**Input Sanitization & SQL Injection**

**Instructions:**

1. **MySQL DBMS**
   1. For these assessments, you need to sanitize user input using MySQLi special escape string function.
   2. Table users will have following properties:
      1. First Name
      2. Last Name
      3. Email
      4. Password
      5. Phone Number
      6. Created At
      7. Updated At
   3. Submit form from first\_page.php, Pass through proper validations as we have done in our previous assignments, and then write an SQL query for insert.

**Sample input**

First\_page.php contains a simple webform

Form should be submitted to second\_page.php and data should be sanitized first before we save into MySQL

**Sample Output**

* Users table should have entries when the form is submitted.
* Users table should not have entries of following reserved keywords:
* SELECT, DELETE, INSERT, UPDATE \*, ; and other special characters.