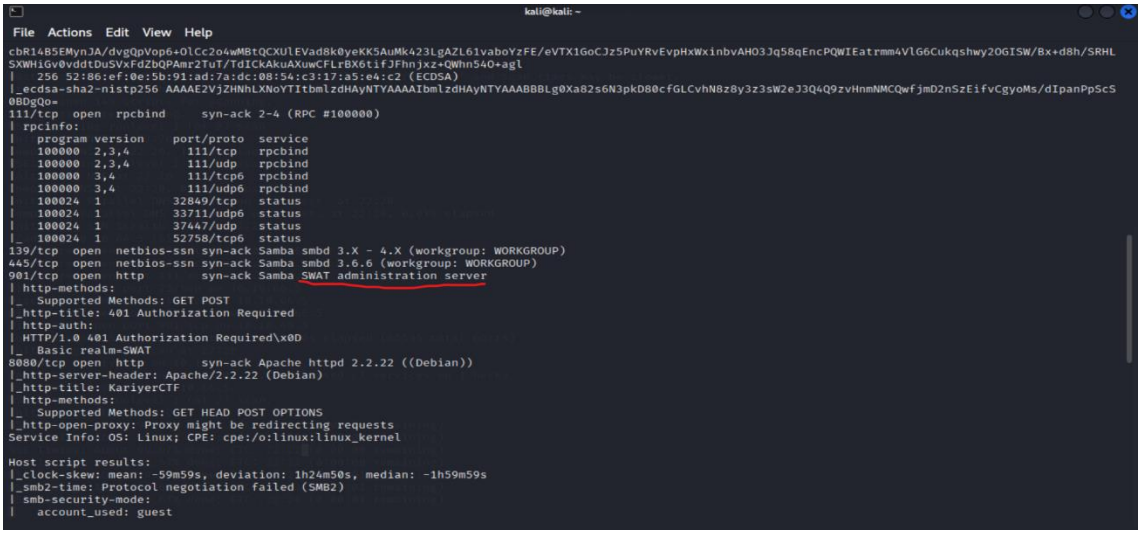
Cyber Security
Emre Cahit TURAN

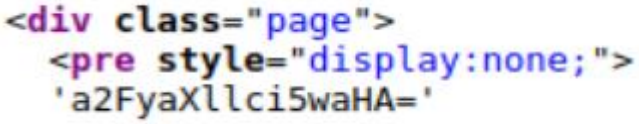
1) 901 numaralı portta ne çalışmaktadır?

nmap <Target Ip> -sCV -T4 -vv -Pn -vv



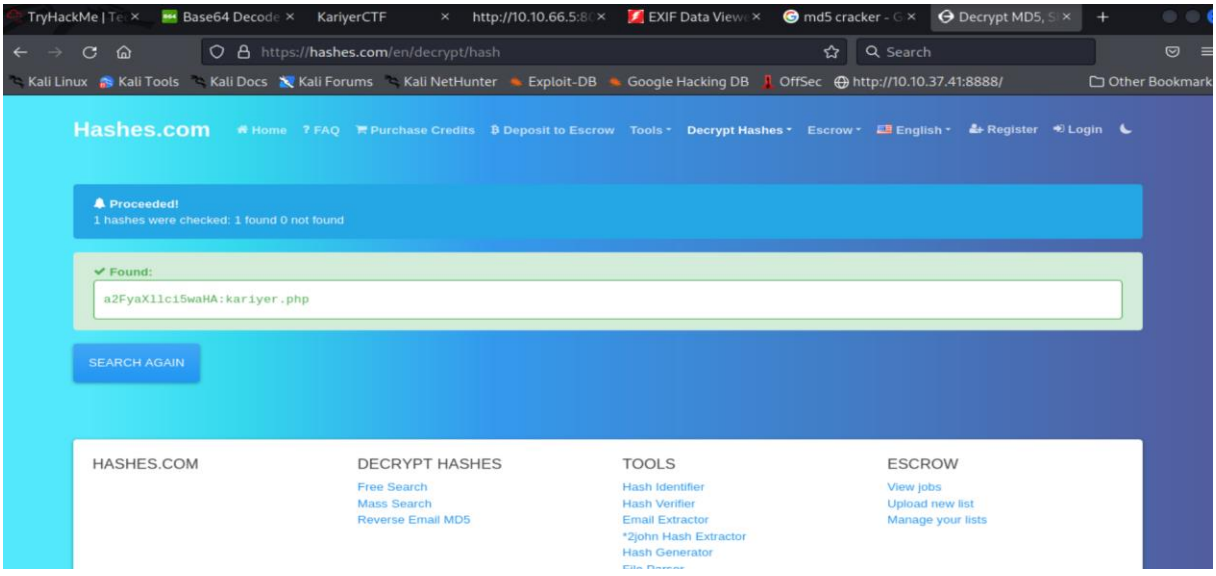
2) Flag nedir ?

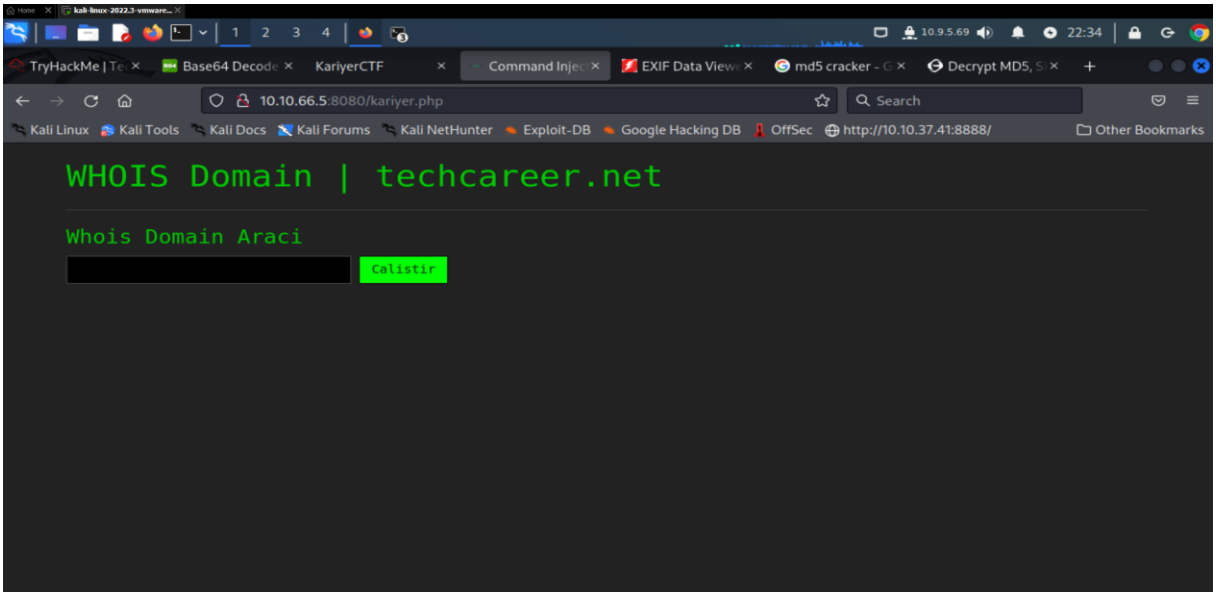
10.10.66.5:8080 potundan giriş yaparak sayfa kaynak kodunu inceliyoruz (Ctrl +u)



Burada şifreli bir metin ile karşılaşıyoruz.

