

# WRITE-UP

~ MABANEKAD ~



By

IndianaJones

baybay

ukiyo\_agusta

# WEB

## Note Manager

Challenge : <http://103.49.238.77:57270>

Flag : TECHCOMFEST23{PHP\_R4c3\_m4k3s\_m3\_f33ls\_l1k3\_a\_r4c3r}

### 1. Summary

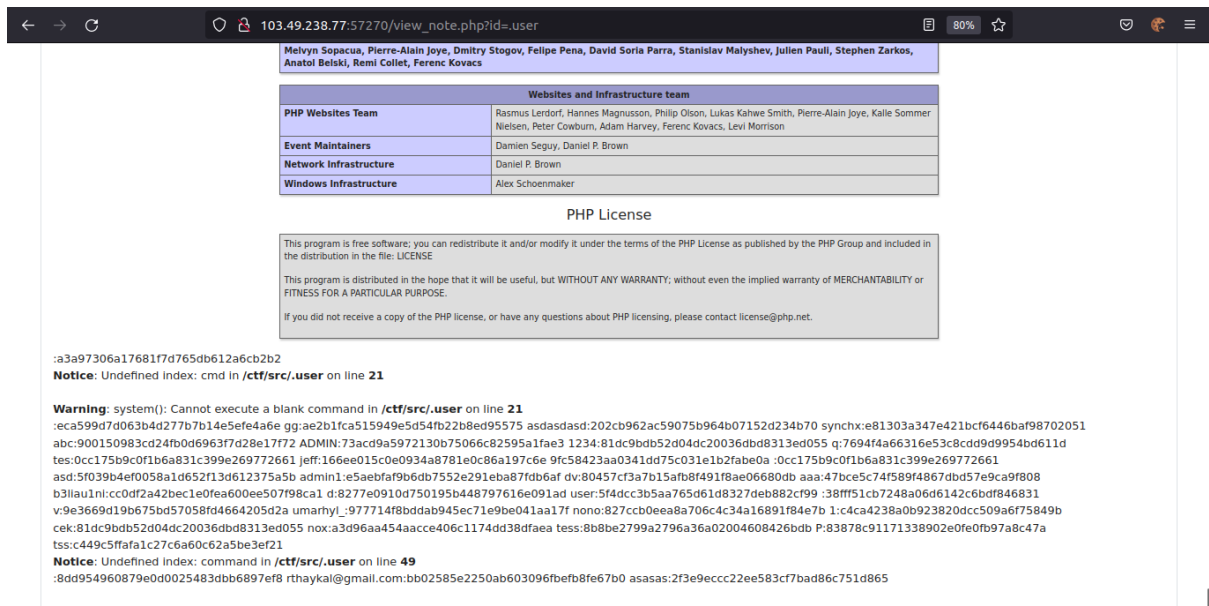
Recently I made a note manager using PHP. However Alice keep talks about how my website is not secure. Can you proof her words?

Author: aimardcr

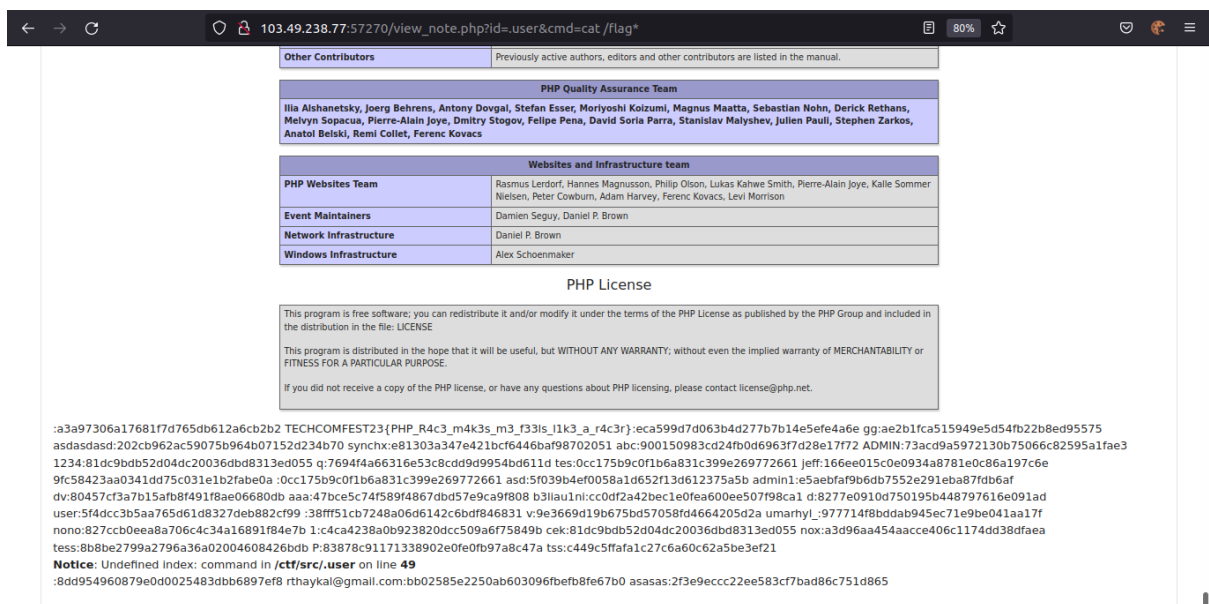
### 2. Technical Report

Jadi terdapat sebuah web yang memungkinkan kita untuk login dan register, jadi coba" register dan tidak menemukan apa", lalu kami berniat melakukan LFI dengan menambahkan code execution pada username berupa command `<?= system($_GET["cmd"]); ?>`. setelah mengotak-atik ternyata terdapat celah LFI pada saat kita melihat note yang telah kita buat pada `view_note.php` yang menggunakan query `id=` yang bisa kita inputkan payload, jadi kita menginput payload `php://filter/convert.base64-encode/resource=index.php` untuk mengambil kode php dari file `index.php`. dan setelah dianalisa kita bisa melihat file `.user` yang berisi username dan password yang sudah di hash menggunakan md5

