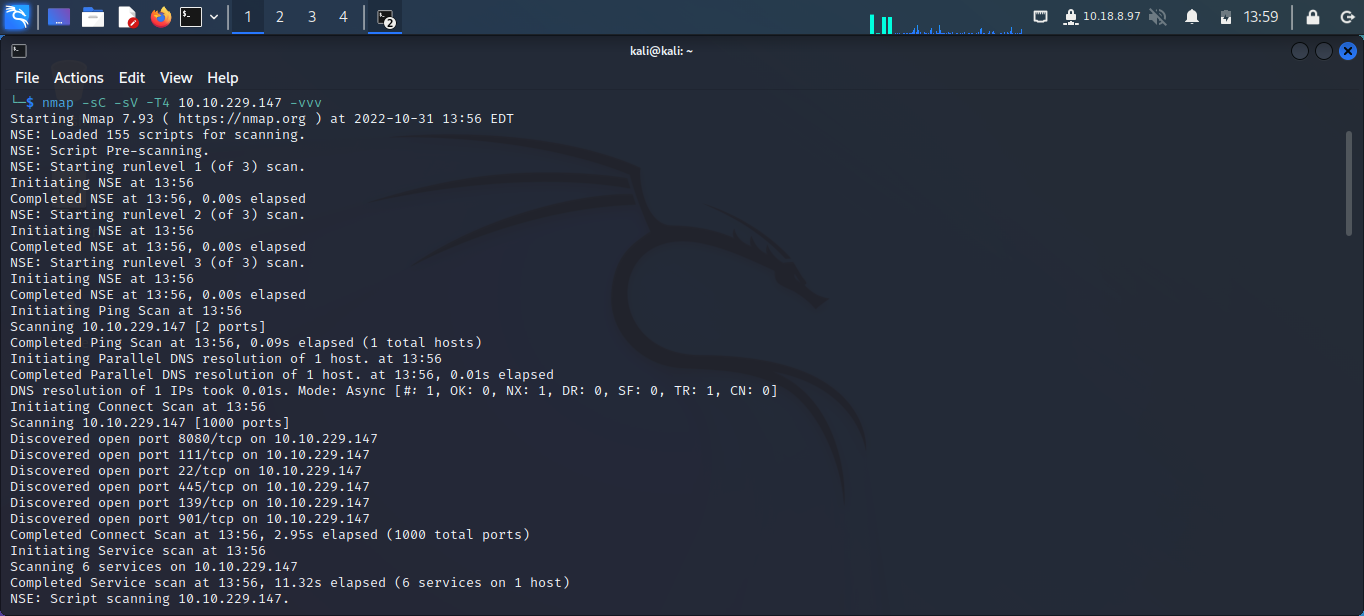
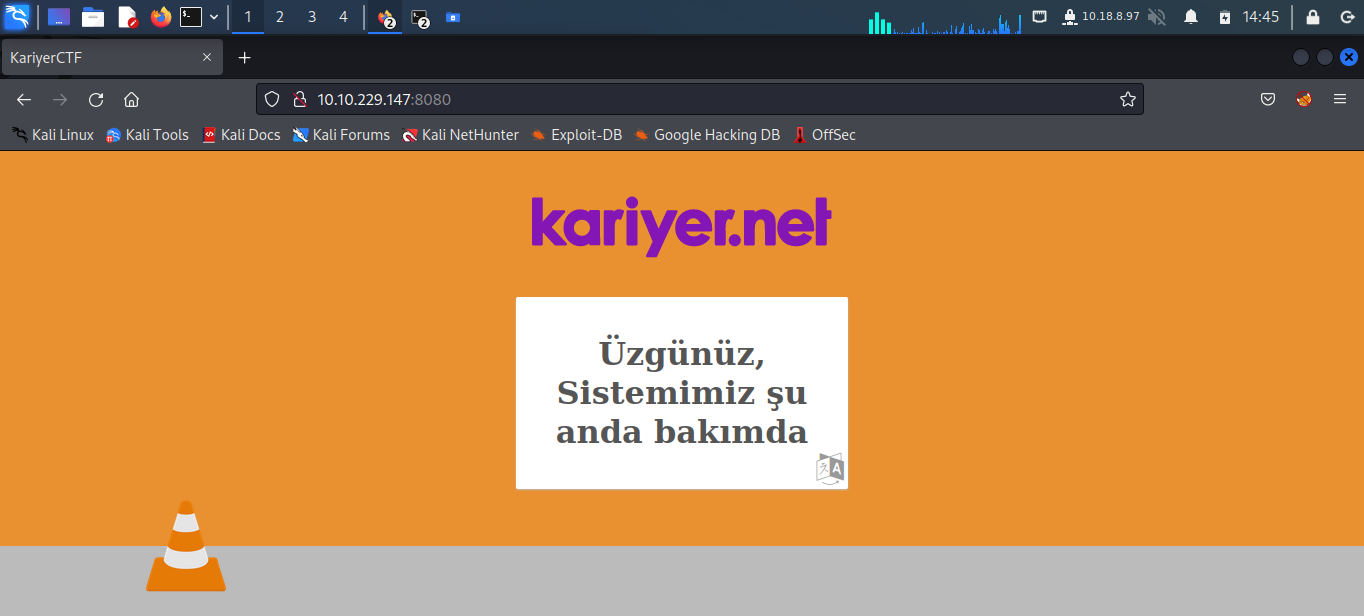
**TechCareerCTF Writeup**