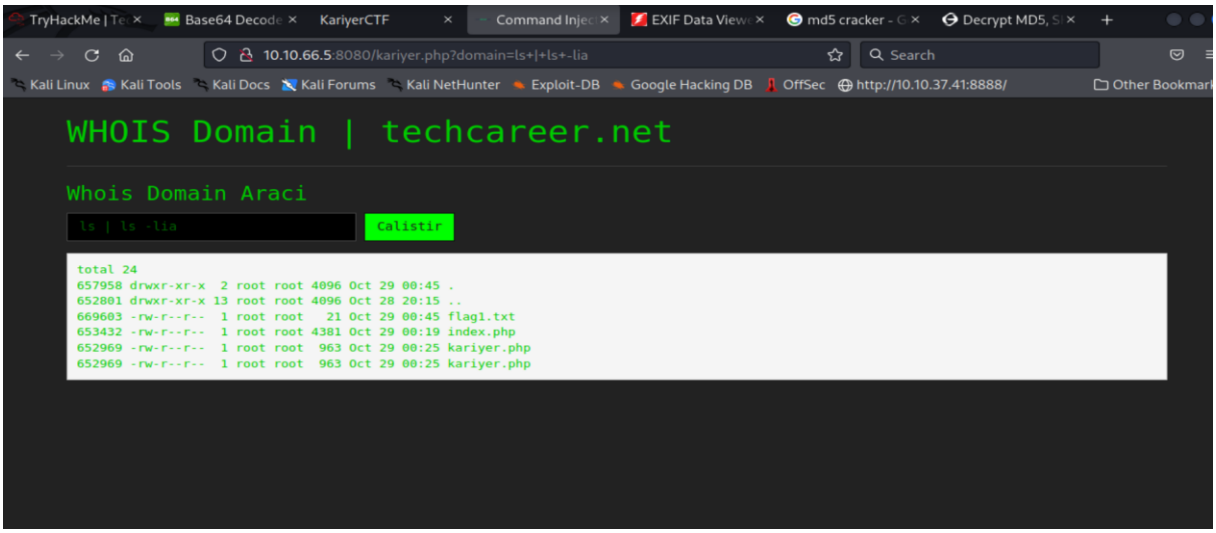
Hashes.com da bu şifreli metini kırıyoruz ve karşımıza kariyer.php geliyor



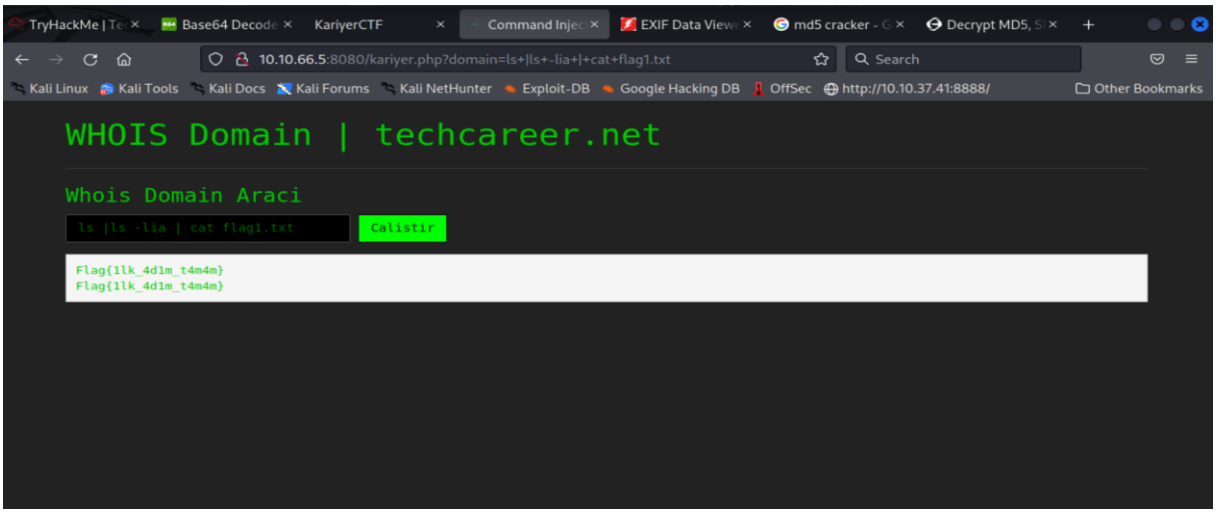


Karşımıza bu ekran geliyor da arama motoruna “ls” yazarsak
Karşımıza bir şey çıkmıyor ancak çift kod yazmak için ‘|’ işaretçisini kullanarak ikili arama yapabiliriz.

“Ls | ls -lia” yazarak



Burada 1.flagimizi buluyoruz bununda okuyabilmek için
“ls | ls -lia |cat flag1.txt” yazarak 1.flagimiza ulaşıyoruz.



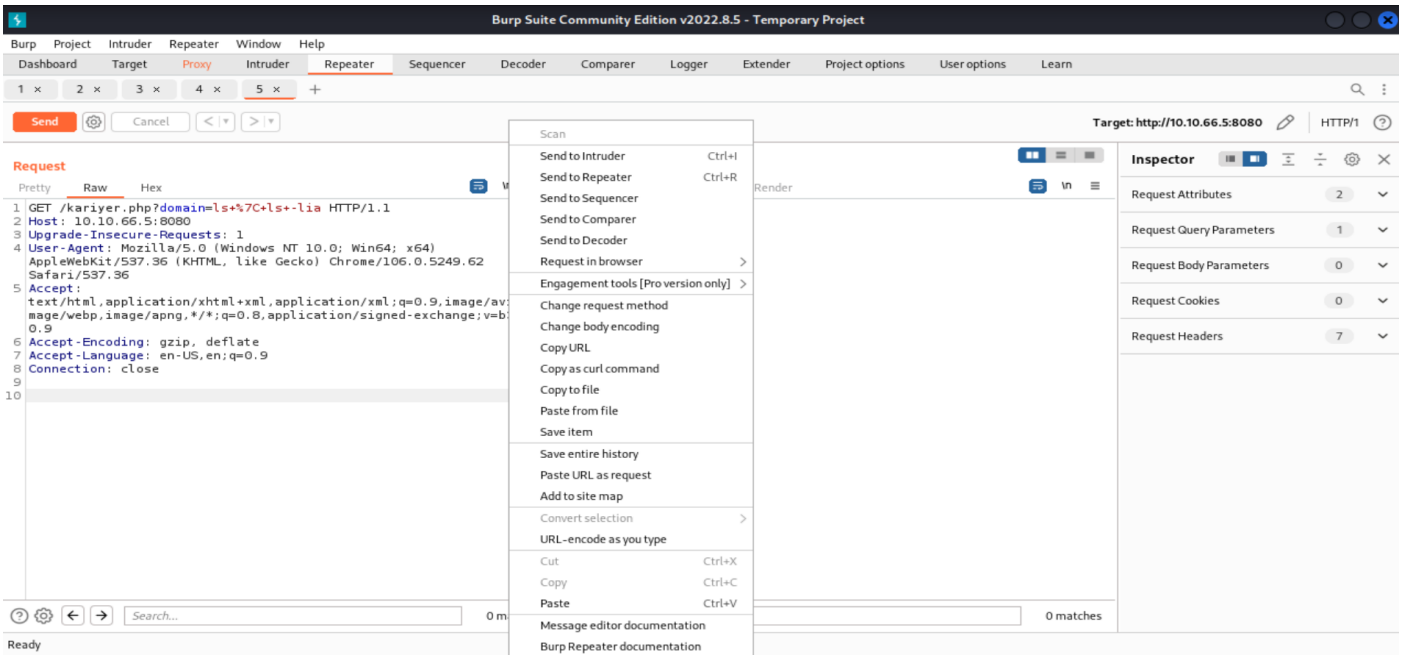
3)Resim İçerisine gizlenen bilgi hangi şifreleme türü ile şifrelenmiştir.
md5

4) "kariyer1" kullanıcısının şifresi nedir ?

