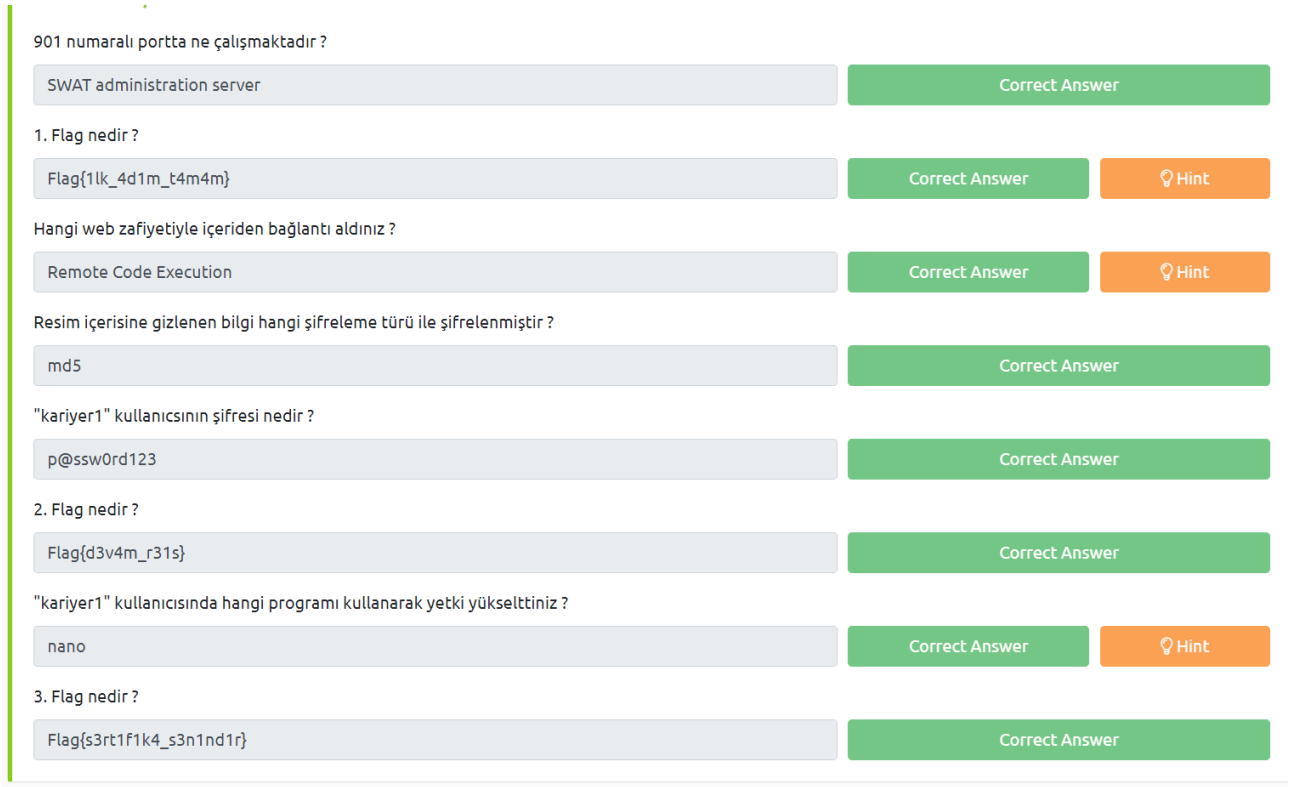
TechCareerCTF

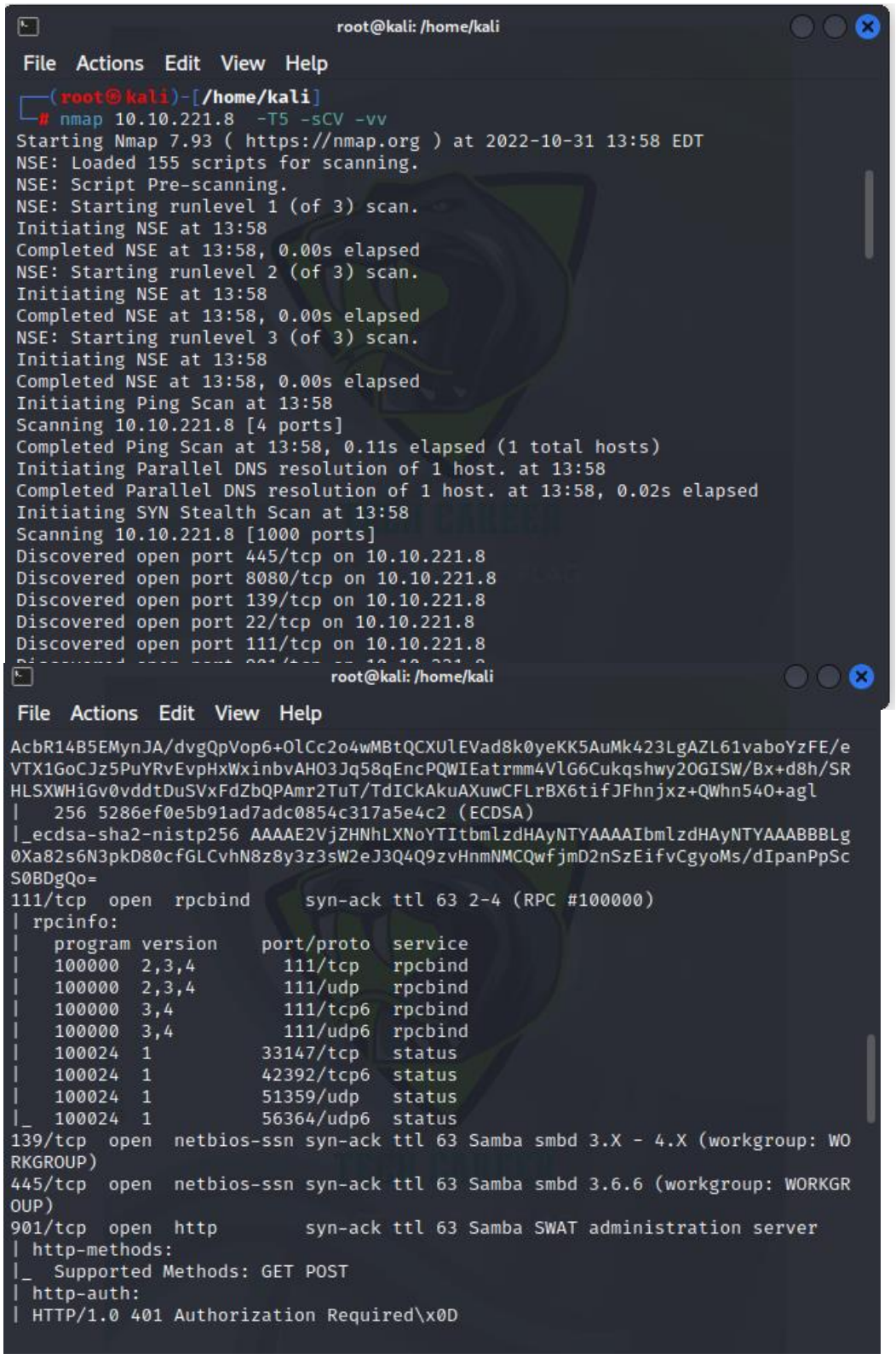
1. Verilen linux makineye sızmanızı ve 3 adet flag tespit etmenizi istiyoruz.
2. Flaglar "Flag{.....}" formatındadır.
3. Hepinize başarılar.

