

SQL Injection

Angriff auf die Datenbank

Funktionsweise

LogIn

USERNAME: *user0*

PASSWORD: *pw0*

```
"SELECT * FROM ACCOUNT WHERE NAME='"+username+"' AND PASSWORD='"+password+"'"
```

Ergebnis

```
'SELECT * FROM ACCOUNT WHERE NAME='user0' AND PASSWORD='pw0'
```

=

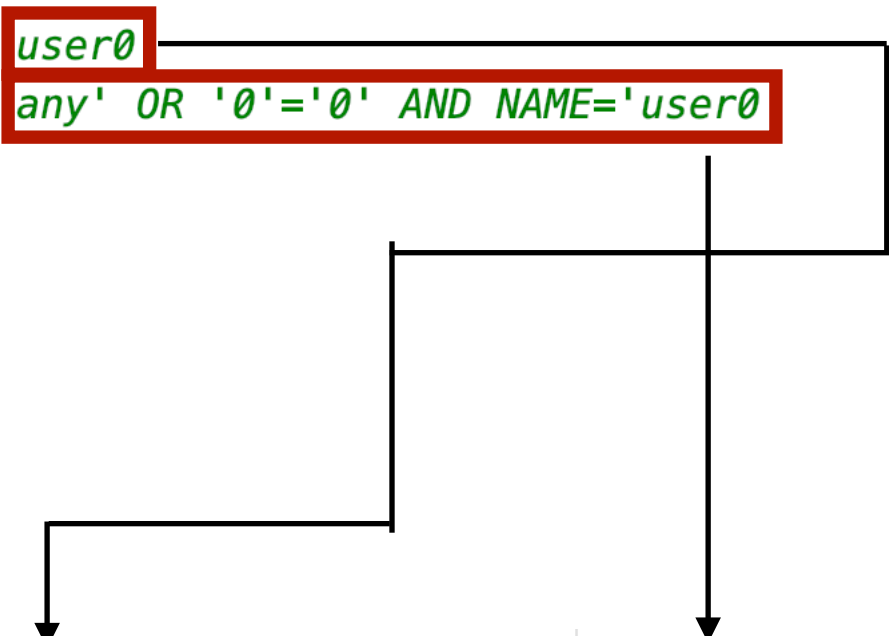
ResultSet
Name: user0
Password: pw0

Problem

LogIn

USERNAME: *user0*

PASSWORD: *any' OR '0'='0' AND NAME='user0*



```
"SELECT * FROM ACCOUNT WHERE NAME=" + username + "' AND PASSWORD=" + password + "'"
```

Ergebnis

```
"SELECT * FROM ACCOUNT WHERE NAME='user0' AND PASSWORD='any' OR '1'='1' AND NAME='user0|'"
```

=

ResultSet
Name: user0
Password: pw0

Problemlösung

Prepared Statements

```
PreparedStatement statement = conn.prepareStatement( sql: "SELECT * FROM ACCOUNT WHERE NAME=? AND PASSWORD=?");  
  
statement.setString( parameterIndex: 1, username);  
statement.setString( parameterIndex: 2, password);  
ResultSet resultSet = statement.executeQuery();
```