Önce nmap taraması yaptım (nmap -sC -sV -T4 10.10.229.147 -vvv)

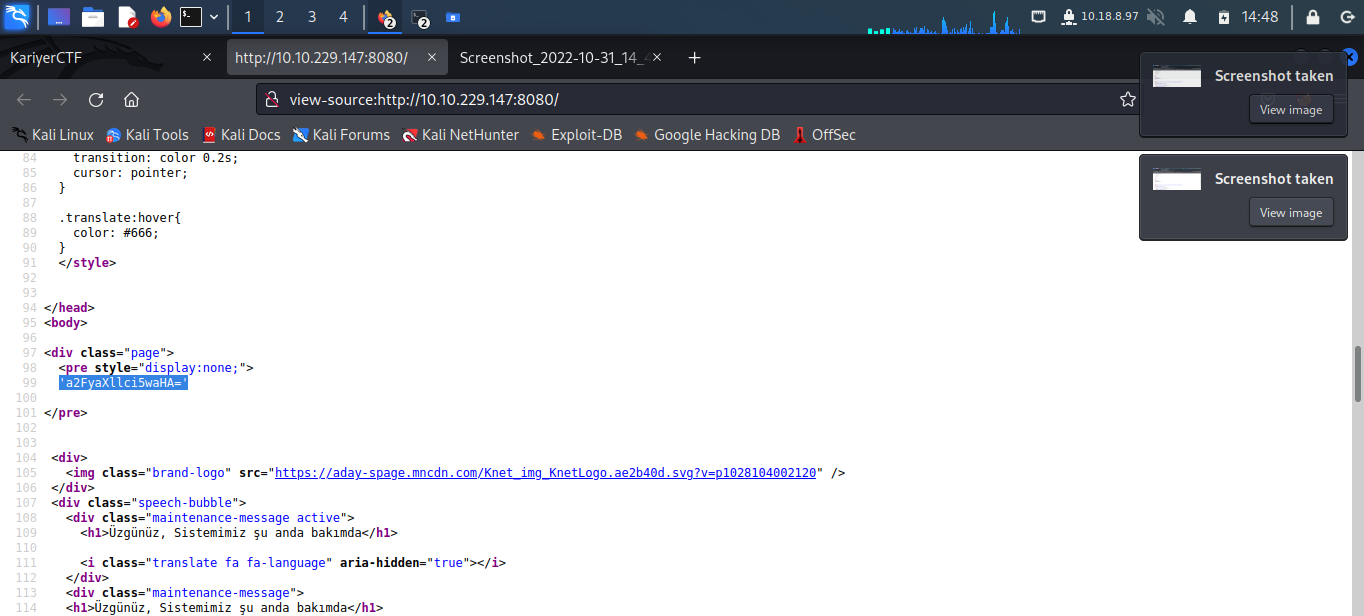


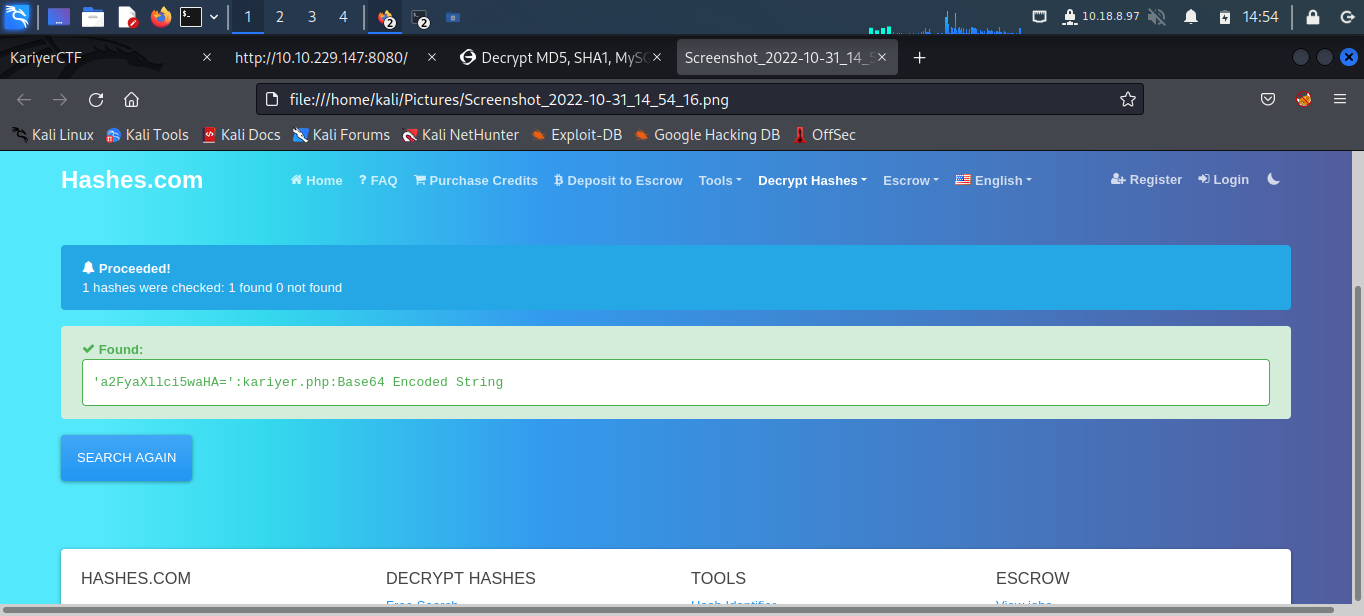