Setelah lama berpikir, lalu kami mencoba menggunakan payload [http://103.49.238.77:57270/view\\_note.php?id=.user](http://103.49.238.77:57270/view_note.php?id=.user) untuk mencoba melihat aktivitas yang masuk ke dalam file `.user` dan didapat banyak username dan password yang berupa md5hash yang sepertinya juga diinput oleh peserta lain. Namun setelah melihat-lihat sampe akhir, saya mendapat keanehan pada tulisan warning system



Dimana pada tulisan Warning: system() Cannot execute a blank command, yang berarti ada command injection yang berhasil namun belum ada command yang dieksekusi. Jadi kami berpikir untuk merubah payload, dan setelah merubah-rubah dan bereksplorasi dengan command apa saja mau dan anehnya ada juga yang nggak mau, mencari cari file flag nya, dan akhirnya didapat payload yang langsung menampilkan flagnya. Payloadnya ternyata simple seperti pada gambar.



## CRYPTOGRAPHY

## Hashllision

Challenge : nc 103.49.238.77 33083  
Flag : TECHCOMFEST23{5uP3r\_E4sY\_CoLL1s10n}

Untuk menyelesaikan challenge ini, kami membuat solver yang dapat me-generate kata-kata acak yang terdiri dari empat karakter. Fungsi hash\_code (terlampir) di-looping dengan argumen berupa kata-kata acak yang di-generate sebelumnya. Dari algoritma tersebut menghasilkan beberapa kata yang memiliki kode hash yang sama dengan SECRET\_WORD yaitu nioP, njOo, njPP, oJno, oJoP, oKOo, oKPP. Berikut merupakan script solver dari challenge ini:

```
SECRET_WORD = "nino"
charlist = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"

def hash_code(s):
    h = 0
    for c in s:
        h = (31 * h + ord(c)) & 0xFFFFFFFF
    return h

def main():
    word = ""
    for i in charlist:
        for j in charlist:
            for k in charlist:
                for l in charlist:
                    word = i + j + k + l
                    if hash_code(word) == hash_code(SECRET_WORD) and word
!= SECRET_WORD:
                        print(word);

if __name__ == "__main__":
    main()
```

## baby-xor

Flag : TECHCOMFEST23{b4by\_x0r\_s00\_ez}

### 1. Summary

Easy chall for you, think you can do it?

Author: **aimardcr**

### 2. Technical Report

Di chall kali ini kami diberikan kode program sebagai berikut

```
#!/usr/bin/python
import os

def encrypt(string):
    key = os.urandom(int(len(string) / 5))

    result = ''
    for i in range(len(string)):
        result += chr(ord(string[i]) ^ (key[int(i / 5)] & 0xff))

    return result

if __name__ == '__main__':
    with open('flag.txt', 'r') as f:
        flag = f.read()

    assert len(flag) % 5 == 0

    print(encrypt(flag).encode('latin1').hex())
```

Diberikan juga flag yang diencrypt, setelah dianalisa, flagnya harus kelipatan 5, dan kami mengecek pada flag yang dienkripsi ternyata terdapat 60 character, dan itu dalam hex yang berarti flagnya memiliki panjang 30 kata. Setelah itu kami menganalisa key nya, yang ternyata didapat dengan merandom string dengan panjang flag/5. Jadi karena tadi flagnya ada 30 karakter, berarti key nya terdiri dari 6 karakter yang tiap 5 karakter flag pertama di encrypt dengan key index ke i/5 dr index karakter tersebut. Lalu kami menggunakan teknik partial known text, karena format flagnya TECKCOMFEST{ lumayan panjang wkwk, kami ambil 10 karakter pertama untuk membrute 2 karakter key pertama. Setelah ada secercah harapan. Kami mencoba brute key sisanya satu persatu lalu mencocokkan mana yang kira" bakal jadi flag. Berikut kode programnya setelah didapat 5 key pertama dan mencari flag terakhir

```

from pwn import *

def encrypt(string, guest):
    key = bytes([64, 111, 19, 115, 204, guest])

    result = ''
    for i in range(len(string)):
        result += chr(string[i] ^ (key[int(i / 5)] & 0xff))
    return result

if __name__ == '__main__':
    flag = unhex(
        "14050308032022292a3c472120687147110a2c0bfcbe93bffc4629130c0b")

    assert len(flag) % 5 == 0

    for i in range(255):
        print(i)
        print(encrypt(flag, i).encode('latin1'))

```

Lalu cek satu", hampir putus asa setelah 4x ngescroll ampe habis ga nemu". Akhirnya setelah pantang menyerah memelototi outputnya. Kami dapat flag nya heheee

## MISC

### Wordle

Challenge : nc 103.49.238.77 34601  
 Flag : TECHCOMFEST23{F14G\_F0r\_Th3\_Ch4mPs}