Bulduğumuz

http://10.10.66.5:8080/kariyer.php?domain=ls+%7C+ls+-lia

Burp suite göndererek trafiği kesiyoruz

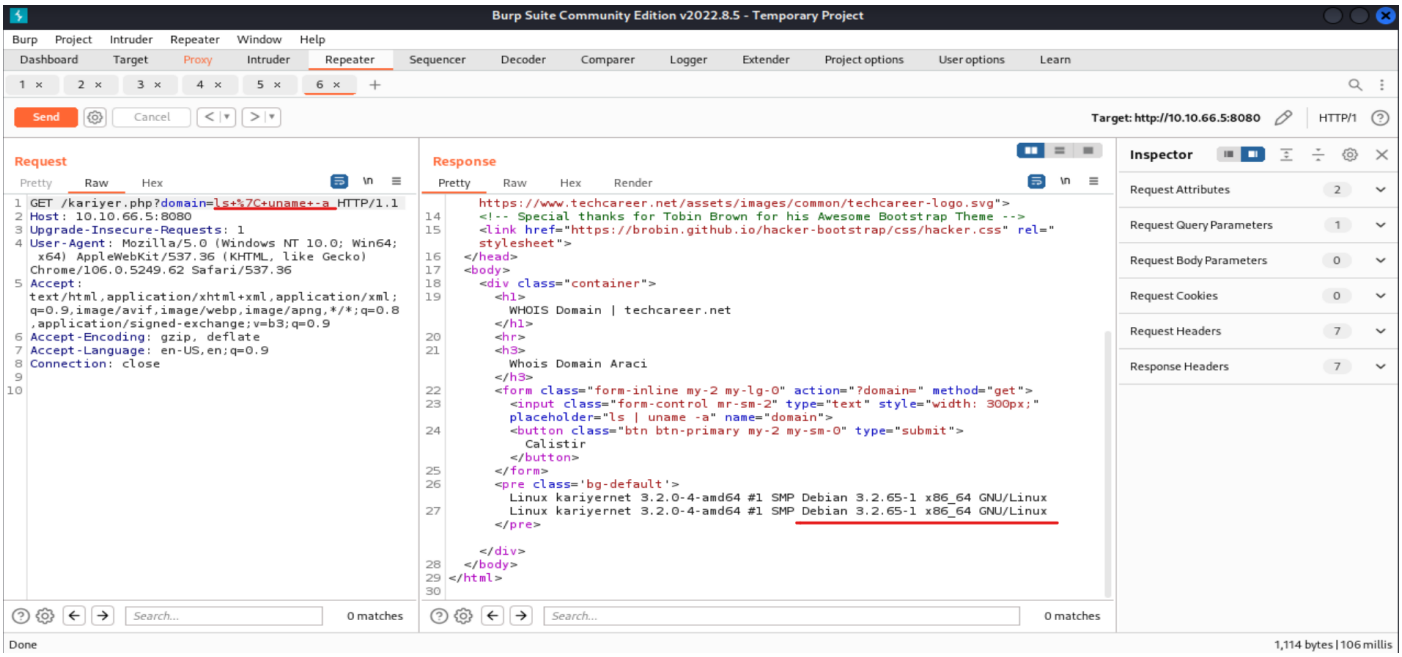


Burası istekleri istediğimiz şekilde gönderip tekrar tekrar sorgulamamıza yarıyor.

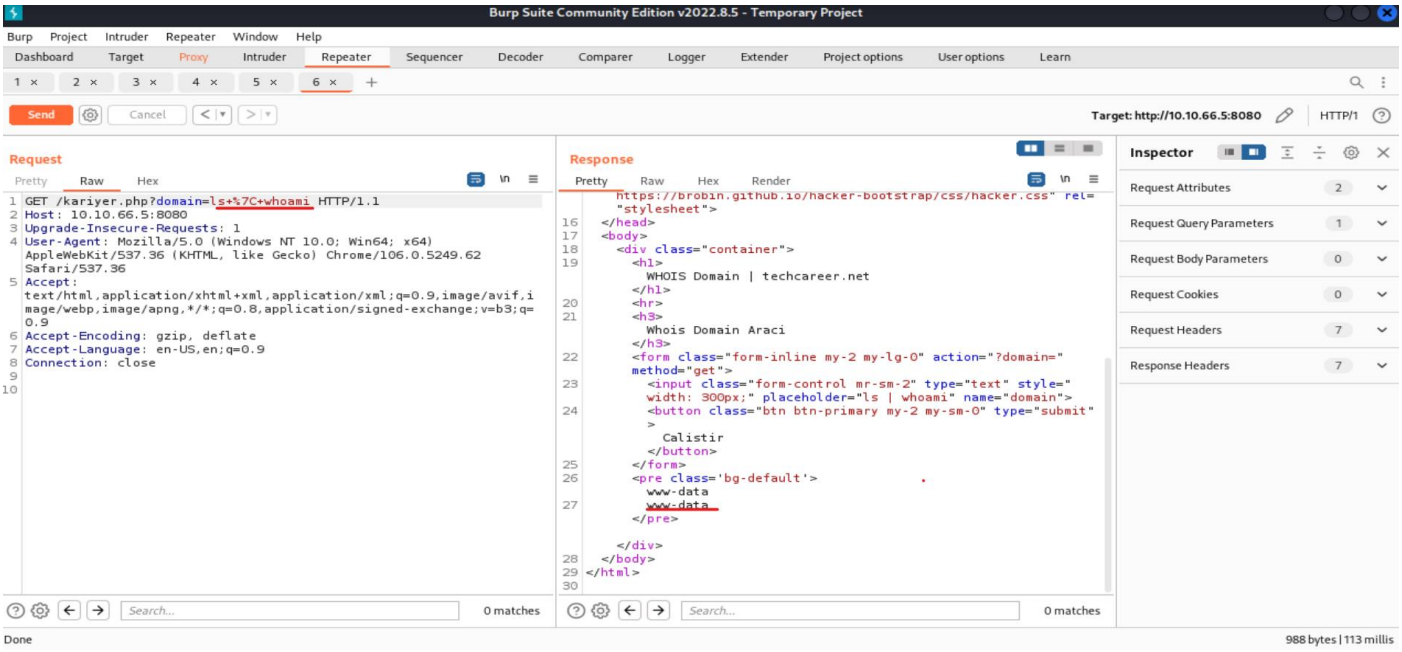
Ardından Repeater'a gönderiyoruz.

"Ls+%7C+uname+-a "

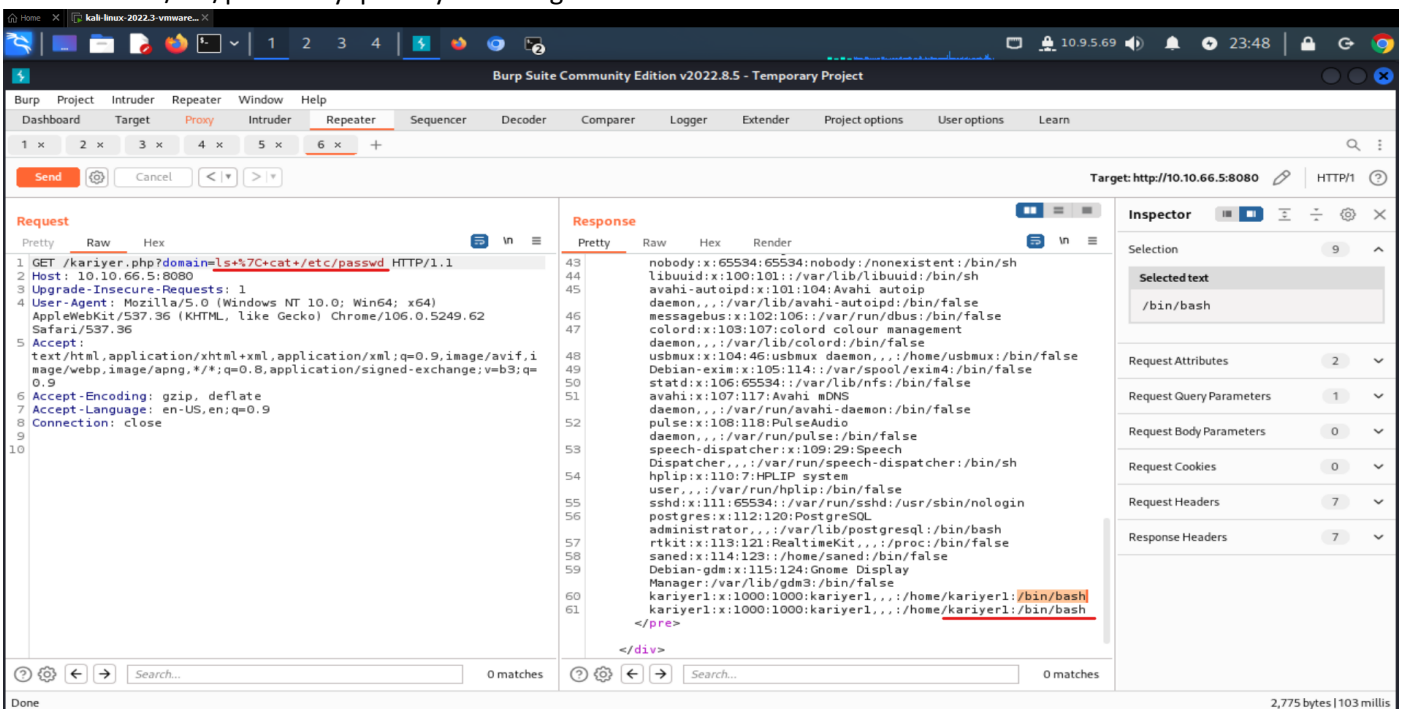
Mevcut sistemin versiyonunu görebiliriz.



Ardından bir sisteme giriş yaptığımızda ya da erişim sağladığımızda direkt olarak girdiğimiz bilgilerin ne olduğunu kontrol etmeliyiz.



“ls+%7C+cat+/etc/passwd” yaparak yetkilileri görebiliriz.

