Ethical Hacker 6 – SQL Injection

* **A lot of interesting MySQL challenges are available where you can to 'create' programming code containing SQL statements.**
  + **DVWA - SQL injection & Blind SQLi (style 1) -> Objective: There are 5 users in the database, with id's from 1 to 5. Your mission... to steal their passwords (hashes) via SQLi.**

Performing an injection attack to get all 5 users: the data in a form is between ‘’ these characters. If one of them is typed in the form, it counts as the end of the message. What goes after is considered actual code and it will be executed. If an information that is always true, such as 1=1, all information will be displayed:

Table

Description automatically generated with medium confidence

Figuring out the number of columns: using the same technique, typing an SQL command after the ‘ character, it will be executed.

Shape

Description automatically generated with medium confidence

In this instance, the table has 2 columns.



Typing the command below inside the textbox will generate this information:

**' UNION SELECT user, password FROM users#**

A picture containing text

Description automatically generated

**Resources:**

* <https://portswigger.net/web-security/sql-injections>