Untuk menyelesaikan challenge ini, kami membuat wordlist yang didapat dengan menggunakan script berikut:

```

from pwn import *
import re

for i in range(9999):
    p = remote("103.49.238.77", 34601)

    p.sendline('a')
    p.sendline('a')
    p.sendline('a')

    pattern = re.compile(r"correct word was '(\w+)'"')
    matches = pattern.finditer(p.recv().decode())

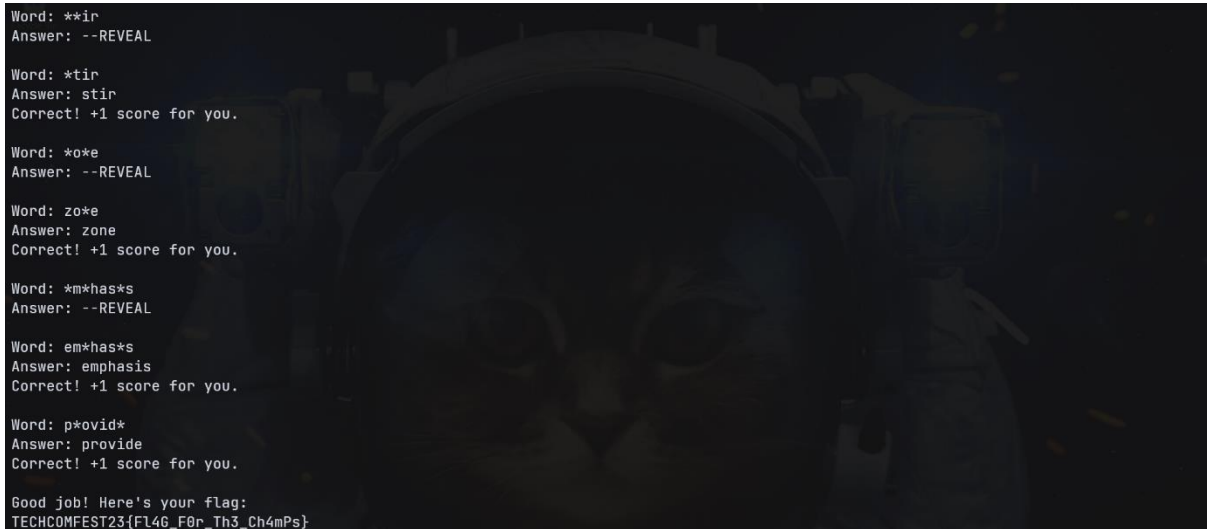
    correct_answers = []
    for match in matches:
        correct_answers.append(match.group(1))

    with open("wordlist.txt", "a", encoding='utf-8') as file:
        for word in correct_answers:

```

```
file.write(word + "\n")
file.close()
```

Setelah itu, kami melanjutkan challenge ini dengan menjawab wordle berdasarkan wordlist yang diperoleh. Terdapat beberapa wordle yang memiliki banyak kemungkinan kata, disitu kami menggunakan commands yang tersedia.



```
Word: **ir
Answer: --REVEAL

Word: *tir
Answer: stir
Correct! +1 score for you.

Word: *o*e
Answer: --REVEAL

Word: zo*e
Answer: zone
Correct! +1 score for you.

Word: *m*has*s
Answer: --REVEAL

Word: em*has*s
Answer: emphasis
Correct! +1 score for you.

Word: p*ovid*
Answer: provide
Correct! +1 score for you.

Good job! Here's your flag:
TECHCOMFEST23{FL4G_F0r_Th3_Ch4mPs}
```

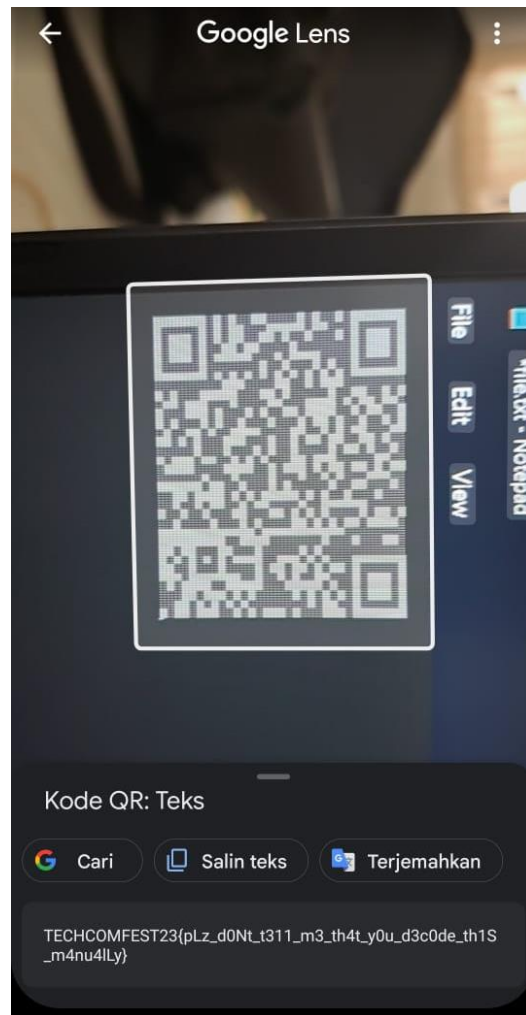
### Ascii Catch

```
Challenge : nc 103.49.238.77 22103
Flag      : TECHCOMFEST23{pLz_d0Nt_t3l1_m3_th4t_y0u_d3c0de_th1S_m4nu4lLy}
```

Untuk menyelesaikan challenge ini, kami mengambil output dari challenge dengan cara:

```
nc 103.49.238.77 22103 > file.txt
```

Dan menghasilkan file baru yang dapat di-scan serta menghasilkan flag seperti pada gambar dibawah:



## FORENSIC

### Pixel

Challenge : nc 103.49.238.77 22103

Flag : TECHCOMFEST23{eniwei\_lu\_ada\_rencana\_masuk\_sunib\_ga\_ngab\_}

mas aseng baru memberi tahu saya kalau dia ingin memberiku pesan. karena pesan sangat rahasia, dia tidak ingin jika pesan ini bisa dibaca oleh sembarang orang. jadi dia mencapture (screenshot) seluruh layar laptopnya. lalu dia menyimpan gambar itu dengan menyusun semua list pixel RGBA secara berurutan dan menaruhnya pada height yang sama. bisakah kamu membantuku mendapatkan pesan aseng :)

