



**Aku adalah aku, di dalam diriku ada aku, tiada aku
melainkan diriku dan tiada diriku melainkan itu aku, aku
kuasa akan aku, karena aku adalah aku**

0xazr



DAFTAR ISI

FORENSIC.....	3
Meowww.....	3
CPNS.....	3
Ngump3t.....	4
ES.....	5
REVERSE ENGINEERING.....	6
Cr4ck312.....	6
STARlight.....	6
Mr.Simple.....	7
Acak-Acakan_D4hhhh.....	8
OSINT.....	10
Arts_Of_Angel.....	10
FindIT!!!!!!.....	10
YouSee1000.....	11
CRYPTO.....	13
DiffieDikky_Broo.....	13
TTSBukanTPS.....	15
Coklat.....	15
Semangat64.....	16
HEXagon.....	17
MISC.....	18
Squidsss.....	18
FREE.....	20
Jogjess.....	20

FORENSIC

Meowwww

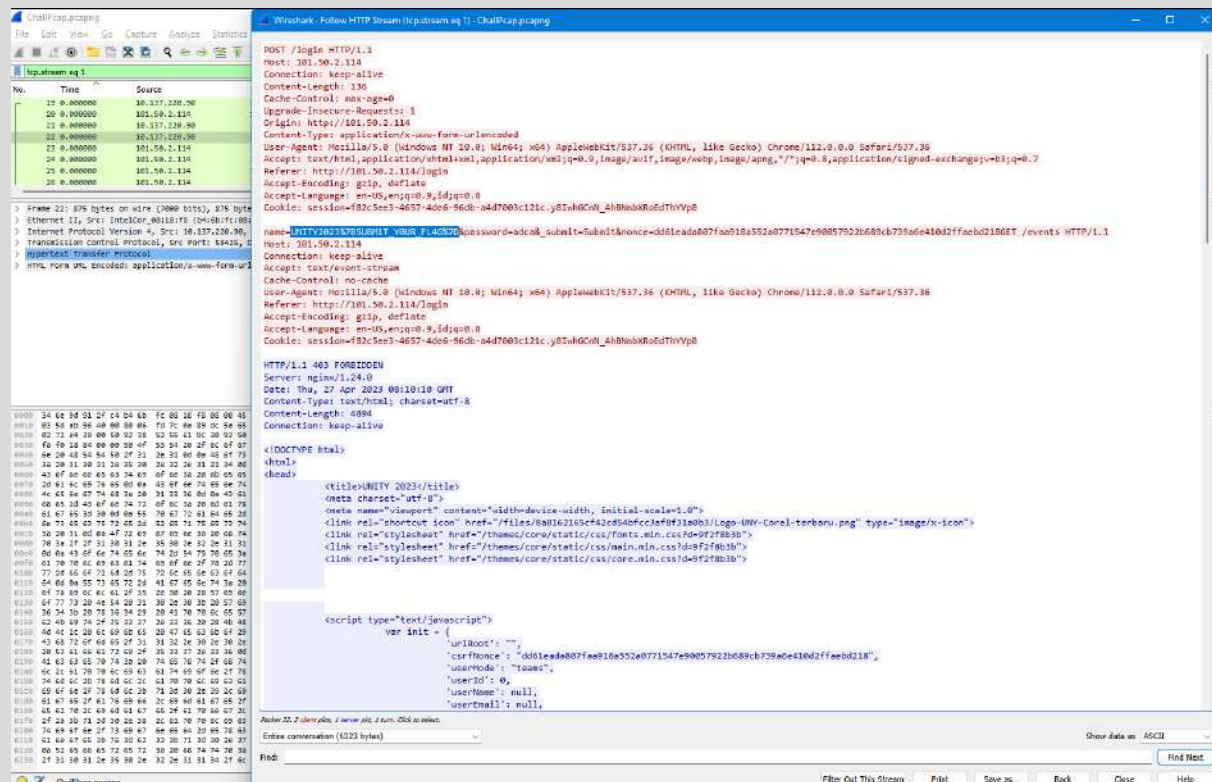
Diberikan sebuah file chall1.jpeg. Karena kami pikir ini adalah chall steganography, langsung saja kami menggunakan tool steghide.

```
index@localhost:/mnt/d/CTF/UNITY_CTF/Meowwww
花 ls
chall.jpeg
index@localhost:/mnt/d/CTF/UNITY_CTF/Meowwww
花 steghide --extract -sf chall.jpeg
Enter passphrase:
wrote extracted data to "flag.txt".
index@localhost:/mnt/d/CTF/UNITY_CTF/Meowwww
花 cat flag.txt
UNITY2023{S4Nt4y_DuLu_G4_SiEEE}
index@localhost:/mnt/d/CTF/UNITY_CTF/Meowwww
花 █
```

