Abstract

Secure coding practices prescribe that queries need to be parameterized. Concatenation of parameters is not recommended.

Description

A parameterized query needs to be build first. Next, the parameter variables should be added. The following functions can be used to achieve this securely. These functions can be used to execute queries against the database.

Class information:

```
package java.sql.Connection
   PreparedStatement prepareStatement(String sql);
package java.sql.PreparedStatement
   void setString(int parameterIndex, String x);
   void setBigDecimal(int parameterIndex, BigDecimal x);
```

Correct code example:

```
import java.sql.*;
...
PreparedStatement prepStatement;
Connection connection;
...
String query="SELECT * from db where name = ?";
prepStatement=connection.prepareStatement(query);
prepStatement.setString( 1, name);
resultSet=prepStatement.executeQuery();
```

Violating this guideline can cause

Mobile vulnerabilities

- Client Side Injection - SQL Injection. Learn more

Web vulnerabilities

- Injection Flaws - SQL Injection. Learn more

Sensei quick fix

Use the **Sensei® Quick Fix technology: Hit Alt+Enter** to fix this guideline violation automatically.