Awalnya diberikan sebuah gambar dengan format PNG, dan gambar tersebut tidak dapat dibuka (mungkin karena anggota kami



menggunakan Windows), bernama pixel.png. Dikatakan kalau pixel gambar tersebut diurutkan di dalam *height* yang sama dan gambar tersebut merupakan hasil *screenshot*. Dari *clue* tersebut bisa direka-reka kalau sebuah hasil *screenshot* layer laptop umumnya berada di ukuran 1920 X 1080. Langkah pertama yang dilakukan adalah mengubah pixel.png menjadi bentuk RGBA-nya. Dengan menggunakan kode python.

```
from PIL import Image
im = Image.open("pixel.png", "r")
px = list(im.getdata())
with open("flag.txt", "w") as file:
    file.write(str(px))
```

Setelah itu dimasukkan ke dalam sebuah berkas bernama flag.txt, yang isinya berupa "[ (255, 255, 255, 255), ... ]", kami membuat kode python Kembali untuk *me-render* gambar tersebut.

```
from PIL import Image
data = #flag.txt di sini
image = Image.new('RGBA', (1920, 1080), "white")
image.putdata(data)
image.save("flag.png", "PNG")
```

Gambar di-render dan hampir membuat laptop panas karena kami memang benar menggunakan Windows *instead of* Linux. Akhirnya gambar berhasil di-render dan menjadi sebuah gambar bernama flag.png.

....🤔🙏🐏❤️👉😁😂😃....

TECHCOMFEST23{eniwei\_lu\_ada\_rencana\_masuk\_sunib\_ga\_ngab\_}

....🤔🙏🐏❤️👉👉😁😂😃....|

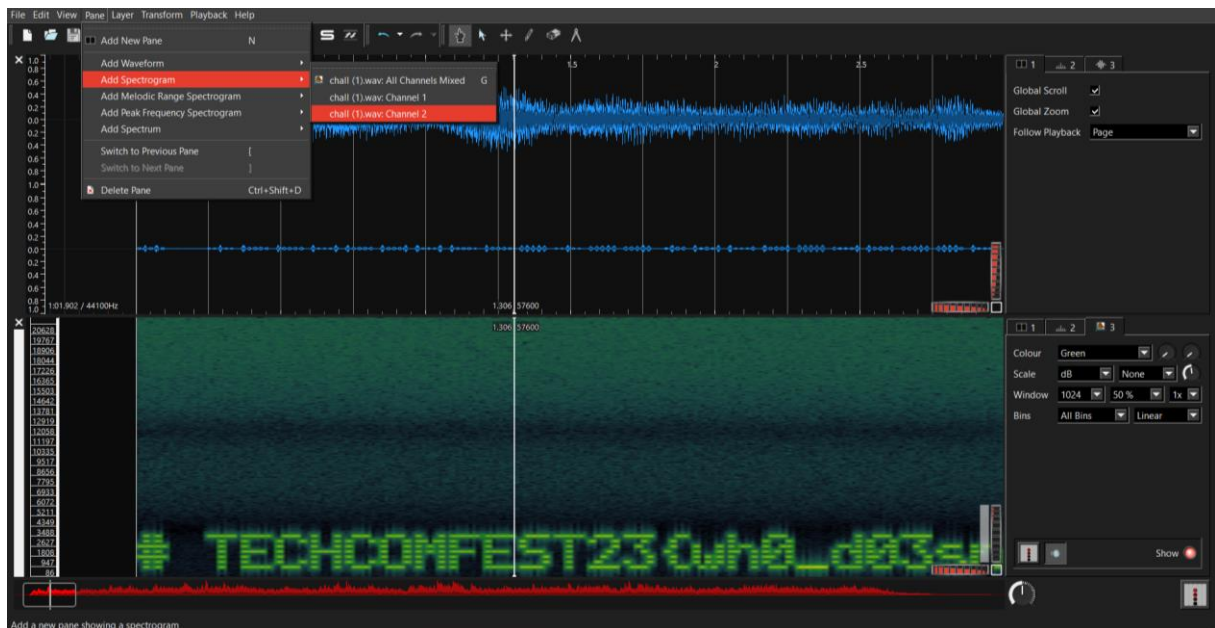
## Mono

Flag :

TECHCOMFEST23{wh0\_d03snT\_LOV3\_F1Ve\_N1GhtS\_At\_fr3DDyS\_R1gHt\_aNyWay\_HeR3\_1s\_u  
R\_FL4G\_alcd6113}

Do you recognize this music? Anyway, what's with the weird sound?

Unduh berkas yang sudah disediakan, chall.wav. Gunakan Sonic Visualizer, buka berkas, dan gunakan kanal kedua.



## Flag Checker

Flag :

```
TECHCOMFEST23{th1S_w4S_m3AnT_T0_b3_r3V3rS1nG_ChAlL_But_0H_w3lL_H3r3_W3_4r3}
```

### 1. Summary

I accidentally lost Flag Checker app which was made for this challenge.

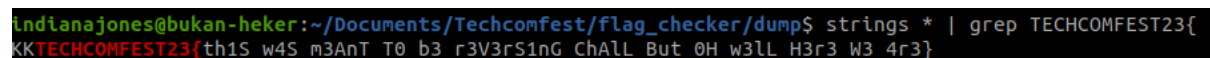
Luckily my android dumped the whole app memory before it went disappear.

Can you help me restore the flag?