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



1. 901 numaralı portta ne çalışmaktadır ?

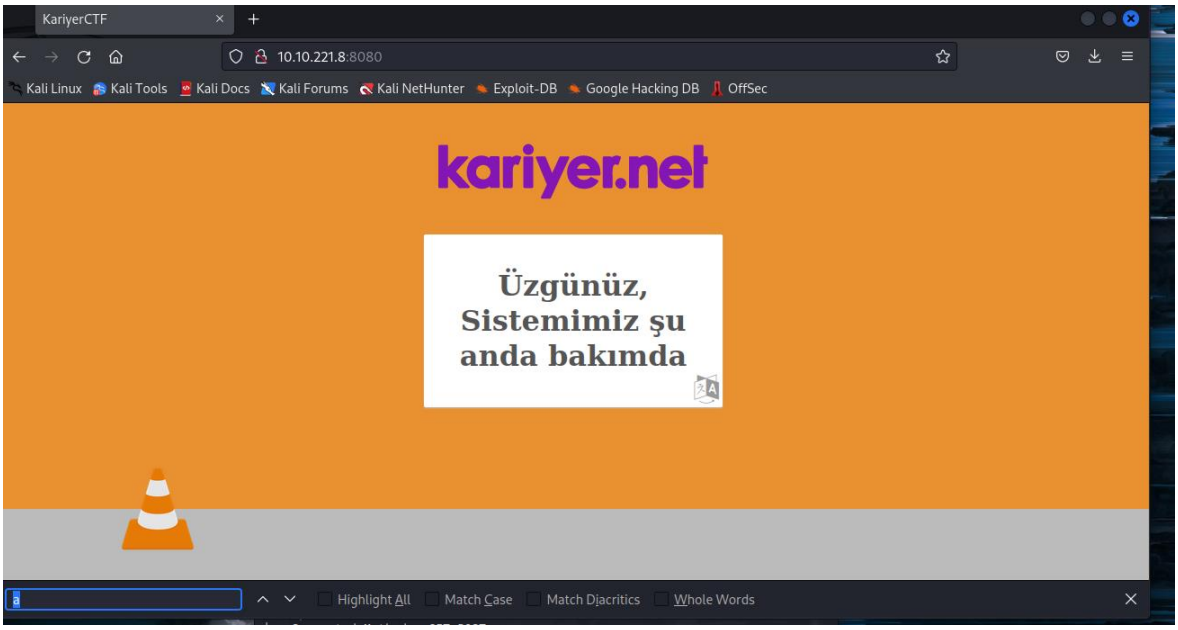
Bu sorunun cevabına erişmek için ve nelerimiz var bakmak için ilk olarak nmap taraması yapıyoruz. Taramamız sonucunda açık olan portlarımızı görüyoruz.



