# OWASP - SQL Injection Exercises

## **Input Validation and Representation**

This is a short practical exercise to demonstrate **SQL Injection.**

This tutorial has been taken from : [How SQL Injection Works](https://www.guru99.com/learn-sql-injection-with-practical-example.html#2) However the code in the example doesn’t work, so I have modified it here.

Create your own database and create the following table :

**-- INIT database**

**CREATE TABLE users (**

**id INT AUTO\_INCREMENT KEY,**

**email VARCHAR(100),**

**password VARCHAR(255)**

**);**

**INSERT INTO users(email, password) VALUES ('maria@atu.ie', md5('123abc#'));**

**INSERT INTO users(email, password) VALUES ('mandy@atu.ie', md5('123def#'));**

**INSERT INTO users(email, password) VALUES ('pauric@atu.ie', md5('456abc#'));**

**-- QUERY database**

**SELECT \* FROM users;**

Note the output - This will return **ALL** users in the database, if you want a specific user then the command would be: (Replace the last line)

**SELECT \* FROM users WHERE email = 'maria@atu.ie' AND password = md5('123abc#');**

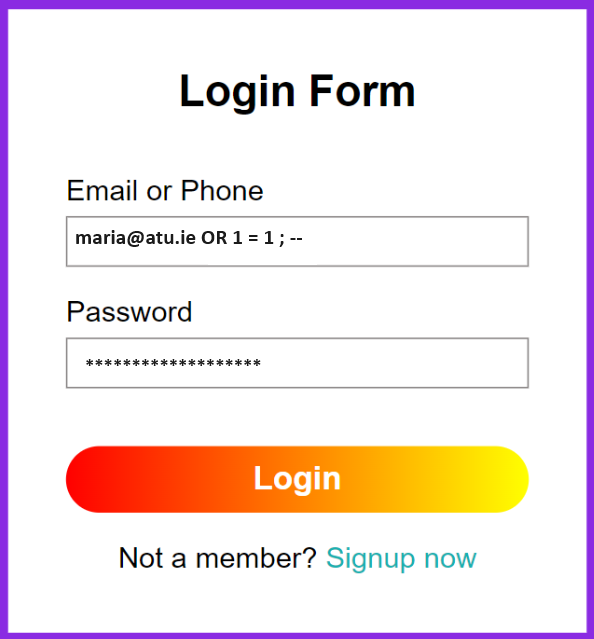
This will just return the user [maria@atu.ie](mailto:maria@atu.ie).

As per the lecture this SQL command can be exploited, if I add : **OR 1 = 1; --**

The equation will always evaluate to true and the two dashed lines (--) signify a comment so everything after that will be ignored. Replace your select command with the line below and it will return **all** users from the database.

**SELECT \* FROM users WHERE email = 'maria@atu.ie' OR 1 = 1; -- AND password = md5('123abc#');**

How does this work in the real world?



* These three sections may help with your understanding and have other tutorials for you to practice:
  + Read: [Automation Tools for SQL Injection](https://www.guru99.com/learn-sql-injection-with-practical-example.html#5)
  + Read: [How to Prevent against SQL Injection Attacks](https://www.guru99.com/learn-sql-injection-with-practical-example.html#6)
  + Activity: [Hacking Activity: SQL Inject a Web Application](https://www.guru99.com/learn-sql-injection-with-practical-example.html#3)
  + Activity: [Hacking Activity: Use Havji for SQL Injection](https://www.guru99.com/learn-sql-injection-with-practical-example.html#7)