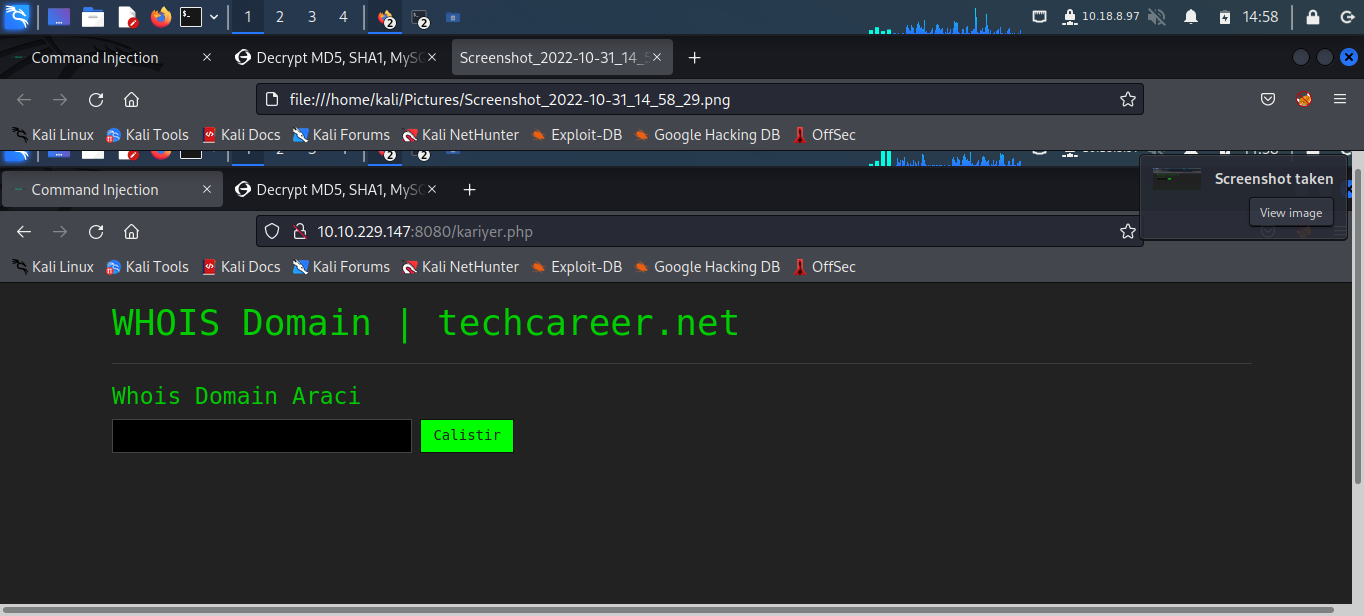
8080 portunun açık olduğunu gördüm. Karşıma böyle bir sayfa çıktı.