Author: **aimardcr**

### 2. Technical Report

pada chall ini kita akan diberikan file chall.zip yang jika diunzip berisi dump memory dari android dalam bentuk file .bin, setelah mencoba menganalisa log pada file com.flag.checker-maps.txt dan mengotak-atik nya dengan volatility, kami pun sedikit putus asa dan mencoba keberuntungan dengan men-strings semua dump file yang ada dan mencari flag dengan command seperti pada gambar



```
Indlanajones@bukan-heker:~/Documents/Techconfest/flag_checker/dump$ strings * | grep TECHCOMFEST23{
KKTECHCOMFEST23{th1S_w4S_m3AnT_T0_b3_r3V3rS1nG_ChAlL_But_0H_w3lL_H3r3_W3_4r3}
```

dan ternyata ada :)

## Cracking

Flag :

```
TECHCOMFEST23{p4rS1nG_S00_m4nY_QR_c0DeS_1sNt_S0_fUN_4fT3r_4LL}
```

### 1. Summary

My friend recently went crazy because he couldn't decode a secret message from this video. He screams "EMMMMMMMMMMM DEEEEEEEEEEEEEEEEEEE FAYFFFFFFFFFFFFFFFFFFFFF" everytime, I don't know what that supposed to mean... Can you help me find the secret message for the sake of my friend?

Author: aimardcr

## 2. Technical Report

Oke, jadi chall ini bisa dibilang sangat rumit karena ada banyak tahap untuk bisa mendapat flagnya. Pertama kita akan diberi sebuah file dengan ekstensi .avi yang berupa video yang berisi gabungan dari banyak QR code yang muncul secara bergantian. Setelah melihat metadata pada video dengan exiftool didapatkan data sebagai berikut.

```
indianajones@bukan-heker:~/Documents/Techcomfest/dump$ exiftool chall.avi
ExifTool Version Number      : 12.40
File Name                    : chall.avi
Directory                   : .
File Size                    : 16 MiB
File Modification Date/Time   : 2022:12:30 00:22:49+08:00
File Access Date/Time        : 2023:01:15 16:33:24+08:00
File Inode Change Date/Time   : 2023:01:15 16:33:23+08:00
File Permissions              : -rw-rw-r--
File Type                    : AVI
File Type Extension          : avi
MIME Type                    : video/x-msvideo
Frame Rate                   : 60.002
Max Data Rate                 : 2005 kB/s
Frame Count                  : 840
Stream Count                  : 1
Stream Type                   : Video
Video Codec                   : FMP4
Video Frame Rate              : 60
Video Frame Count             : 840
Quality                      : Default
Sample Size                   : Variable
BMP Version                   : Windows V3
Image Width                   : 370
Image Height                  : 370
Planes                       : 1
Bit Depth                     : 24
Compression                   : FMP4
Image Length                  : 410700
Pixels Per Meter X            : 0
Pixels Per Meter Y           : 0
Num Colors                    : Use BitDepth
Num Important Colors          : All
Software                      : Lavf58.76.100
Image Size                    : 370x370
Megapixels                    : 0.137
Duration                      : 14.00 s
```

Diketahui video tersebut memiliki frame rate 60 fps yang bisa digunakan untuk mengekstrak semua gambar qrcode yang ada dalam

video dengan menggunakan command ffmpeg pada terminal linux. Command lengkap ffmpeg bisa dilihat pada gambar dibawah

```
indianajones@bukan-heker:~/Documents/Techconfest/dump$ ffmpeg -i chall.avi -r 60 -f image2 image-%3d.jpeg
ffmpeg version 4.4.2-0ubuntu0.22.04.1 Copyright (c) 2000-2021 the FFmpeg developers
  built with gcc 11 (Ubuntu 11.2.0-19ubuntu1)
  configuration: --prefix=/usr --extra-version=0ubuntu0.22.04.1 --toolchain=hardened --libdir=/usr/lib/x86_64-linux-gnu
--incdir=/usr/include/x86_64-linux-gnu --arch=amd64 --enable-gpl --disable-stripping --enable-gnutls --enable-ladspa --
enable-libaom --enable-libass --enable-libbluray --enable-libsbs2b --enable-libcaca --enable-libcdio --enable-libcodecs2
--enable-libdav1d --enable-libflite --enable-libfontconfig --enable-libfreetype --enable-libfribidi --enable-libgme --
enable-libgsm --enable-libjack --enable-libmp3lame --enable-libmysofa --enable-libopenjpeg --enable-libopenmpt --enable-
libopus --enable-libpulse --enable-librabbitmq --enable-librubberband --enable-libshine --enable-libsnappp --enable-li
bsoxr --enable-libspeex --enable-libsrt --enable-libssh --enable-libtheora --enable-libtwolame --enable-libvidstab --en
able-libvorbis --enable-libvpx --enable-libwebp --enable-libx265 --enable-libxml2 --enable-libxvid --enable-libzimg --e
nable-libzmq --enable-libzvt --enable-lv2 --enable-omx --enable-opengl --enable-openc1 --enable-opengl --enable-sdl2 --
enable-pocketsphinx --enable-libsrt --enable-libmfx --enable-libdc1394 --enable-libdrm --enable-libiec61883 --enable-
chromaprint --enable-frei0r --enable-libx264 --enable-shared
  libavutil      56. 70.100 / 56. 70.100
  libavcodec     58.134.100 / 58.134.100
  libavformat    58. 76.100 / 58. 76.100
  libavdevice    58. 13.100 / 58. 13.100
  libavfilter    7.110.100 / 7.110.100
  libswscale     5.  9.100 / 5.  9.100
  libswresample  3.  9.100 / 3.  9.100
  libpostproc   55.  9.100 / 55.  9.100
Input #0, avi, from 'chall.avi':
  Metadata:
    software      : Lavf58.76.100
  Duration: 00:00:14.00, start: 0.000000, bitrate: 9806 kb/s
  Stream #0:0: Video: mpeg4 (Simple Profile) (FMP4 / 0x34504D46), yuv420p, 370x370 [SAR 1:1 DAR 1:1], 9802 kb/s, 60 fps
, 60 tbr, 60 tbn, 60 tbc
Stream mapping:
  Stream #0:0 -> #0:0 (mpeg4 (native) -> mjpeg (native))
Press [q] to stop, [?] for help
[swscale @ 0x557fe78c9c80] deprecated pixel format used, make sure you did set range correctly
Output #0, image2, to 'image-%3d.jpeg':
  Metadata:
    software      : Lavf58.76.100
    encoder       : Lavf58.76.100
  Stream #0:0: Video: mjpeg, yuvj420p(pc, progressive), 370x370 [SAR 1:1 DAR 1:1], q=2-31, 200 kb/s, 60 fps, 60 tbn
```

