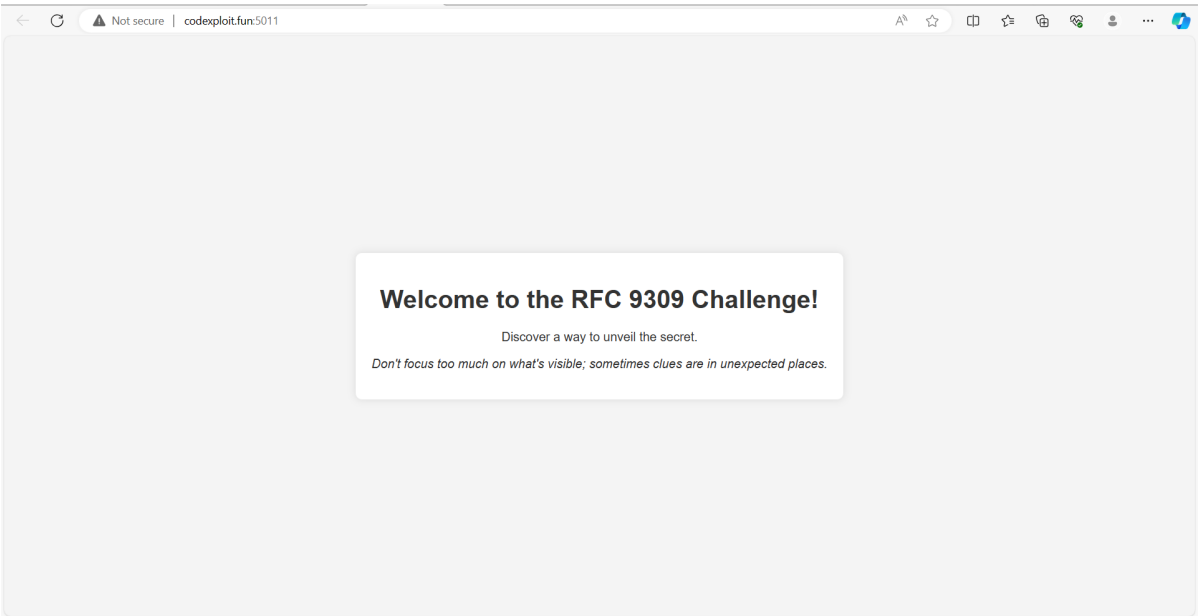
RFC 9309
Warm Up

Deskripsi Soal :

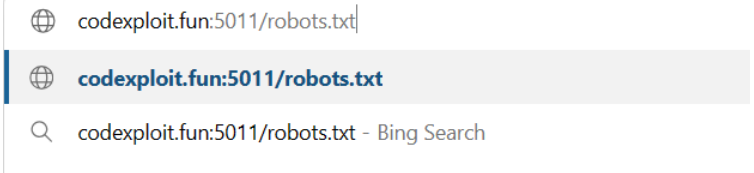


Link web: http://codexploit.fun:5011/

Ketika web dibuka :

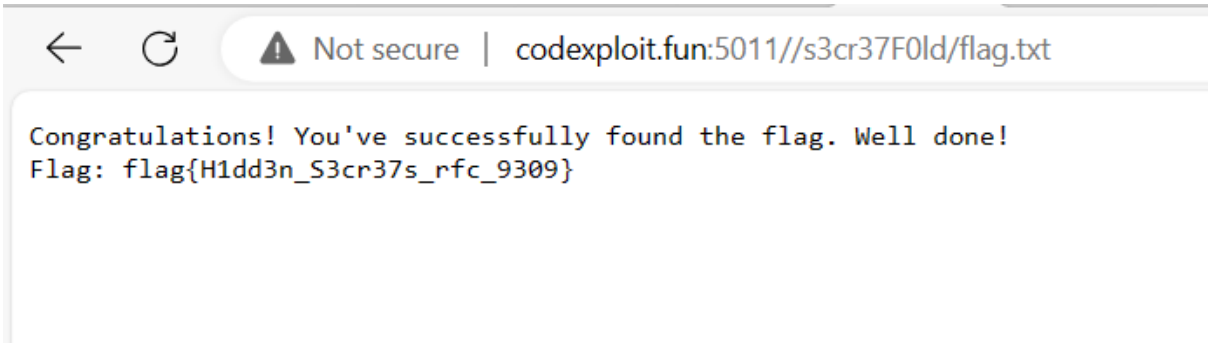


Solusi :
Karena RFC 9309 termasuk Robots Exclusion Protocol maka dapat dieksekusi dengan penambahan /robots.txt pada search bar



maka akan muncul sebagai berikut :

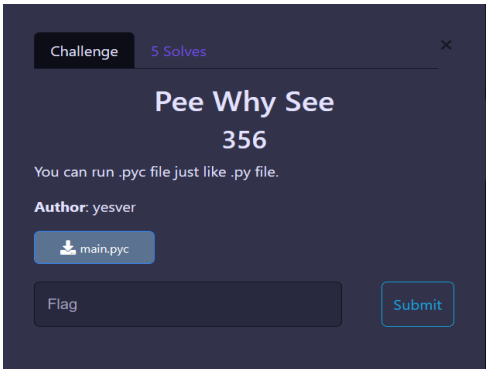
maka akan coba kita input satu persatu pada search bar :



Flag: flag{H1dd3n_S3cr37s_rfc_9309}

Pee Why See
Reverse Engineering

Deskripsi Soal:



Link File:
https://codexploit.fun/files/73090e856e51baf17fae8c68b9133f20/main.pyc?token=eyJ1c2VyX2lkIjo4LCJ0ZWFtX2lkIjpudWxsLCJmaWxlX2lkIjo2fQ.ZVfQPQ.pAd65ky2-5sXJAl4tDehdOtXFWE

Solusi:
kita perlu mendecompile file .pyc ke .py agar dapat membuka file tersebut.
untuk men-decompile file ini saya menggunakan tools online

```python
# uncompyle6 version 3.5.0
# Python bytecode 3.8 (3413)
# Decompiled from: Python 2.7.5 (default, Jun 20 2023, 11:36:40)
# [GCC 4.8.5 20150623 (Red Hat 4.8.5-44)]
# Embedded file name: .\main.py
# Size of source mod 2**32: 397 bytes
data = [
 102, 108, 97, 103, 123, 99, 111, 109, 112, 105, 108, 101, 100, 95, 112, 121, 116, 104, 111, 110,
 95, 105, 115, 95, 101, 97, 115, 121, 95, 116, 111, 95, 100, 101, 99, 111, 109, 112, 105, 108, 101, 125]
flag = input('Enter the flag: ')
for i, e in enumerate(flag):
    if ord(e) != data[(i % len(data))]:
        print('Nice try.')
        exit(0)

print('You got the flag!')
```

setelah itu kita perlu membuat script file sederhana agar mendapatkan output flagnya

```python
data = [
    102, 108, 97, 103, 123, 99, 111, 109, 112, 105, 108, 101, 100, 95, 112, 121, 116, 104, 111, 110,
    95, 105, 115, 95, 101, 97, 115, 121, 95, 116, 111, 95, 100, 101, 99, 111, 109, 112, 105, 108, 101, 125
]

decoded_data = ''.join(chr(char) for char in data)
print(decoded_data)
```

```
PS C:\Users\Steven\OneDrive\VEN\.vscode> python
flag{compiled_python_is_easy_to_decompile}
PS C:\Users\Steven\OneDrive\VEN\.vscode>
```

Flag : flag{compiled_python_is_easy_to_decompile}

🎵 hajiman nan marya neoui bakkeseon sal su eopseo 🎵
OSINT

Deskripsi soal:

Link File :
https://drive.google.com/drive/folders/10Zsxtlgv2Bmgm57cdZKIUF03hh1kV390?usp=sharing

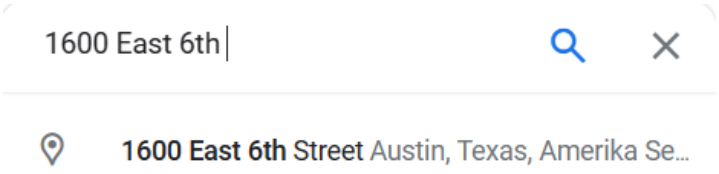
Ketika file dibuka:

Solusi:

Dapat kita simpulkan bahwa kita perlu mencari toko yang ada pada gambar lalu melihat ulasannya pada Google Maps

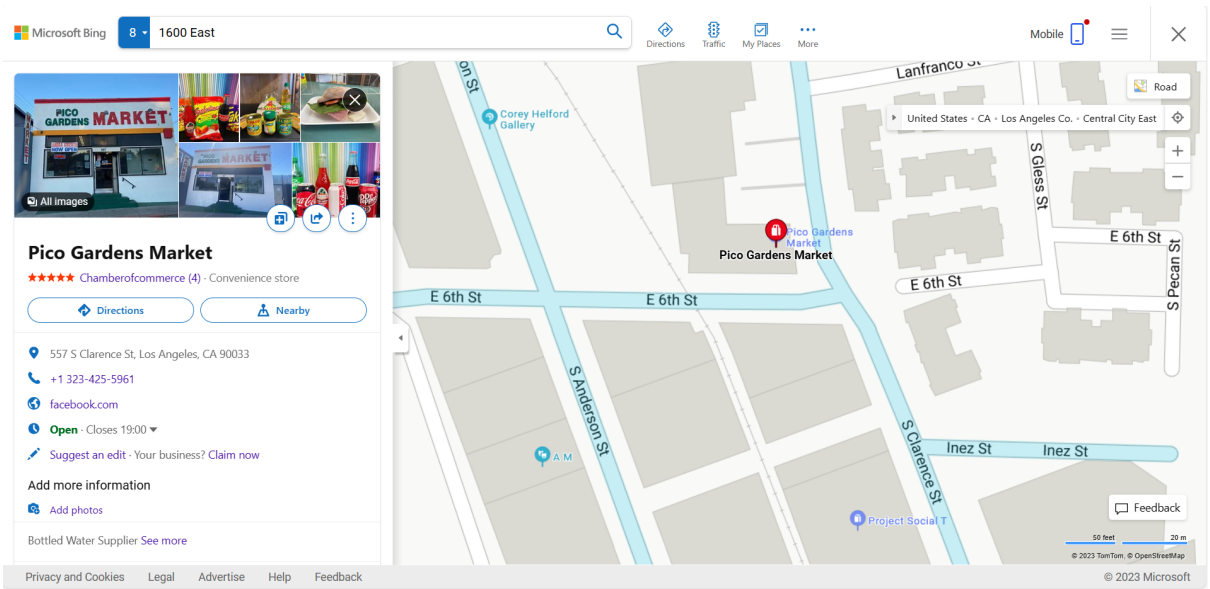
Foto pertama:
dapat kita lihat nama jalan pada foto tersebut

Selanjutnya kita cari pada Google Maps

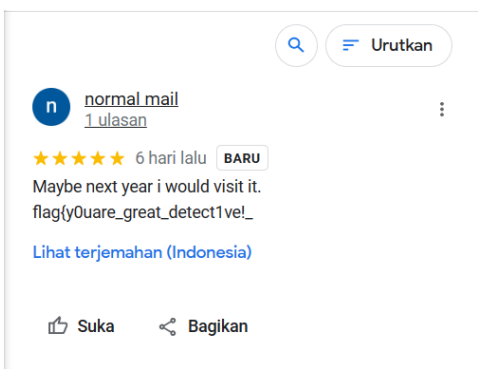


Dapat kita lihat bahwa daerah tersebut merupakan daerah Austin, Texas, AS

Selanjutnya, kita cari market yang sesuai dengan foto tersebut



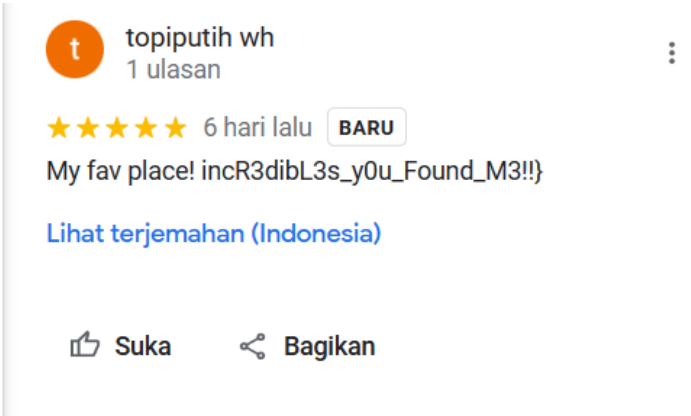
Setelah itu, lihat ulasannya



Hal yang sama juga kita lakukan pada foto kedua

Dapat disimpulkan bahwa foto tersebut terletak pada negara Jepang dekat dengan Austrian Embassy