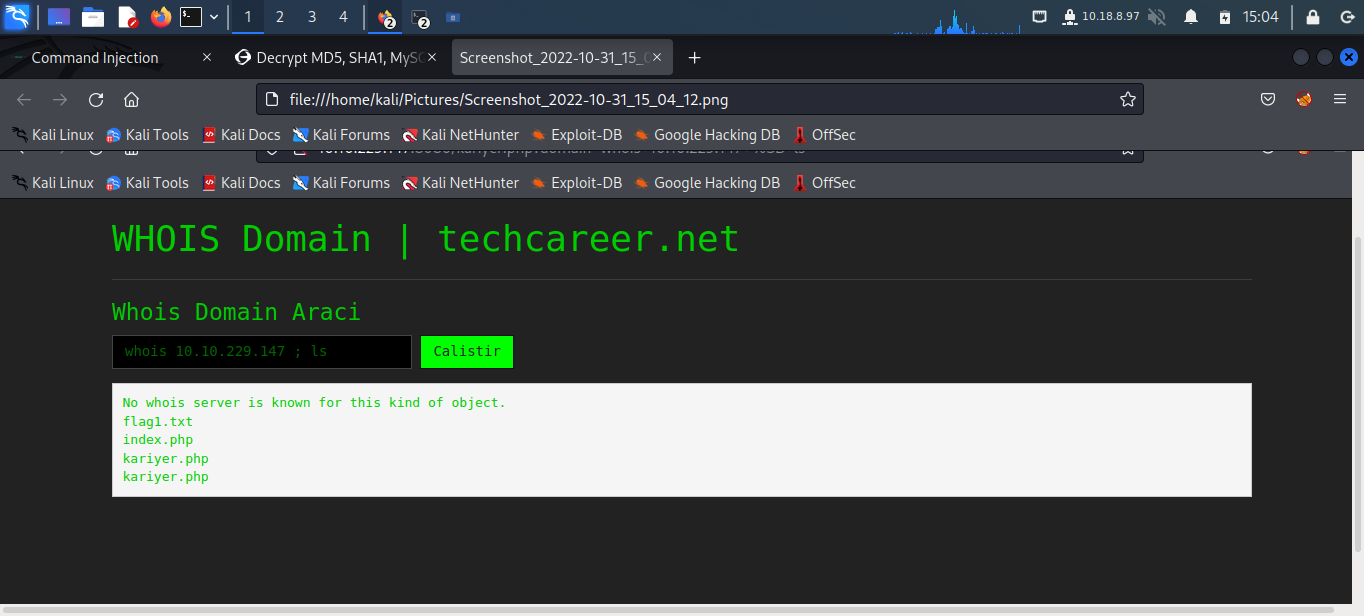


Sayfanın kaynak kodunu görüntüledim ve şifreli bir mesaj buldum.

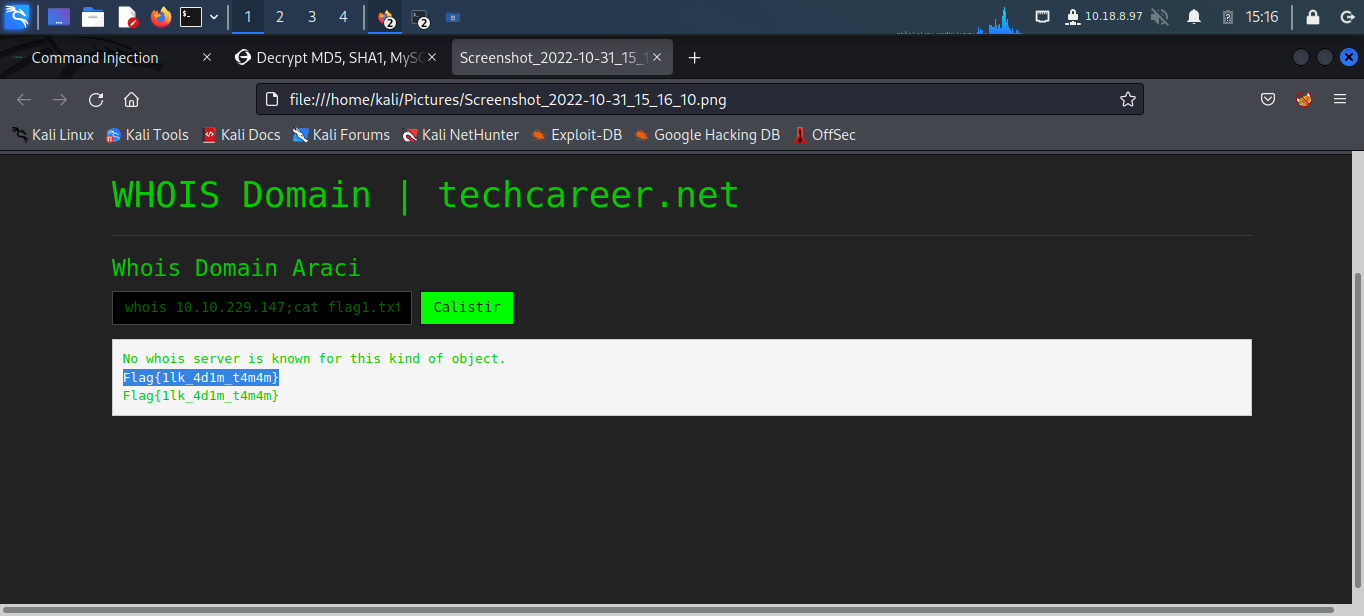
'a2FyaXllci5waHA='