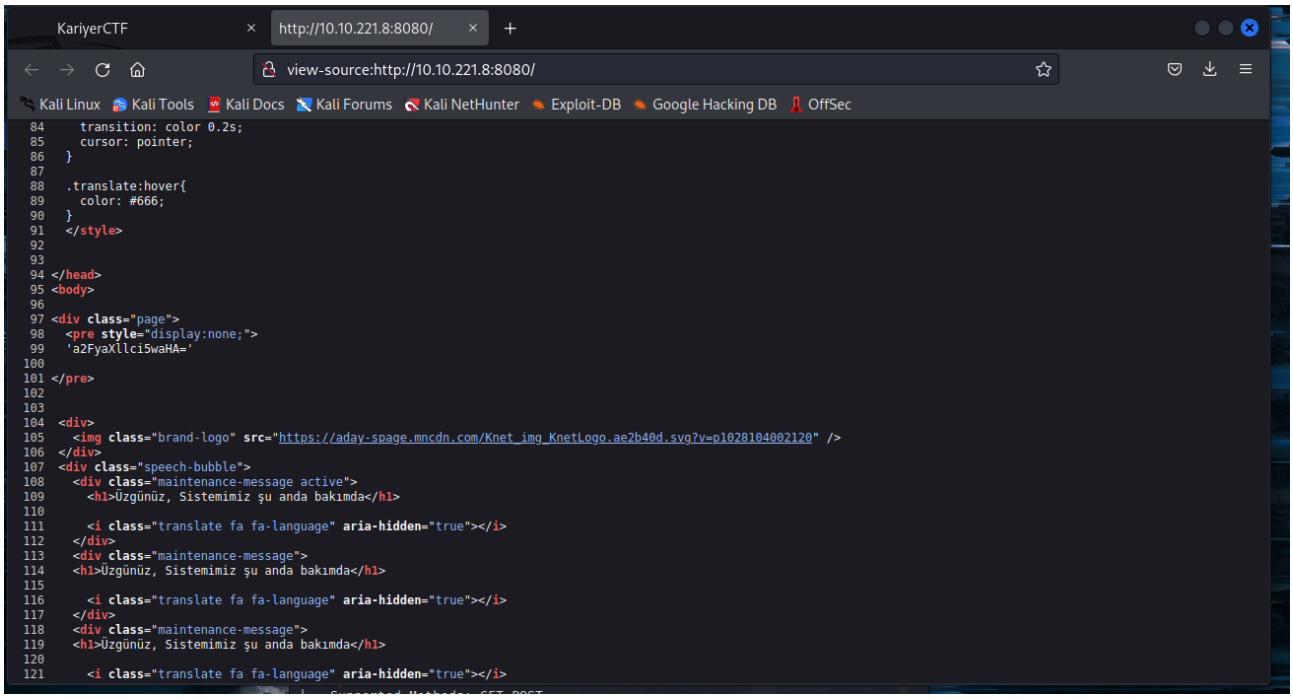
Taramanın ilerleyen kısımlarında 901 numaralı portta ;
‘SWAT administration server’ çalıştığını görüyoruz.

2. 1. Flag nedir ?

Nmap taramamız sonucunda 8080 portunun açık olduğunu görüyoruz.



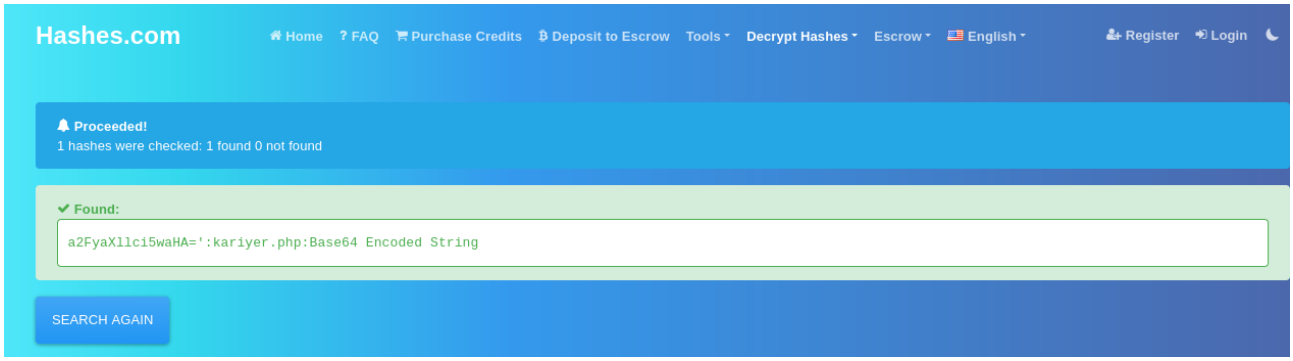
Sayfaya erişim sağladık ancak farklı bir şey göremiyoruz. Kaynak koduna bakıyoruz



Kaynak kodunu incelediğimizde kodla alakası olmayan bir bilgi ile karşılaşıyoruz;