Flag: UNITY2023{S4Nt4y_DuLu_G4_SiEEE}

CPNS

Diberikan sebuah file ChallPcap.pcapng. Langsung saja buka dengan wireshark. Kami menggunakan filter `tcp contains "UNITY2023"` untuk memudahkan mencari flag.



Flag: UNITY2023{5U8M1T_Y0UR_FL4G}

Ngump3t

Diberikan sebuah file tar.gz. Ketika diekstrak kita akan mendapatkan file UNITY.jpg. Selanjutnya gunakan steghide tanpa passphrase untuk mendapatkan flag.

```
index@localhost: /mnt/d/CTF/UNITY_CTF/Ngump3t
花 ls
chall.tar.gz
index@localhost: /mnt/d/CTF/UNITY_CTF/Ngump3t
花 tar -xvf chall.tar.gz
UNITY.jpg
index@localhost: /mnt/d/CTF/UNITY_CTF/Ngump3t
花 steghide --extract -sf UNITY.jpg
Enter passphrase:
wrote extracted data to "Flag.txt".
index@localhost: /mnt/d/CTF/UNITY_CTF/Ngump3t
花 cat Flag.txt
UNITY2023{D4p3t_Y44444_B4n9999_99_93m!n9}
index@localhost: /mnt/d/CTF/UNITY_CTF/Ngump3t
花
```

Flag: UNITY2023{D4p3t_Y44444_B4n9999_99_93m!n9}

ES

Diberikan file UENYEH.JPG selanjutnya kami coba cek isinya dan ternyata terdapat string flag.

```
→ es xxd UENYEH.jpg
00000000: 554e 4954 5932 3032 337b 5468 3173 5f31  UNITY2023{Th1s_1
00000010: 735f 4e30 375f 4631 3439 7d09 2020 2020  s_N07_F149}.
00000020: 2009 2020 2020 2020 2009 2020 0920 2020  . . . .
00000030: 0920 0920 2020 2020 0a20 2020 2020 0920  . . . .
00000040: 2020 0920 2020 2009 2020 0920 2020 2020  . . . .
00000050: 2020 0920 2020 2009 2020 2020 0920 2020  . . . .
00000060: 0920 2020 2020 0920 2020 2020 200a 2020  . . . .
00000070: 2020 0920 2009 2020 0909 2020 2020 2009  . . . .
00000080: 2009 2020 2020 2009 2020 2020 0920 2009  . . . .
00000090: 2020 2020 200a 2020 2020 2009 2020 2020  . . . .
000000a0: 0920 2020 2020 2020 0909 2020 0920 2020  . . . .
000000b0: 2020 0920 2020 0920 0920 2009 200a 2020  . . . .
000000c0: 2020 2009 2009 2020 2020 0920 2020 2020  . . . .
000000d0: 2009 2020 2020 2020 2009 2020 2009 2020  . . . .
000000e0: 2020 0920 2020 2009 2020 2020 2020 0a09  . . . .
000000f0: 2020 0920 2020 2020 2020 0920 2020 2020  . . . .
00000100: 2020 0920 0920 2020 2020 0920 2020 2009  . . . .
00000110: 2020 2020 2020 0920 2020 200a 0920 2020  . . . .
00000120: 2009 2020 2020 0920 2009 2020 2020 2020  . . . .
00000130: 0920 2020 2020 2009 2020 2020 2020 2009  . . . .
00000140: 2020 2009 0920 2020 2020 0a20 2020 2009  . . . .
00000150: 2020 2020 0920 2020 2009 2020 2020 2020  . . . .
00000160: 0920 2020 2009 2020 0920 2020 2020 2009  . . . .
00000170: 2020 2020 0920 200a 0920 2009 2020 2020  . . . .
00000180: 2020 0920 2020 2020 0920 2020 0920 0a  . . . .
```