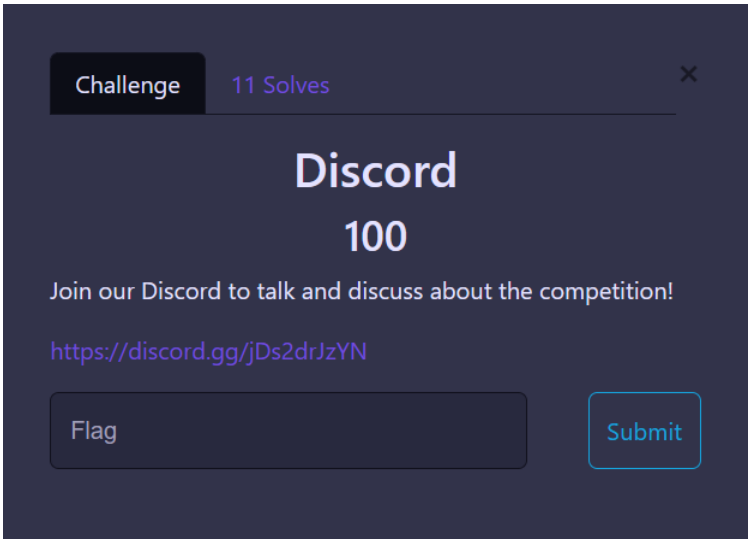
Setelah melakukan pencarian, ditemukan tempat (toko) yaitu St.Moritz sesuai dengan tempat difoto. Setelah itu kita tinggal melihat ulasan dari toko tersebut.



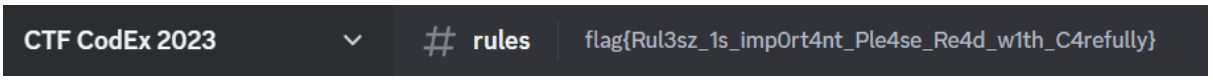
Flag : flag{y0uare_great_detect1ve!_incR3dibL3s_y0u_Found_M3!!}

Discord
Miscellaneous

Deskripsi Soal :



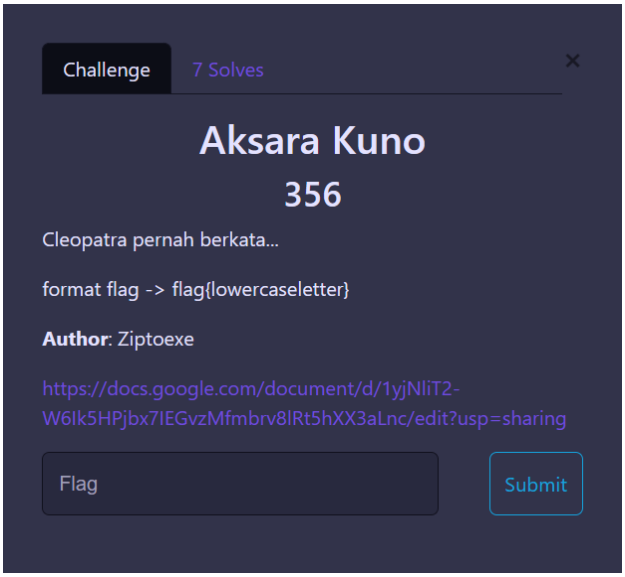
Solusi:
Kita hanya perlu mencari flag yang terdapat dalam discord tersebut.



Flag: flag{Rul3sz_1s_imp0rt4nt_Ple4se_Re4d_w1th_C4refully}

Aksara Kuno
Miscellaneous

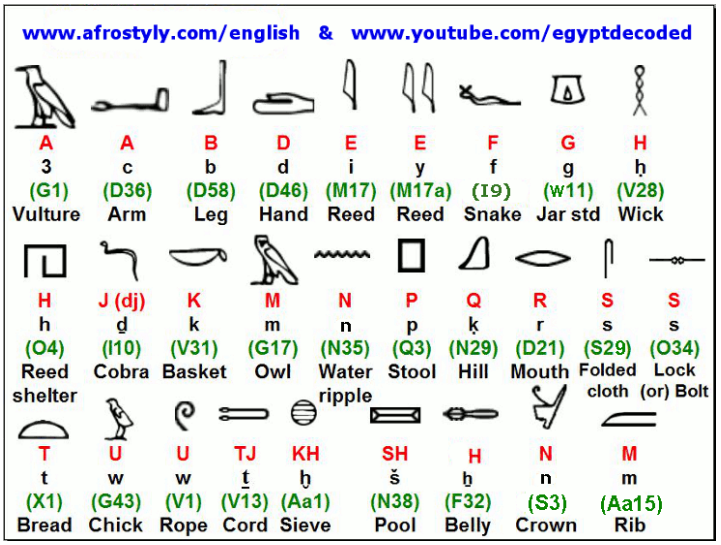
Deskripsi Soal:



Link Filel:
[MyOldSecret - Google Dokumen]

Solusi:
Pada file tersebut, terdapat beberapa gambar yang merupakan hieroglif mesir.

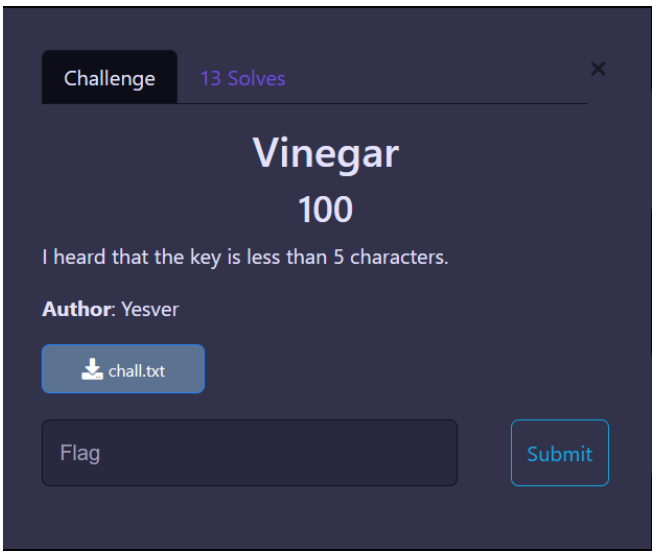
Kemudian dapat kita cocokkan dengan gambar berikut dan akan menghasilkan suatu kalimat



Flag : flag{hieroglifancientegypt}

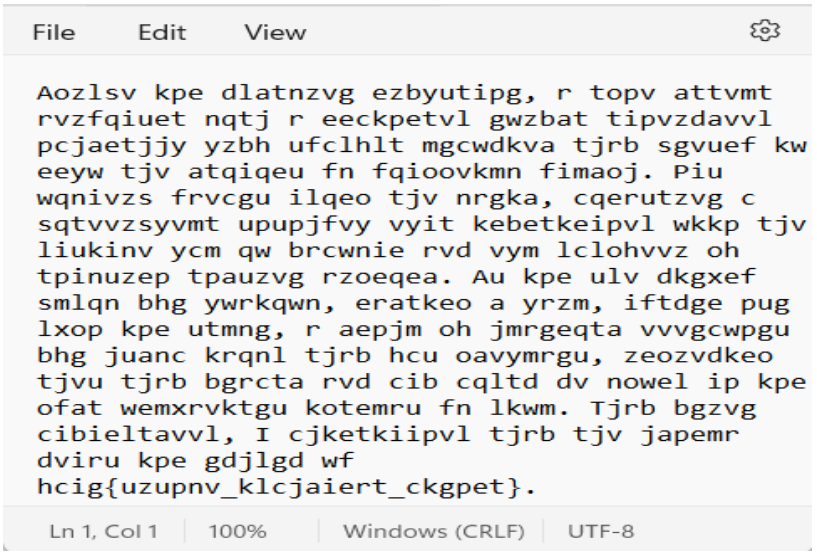
Vinegar
Crypthography

Deskripsi soal:

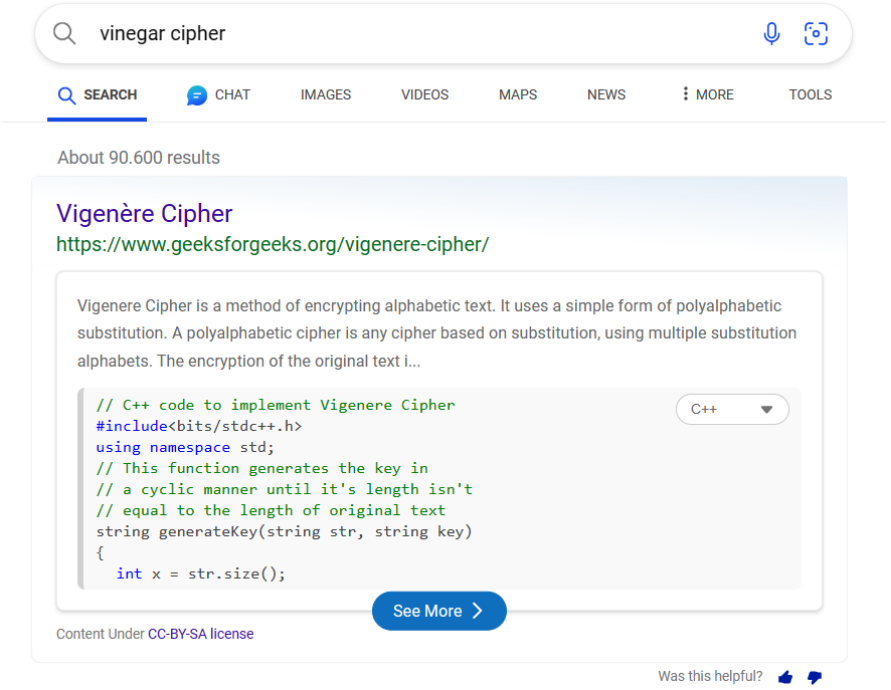


Link File :
https://codexploit.fun/files/e66ca73ff30f8f42bd2b9e19a157d48e/chall.txt?token=eyJ1c2VyX2lkIjo4LCJ0ZWFtX2lkIjpudWxsLCJmaWxlX2lkIjo1fQ.ZVfGBQ.Ix-zc-3azGZ5zZAygwL5DBvyEcE