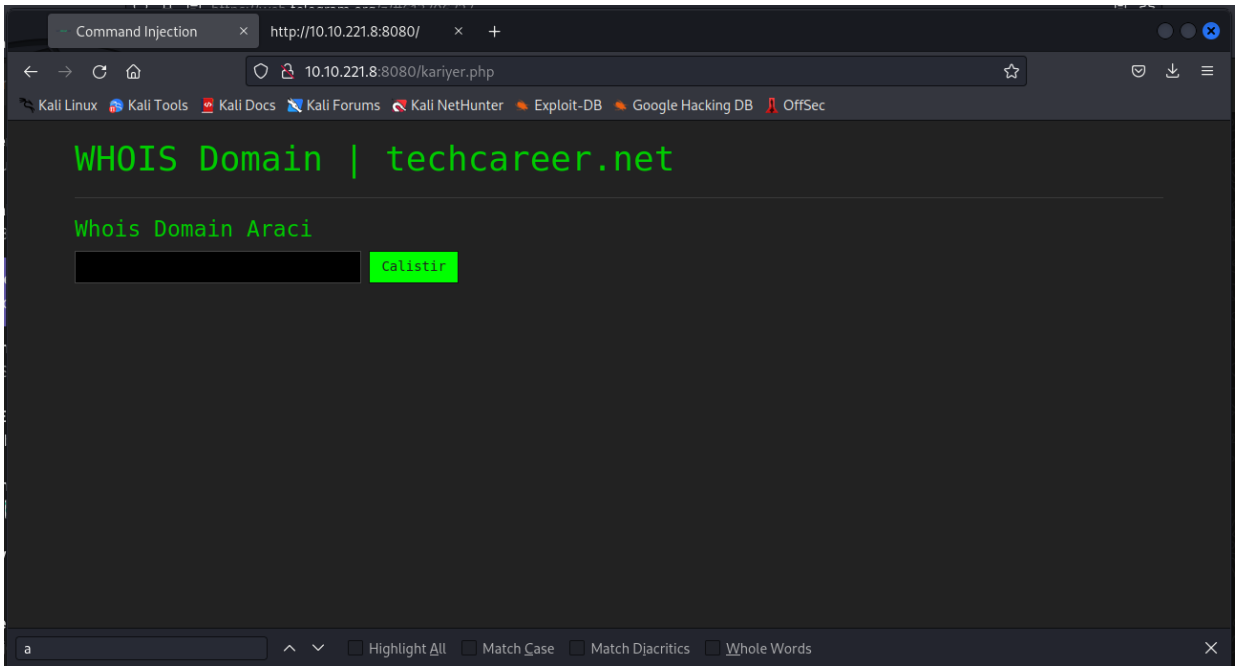
a2FyaXllci5waHA=

Anlayamadığımız için hashes.com'u kullanarak metini çözümlüyoruz.