Flag : UNITY2023{Th1s_1s_N07_F149}

REVERSE ENGINEERING

Cr4ck312

Diberikan file ELF 64 bit dengan nama Cr4ck3r. Langsung saja kami menggunakan tool strings untuk melihat semua string yang ada pada file tersebut.

```
index@localhost:/mnt/d/CTF/UNITY_CTF/Cr4ck312
花 strings chall
/lib64/ld-linux-x86-64.so.2
puts
__libc_start_main
printf
__isoc99_scanf
libc.so.6
GLIBC_2.7
GLIBC_2.2.5
GLIBC_2.34
__gmon_start__
PTE1
H=@@
Enter Password : -
correct! You G0t M3 UNITY2023{B3l4j4r_J4d!_Hacker_B4n9}
wrong
;*3$"
GCC: (Debian 12.2.0-14) 12.2.0
.shstrtab
.interp
.note.gnu.property
```

Flag: UNITY2023{B3l4j4r_J4d!_Hacker_B4n9}

STARlight

Diberikan sebuah file ELF 64 bit dengan nama STARSSS. Langsung saja kami menggunakan tool strings untuk melihat semua string yang ada pada file tersebut.


```
index@localhost:/mnt/d/CTF/UNITY_CTF/STARlight  
花 strings chall  
/lib64/ld-linux-x86-64.so.2  
fgets  
stdin  
puts  
__libc_start_main  
printf  
libc.so.6  
GLIBC_2.2.5  
GLIBC_2.34  
__gmon_start__  
PTE1  
H=(@@  
yOu G07 m3 UNITY2023{H3h3h3h3h3h3h3h3h_Br0h_ini_masih_belum_apapa}  
target is %d  
;*3$"  
GCC: (Debian 12.2.0-14) 12.2.0  
.shstrtab  
.interp  
.note.gnu.property  
.note.gnu.build-id  
.note.ABI-tag
```

[illegible]

Mr.Simple

Diberikan sebuah file ELF 64 bit dengan nama HEAP. Langsung saja kami menggunakan tool strings untuk melihat semua string yang ada pada file tersebut.

```
index@localhost:/mnt/d/CTF/UNITY_CTF/Mr.Simple
花 strings chall
/lib64/ld-linux-x86-64.so.2
puts
exit
__libc_start_main
libc.so.6
GLIBC_2.2.5
GLIBC_2.34
__gmon_start__
PTE1
H= @@
UNITY2023{H3h3_S3d3rh4n4_4J4}
Welcome To Sahara!
;*3$"
GCC: (Debian 12.2.0-14) 12.2.0
.shstrtab
.interp
.note.gnu.property
```

Flag: UNITY2023{H3h3_S3d3rh4n4_4J4}

Acak-Acakan_D4hhhh

Diberikan sebuah file ELF 64 bit dengan nama Randomm. Langsung saja kami menggunakan tool strings untuk melihat semua string yang ada pada file tersebut.


```

_ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_0_ES6_
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE12_M_constructIPKcEEvT_S8_St20forward_iterator_tag
_ZSt3cin
_ZNSt8ios_base4InitD1Ev
_ZNSolsEPFRSoS_E
__gxx_personality_v0
_ZNSaIcEC1Ev
_ZNKS7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE7_M_dataEv
_ZNSaIcED2Ev
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc
_ZNSt8ios_base4InitC1Ev
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE9_M_createERmm
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE1Ev
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE13_M_set_lengthEm
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE10_M_disposeEv
_ZSt4cout
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE13_M_local_dataEv
_ZSt19__throw_logic_errorPKc
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE12_Alloc_hiderC1EPcRWS3_
_Unwind_Resume
time
strlen
__cxa_atexit
__libc_start_main
srand
__cxa_finalize
libstdc++.so.6
libgcc_s.so.1
libc.so.6
GCC_3.0
GLIBC_2.34
GLIBC_2.2.5
CXXABI_1.3
GLIBCXX_3.4.21
GLIBCXX_3.4
PTE1
u+UH
UNITY2023{H3h3_D1K!t_B12ut3_B4n9}
Selamat! Kamu menang! Ini adalah flag-nya:
Tebak angka
Maaf, angka yang kamu tebak salah.
Kamu gagal menebak angka yang benar. Angka yang benar adalah

```

Flag: UNITY2023{H3h3_D1K!t_B12ut3_B4n9}

OSINT

Arts_Of_Angel

Diberikan gambar sebagai berikut :



Dari soal peserta diminta untuk menemukan pencipta dan tahun dibuatnya patung tersebut. Setelah googling, kami menemukan bahwa penciptanya adalah **Micahelangelo** dan tahun dibuatnya adalah 1501-1504. Langsung saja kami coba dengan flag berikut dan ternyata benar.

