Secure coding practices prescribe that queries need to be parameterized. Concatenation of parameters is not recommended.
To create a parameterized query, replace all variables with `?` placeholders. Then create a Prepared Statement and use methods from this class to bind any parameter variables.

Before

```
Statement stmt = conn.createStatement();
        String query = "SELECT * FROM user WHERE username = "+ username;
        return stmt.executeQuery(query)
```

After

```
PreparedStatement stmt = conn.prepareStatement(query);
        String query = "SELECT * FROM user WHERE username = ?";
        stmt.setString(1, username);
        return stmt.executeQuery()
```

Violating this guideline can cause

- Injection Flaws - SQL Injection. Learn more