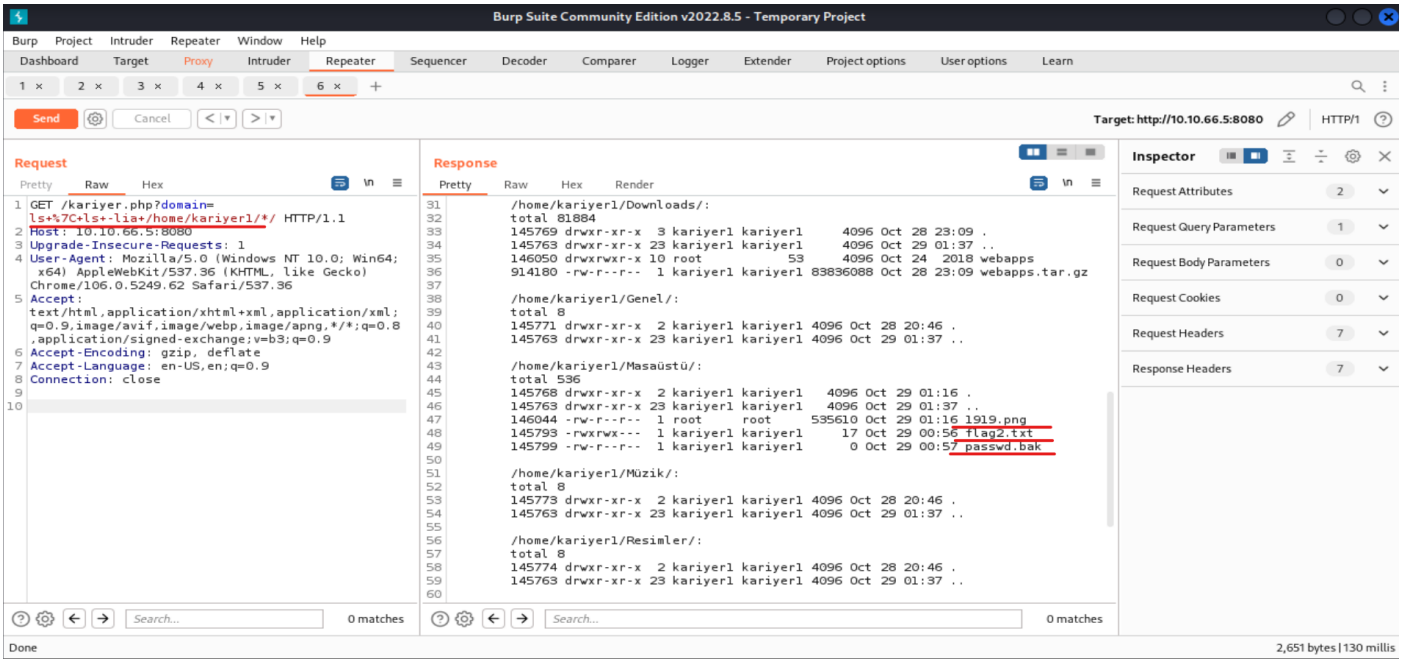


Ardından yani kali de olduğu gibi;

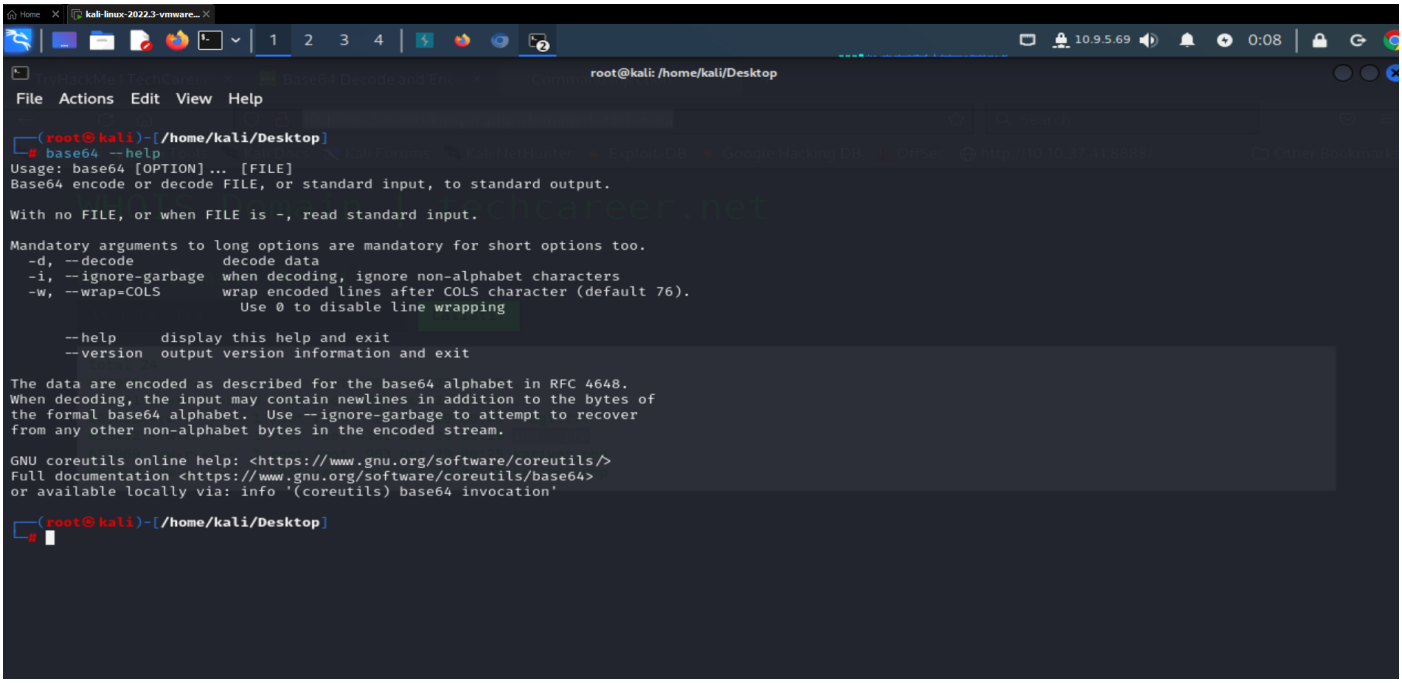
pwd yazdığımızda bulunduğu dizini gösteriyordu.

Burada da “/home/kariyer1/*/” dediğimiz zaman bize sistemde home’un içindeki kariyer1 dosyasının içindekileri gösterecektir.

Not: * koymamızın nedeni ise dizinde bulunan tüm klasörleri göstermesi için.



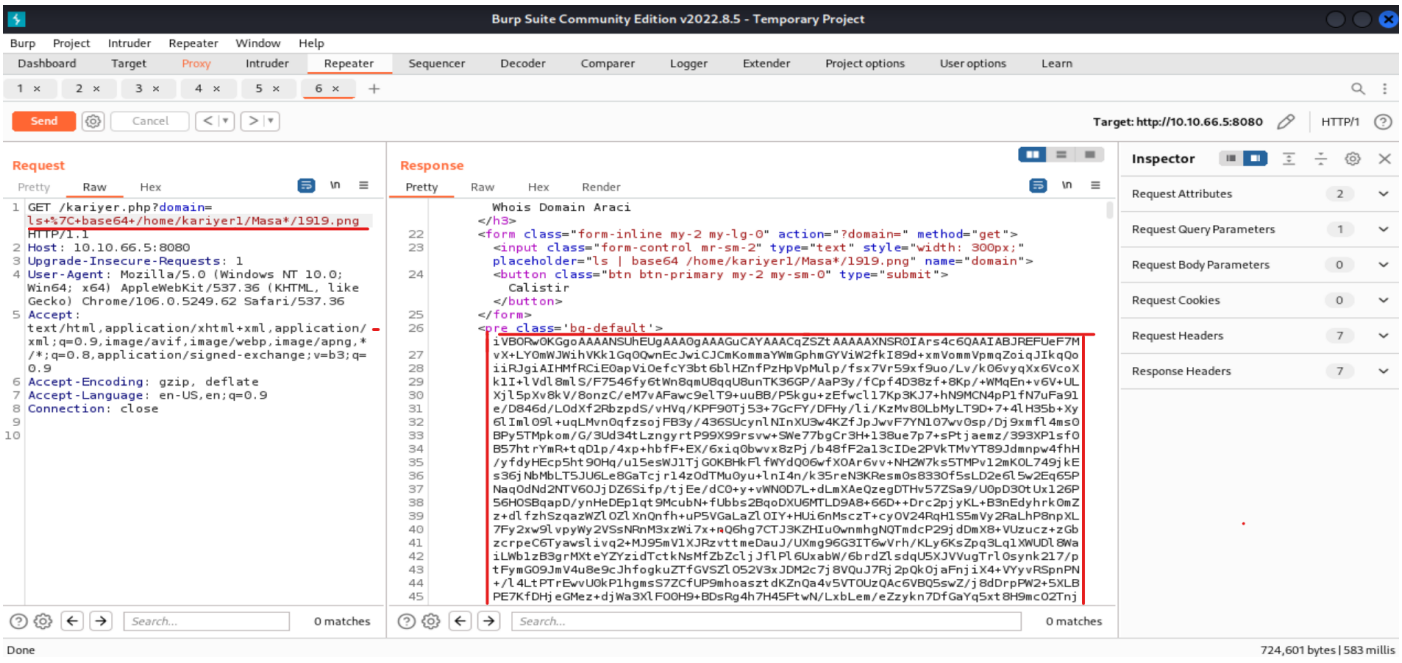
Kali linux de base64 un nasıl yapıldığına bakalım.



