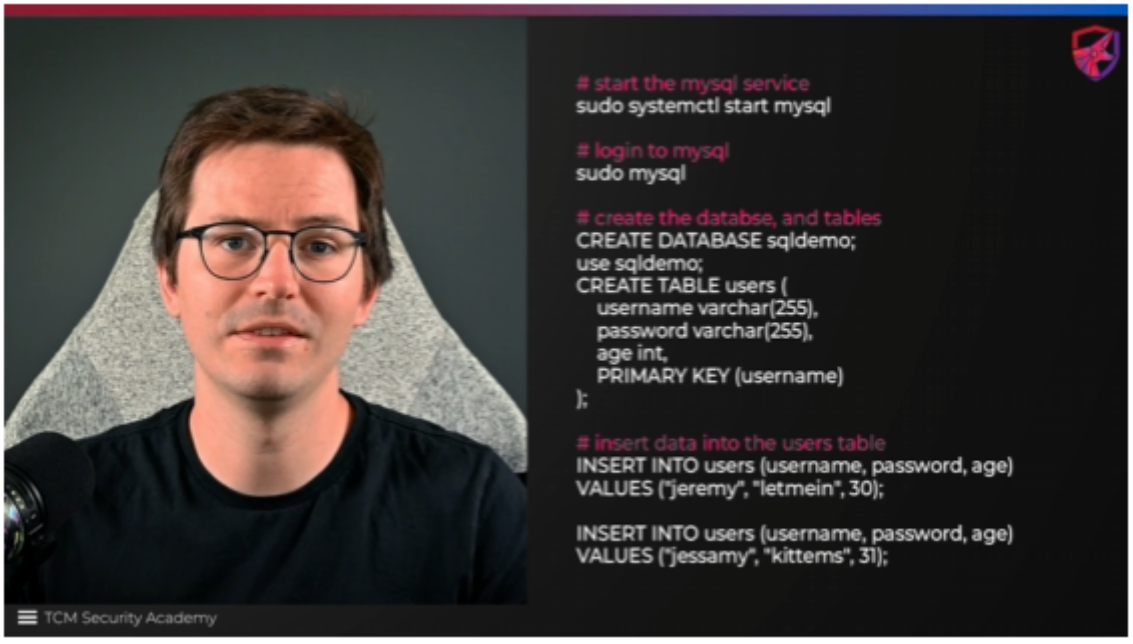
01 - SQL Injection - Intro

The concept is pretty straight forward. We inject SQL code to bypass authentication mechanisms, to dump the data from the database and possibly get more info on users and passwords as well. In some instances, we can also manipulate the database, by injecting users and passwords so we can get an initial access. Here, the input field being tested needs to be retrieving data through SQL, meaning it is going to query the database using SQL code. If the website in scope is using NoSQL databases, or other ones, than this attack will not work. This is SQL Injection.




```
MariaDB [sqldemo]> select age from users where username = "jeremy" or username = "jessamy";
+-----+
| age |
+-----+
|  30 |
|  31 |
+-----+
2 rows in set (0.000 sec)

MariaDB [sqldemo]> select age from users where username = "jeremy" union select password from users;
+----------+
| age      |
+----------+
| 30       |
| letmein  |
| kittens  |
+----------+
3 rows in set (0.001 sec)

MariaDB [sqldemo]>
```

Notice here in the example above, we new there was a user named jeremy, and then we were able to pull data relating to another username. Never though about doing this. As long as the initial statement is true, and there is an username named jeremy, then we can add more data to that output.

Notice in the second SQL query, we ask for a user we know, and then because there is a field called "password" in the "users" table, we retrieve all the passwords that were stored in there.