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

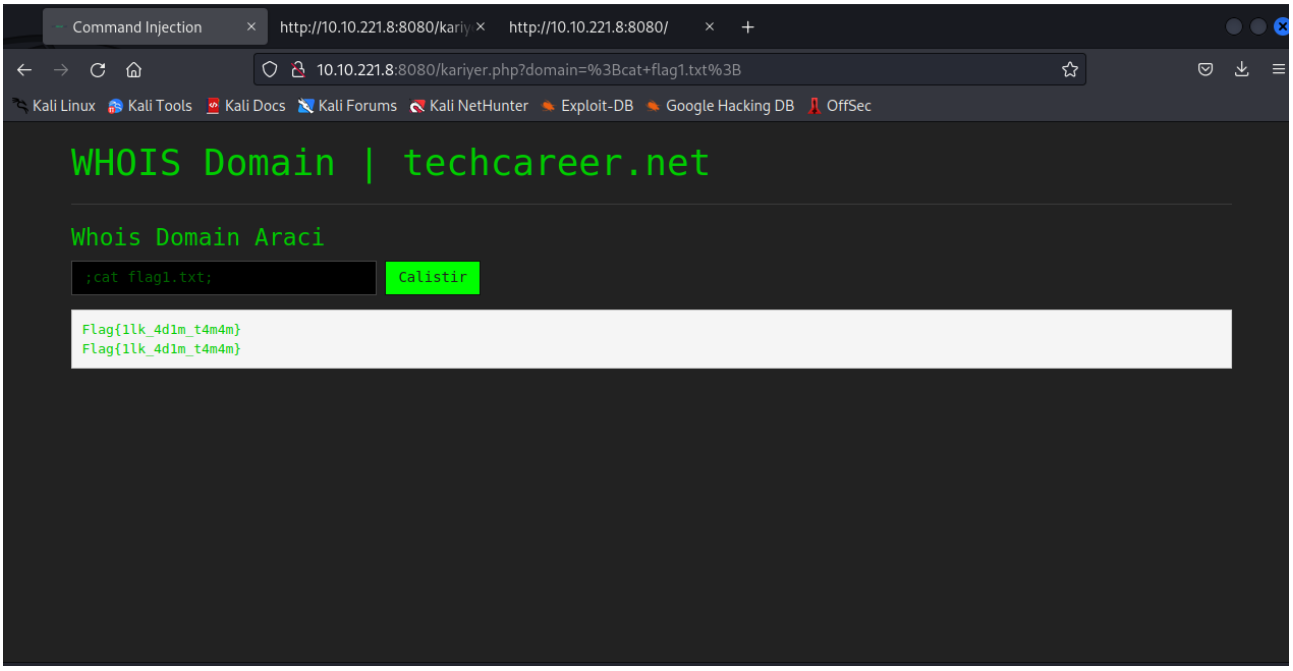
http://10.10.221.8:8080/kariyer.php



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

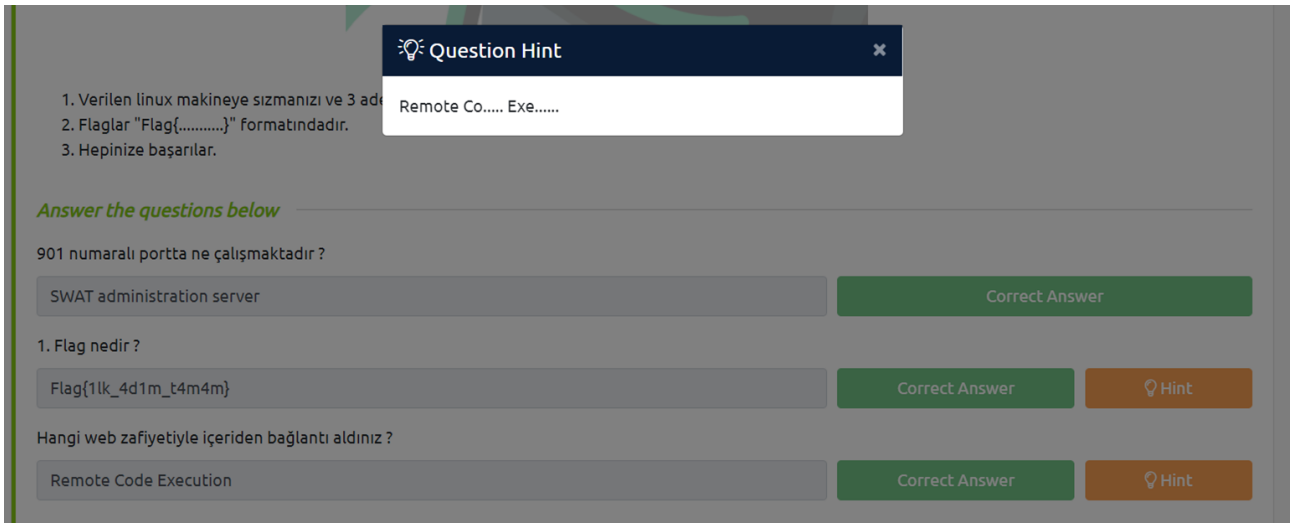
;ls; komutunun çalıştığını görüyoruz ve flag1 de orada duruyor.

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



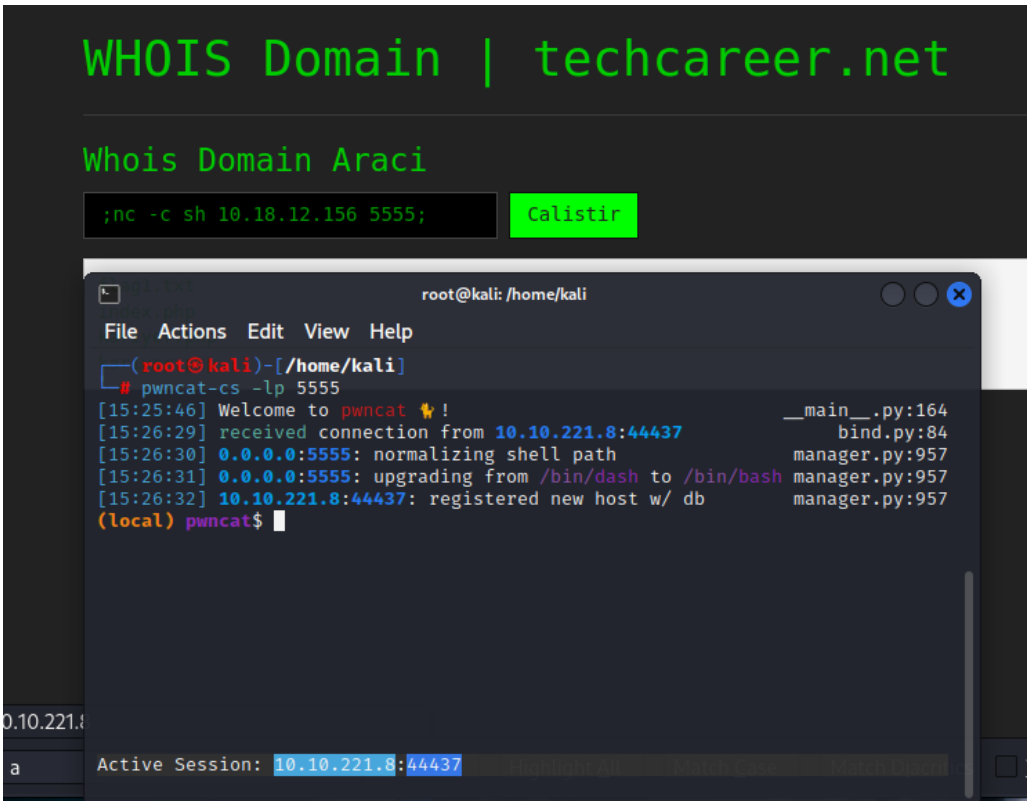
Flag1'e ulaştığımız için mutluluktan uçmuyor çözmeye devam ediyoruz.