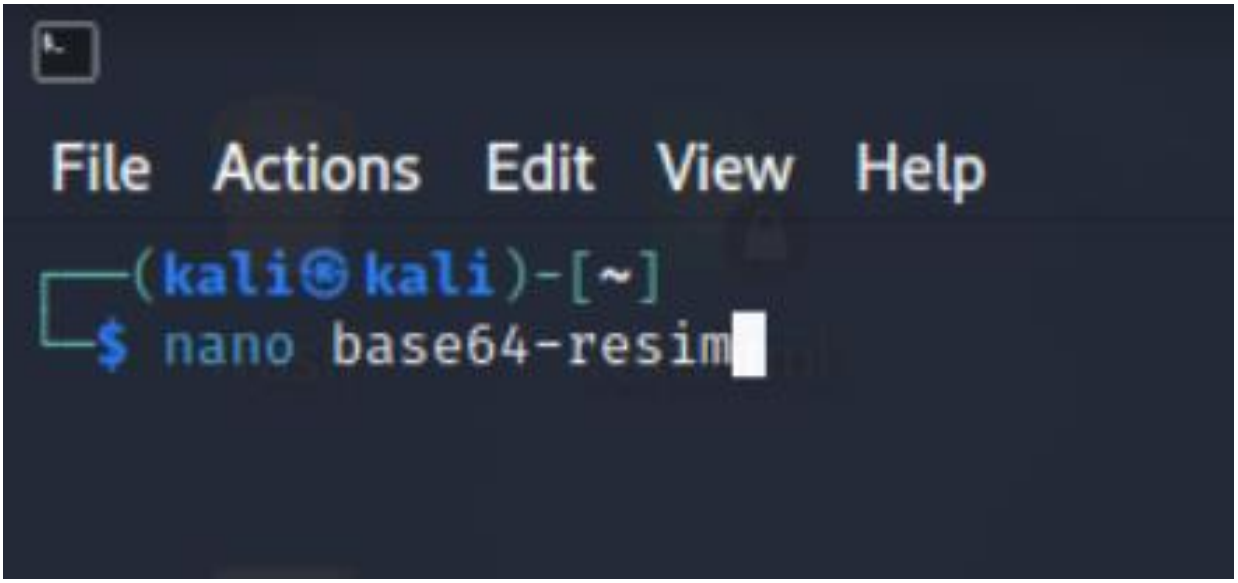
Dediğimiz zaman base64’ün komutlarını görebiliriz.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nano text.html