Setelah tu akan didapat 840 file image.jpeg yang berisi QR code acak, jadi kami menggunakan python untuk men decodenya 1 persatu karena klo manual capek, lalu hasilnya akan kami input ke hasil.txt  
berikut adalah solver kami

```
import cv2
import os

from cv2 import QRCodeDetector
f = open('hasil.txt','a+')
directory = 'dump'

file = os.scandir(directory)
file = list(map(str, file))
file = [x[11:-2] for x in file]
for x in file:
    file = sorted(file)

for filename in file:
    print(str(filename))
    img = cv2.imread('dump/' + filename)
    qr = QRCodeDetector()
    try:
        data, _ , _ = qr.detectAndDecode(img)
    except:
        continue
    print(data)
    if len(data) == 0:
        f.write('\n')
    else:
        f.write(data + '\n')
```

```
0QtZCMhxonmKiKwDI8M8k0esARaXEFt0
IW8GwJMcGDCQSBtIKmo37XkKVVR10f8N
VUcpXPDCbKyZ2P00awt95q0zBsWGzpF6
jM0nDuC8w9S2hSZ6lwJWem3G0hexpsNl
CvmN1LDJBB8VDG790TzzexHCBdS0wxXi
ZFf5y76ut7dBoxGIkSR6BLQckxTmR74F
5206560a306a2e085a437fd258eb57ce
TKxtAaW7NwxHyv3kPYJHG2U9BUI1E76m
Ipr0gX0kRNoqILSj1nB4XofCmnNWGFLR
IQExM0Jvuls2wjvAXFKeIt0CjBYyfH7C
FpJSjvQnuUhFl0yupkwMQRjKvvlst12T
ilaLxjmbXw175lQUtITZPYV0Ej2ETctT
3a3ea00cfc35332cedf6e5e9a32e94da
nCisCQJ4MJoo91jeI9NEILgA6BCjywLS
gZIdHtwIDT0TiCKBte9vcFkIkB2CytGI
sNyaf5vAopulcQbTNaHNZKq4NctmSbJP
hnCTmmQ1Fs7qytIaBNreneqNhjPXmplo
SjoUflcHBXAewwdknoC400zyDzUbnaLg
VYWtWakFlIoI7wlloedPCV0i90lG7Kpl
HXC0YQejevZc9GFEDkt0cm8SYn8XaRGR
5206560a306a2e085a437fd258eb57ce
ITICSUsjZBLpEF2ZxKFJybho0MabudMp
kkeWdKmgeueo6RDqvQpsU6FUqt8fVrxp
zEX7BnXe8drsJjkb7h2x72Dh649PJL6b
UtyD4PS2Zz4hSVr7ywNAaTDFUpl5lgAC
rR0ipyI00jshCYNwjNKZcFN8Va1VIcCv
cQHrcrGL56N1MjlfZ5Njqb2pMdsHqt3d
UJAFFq0bRJGF0K9S9raPhF99TRCX9XW5
z9DP84muNIobDV9kJJQP8DNvLbmTMiFc
TSuZwKgYYgXzYVWvqIJLIWYvvrwpsugX
kR1n1ok4Q5AbNT4kaYowyQZnEQ1Qmg5
JD0dGJCSuKQuYs9uMHk4M0qRobawIpCw
Z9aGpf40CGcxmREcizz3h9w4bUxidZKh
fe5CxPZJFNoCIZBgGNoyMsADGfFPi4wE
4bxaZ61ugzH51AH7x1YLS69CBah5QFK7
eKTUorI3jJgdtBYLHNvv3SjEkJypvXHy
```

Dan hasil yang didapatkan berupa data dump yang kami sebenarnya bingung mau diapain namun setelah melihat-lihat kembali soal, ada clue yang menyebutkan md5, dan setelah diperhatikan dalam data dump tersebut ternyata terdapat baris-baris yang datanya berupa hex dan ketika coba saya decrypt md5 akan menghasilkan char. Terus mencoba manual dan mulai putus asa karena hasil decryptnya tidak menunjukkan indikasi flag, kami iseng untuk men decrypt hash terakhir dan menghasilkan '=', dan kami pun mendapat ide untuk menggabungkan hasil decrypt md5 hash tersebut dan mendecodenya dengan base64 dan mencoba membuat solver sederhana. Berikut solver kami

```

import string
import hashlib

wordlist = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz1234567890'

lines = [line.strip('\n') for line in open('hasil.txt', 'r').readlines()]

def is_hex(s):
    hex_digits = set(string.hexdigits)
    # if s is long, then it is faster to check against a set
    return all(c in hex_digits for c in s)

md5decode = ''
for i in lines:
    for j in wordlist:
        result = hashlib.md5(j.encode())
        if(result.hexdigest() == i):
            md5decode += j
        else:
            continue

is_hex(md5decode)
print(md5decode)

```

Dan didapatkan output berupa base64 dan langsung ja di decode tar dpt flag hehe

```

indianajones@bukan-heker:~/Documents/Techcomfest$ echo 'VEVDSENPTUFU1QyM3twNHJTMW5HX1MwMF9t
NG5ZX1FSX2MwRGVTXzFzTnRfUzBfZlVOXzRmVDNyXzRMTH0' | base64 -d
TECHCOMFEST23{p4rS1nG_S00_m4nY_QR_c0DeS_1sNt_S0_fun_4fT3r_4LL}base64: invalid input

