

Security Review Process

Bad



```
String query =
```

```
"SELECT account_balance FROM user_data WHERE user_name = " +  
request.getParameter("customerName");
```

Good



```
String query =
```

```
"SELECT account_balance FROM user_data WHERE user_name = ? ";  
PreparedStatement pstmt = connection.prepareStatement( query );
```