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat text.html
emre

┌──(root㉿kali)-[/home/kali/Desktop]
└─# base64 text.html
ZW1yZQoK

┌──(root㉿kali)-[/home/kali/Desktop]
└─# sS
```

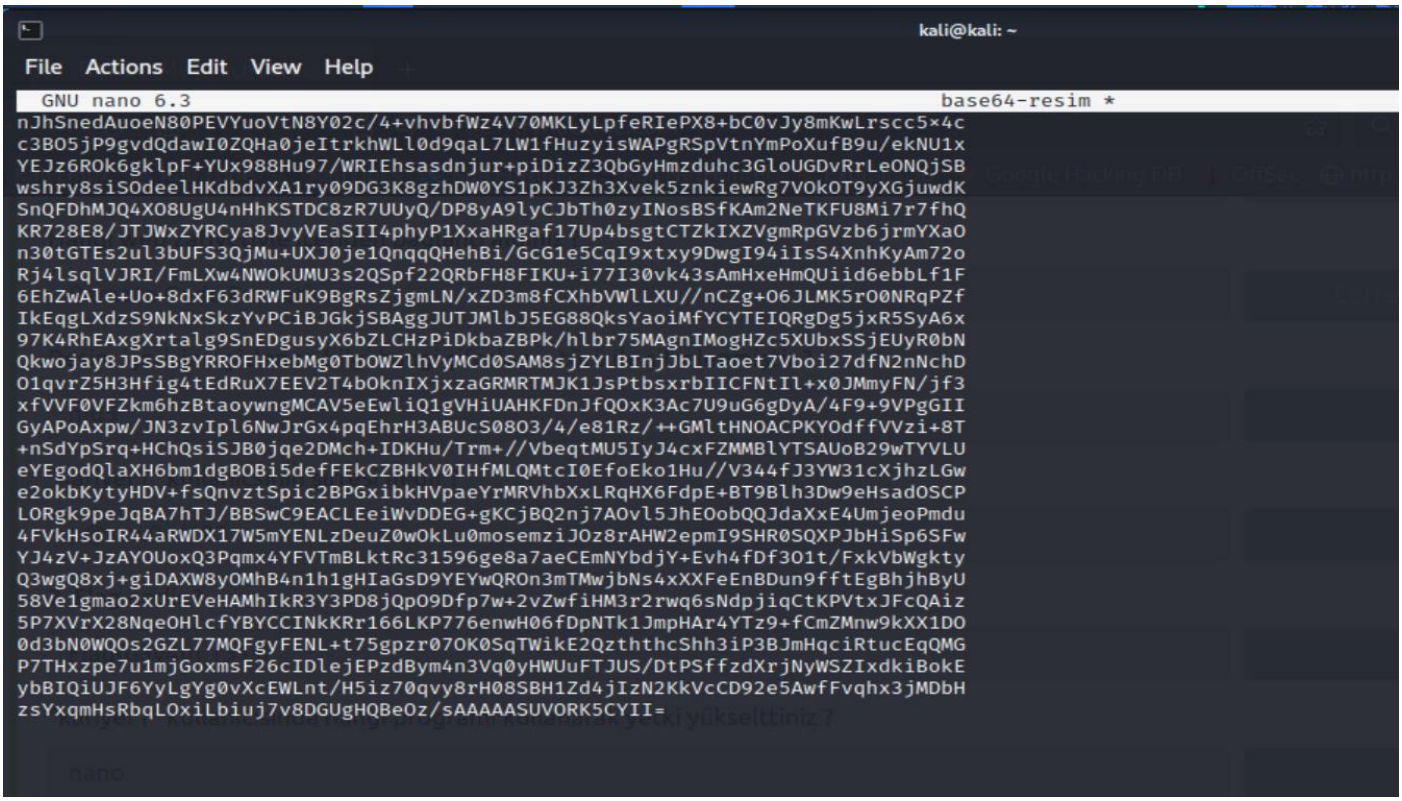
Burada base64 ün çalışma prensibini görüyoruz.
Aynı şeyi bir de resmimizin içinde deneyelim.

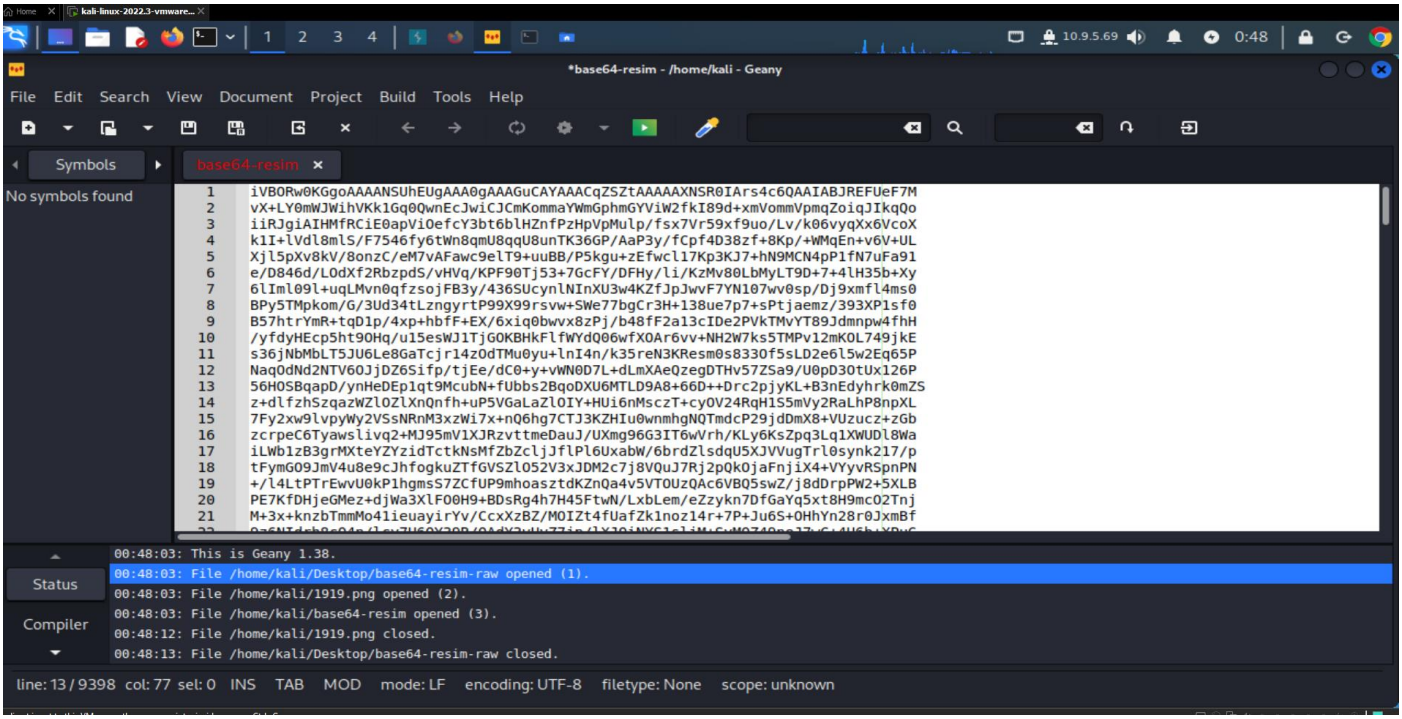


Yukarıda base64 modunda almamızın sebebi kendi bilgisayarımıza kaydetmek için kopyalıyoruz ve ardından,



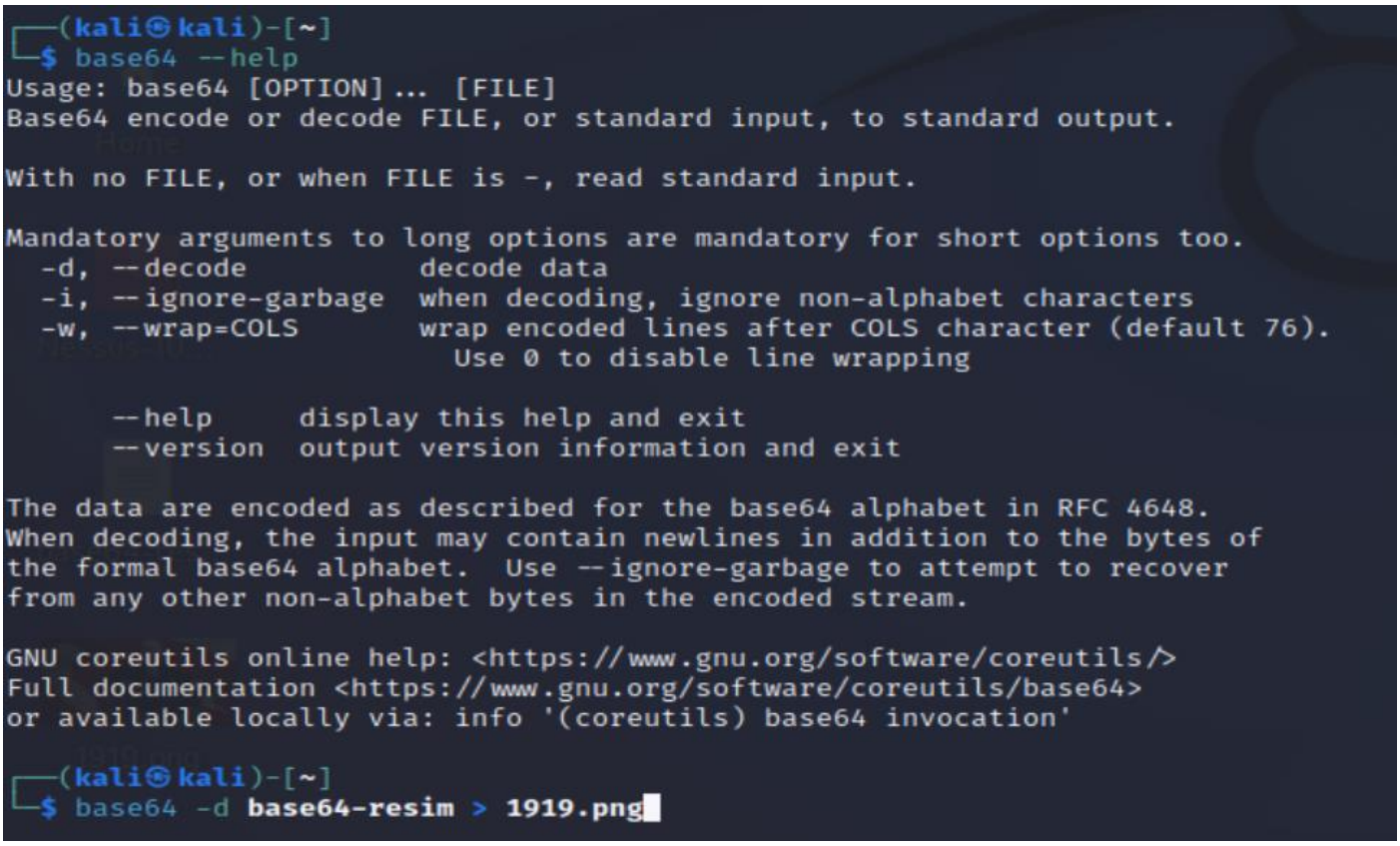