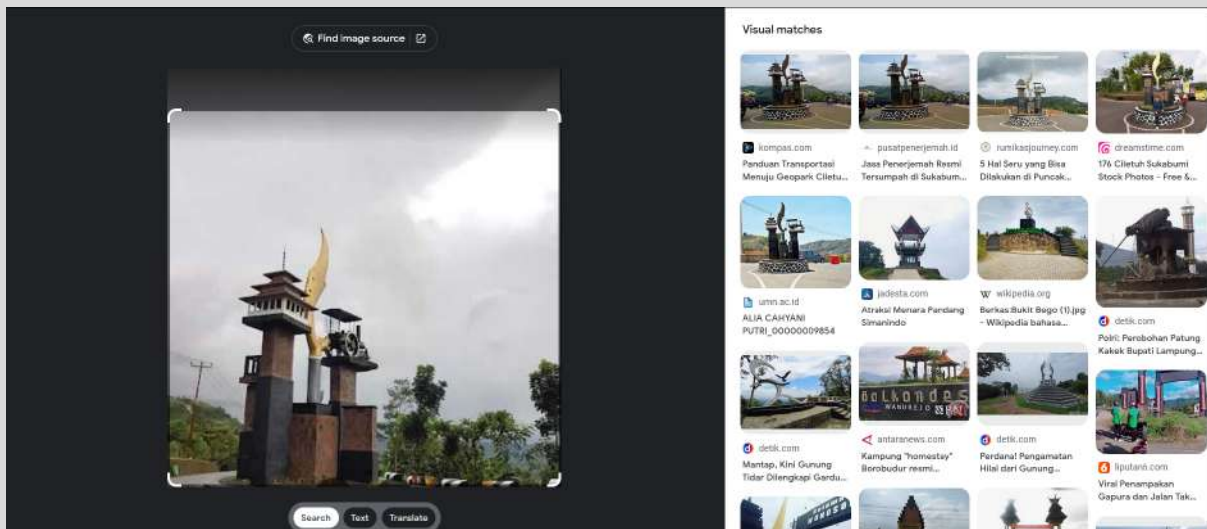
Flag: UNITY2023{Micahelangelo_1501}

FindIT!!!!!!

Diberikan gambar sebagai berikut:



Dari deskripsi soal peserta diminta untuk mencari nama pantai dengan clue gambar di atas. Setelah melakukan pencarian dengan Google Images, kami menemukan bahwa pantai tersebut adalah Geopark Ciletuh.



