Lab Exercise sql-injection

This is a lab exercise on developing secure software. For more information, see the introduction to the labs.

1. Goal

Practice constructing parameterized statements to prevent SQL injection attacks.

2. Background

Parameterized statements are used to prevent SQL injection attacks by seperating SQL code from its data inputs. Parameterized statements are SQL queries which utilize place holders instead of directly embedding user inputs into a query. This prevents queries from being injected with malicious code.

3. Task Information

In this lab, you will study and modify code relating to SQL injection attacks. You will answer a couple of questions related to prepared/parameterized statements.

Use the “hint” and “give up” buttons if necessary.

4. Interactive Lab (COMPLETE!)

Looking at the following example code in Java, we can see that this is an example of vulnerable code. (This example was taken directly from the Secure Software Development Fundamentals course content.) Rewrite these statements so this sequence uses a prepared statement (a kind of parameterized statement). In the first part, create variable named `pstmt` of type `PreparedStatement`. In the second part, use `setString` to set what we're searching for, and put the results in a variable named `results` with type `ResultSet`. Use `executeQuery` to execute the query, since in this case we want a collection of results.

```
  // Prepare to execute a query.
  String QueryString
    "select * from authors where lastname =?";
  PreparedStatement pstmt =
connection.prepareStatement(QueryString);
```

```
   // Execute the query.
pstmt.setString(1,search_lastname);
ResultSet results = pstmt.executeQuery();
```

Hint Reset Give up

This lab was developed by Elijah Everett, Jeremiah Howard, and Emily Lovell as part of the Contributor Catalyst Program, as well as by David A. Wheeler.

Completed 2025-02-24T22:01:29.256Z 41335fb8-5538-48be-b635-5e0cecd67236 0pacjji0ysyaps