Dediğimizde Çıkan pencereye kaydetmiş olduğumuz base64 kodunu kopyalıyoruz.





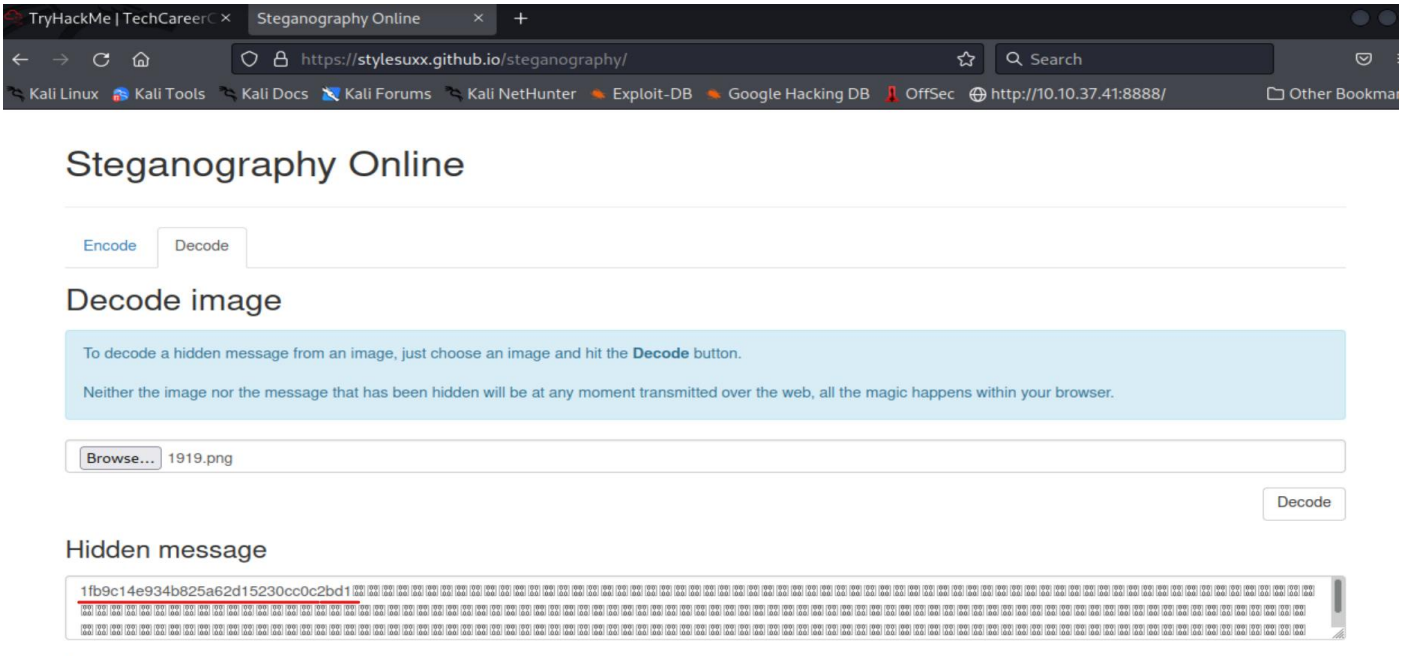
Resmimiz base64 kodu olarak kaydettik şimdi ise bunu png formatına dönüştürelim.

Ve ardından kali terminalimizi açarak.



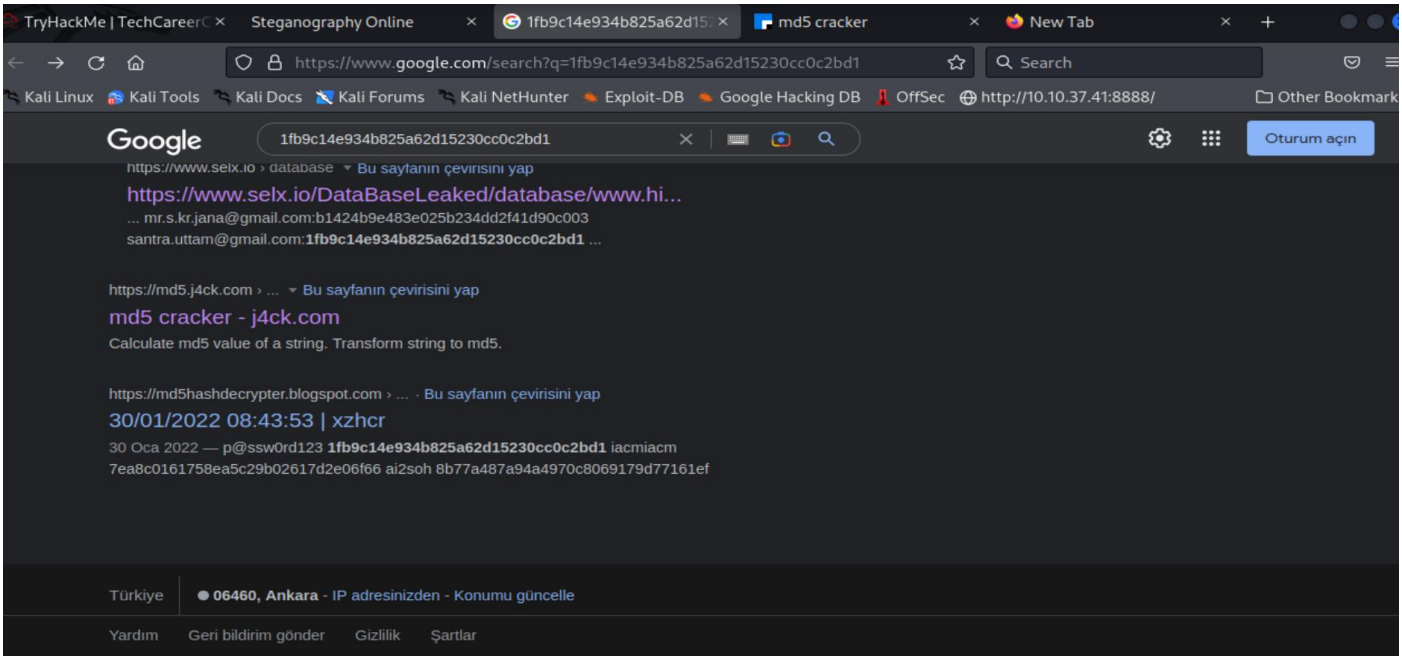
Bilgisayarımıza resmimizi kaydetmiş bulunuyoruz.

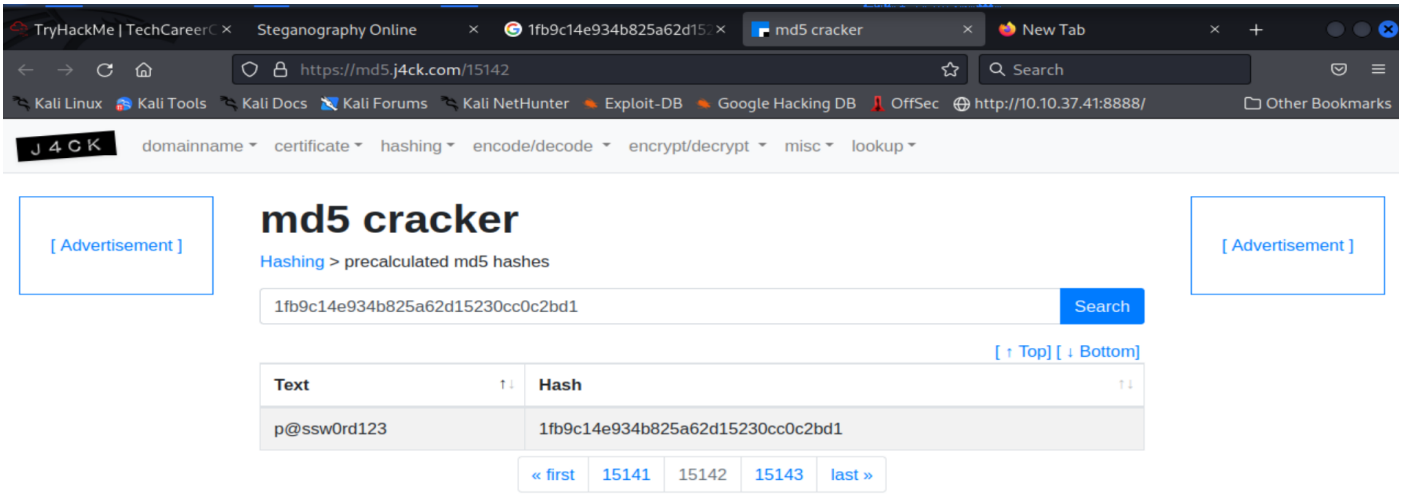
Steganography'sini çözebilmek için onlie Steganography sitelerine resmimizi yüklüyoruz.



Burada bize kod veriyor bunun ne olduğunu anlamamız gerekiyor…