```

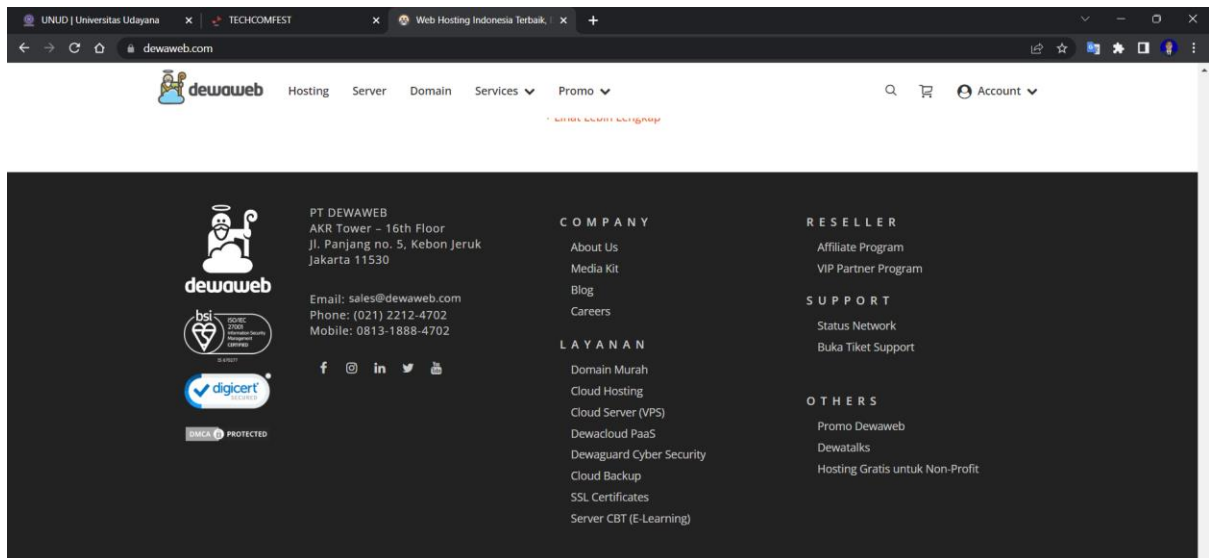
## OSINT

### Dewaweb

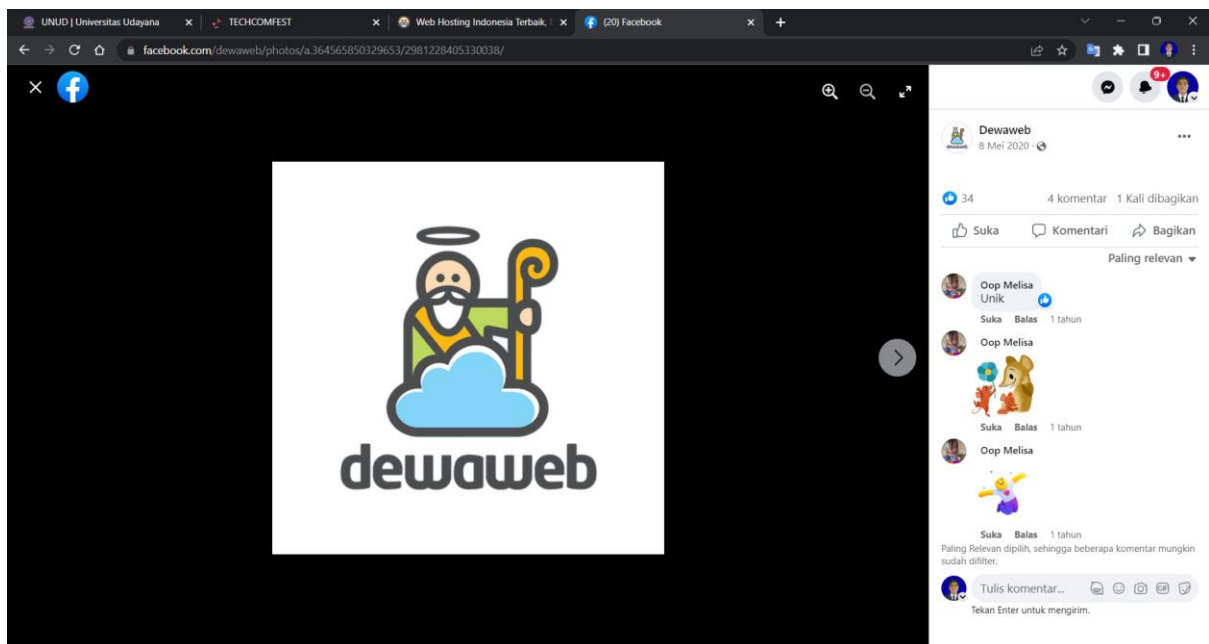
Flag : TECHCOMFEST23{Th4nkS\_T0\_Dewaweb\_F0r\_Sp0nS0r1ng\_Us}

Kami menemukan flag tersebut pada kolom komentar di laman Facebook resmi milik Dewaweb. Pertama, kami mencoba mengecek website Dewaweb dan mengecek beberapa sosial media dari Dewaweb.





Setelah menjelajah, akhirnya kami menemukan flag



## Runaway

Flag : TECHCOMFEST23{-8.7:115.2}

### 1. Summary

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

tower that tracked his phone: **248440**, but unfortunately he also removed the tower location too. Can you help us find approximate location of the tower with the **eNB ID** we provided?