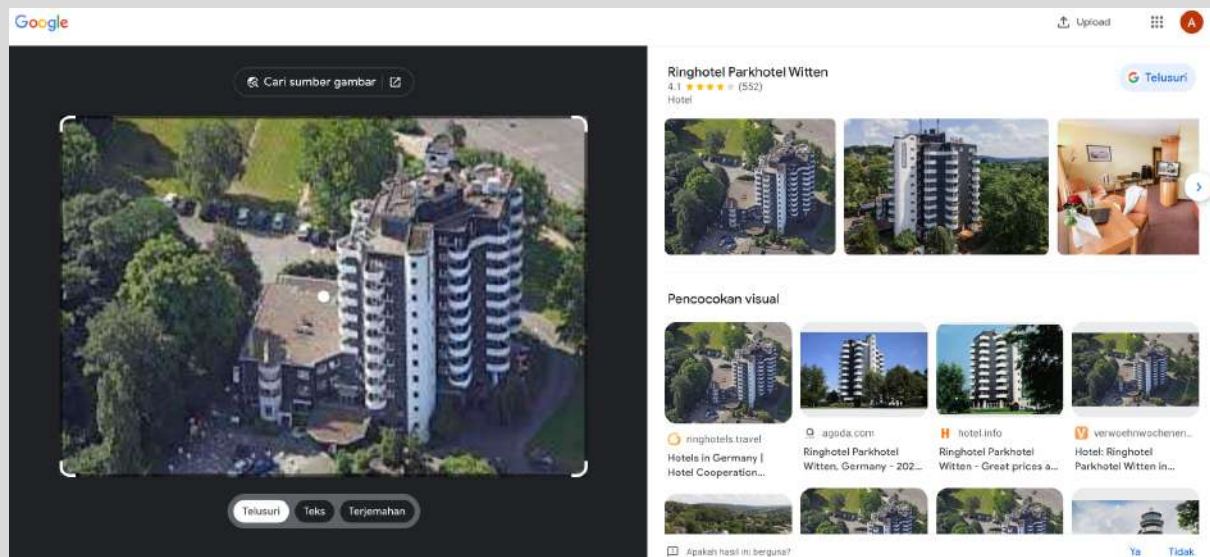
Flag: UNITY2023{Geopark_Ciletuh}

YouSee1000

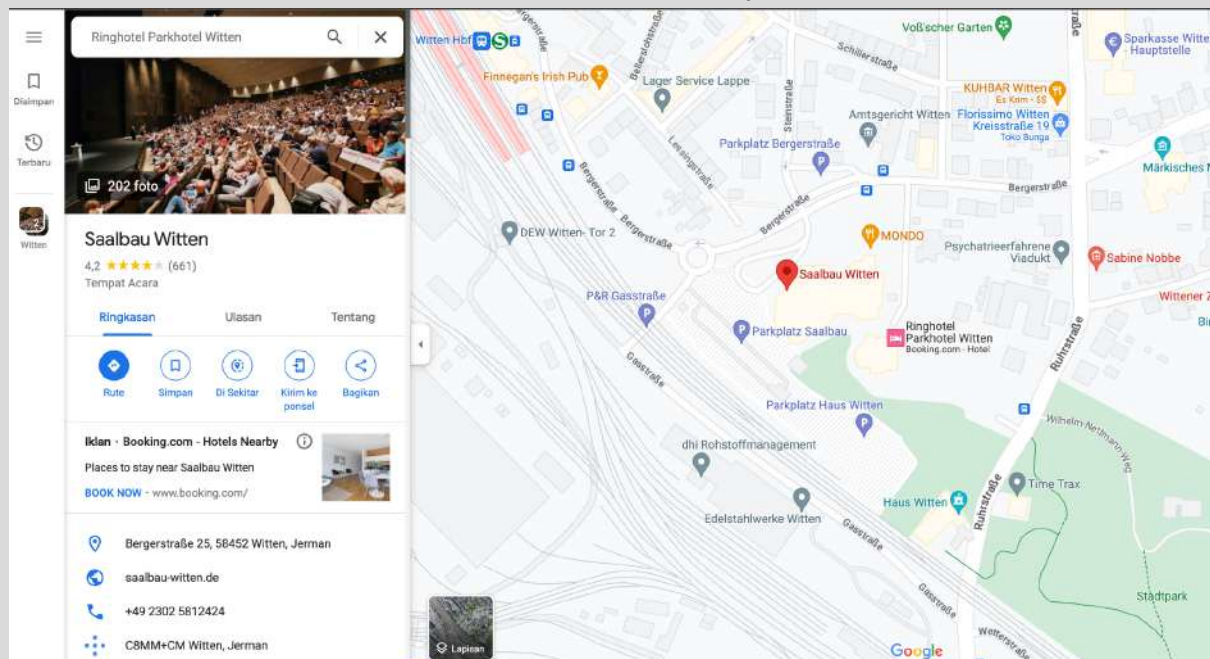
Diberikan gambar sebagai berikut dengan nama file Opera_Chinaaaa_haiyaaaa.jpeg



Selanjutnya cari dengan google image



Didapatkan nama tempat tersebut adalah Ringhotel Parkhotel Witten. Selanjutnya coba cari di maps dan cek ulasan. Ternyata tidak ada apa apa, kemudian melihat kembali ke nama file yaitu opera yang mana foto tersebut merupakan hotel. Jadi selanjutnya kami coba cari di sekitar hotel apakah ada opera atau tidak dan ternyata ada.