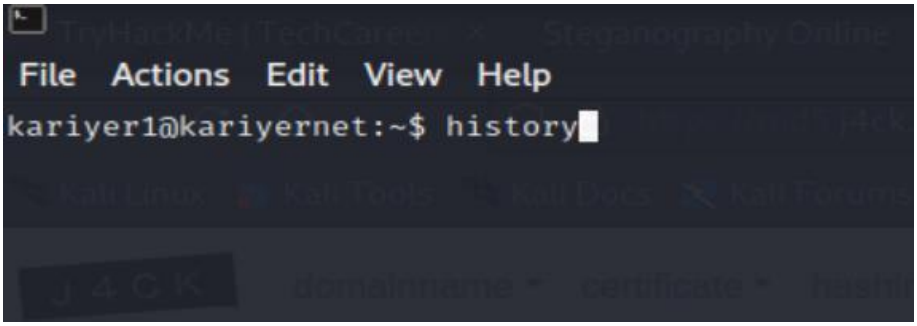
Kopyaladığımız kodu Google da arattığımızda…



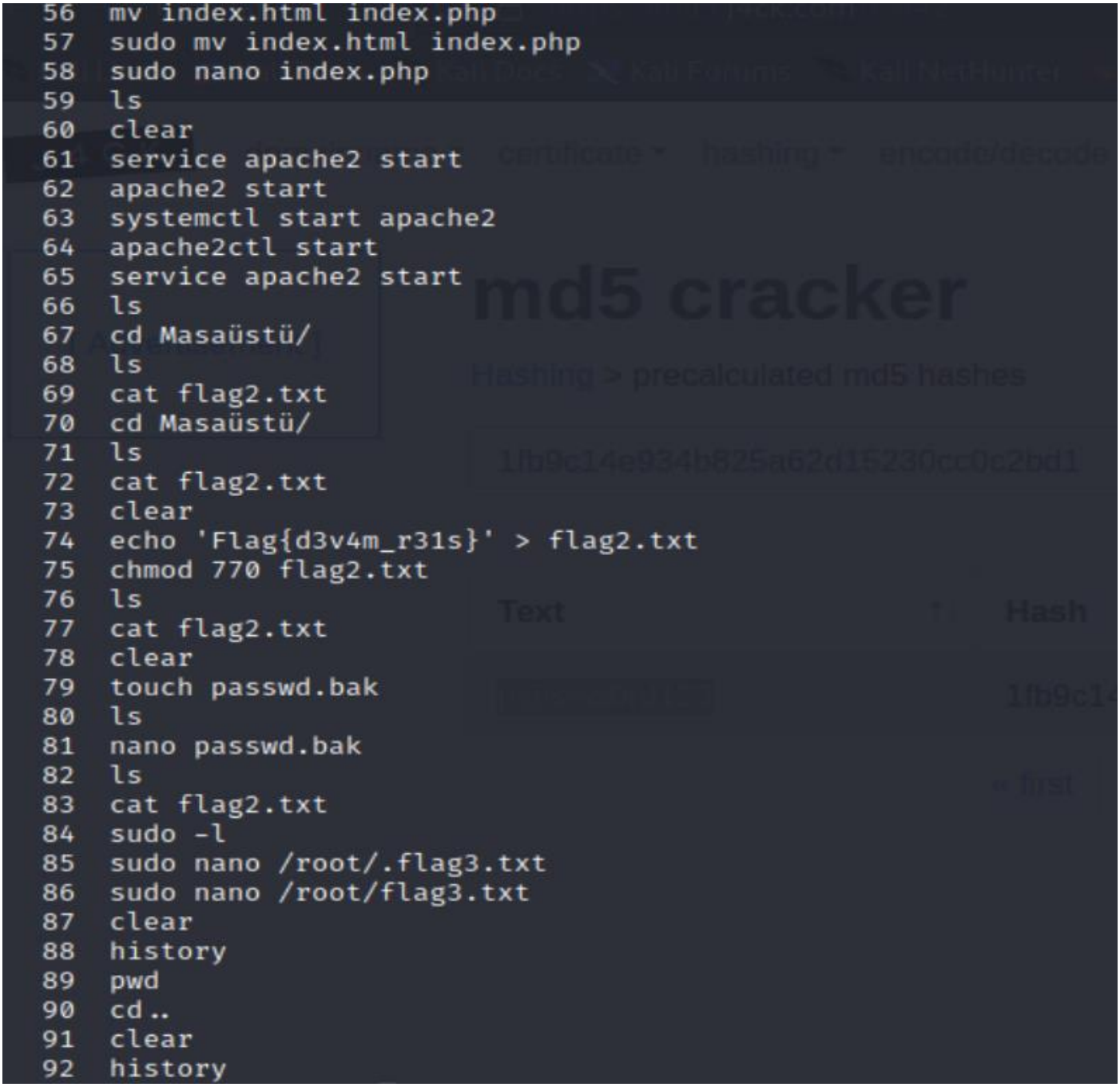


Kariyer1 kullanıcımızın Şifresine erişmiş oluyoruz…

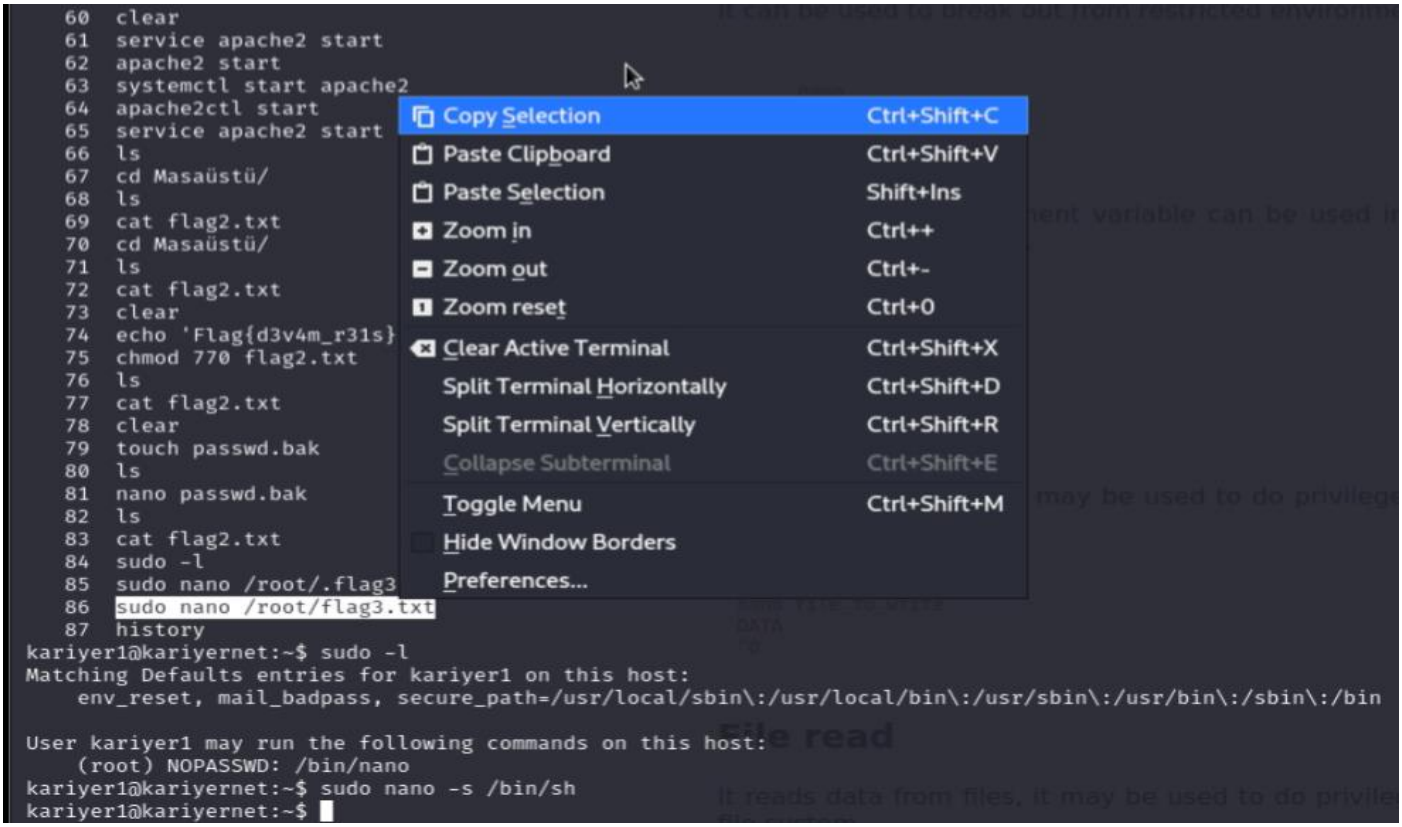
5)2.Flag nedir?



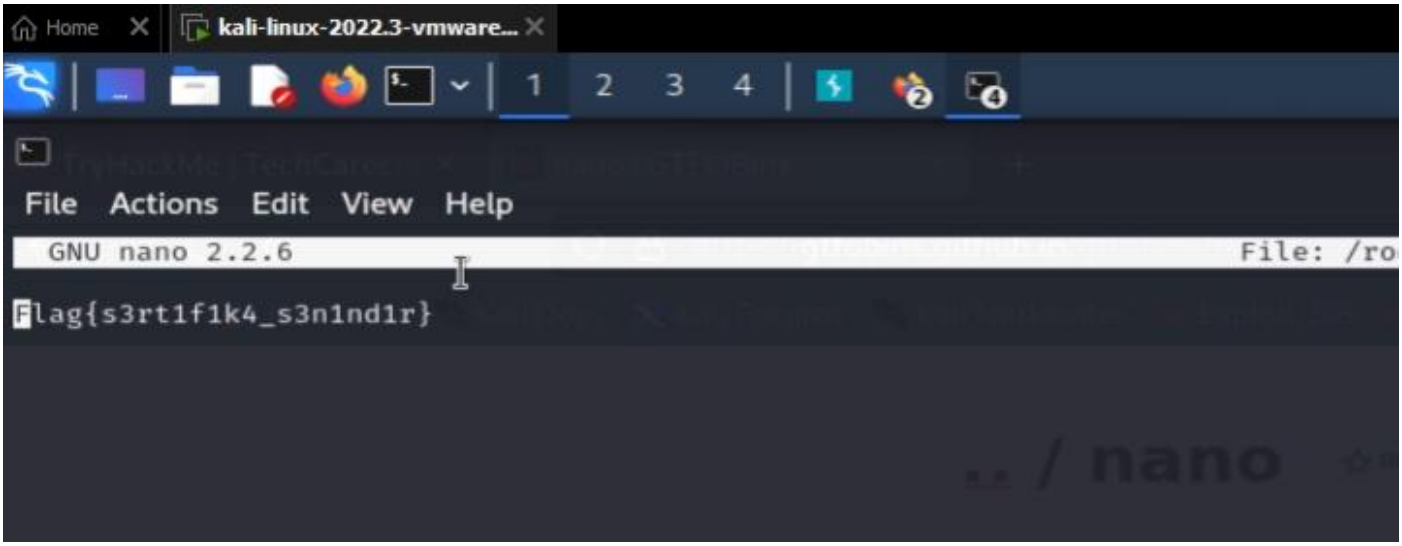
Yazdığımız zaman bize bilgisayarın geçmişini veriyor.



Kariyer1 kullanıcısını nano ile yetki yükseltiyoruz.



Kopyalayarak açtığımızda flag direk karşımıza çıkıyor.



Umarım kolay ve anlaşılır bir sunum olmuştur…