3. Hangi web zafiyetiyle içeriden bağlantı aldınız ?



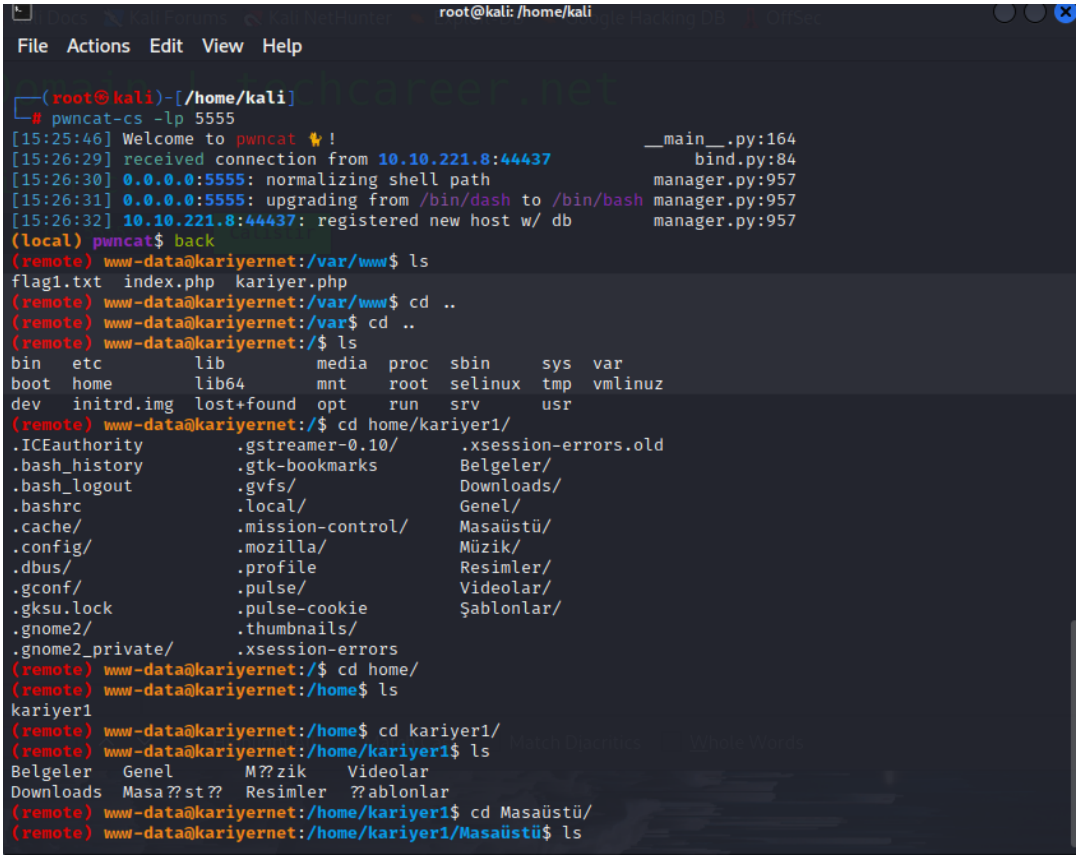
Remote Code Evaluation (RCE) Türkçe anlamı ile Uzaktan Kod Yürütme olan bu güvenlik açığı bir saldırganın bir başkasının cihazına erişim sağlamak için uzaktan kod yürütüp programlama dilin de değerlendirme yapıp içeriği sunmasıdır. Böyle bir güvenlik açığını uygulayabilen bir saldırgan genellikle programlama 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 ?

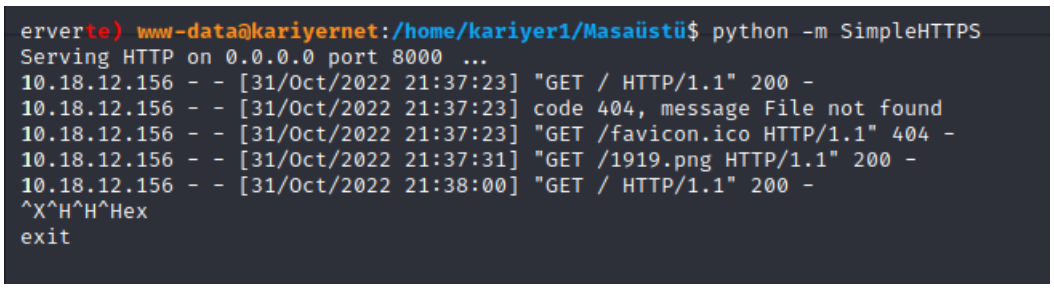


Flag1'i bulduk ancak başka işlem yapmak için shell almamız gerekiyor.
netcat komutunu kullanarak kariyernet üzerinde ağı dinliyoruz

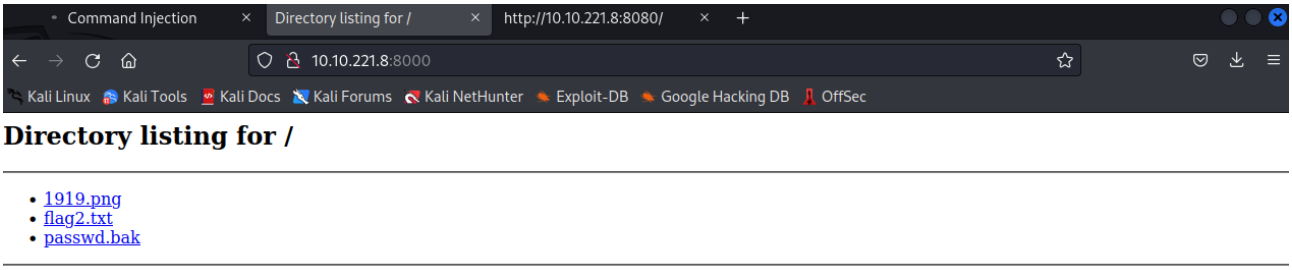
pwncat kullanarak kariyernet üzerinde reverse shell işlemi gerçekleştiriyoruz.