Cek ulasan dan dapat flag



Wahyu Santoso

1 ulasan



seminggu lalu

BARU

I think this opera is good thats want to be say it, no trash and good condition of chair in the opera. Thats good for healty because the art is so beautifull i hope so. In my opinion i think this is the tim broh

VU5JVFkyMDIze1kwVV9HMDdfTTNfQjEyMDB9Cg==

[Lihat terjemahan](#)



1



Bagikan

Flag : UNITY2023{Y0U_G07_M3_B1200}

CRYPTO

DiffieDikky_Broo

Diberikan data sebagai berikut

public key 1 $P = 137$ $g = 5$ $a = 98$

public key 2 $p = 137$ $g = 5$ $b = 125$

Diketahui dari judul dan variable bahwa kemungkinan ini adalah diffie hellman key exchange. Berikut solver untuk mendapatkan shared secretnya

$P = 137$

$g = 5$

$a = 98$

$b = 125$

```

pk_a = pow(g,a,P)
ss1 = pow(pk_a,b,P)
pk_b = pow(g,b,P)
ss2 = pow(pk_b,a,P)
# print(pk_a)
# print(pk_b)
print(ss1)
print(ss2)
print(pow(g,a*b,P))
assert(ss1 == ss2)
assert(ss2 == pow(g,a*b,P))

```

Karena jawabannya salah , maka lakukan bruteforce saja karena kemungkinannya cukup kecil yakni dibawah nilai P (137) . Berikut script yang kami gunakan untuk bruteforce

```

import requests
import time

r = requests.session()
header = {

'Cookie': 'session=41f501d9-99d0-4636-8da9-c365c481da38.N268ggiFQXFGEZkJCWJvYc-f3ZM',

'CSRF-Token': '72e2a3c3527477c00222c497af16d6b7e7540cf913a4c62f41a9dc6b9ee4cf7a'
}

url = 'http://101.50.2.114/api/v1/challenges/attempt'

data = {
    "challenge_id": 25,
    "submission": "UNITY2023{11}"
}

for i in range(10,100):
    data['submission'] = "UNITY2023{" + str(i) + "}"
    resp = r.post(url, headers = header, json=data)
    print(i, resp.text)
    time.sleep(10)

# 64 {"success": true, "data": {"status": "correct", "message": "Correct"}}

```



```

[→ diffie python3 brute.py
63 {"success": true, "data": {"status": "incorrect", "message": "Incorrect"}}
64 {"success": true, "data": {"status": "correct", "message": "Correct"}}
65 {"success": true, "data": {"status": "already_solved", "message": "You already solved this"}}
66 {"success": true, "data": {"status": "already_solved", "message": "You already solved this"}}
67 {"success": true, "data": {"status": "already_solved", "message": "You already solved this"}}
68 {"success": true, "data": {"status": "already_solved", "message": "You already solved this"}}
69 {"success": true, "data": {"status": "already_solved", "message": "You already solved this"}}

^CTraceback (most recent call last):
  File "/Users/kosong/ctf/unity/crypto/diffie/brute.py", line 23, in <module>
    time.sleep(7)
KeyboardInterrupt

```

Flag : UNITY2023{64}

TTSBukanTPS

Diberikan data (2 1 25 9 10 21 7 1 20 1 8 21) , terlihat seperti index pada alphabet. Jadi tinggal lakukan substitusi dengan alphabet.

```

import string

a = "2 1 25 9 10 21 7 1 20 1 8 21".split(" ")
list_char = string.ascii_lowercase
flag = ""
for i in a:
    flag += list_char[int(i)-1]
print(flag)

```

```

[→ ttsbukantps python3 solver.py
bayijugatahu

```

Flag : UNITY2023{bayijugatahu}

Coklat

Diberikan data sebagai berikut

key 1 : MULTI key 2 : TIMUN

monggo : UNITY2023{LN TI UT MN_TI IU MN_UT MT MN_UT MT LN MT TM UI}

Panjang key1 == panjang key2, disini kami coba petakan nilai tersebut dengan format baris x kolom. Kemudian selanjutnya kami petakan nilai setiap value sesuai dengan index dari key1 dan key2 nya dimana key1 sebagai kolom dan key2 sebagai row. Berikut solver yang kami gunakan


```

import string

a = "LN TI UT MN TI IU MN UT MT MN UT MT LN MT TM UI"

key1 = "MULTI"
key2 = "TIMUN"

matrix = []
counter = 0
for i in range(len(key1)):
    row = []
    for j in range(len(key2)):
        row.append(string.ascii_lowercase[counter])
        counter += 1
    matrix.append(row)

flag = ""
for i in a.split(" "):
    col = key1.index(i[0])
    row = key2.index(i[1])
    flag += matrix[row][col]
print(flag)