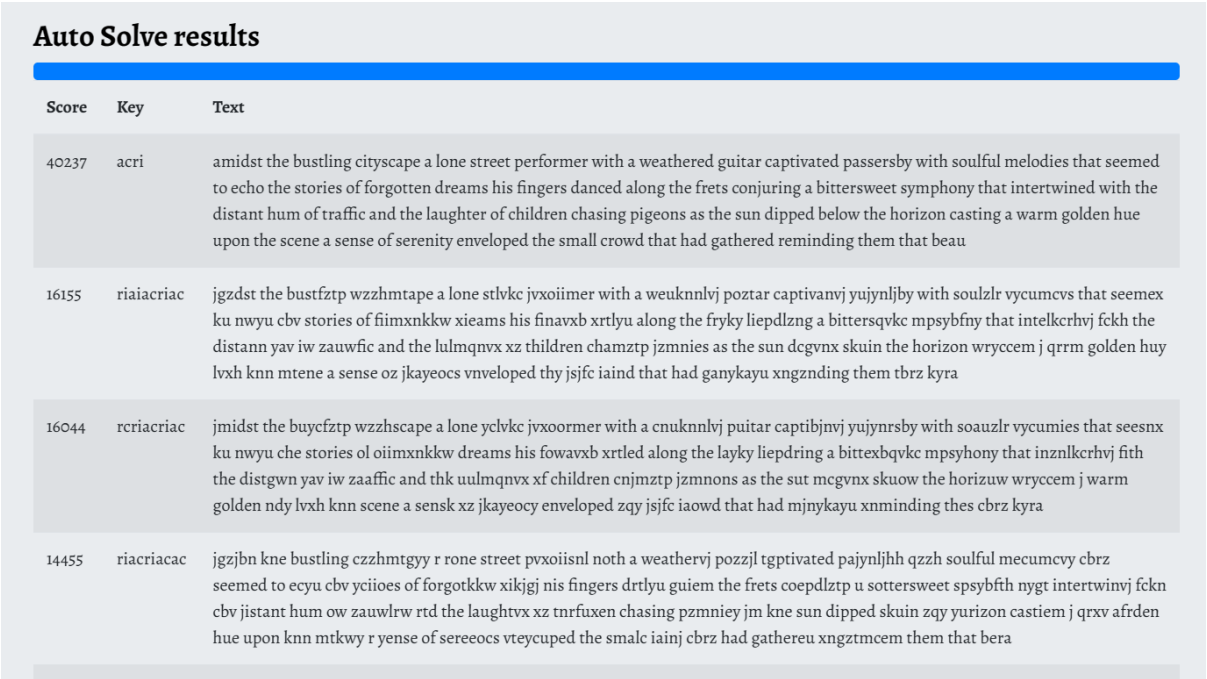
Solusi:
Ketika dibuka maka akan terlihat seperti berikut:



Namun, ketika kita mencari pada Google, akan ditampilkan sebagai berikut:



Maka dapat kita simpulkan bahwa kode tersebut merupakan kode vigenere. Langkah selanjutnya adalah kita akan men-*decode* teks tersebut menggunakan vigenere cipher.

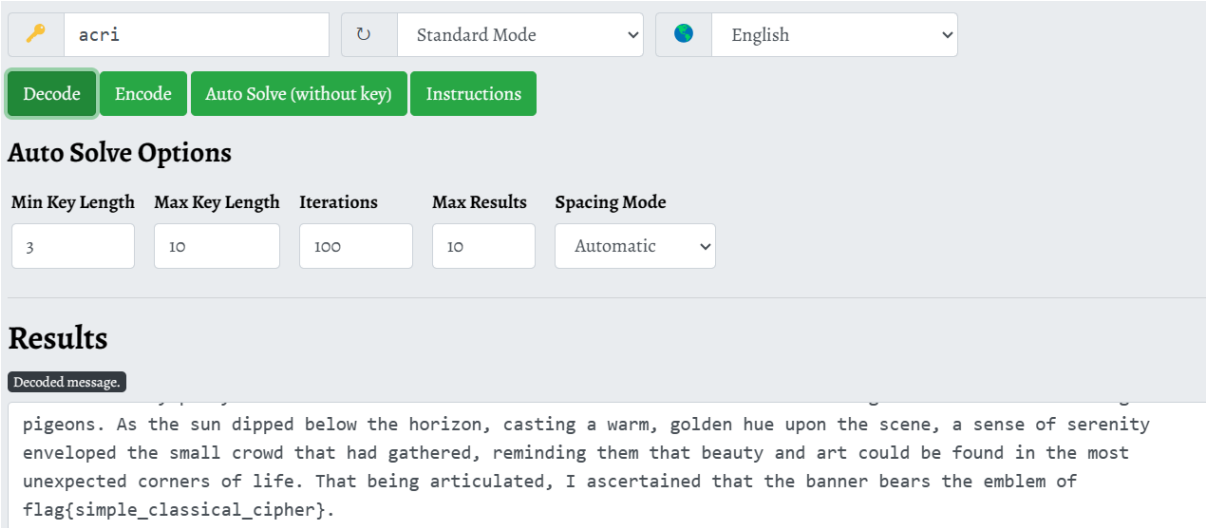


Auto Solve results

Score	Key	Text
40237	acri	amidst the bustling cityscape a lone street performer with a weathered guitar captivated passersby with soulful melodies that seemed to echo the stories of forgotten dreams his fingers danced along the frets conjuring a bittersweet symphony that intertwined with the distant hum of traffic and the laughter of children chasing pigeons as the sun dipped below the horizon casting a warm golden hue upon the scene a sense of serenity enveloped the small crowd that had gathered reminding them that beau
16155	riaiacriac	jgzdst the bustfztp wzzhmtape a lone stlvkc jvxoiimer with a weuknnlvj poztar captivanvj yujynljby with soulzlr vycumcvs that seemex ku nwyu cbv stories of fiimxnkkw xieams his finavxb xrtlyu along the fryky liepdlzng a bittersqvkc mpsybfny that intelkcrhvj fckh the distann yav iw zauwfic and the lulmqnvx xz thildren chamztp jzmnies as the sun dcgvnx skuin the horizon wryccem j qrrm golden huy lvxh knn mtene a sense oz jkayeocs vnveloped thy jsjfc iaind that had ganykayu xngznding them tbrz kyra
16044	rcriacriac	jmidst the buycfztp wzzhscape a lone yclvkc jvxoormer with a cnuknnlvj puitar captibjnvj yujynrsby with soauzlr vycumies that seesnx ku nwyu che stories ol oiimxnkkw dreams his fowavxb xrtled along the layky liepdring a bittexbqvkc mpsyhony that inznlkcrhvj fith the distgwn yav iw zaaffic and thk uulmqnvx xf children cnjmztp jzmnons as the sut mcgvnx skuow the horizuw wryccem j warm golden ndy lvxh knn scene a sensk xz jkayeocy enveloped zqy jsjfc iaowd that had mjnykayu xnminding thes cbrz kyra
14455	riacriacac	jgzjbn kne bustling czzhmtgyy r rone street pvxoiisnl noth a weathervj pozzjl tgptivated pajynljhh qzzh soulful mecumcvy cbrz seemed to ecyu cbv yciioes of forgotkkw xikjgj nis fingers drtlyu guiem the frets coepdlztp u sottersweet spsybfth nygt intertwinvj fckn cbv jistant hum ow zauwlrw rtd the laughtvx xz tnrfuxen chasing pzmniey jm kne sun dipped skuin zqy yurizon castiem j qrxv afrden hue upon knn mtkwy r yense of sereeocs vteycuped the smalc iainj cbrz had gathereu xngztmcem them that bera

Karena key < 5 character, maka kita masukkan “acri” sebagai key

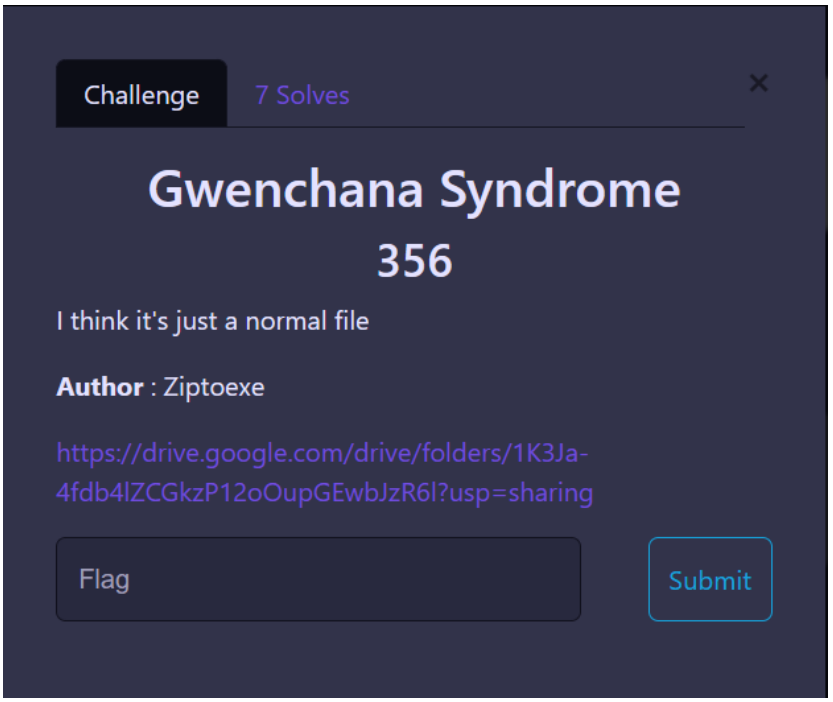
Maka, hasil decode nya adalah



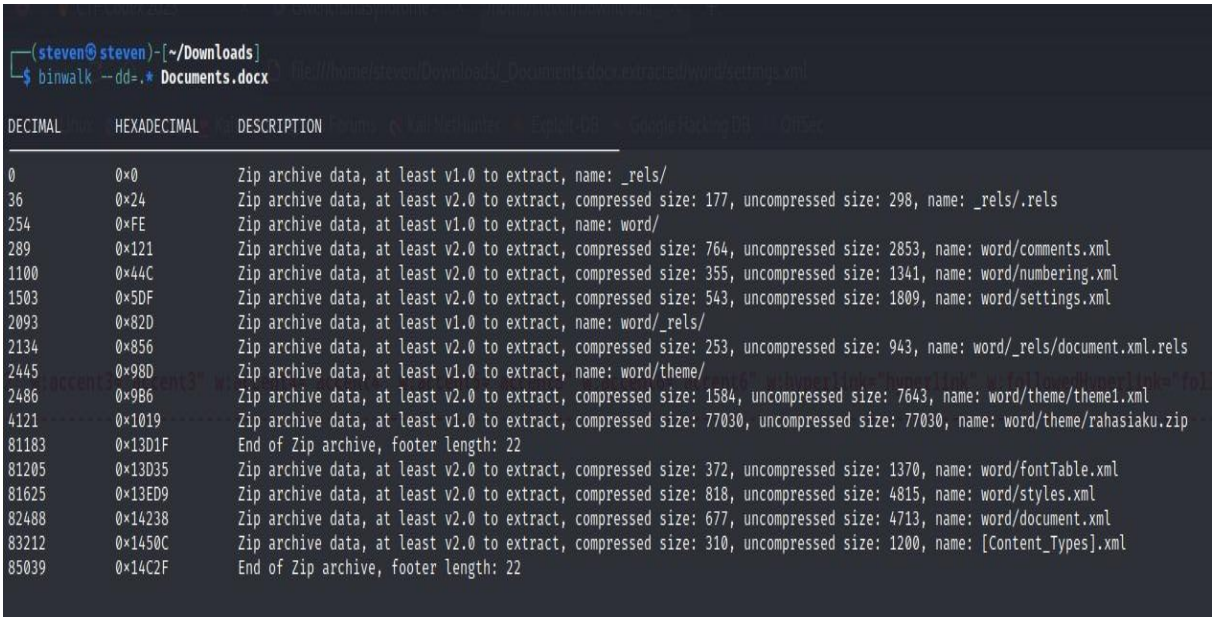
Flag: flag{simple_classical_cipher}

Gwenchana Syndrome
Crypthography

Deskripsi soal:

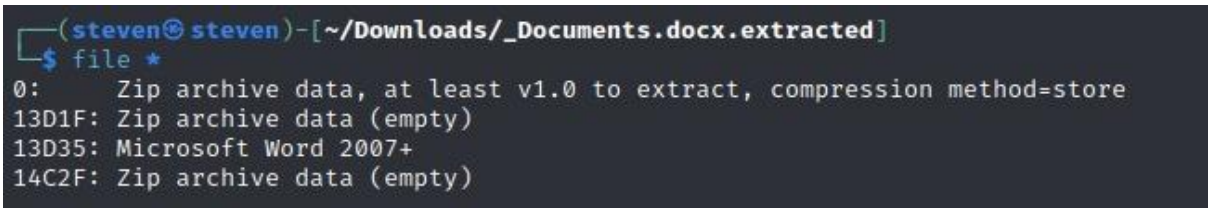


Link file:
https://drive.google.com/drive/folders/1K3Ja-4fdb4lZCGkzP12oOupGEwbJzR6l?usp=sharing
solusi:
untuk mendapatkan flag dari soal ini, saya menggunakan linux
pertama, saya menggunakan tools *binwalk* untuk menganalisis dan mengextract file tersebut

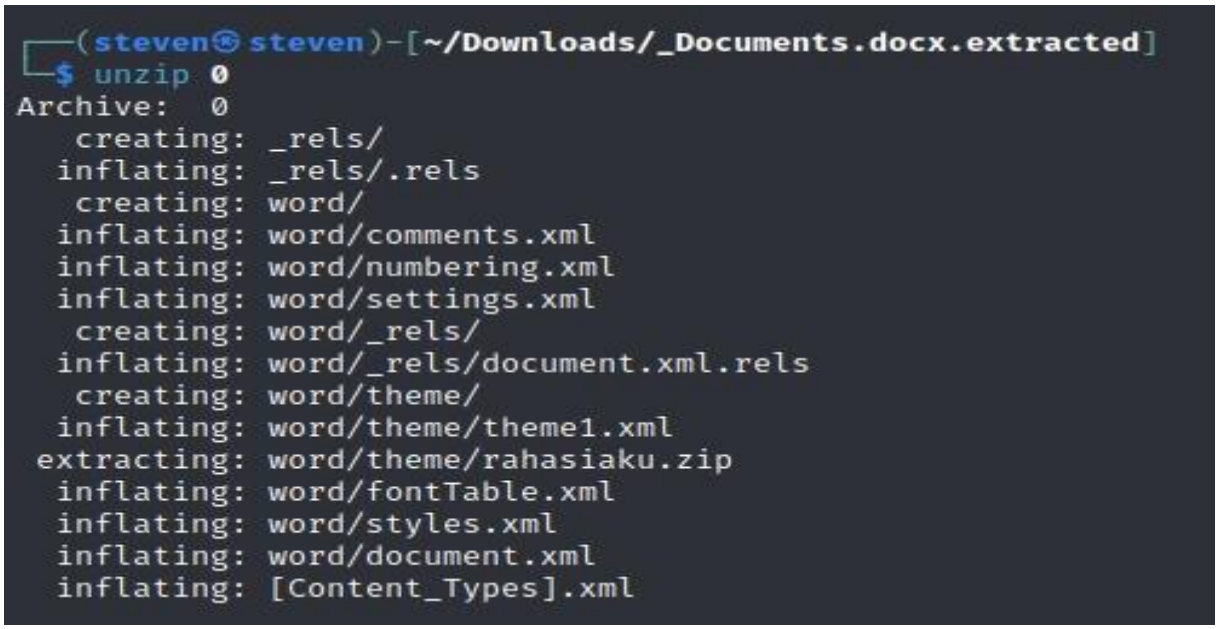


setelah itu kita masuk kedalam directories yang ada setelah kita extract tadi. Disini terdapat beberapa file didalamnya

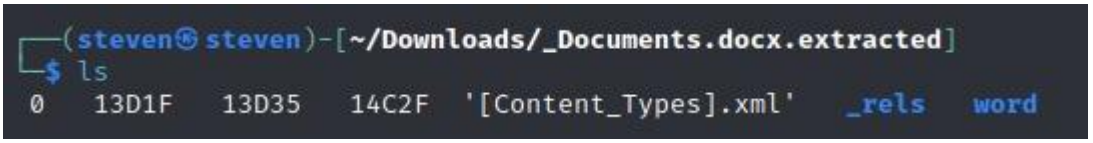
Setelah itu, dengan menggunakan command ‘file *’ didapatkan bahwa file ‘0’ merupakan zip file.



Maka, selanjutnya saya meng-*unzip* file tersebut.



Diketahui bahwa terdapat beberapa directories lagi didalamnya



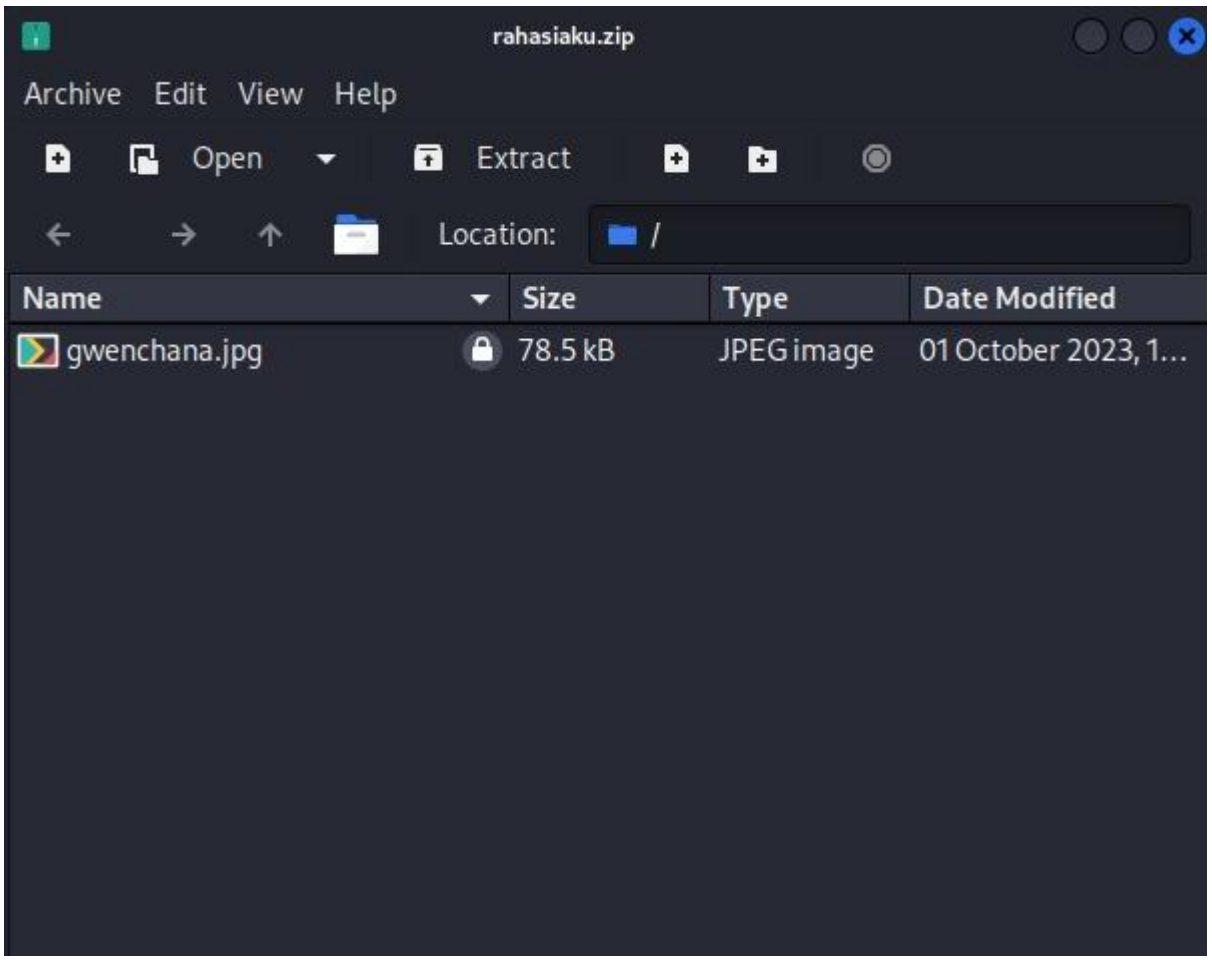
setelah mencoba satu persatu, didapatkan directories didalam ‘word’ dengan title ‘theme’

```
┌──(steven㉿steven)-[~/Downloads/_Documents.docx.extracted]
└─$ cd word

┌──(steven㉿steven)-[~/Downloads/_Documents.docx.extracted/word]
└─$ ls
_rels  comments.xml  document.xml  fontTable.xml  numbering.xml  settings.xml  styles.xml  theme
```

didalam theme terdapat sebuah zipped file yaitu ‘rahasiaku.zip’

```
┌──(steven㉿steven)-[~/Downloads/_Documents.docx.extracted/word/theme]
└─$ ls
rahasiaku.zip  theme1.xml

┌──(steven㉿steven)-[~/Downloads/_Documents.docx.extracted/word/theme]
└─$ open rahasiaku.zip
```

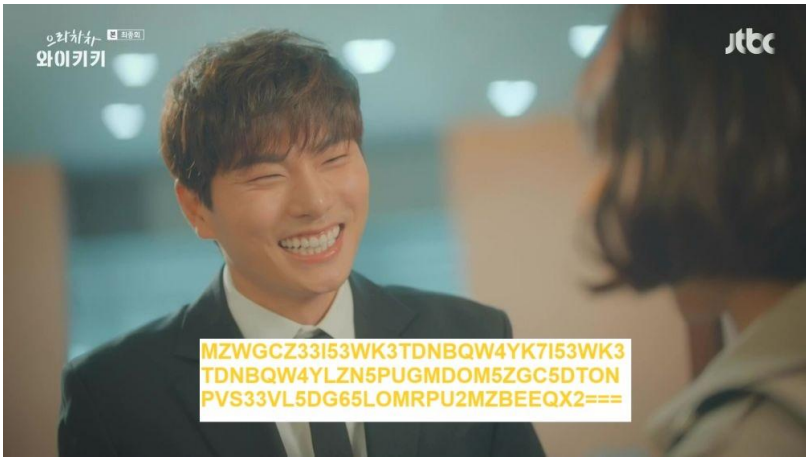
setelah mencoba membuka zipped file tersebut, terdapat file yang memerlukan password untuk membukanya.