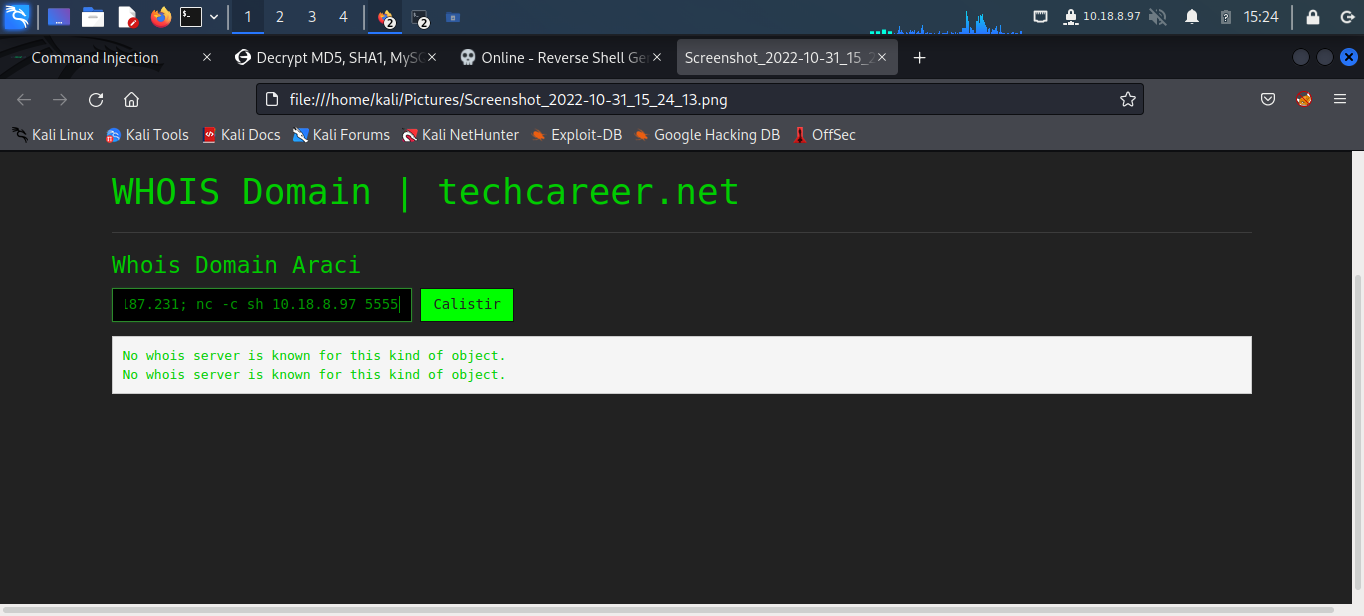
Kariyer.php sayfasına gittiğimizde whois sorgusu olan bir sayfa açılıyor.Whois 10.10.229.147 ; ls komutu ile dosyaları görüntüledim.



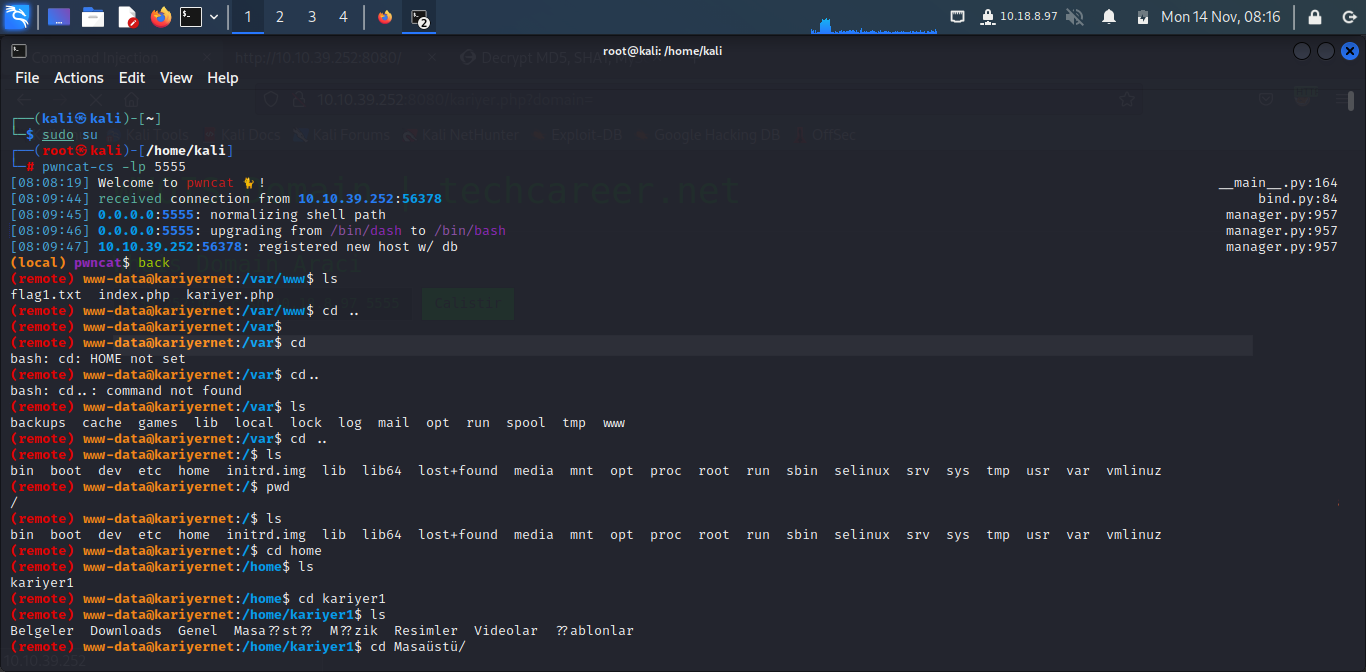
whois 10.10.229.147 ; cat flag1.txt kodunu yazdım. Flag{1lk\_4d1m\_t4m4m} ilk flagı buldum.



