Exploiting SQL Injection (A03:2021)

1. Type the command on your terminal:

```
sudo docker run --rm -it -d -p 127.0.0.1:8080:80 vulnerables/web-dvwa:patched
```

And press Enter to run the DVWA web application in the docker.

2. Click on the Firefox ESR (Browser) icon to launch the browser.
In the address type *127.0.0.1:8080* and Enter to open the DVWA web application that is running on port number 8080.

3. In the Username field, (DVWA) enter *admin* and in the Password, field enter *password*.

4. Click on DVWA Security from the left column to open the page and from Security Level section, make sure that the security level is on Low and then click Submit.

5. Click on SQL Injection from the left column to open the vulnerability: SQL Injection page.

6. In the User ID input field, type 1 and click on Submit and you will see that the ID, first name and surname will be reflected.

7. Now type ’’’

~In the input field & click on submit.
~You will get an error page with an error message, from which we can understand that this web application uses MariaDB and that we can use ’ character to balance our query.

8. Go back to the DVWA page and type ***’ or 1=1#*** in the input field and click on

submit. This query is injected to bypass authentication where 1=1 means true and # is used to comment so that the injected query is not identified. By doing this we got the user information of this web application.

9. Type ***'union select null#*** in the input field and click on Submit. This query gives us an error message through which we can understand that there is more than 1 column.

10. Go back to the DVWA page and type:
'union select null,null#
,in the input field and click on Submit. This query gives us an output through which we understand that there are 2 columns.

11. Type: ***'union select @@version,@@hostname#***
in the input field and click on Submit. This query gives us the version and hostname information about the database.

12. Type ***'union select user(),database()#***
in the input field and click on submit. This query gives us the username and the database name of this web application.

13. Type: ***'union select null, table_name from information_schema.tables#***
in the input field and click on submit. This query gives us the list of table names from the database.

14. Now we shall try to find more information about the users table. For this, type:
'union select null, column_name from information_schema.columns where table_name='users'#
in the input field and click on submit. This query will give us the list of column names from the users table.

15. Type **' union select concat(user_id,0x0a,first_name,0x20,last_name),concat(user,0x3a,password) from users#** in the input field and click on **Submit**. This query will give us the list of

the user's information like the user ID, first name, last name, username and password.

Here **0x0a** means **new line**, **0x20** means **space** and **0x3a** means **semicolon**.

16. We can see that the password is saved in hashes. To crack these hash values, copy all the usernames with the hashed passwords one by one and paste them into a text editor. Click on the **Text Editor** icon to launch the text editor.

17. Now paste all the values here one by one.