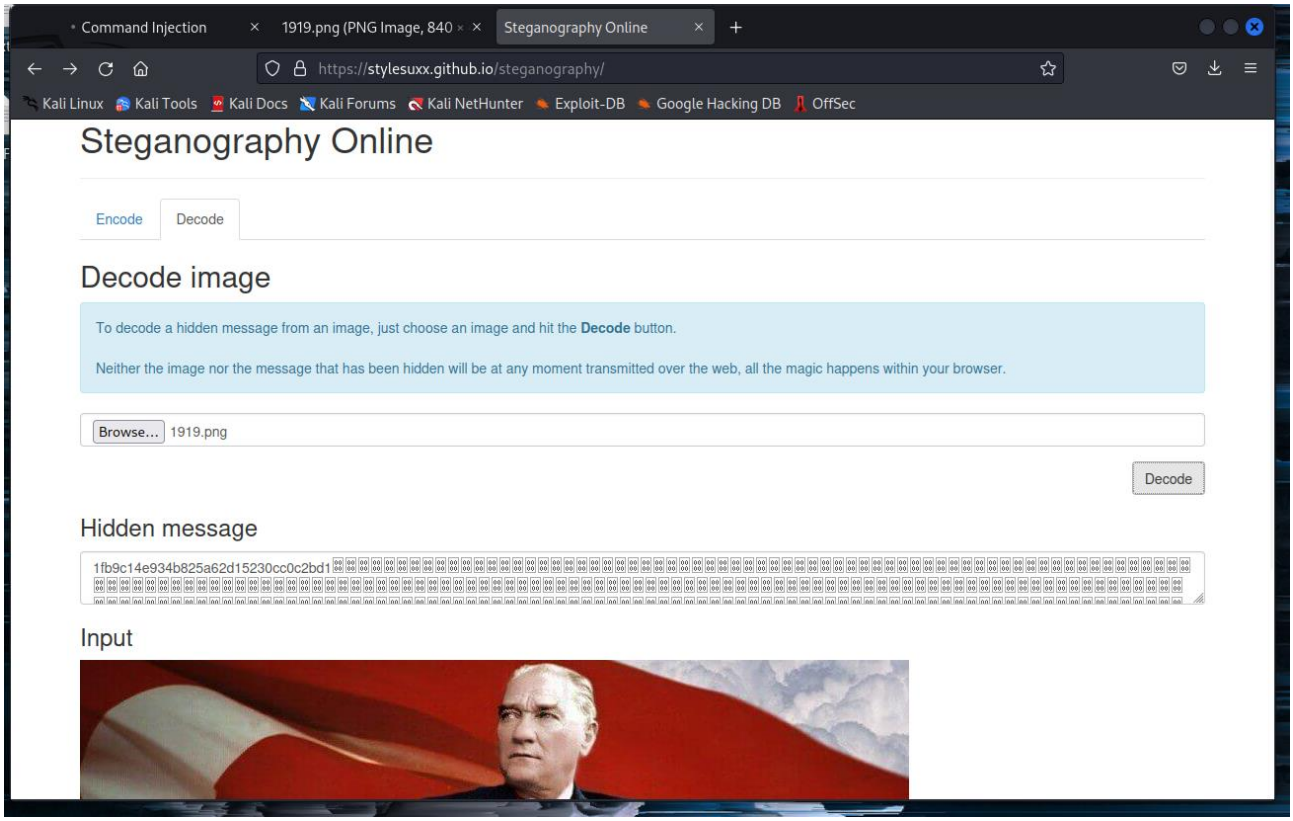
Klasörlerin içine bakıyoruz ve resim dosyamızı arıyoruz. Resim dosyamızı bulduk ama açamıyoruz. Resim dosyamızı indirebilmek için python server açıyoruz. (https://www.hackerearth.com/practice/notes/simple-http-server-in-python/)



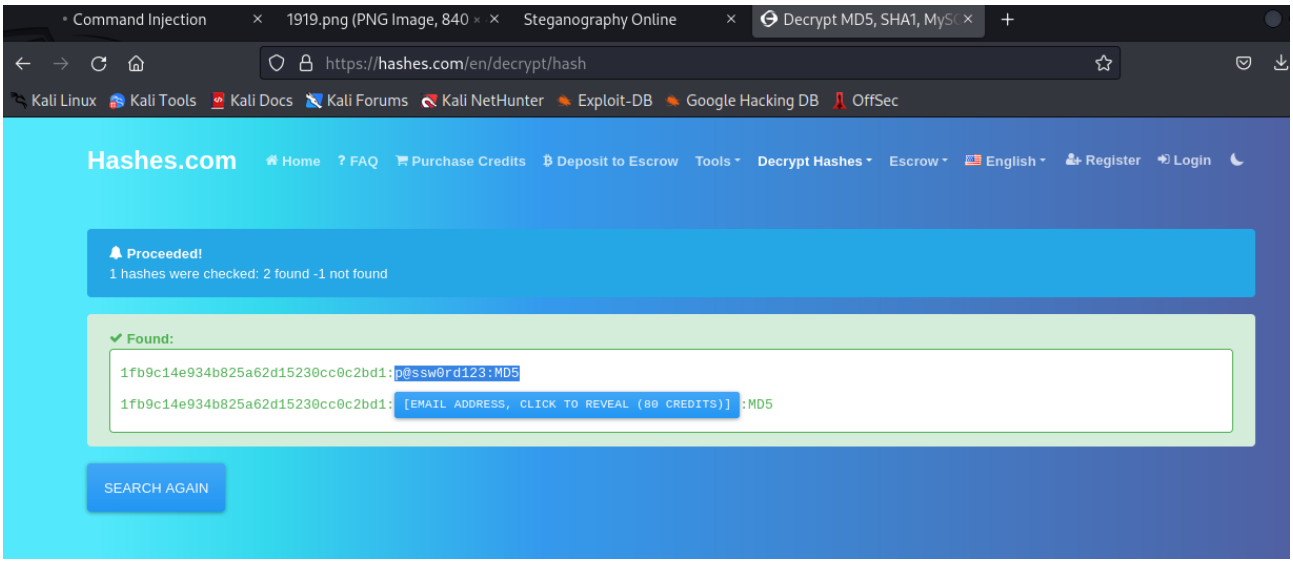
Python server ile resime erişim sağladık