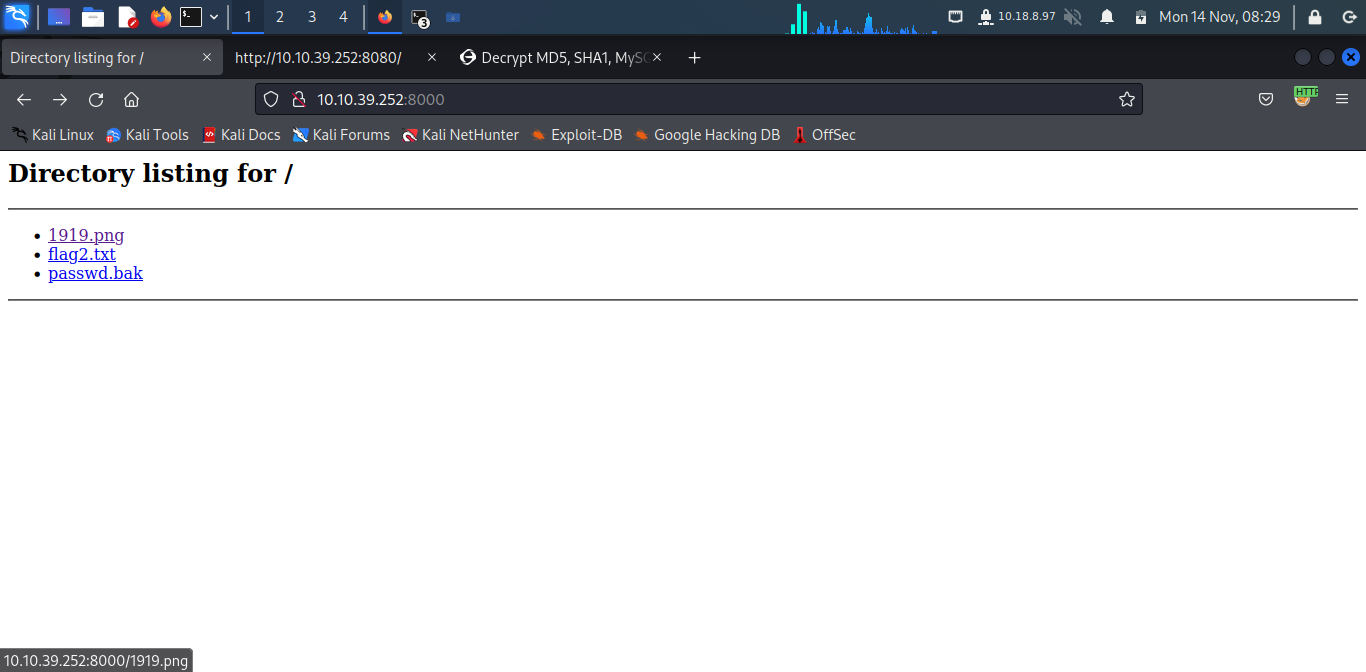
Reverseshell yaptım nc –c sh komutunu kullandım.(Bağlantım burda koptu bu işlemleri tekrar yaptım.)