Note: Submit the latitude and longitude with the maximum 1 number of the decimal (separate with :)

For example:

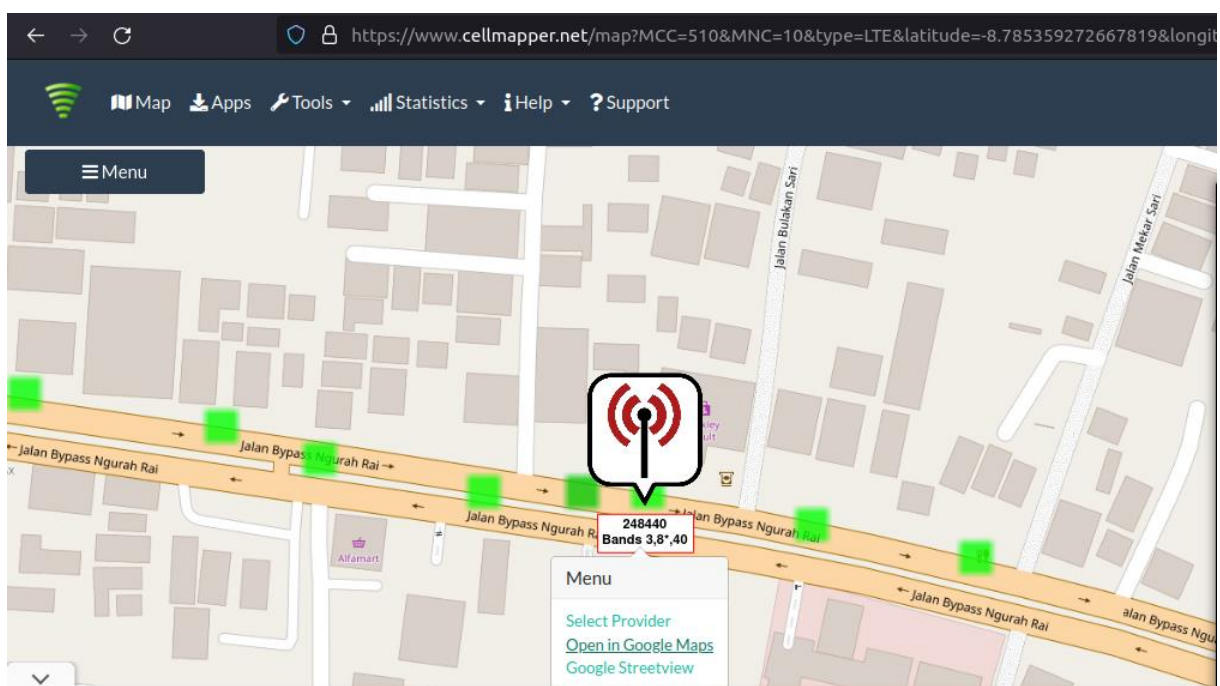
Correct : TECHCOMFEST23{-420.6:69.4}

Wrong : TECHCOMFEST23{-420:69}

Author: aimardcr

## 2. Technical Report

Pada soal kali ini kita disuruh untuk melacak tower dari provider yang dipakai oleh hacker, pada soal kita diberi tahu bahwa providernya itu telkomsel dan eNB id nya 248440, jadi kami langsung mencari di google tower dengan eNB id seperti pada soal, dan didapat tower tersebut berada di jalan by pass ngurah rai seperti pada gambar



selanjutnya kita klik open in google maps untuk mencari longitude dan latitudenya

<https://www.google.com/maps/@-8.7855794,115.2014062,15z>

didapat longitude dan latitude nya dan tinggal masukin ke format flagnya

## Contact

Flag : TECHCOMFEST{628988117322:Chariovalda Efstathios}

### 1. Summary

(This challenge is a sequel after the Runaway story)  
Thanks to you, we've captured the hacker we have been catching for so long. Now that we have his phone, we went through his contact and found a lot fake numbers. He said that he only save his partner number, but his partner changed the number a lot to prevent being tracked. He did said that one of the number in the contact is still active, but he won't tell us which one. For the sake of this country, can you find the correct phone number and his partner real name?

Note: The names in the .vcf file are fake names, find the real name!

Format FLAG: TECHCOMFEST23{Number:FullName}

Example: TECHCOMFEST23{621234567890:Rick Astley}

Author: **aimardcr**

### 2. Technical Report

Pada challenge ini kita diberikan file contact.vcfm dan setelah dilihat isinya seperti ada data dan nomor telepon

```
indianajones@bukan-heker:~/Documents/Techcomfest/contact$ cat contacts.vcf
BEGIN:VCARD
VERSION:4.0
FN:XXXXXXXXXXXXX
N:XXXXXXXXXXXXX
ORG:
TEL;WORK;VOICE:62517250808
EMAIL:
ADR;HOME:
BDAY:
END:VCARD
BEGIN:VCARD
VERSION:4.0
FN:XXXXXXX
N:XXXXXXX
ORG:
TEL;WORK;VOICE:620317405693
EMAIL:
ADR;HOME:
BDAY:
END:VCARD
BEGIN:VCARD
VERSION:4.0
FN:XXXXXXXXXX
N:XXXXXXXXXX
ORG:
TEL;WORK;VOICE:62799999394
EMAIL:
ADR;HOME:
BDAY:
END:VCARD
BEGIN:VCARD
VERSION:4.0
FN:XXXXXXXXXXXXX
N:XXXXXXXXXXXXX
ORG:
TEL;WORK;VOICE:62297273800
EMAIL:
```

Dari banyak no telepon tersebut kami coba untuk mencari semuanya di getcontact dan didapatkan nomor 628988117322 dengan nama Chariovalda Efstathios yang ada tag This is the correct answer, jadi kami asumsikan itu flagnya, submit dan benar



Tambahkan Penanda



**Chariovalda Efstathios**

+628988117322 - ID

GTC



Panggilan



Obrolan



Tambahkan



Laporkan



**1 Penanda Lainnya**

Ada 1 penanda yang ditambahkan ke nomo...

