# PHP Homework Assignment: Fixing SQL Injection Vulnerabilities

**Objective:** Learn how to identify and fix SQL Injection vulnerabilities in PHP code by improving a given form that is susceptible to such attacks.

**Assignment Overview:** In this assignment, you will be provided with a PHP script that contains a form handling code. The current implementation is vulnerable to SQL Injection. Your task is to analyze the code, identify the vulnerabilities, and implement the necessary fixes using prepared statements.

### Part 1: Understanding SQL Injection

**Step 1: Research SQL Injection**

* Understand what SQL Injection is, how it works, and the potential risks associated with it.
* Explore common methods used to prevent SQL Injection in PHP.
* Reference the [Demonstration](https://slccbruins.sharepoint.com/:f:/s/ITComputerApplicationCurriculumDevelopment/Eh-oLtUNqhRDnl9C0wUxzIwBgc6ZNXXIOiJEfjuUh3XKvw?e=dU1AiD).

**Step 2: Identify Vulnerable Code**

* Review the provided PHP script and identify where the SQL Injection vulnerabilities exist.

### Part 2: Fixing the Vulnerabilities

**Step 3: Fix the Code**

* Refactor the code to use prepared statements and parameterized queries to prevent SQL Injection.

**Step 4: Test the Fixed Code**

* Test your refactored code to ensure that the SQL Injection vulnerabilities have been eliminated.

### Assignment Instructions

1. **Identify Vulnerabilities:**
   * Identify why the $sql statement in the provided script is vulnerable to SQL Injection.
2. **Refactor the Code:**
   * Refactor the provided script to use prepared statements.
   * Ensure that the user inputs are properly sanitized and secured.
3. **Testing:**
   * Use the provided test cases below to verify that the SQL Injection vulnerability has been fixed.
   * Test with different inputs, including those that would previously exploit the vulnerability.

### Test Cases

**Valid Input:**

* username: testuser
* password: testpassword
* **Expected Result:** "Login successful!"

**Invalid Input:**

* username: wronguser
* password: wrongpassword
* **Expected Result:** "Invalid username or password."

**SQL Injection Attempt:**

* username: ' OR '1'='1
* password: ' OR '1'='1
* **Expected Result:** "Invalid username or password."

### Submission

Submit the following:

* The refactored PHP script with comments explaining the changes made.

By completing this assignment, you will gain practical experience in identifying and mitigating SQL Injection vulnerabilities, ensuring the security of your PHP applications.