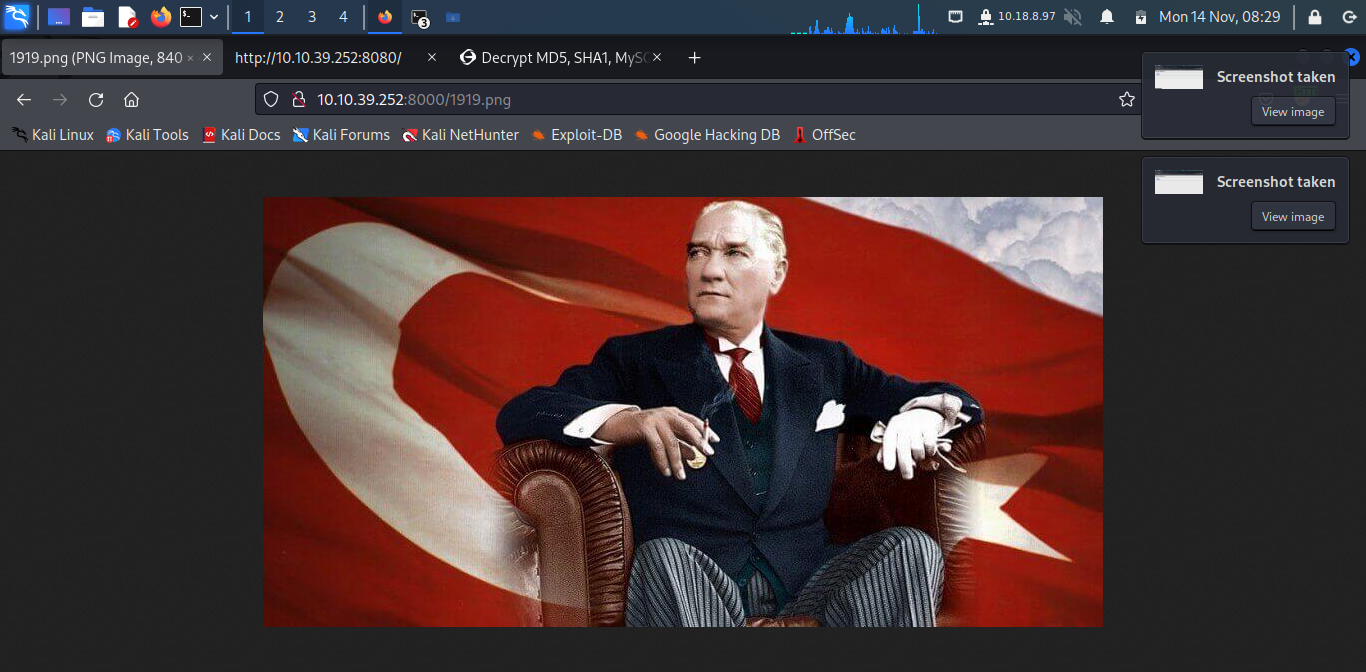


Burda yetkilendirme komutları kullanarak home dizinine geldim. Masaüstünde resim ve txt dosyası buldum fakat txt dosyası açılmadı.Bende resim dosyasını python simple server kullanarak indirdim.