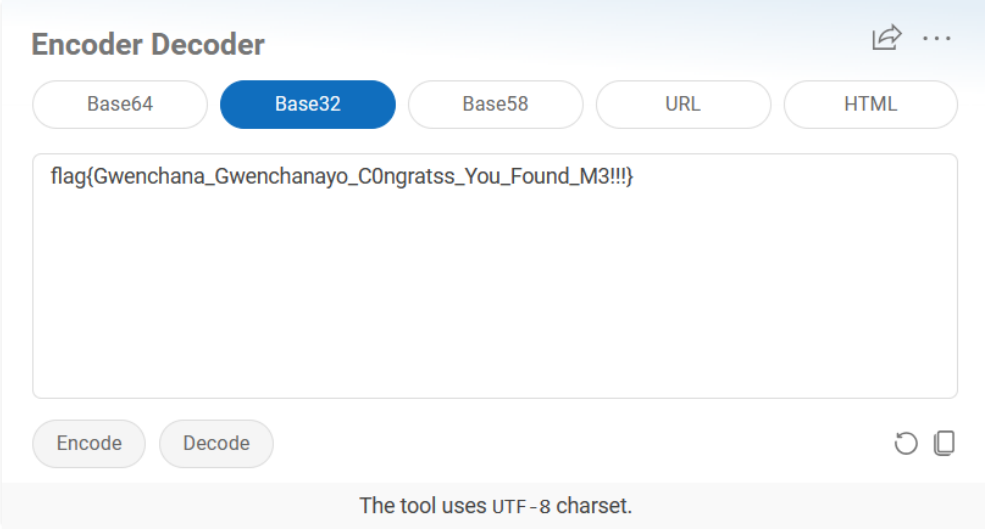
Setelah dilakukan pencarian akhirnya didapatkan password berada dalam ‘settings.xml’

```
:settings>Password ZIP -> in1P4ssw0rdnyaGw3nCh4nA
----------^
```

Setelah itu, kita dapatkan sebuah kode yang telah dienkripsi.



kode tersebut merupakan text yang dienkripsi dengan Base32, kemudian setelah di dekripsi akan menghasilkan:

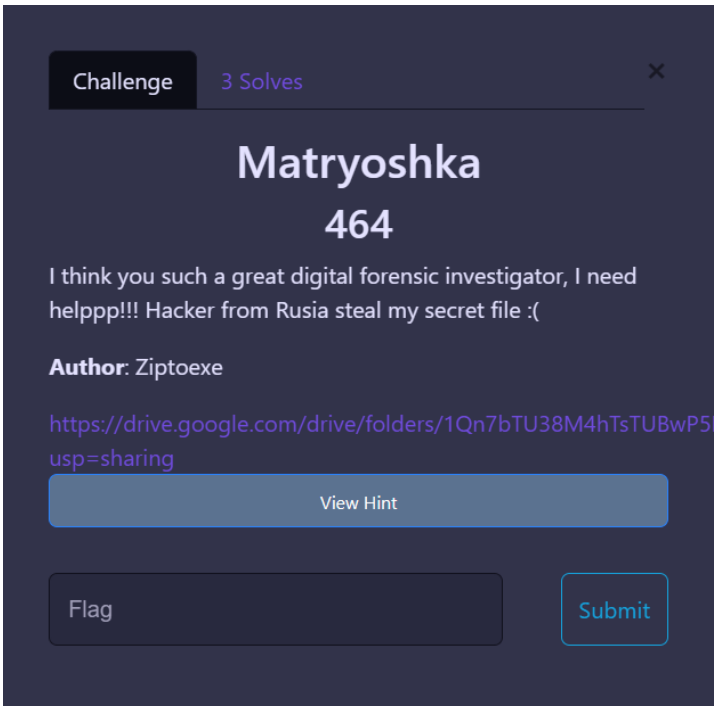


Flag: flag{Gwenchana_Gwenchanayo_C0ngratss_You_Found_M3!!!}

Matryoshka

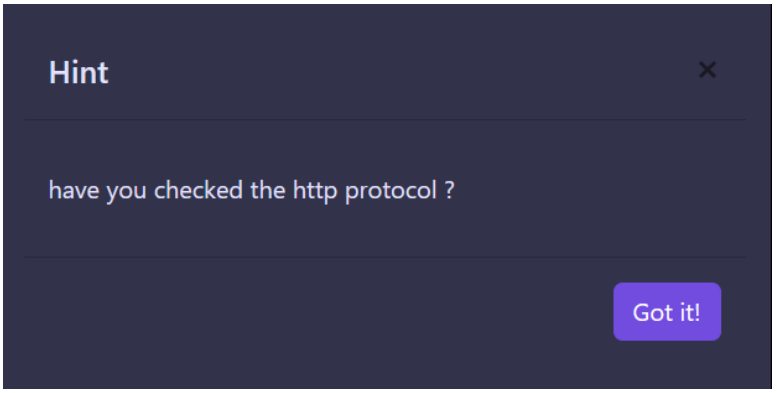
Forensics

Deskripsi Soal:



Link File:
https://drive.google.com/drive/folders/1Qn7bTU38M4hTsTUBwP5RwQi7bAYxNnEt?usp=sharing

Solusi:
Untuk tools yang saya gunakan adalah wireshark.
Awalnya saya kebingungan dengan soal ini, namun hint yang diberikan sangat membantu



setelah dicek terdapat beberapa file sebagai ‘tipuan’

http

No.	Time	Source	Destination	Protocol	Lengt	Info
18061	380.477494448	54.147.59.206	192.168.171.129	HTTP	709	HTTP/1.0 404 File not found (text/html)
18092	390.093741443	192.168.171.129	54.147.59.206	HTTP	599	GET /flag.txt HTTP/1.1
18098	390.353878784	54.147.59.206	192.168.171.129	HTTP	279	HTTP/1.0 200 OK (text/plain)
18141	406.186816584	192.168.171.129	54.147.59.206	HTTP	599	GET /test.txt HTTP/1.1
18147	406.443402973	54.147.59.206	192.168.171.129	HTTP	688	HTTP/1.0 200 OK (text/plain)
18174	421.525444266	192.168.171.129	54.147.59.206	HTTP	601	GET /etc/shadow HTTP/1.1
18178	421.788439109	54.147.59.206	192.168.171.129	HTTP	709	HTTP/1.0 404 File not found (text/html)
18198	430.419136206	192.168.171.129	54.147.59.206	HTTP	600	GET /flag2.txt HTTP/1.1
18200	430.698653211	54.147.59.206	192.168.171.129	HTTP	266	HTTP/1.0 200 OK (text/plain)
18251	449.865536136	192.168.171.129	54.147.59.206	HTTP	606	GET /masitroshka.zip HTTP/1.1
18263	450.145445233	54.147.59.206	192.168.171.129	HTTP	709	HTTP/1.0 404 File not found (text/html)
18288	461.963780143	192.168.171.129	54.147.59.206	HTTP	605	GET /mtryushoka.zip HTTP/1.1
18294	462.224811242	54.147.59.206	192.168.171.129	HTTP	709	HTTP/1.0 404 File not found (text/html)
18310	467.852224620	192.168.171.129	54.147.59.206	HTTP	606	GET /matryushoka.zip HTTP/1.1
18314	468.137098605	54.147.59.206	192.168.171.129	HTTP	709	HTTP/1.0 404 File not found (text/html)
18342	483.034511807	192.168.171.129	54.147.59.206	HTTP	607	GET /matariyoshka.zip HTTP/1.1
18354	483.296111202	54.147.59.206	192.168.171.129	HTTP	709	HTTP/1.0 404 File not found (text/html)
18375	493.886312064	192.168.171.129	54.147.59.206	HTTP	605	GET /matryoshka.zip HTTP/1.1

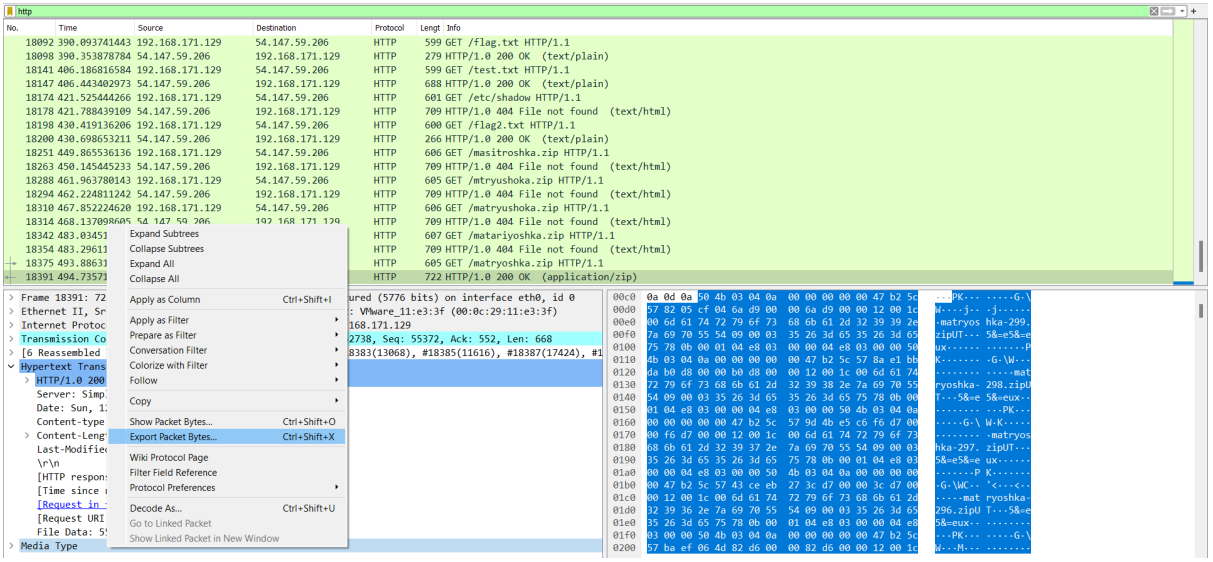
namun, ketika dicek lebih teliti terdapat 1 file yang menarik

18375	493.886312064	192.168.171.129	54.147.59.206	HTTP	605	GET /matryoshka.zip HTTP/1.1
18391	494.735717584	54.147.59.206	192.168.171.129	HTTP	722	HTTP/1.0 200 OK (application/zip)

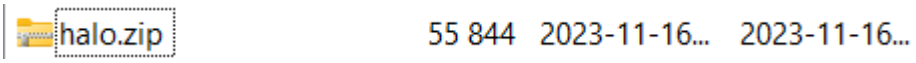
yang mana terdapat nested zip file

```
GET /matryoshka.zip HTTP/1.1
Host: 54.147.59.206:8090
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: user=Tzo2OiJteXNob3AiOjQ6e3M6MTE6ImNvb2tpZV90eXBlIjtzOjk6InBvcm9zeGJjYyI7czo5OiJ1c2VyX3R5cGUiO3M6MTE6IkNvbW1vbl9Vc2VyIjtzOjY6InhbGxldCI7aToxMDtzOjEzOiJwdXJjaGFzZWRGbGFnIjtiOjA7fQ%3D%3D
Upgrade-Insecure-Requests: 1

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.10.12
Date: Sun, 12 Nov 2023 19:00:36 GMT
Content-type: application/zip
Content-Length: 55844
Last-Modified: Sat, 28 Oct 2023 15:28:01 GMT

PK..
.....G.\W....j...j.......matryoshka-299.zipUT        ..5&=e5&=eux.............PK..
.....G.\W................matryoshka-298.zipUT        ..5&=e5&=eux.............PK..
.....G.\W.K..............matryoshka-297.zipUT        ..5&=e5&=eux.............PK..
.....G.\WC..'<...<.......matryoshka-296.zipUT        ..5&=e5&=eux.............PK..
.....G.\W...M............matryoshka-295.zipUT        ..5&=e5&=eux.............PK..
.....G.\W..r.............matryoshka-294.zipUT        ..5&=e5&=eux.............PK..
.....G.\W.m/Y............matryoshka-293.zipUT        ..5&=e5&=eux.............PK..
.....G.\W^J.6T...T.......matryoshka-292.zipUT        ..5&=e5&=eux.............PK..
.....G.\W|.aL............matryoshka-291.zipUT        ..5&=e5&=eux.............PK..
.....G.\W0...............matryoshka-290.zipUT        ..5&=e5&=eux.............PK..
.....G.\W4_YP&...&.......matryoshka-289.zipUT        ..5&=e5&=eux.............PK..
.....G.\W....l...l.......matryoshka-288.zipUT        ..5&=e5&=eux.............PK..
.....G.\W.r..............matryoshka-287.zipUT        ..5&=e5&=eux.............PK..
.....G.\W@.\.............matryoshka-286.zipUT        ..5&=e5&=eux.............PK..
.....G.\W.`.X>...>.......matryoshka-285.zipUT        ..5&=e5&=eux.............PK..
.....G.\W...?............matryoshka-284.zipUT        ..5&=e5&=eux.............PK..
.....G.\W................matryoshka-283.zipUT        ..5&=e5&=eux.............PK..
.....G.\W..#W............matryoshka-282.zipUT        ..5&=e5&=eux.............PK..
.....G.\W....V...V.......matryoshka-281.zipUT        ..5&=e5&=eux.............PK..
.....G.\W................matryoshka-280.zipUT        ..5&=e5&=eux.............PK..
.....G.\Wk.y.............matryoshka-279.zipUT        ..5&=e5&=eux.............PK..
.....G.\W....(...(.......matryoshka-278.zipUT        ..5&=e5&=eux.............PK..
.....G.\W.:.*n...n.......matryoshka-277.zipUT        ..5&=e5&=eux.............PK..
```