```

→ **coklat** python3 solver.py
wibuitubawang

Selanjutnya tinggal sesuaikan dengan ciphertext yaitu penambahan format flag dan underscore

Flag : UNITY2023{wibu_itu_bau_bawang}

Semangat64

Diberikan sebuah string sebagai berikut :

VU5JVfkyMDIze0N1bTRfODRzMzY0X2I0bjI9ICAgICAgIAo=

Berdasarkan judul soal, string tersebut kemungkinan adalah base64 encoding. Kami

menggunakan tool Cyberchef agar memudahkan proses decode.

The screenshot shows the CyberChef web application. On the left is a sidebar with 'Operations' and 'Favourites'. The 'Recipe' panel in the center has a 'From Base64' recipe selected. The 'Alphabet' dropdown is set to 'A-Za-z0-9+/' and 'Remove non-alphabet chars' is checked. The 'Input' panel on the right contains the string 'VU5JVfkyMDIze0N1bTRfODRzMzY6X2I0bj19ICAgICAgIAQ=' and the 'Output' panel shows the decoded result: 'UNITY2023{Cum4_84s364_b4n9}'.

Flag: UNITY2023{Cum4_84s364_b4n9}

HEXagon

Diberikan sebuah string sebagai berikut :

554e495459323032337b593468685f47346d70346e395f593434345f4d345331685f333473795f6c30307d

Berdasarkan judul soal, string tersebut kemungkinan adalah kode hex. Kami menggunakan tool Cyberchef agar memudahkan proses decode.

The screenshot shows the CyberChef web application with the 'From Hex' recipe selected in the 'Recipe' panel. The 'Delimiter' is set to 'Auto'. The 'Input' panel contains the hexadecimal string '554e495459323032337b593468685f47346d70346e395f593434345f4d345331685f333473795f6c30307d'. The 'Output' panel shows the decoded result: 'UNITY2023{Y4hh_G4mp4n9_Y444_M4S1h_34sy_100}'.