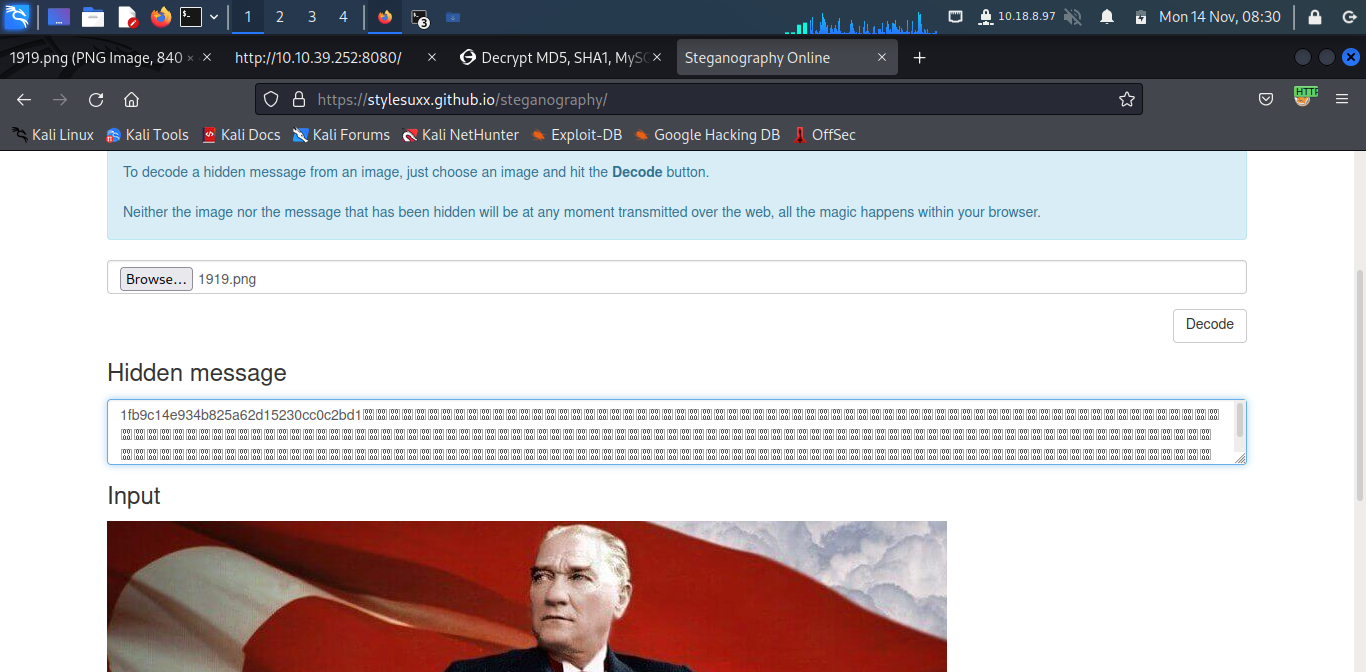


Resim dosyasında steganografi olduğunu düşündüm.

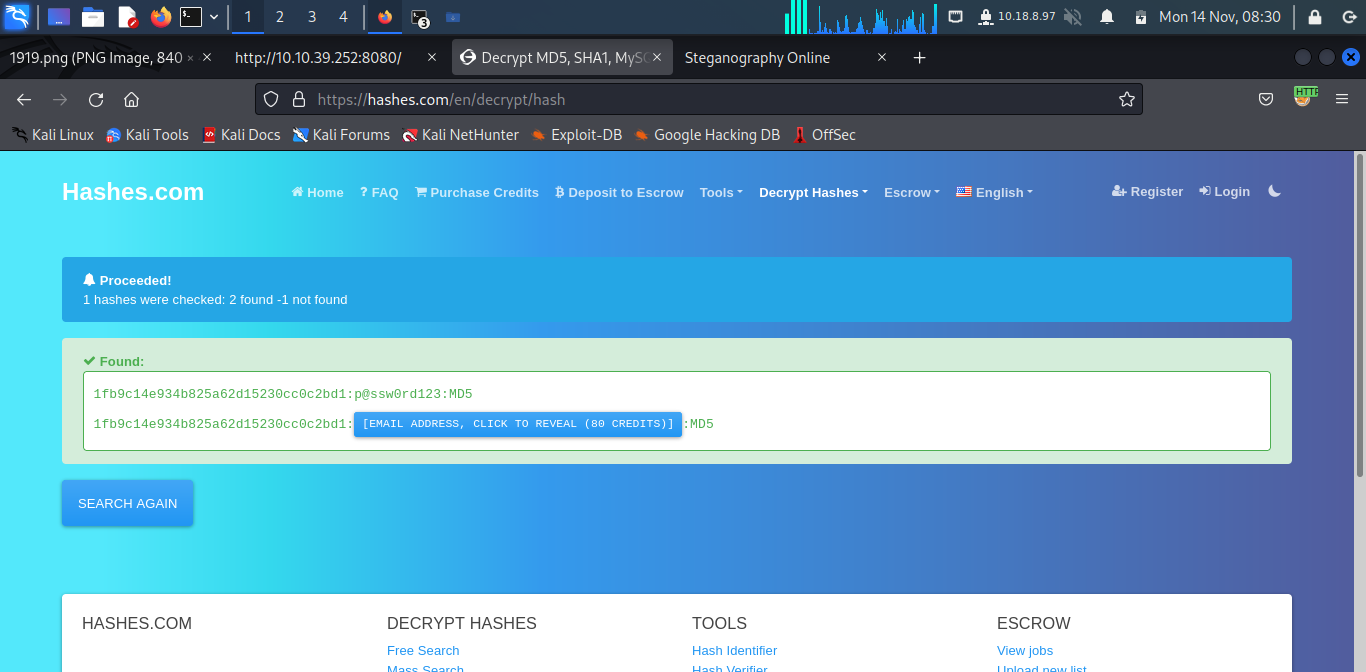




<https://stylesuxx.github.io/steganography/> sayfasından decode ettim .



Hash li kodu çözdüğümüzde MD5 türünde passwordümüzü buluyoruz.



Kariyer1 kullanıcısına geçiş yapıp flag2.txt dosyasını açıyoruz. Son olarak flag3 kaldı onunda root kullnıcında olduğunu düşünüp sudo –1 ile yetkilendiriyoruz. Ve nano ile flag 3 e ulaşıyoruz.

Flag{s3rt1f1k4\_s3n1nd1r}.

**Cansu Avcı Yalçın**