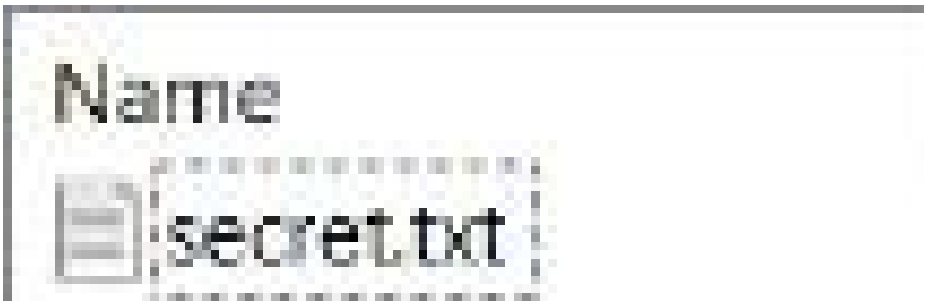
setelah itu, saya export pocket bytes



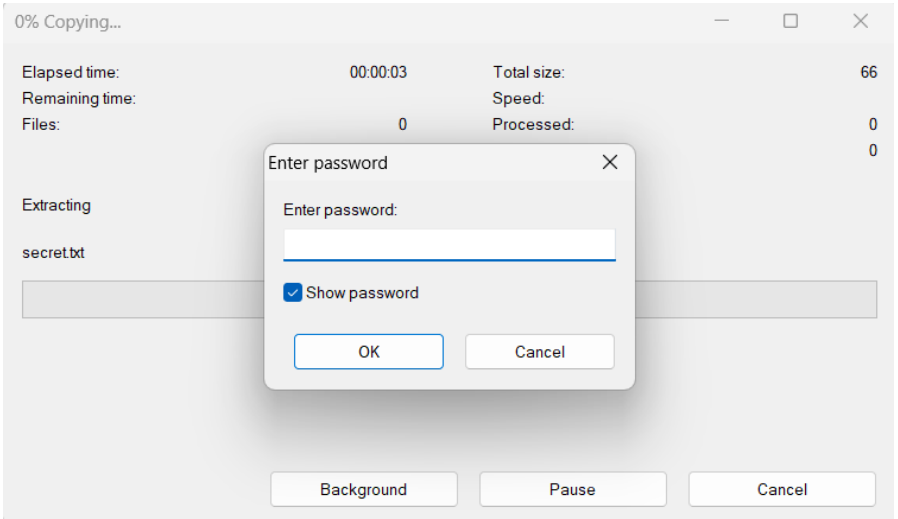
lalu saya rename dengan nama halo.zip



kemudian setelah membuka nested zip yang ada, didapatkan



tetapi untuk membuka file tersebut, diperlukan sebuah password



setelah mencari password menggunakan command tcp and frame contains “password”, ditemukan beberapa protocol FTP yang mencurigakan

tcp and frame contains "password"

No.	Time	Source	Destination	Protocol	Lengt	Info
18554	588.119357366	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
18596	615.031604251	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
18673	694.305222674	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
18773	813.761965803	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
18811	842.908435677	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
18847	889.133248858	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
18896	913.128394987	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
18979	947.563569776	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
19012	962.890199600	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
19045	982.044095660	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
19083	1010.3305505…	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
19128	1039.7901451…	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
19174	1064.8307656…	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.

yang mana terdapat password didalamnya

Wireshark · Follow TCP Stream (tcp.stream eq 129) · evidence-matryoshka.pcapng

```
220 Anonymous FTP server
USER anonymous
331 Please specify the password.
PASS anonymous
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features:
 EPRT
 EPSV
 MDTM
 PASV
 REST STREAM
 SIZE
 TVFS
211 End
TYPE I
200 Switching to Binary mode.
SIZE p3
550 Could not get file size.
EPSV
```

karena bersifat anonymous, sehingga harus mencari passwordnya didalam protocol FTP

ftp

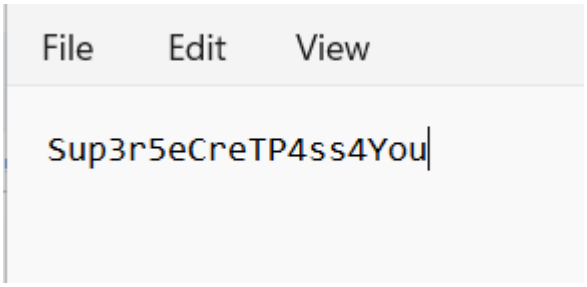
No.	Time	Source	Destination	Protocol	Lengt	Info
18550	583.859766806	54.147.59.206	192.168.171.129	FTP	80	Response: 220 Anonymous FTP server
18552	587.857019549	192.168.171.129	54.147.59.206	FTP	70	Request: USER anonymous
18554	588.119357366	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
18559	591.943809283	192.168.171.129	54.147.59.206	FTP	70	Request: PASS anonymous
18561	592.209848633	54.147.59.206	192.168.171.129	FTP	77	Response: 230 Login successful.
18563	592.210332164	192.168.171.129	54.147.59.206	FTP	60	Request: SYST
18565	592.473405075	54.147.59.206	192.168.171.129	FTP	73	Response: 215 UNIX Type: L8
18566	592.473918567	192.168.171.129	54.147.59.206	FTP	60	Request: FEAT
18569	592.736839357	54.147.59.206	192.168.171.129	FTP	111	Response: 211-Features:
18570	592.737297194	54.147.59.206	192.168.171.129	FTP	77	Response: SIZE
18573	598.993645680	192.168.171.129	54.147.59.206	FTP	60	Request: EPSV
18589	611.427835895	54.147.59.206	192.168.171.129	FTP	80	Response: 220 Anonymous FTP server
18592	614.751010455	192.168.171.129	54.147.59.206	FTP	70	Request: USER anonymous
18596	615.031604251	54.147.59.206	192.168.171.129	FTP	88	Response: 331 Please specify the password.
18598	618.912935877	192.168.171.129	54.147.59.206	FTP	70	Request: PASS anonymous
18600	619.194991464	54.147.59.206	192.168.171.129	FTP	77	Response: 230 Login successful.
18602	619.195337610	192.168.171.129	54.147.59.206	FTP	60	Request: SYST
18604	619.475674612	54.147.59.206	192.168.171.129	FTP	73	Response: 215 UNIX Type: L8

setelah mencari cukup lama, didapatkan bahwa dalam column Info dengan response SIZE terdapat beberapa potongan huruf.

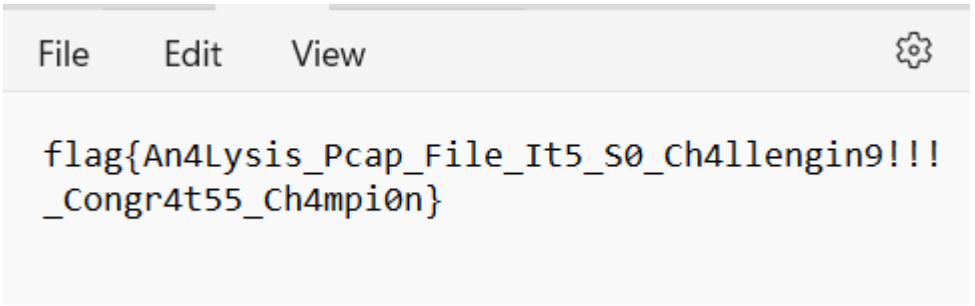
`Request: SIZE Su` `SIZE p3` `SIZE r5` `SIZE eCr` `SIZE eT` `SIZE P4`

`SIZE ss4` `SIZE Yo` `SIZE u`

yang mana jika disatukan menjadi



lalu, setelah berhasil mengakses file secret.txt akan mendapatkan flagnya



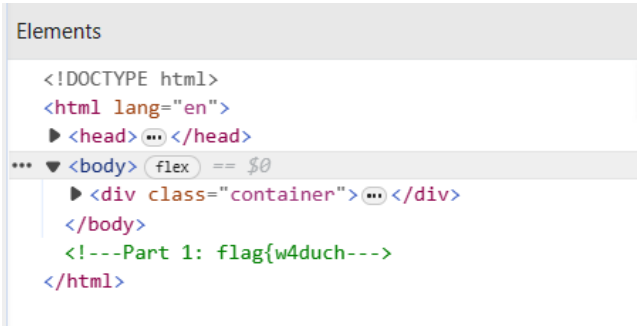
Flag: flag{An4Lysis_Pcap_File_It5_S0_Ch4llengin9!!!_Congr4t55_Ch4mpi0n}

Inspector Ladusingh
Web Exploitation

Deskripsi Soal:

Link Web : http://codexploit.fun:5013/

Solusi:
Ketika dilakukan inspect element:




```
/* Styling halaman utama */
body {
    background: url('background.jpg') center/cover no-repe
    font-family: Arial, sans-serif;
    display: flex;
    justify-content: center;
    align-items: center;
    height: 100vh;
/* Part 2: _k3t4huAn} */
}
```

Flag : flag{w4duch_k3t4huAn}

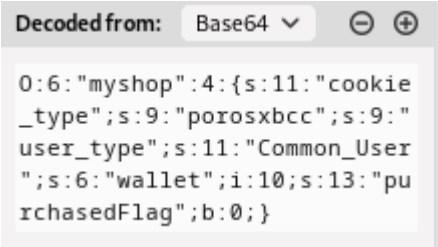
Tingky Wingky Dipsi Lala PuhSepuh
Web Exploitation

Deskripsi soal:

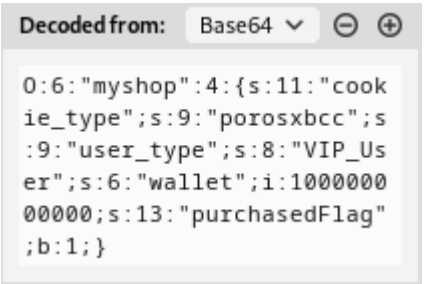
Link Web : http://codexploit.fun:5001/

Solusi:
untuk mendapatkan flagnya, disini saya memanipulasi cookies dengan menggunakan burp suite

disini, tertulis bahwa user_type adalah Common_user dan Integer dari wallet adalah 10 dan PurchasedFlag; b:0 > yang mana false



setelah itu saya ubah cookies menjadi:



Setelah itu, sudah bisa membeli flag dan mendapatkan flagnya

This Piece Of Flag For You,

flag{InSeCure_D3s3rializ4

This Piece Of Flag For You,

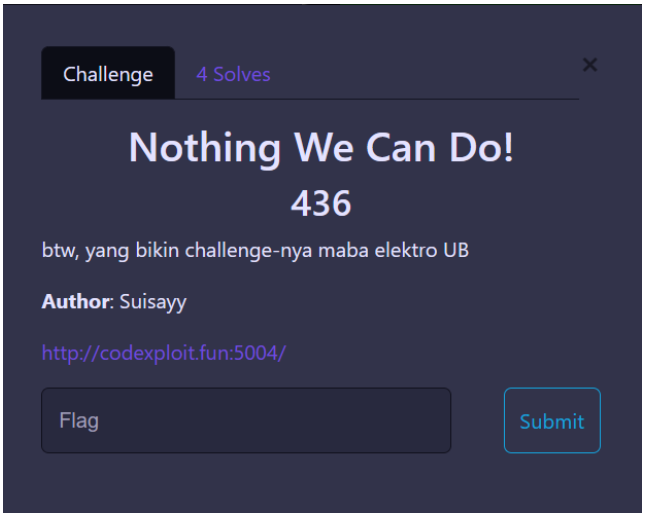
ti0n!!!_M4ntappp_

PuhSepuh_YangMoyang_HuSuhu}

Flag: flag{InSeCure_D3s3rializ4ti0n!!!_M4ntappp_PuhSepuh_YangMoyang_HuSuhu}

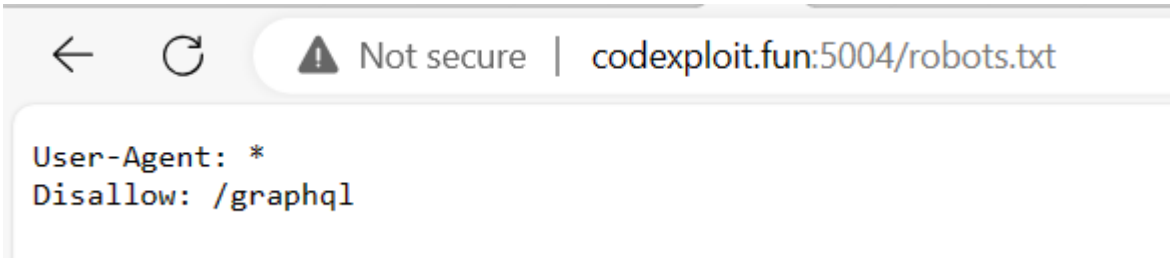
Nothing We Can Do!
Web Exploitation

Deskripsi soal:

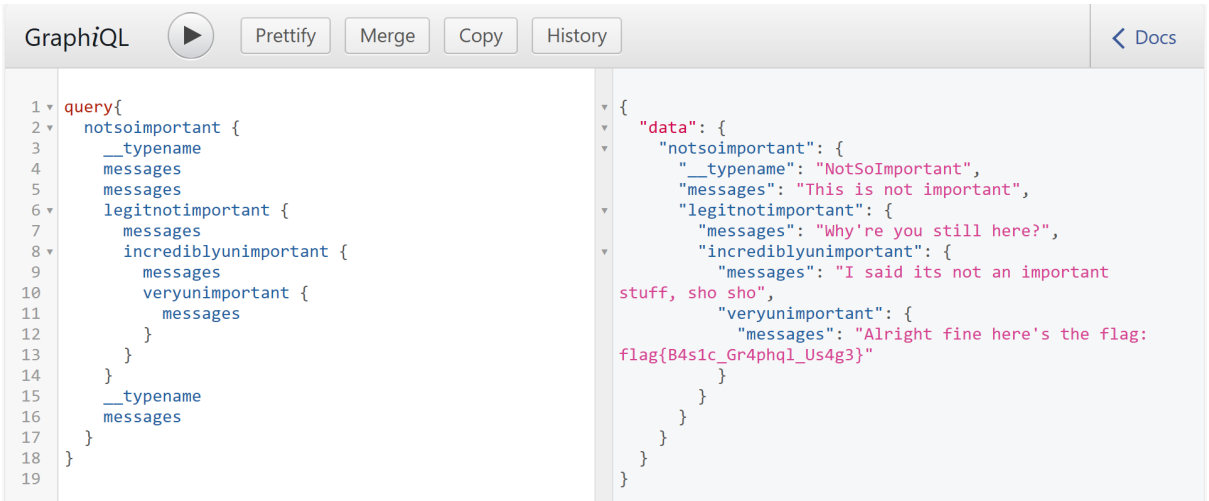


Link Web : http://codexploit.fun:5004/

Solusi:
setelah dimasukkan keyword ‘robots.txt’ didapatkan bahwa web ini dibuat dengan menggunakan bahasa graphql



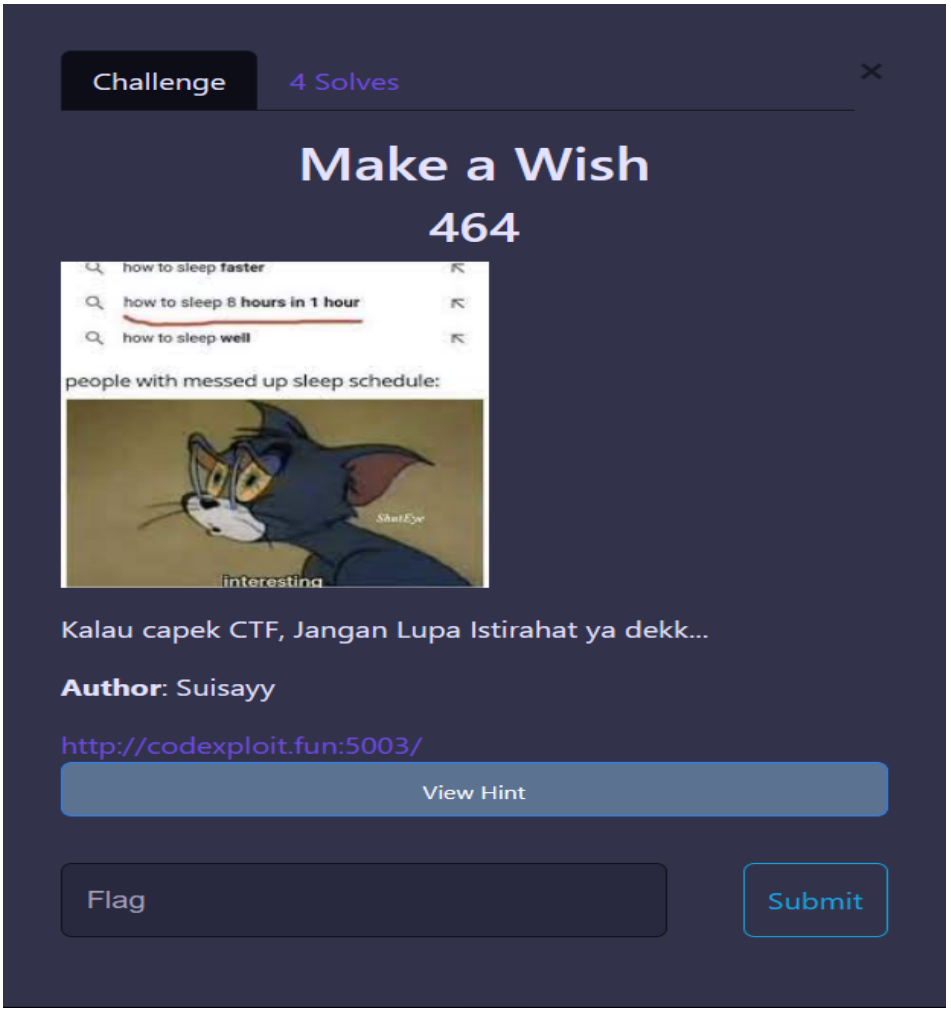
setelah dilakukan graphql Injection menggunakan graphql introspection untuk mendapatkan informasi, maka flag akan didapatkan



Flag : flag{B4s1c_Gr4phql_Us4g3}

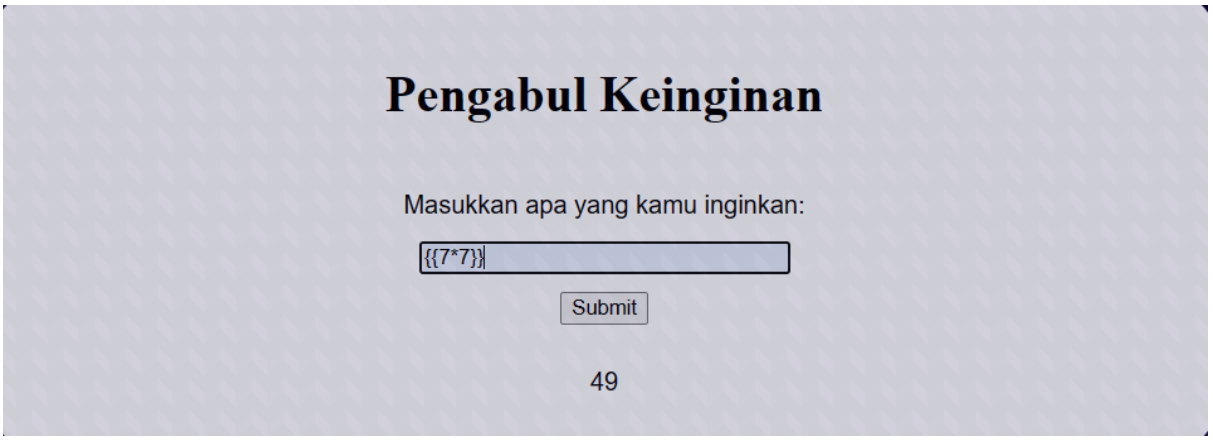
Make A Wish
Web Exploitation

Deskripsi soal

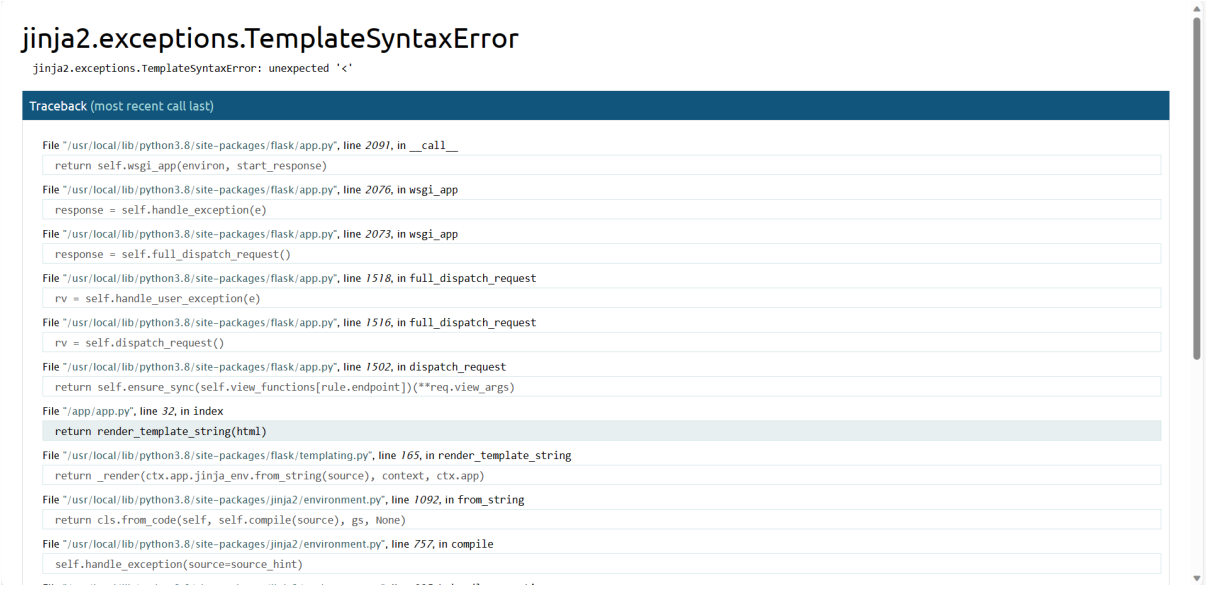


Link Web: http://codexploit.fun:5003/

Solusi:
Awalnya menggunakan bruteforce command pada kolom input, hingga

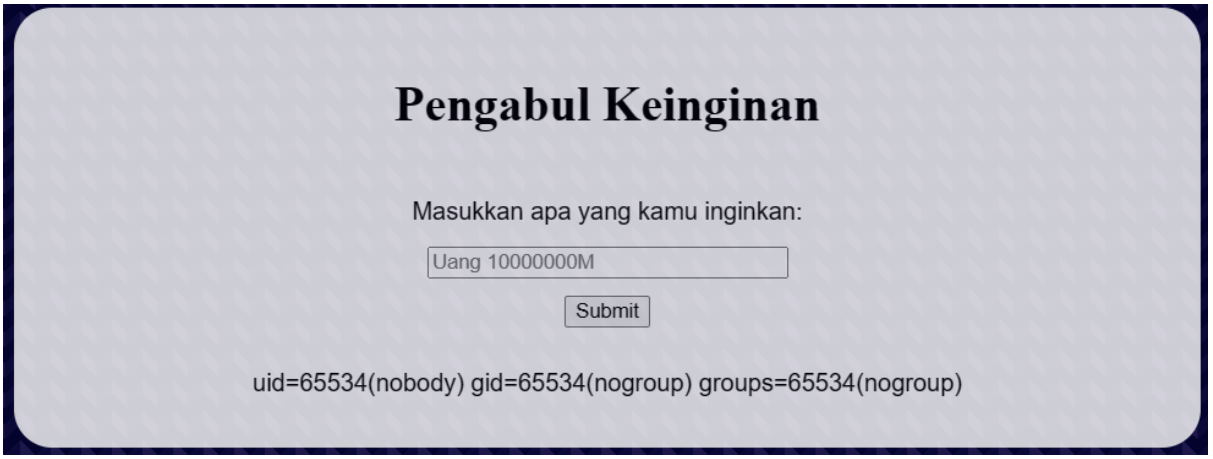


lalu dipastikan kembali dan menghasilkan

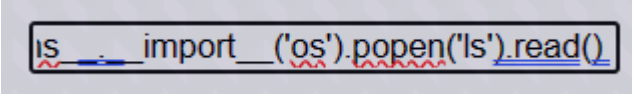


disini dapat dilihat bahwa web di buat menggunakan template jinja2, maka akan kita gunakan server side template injection. Kita coba command tersebut kedalam web.