Flag: UNITY2023{Y4hh_G4mp4n9_Y444_M4S1h_34sy_100}

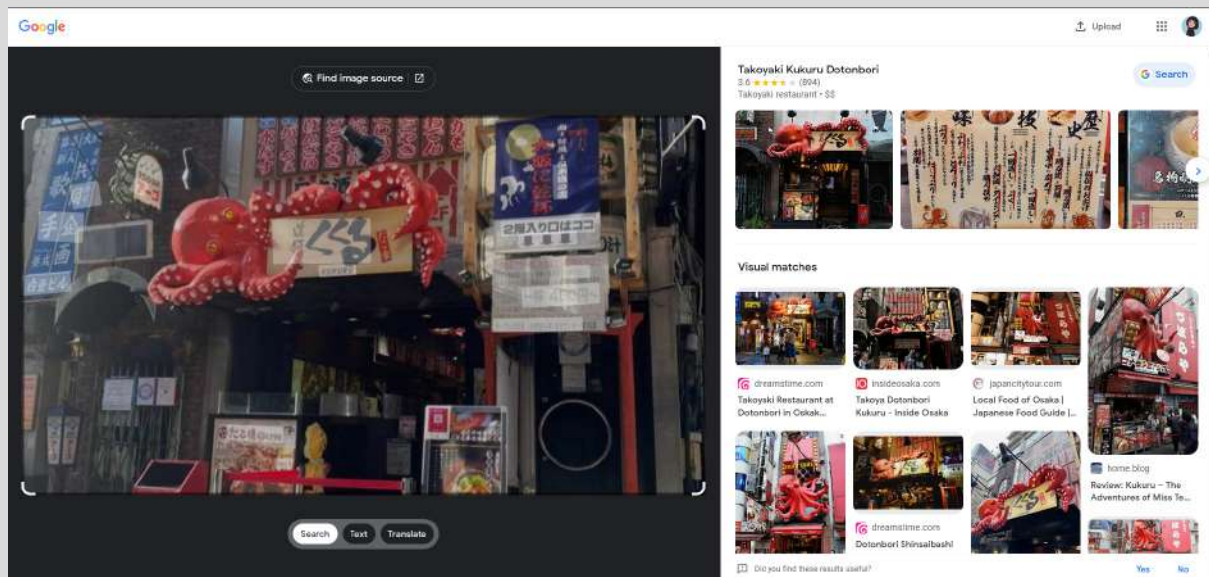
MISC

Squidsss

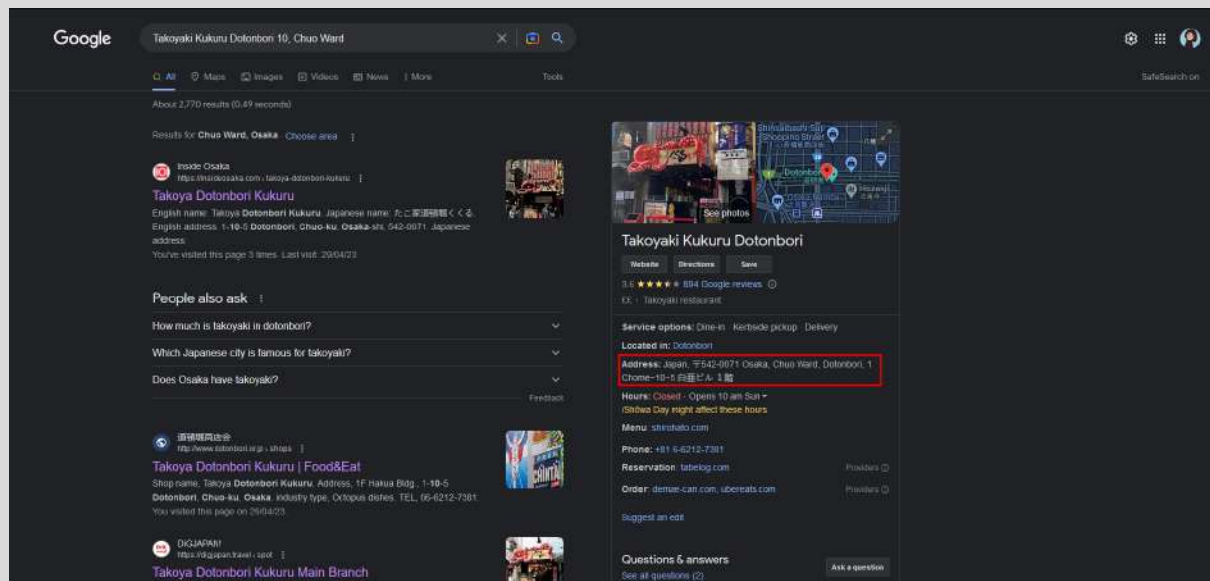
Diberikan sebuah file gambar sebagai berikut :



Kami mencari lokasi dari tempat yang ada dalam gambar tersebut menggunakan Google Images. Kami menemukan bahwa tempat tersebut adalah **Takoyaki Kikuri Dotonburi**.



Selanjutnya kami mencari lebih lanjut Postal Code dan nama distrik dari lokasi tersebut.



Postal Kode: 542-0071

Nama Distrik: Dotonbori

Namun, ketika kami mensubmit sesuai dengan format flag ternyata masih salah. Selanjutnya kami mencoba menggunakan nama distrik lain seperti Dotombori, Minami, Chuo, Chuoku, Chuoku-Ward. Ternyata yang benar adalah Chuoku-Ward (padahal kami yakin tidak ada distrik di Osaka dengan nama Chuoku-Ward 😊, tapi yaudahlah).

Flag: UNITY2023{542-0071_Chuchu-Ward}

FREE

Jogjess

Diberikan soal tidak jelas dengan deskripsi sebagai berikut :

Aduh Ada robot gundam lariiiiiiiiiiiiiiiiiiiiiii

UNITY2023} Author : Chronicless

Dengan menggabungkan kekuatan dukun milik kami, kami berhasil menemukan flag nya di <http://101.50.2.114/robots.txt>

```
User-agent: *
Disallow: /admin
UNITY2023{FR33_FLAG_S1r}
```

Flag: UNITY2023{FR33_FLAG_S1r}