Resmi indiriyoruz taramak için https://stylesuxx.github.io/steganography/ siteyi kulanıyoruz. Resmi decode ediyoruz ve şifreli metine ulaşıyoruz.

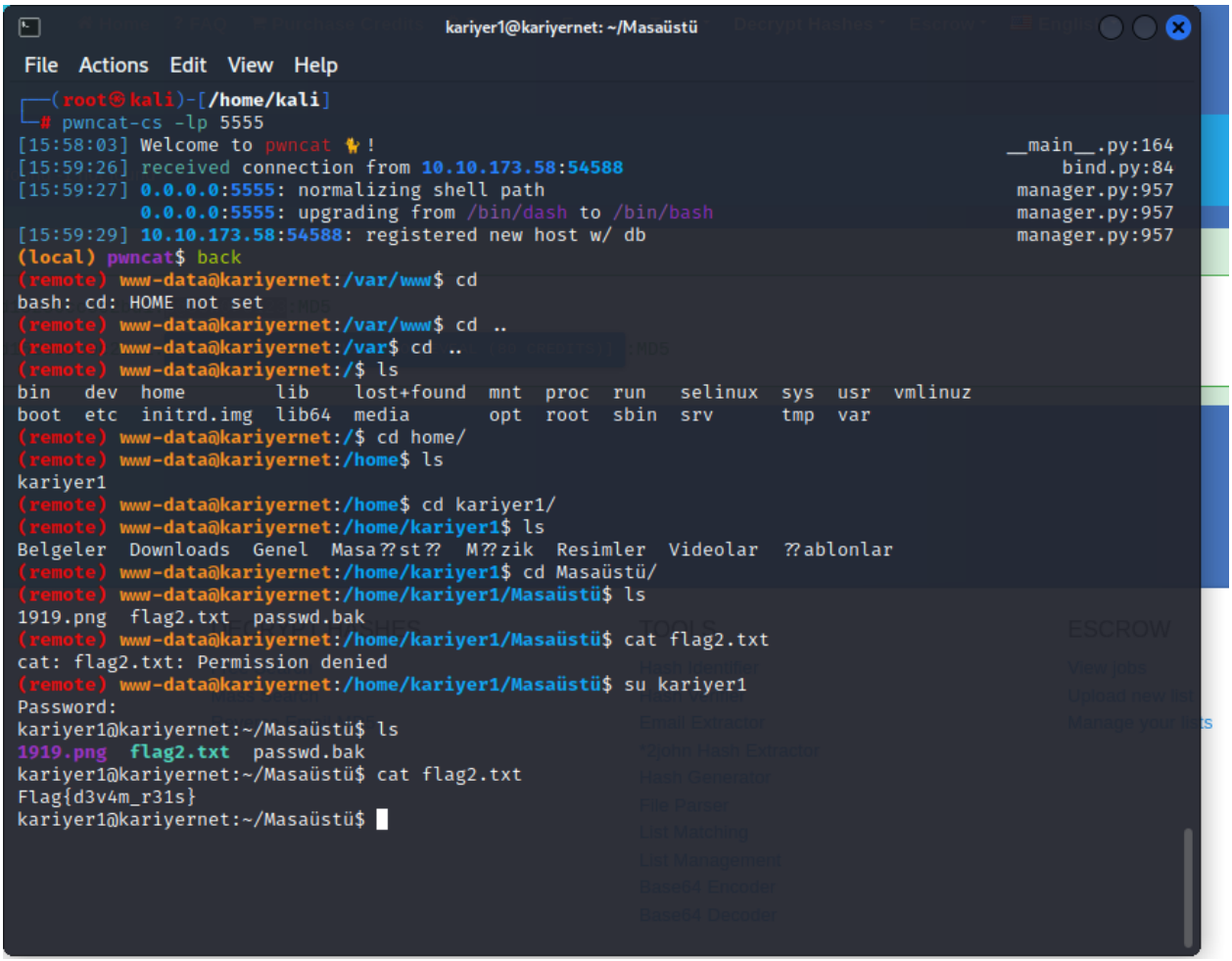


5. "kariyer1" kullanıcısının şifresi nedir ?



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 diyoruz.

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:/$
```