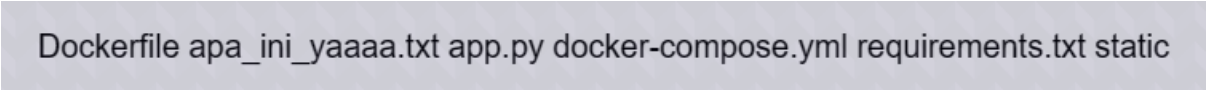
Setelah memasukkan command tersebut, command tersebut tereksekusi dengan baik



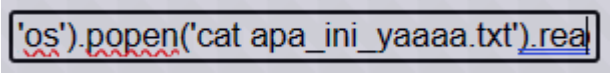
lalu kita ganti dengan ‘ls’



didapatkan



langsung saja, menggunakan command cat untuk mendapatkan isi dari file .txt tersebut



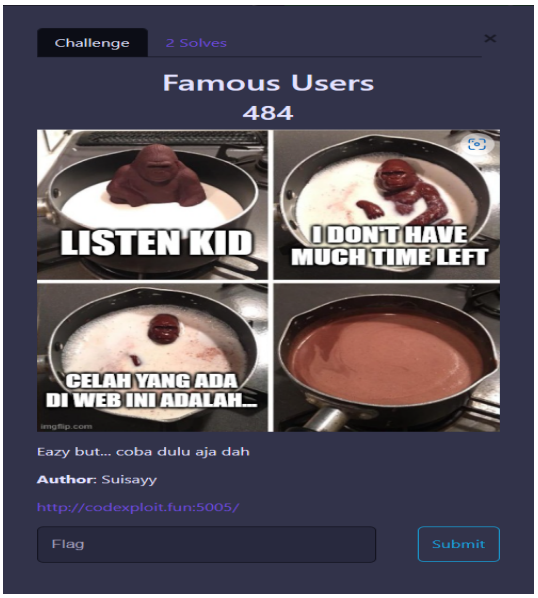
maka, outputnya adalah

```
flag{1nTrOduCT1on_7o_PyTh0n_W3b_1nj3cT1on}
```

Flag : flag{1nTrOduCT1on_7o_PyTh0n_W3b_1nj3cT1on}

Famous Users
Web Exploitation

Deskripsi soal



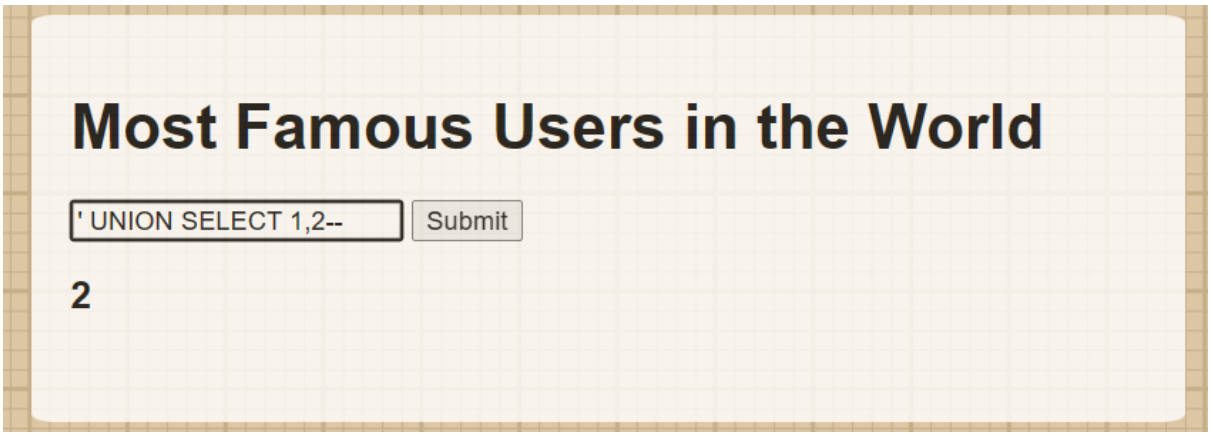
Link Web : http://codexploit.fun:5005/

Solusi:
Pada awalnya, bruteforce menggunakan command” yang umum digunakan. Hingga

didapatkan bahwa command ‘ berfungsi dalam web tersebut, sehingga dapat disimpulkan bahwa dapat kita manfaatkan celahnya dengan SQL Injection.

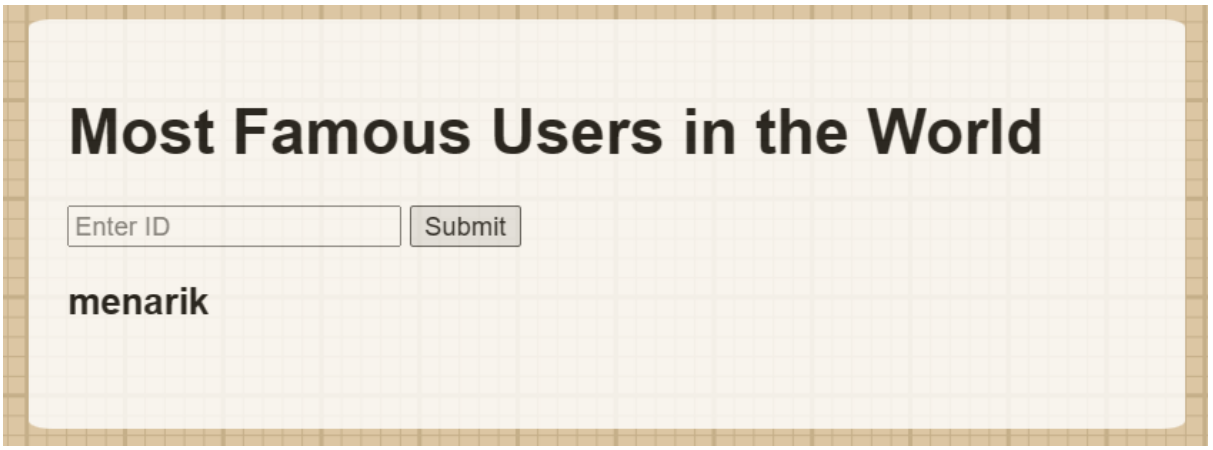
Step selanjutnya adalah dengan mencari jumlah columns

didapatkan bahwa jumlah columnsnya adalah 2 karena pada inputan ke 3 menghasilkan error.
disini saya mencoba menggunakan command ‘UNION SELECT’ untuk mencoba apakah berfungsi



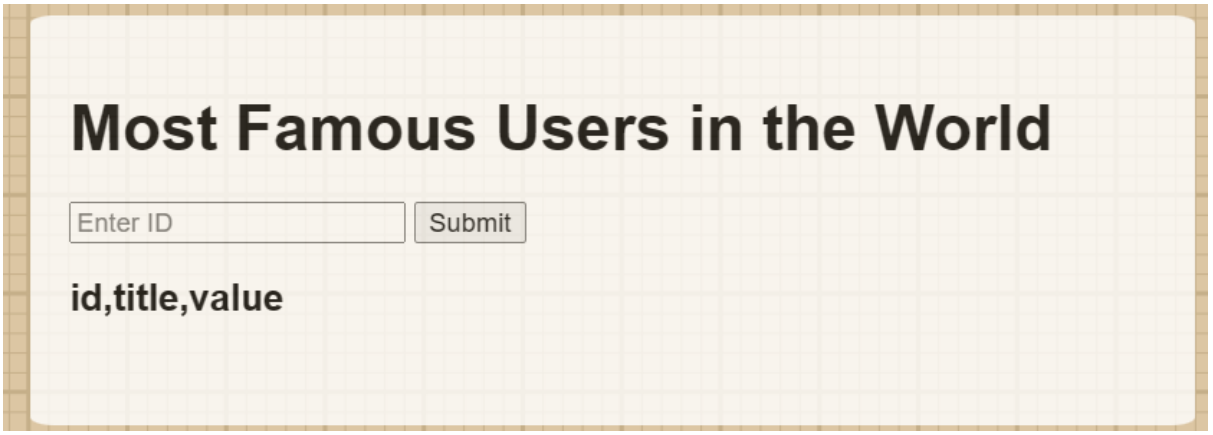
dan setelah dicoba menghasilkan output 2 yang mana ‘Angka Ajaib’ nya adalah 2
step selanjutnya adalah dengan cara memunculkan nama table dengan command
' union select 1,table_name from information_schema.tables where table_schema=database()--

dan menghasilkan

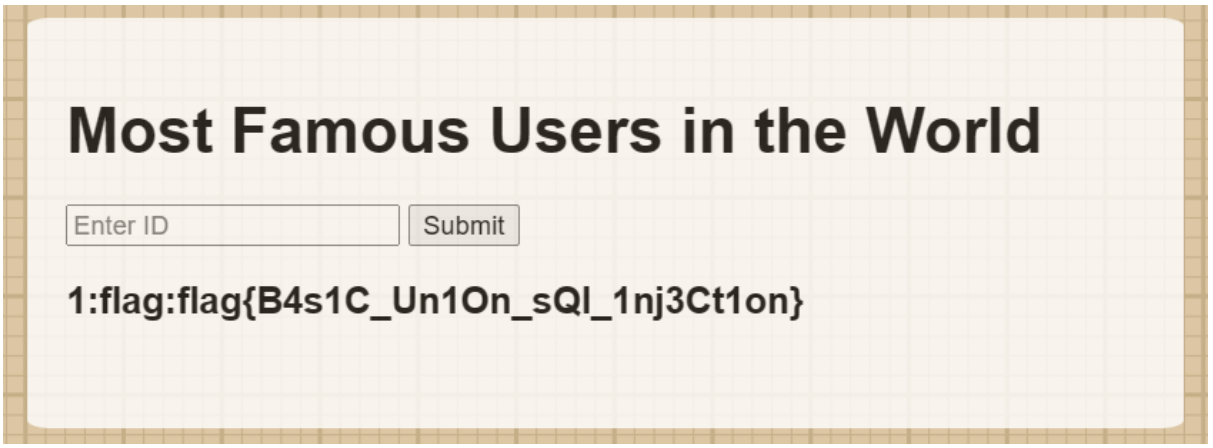


setelah itu, kita memunculkan daftar columns dengan cara mengkonversi nama table ke hex sehingga commandnya menjadi
' union select 1,group_concat(column_name) from information_schema.columns where table_name=0x6d656e6172696b--

menghasilkan



lalu, step terakhir adalah dengan cara memunculkan datanya dengan command
' union select 1,group_concat(id,0x3a,title,0x3a,value) from menarik--



Flag : flag{B4s1C_Un1On_sQl_1nj3Ct1on}