$$\begin{tikzcd}\boxed{\text{App}} \arrow[d, shift right] \\ \boxed{\text{DBMS}} \arrow[u, shift right]\end{tikzcd}$$

JDBC

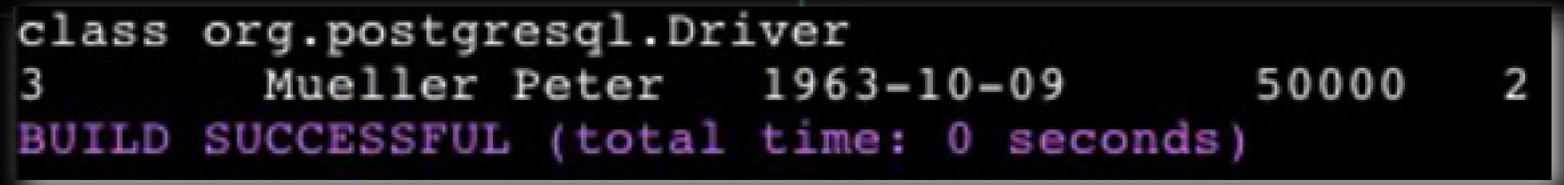
Postgres

```java
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.ResultSetMetaData;
import java.sql.SQLException;
import java.sql.Statement;

public class JDBCExample {

    public static void outputResultSet(ResultSet rset) throws SQLException{
        ResultSetMetaData rsmd = rset.getMetaData();
        final int numberOfColumns = rsmd.getColumnCount();
        while (rset.next()) {
            for (int i = 1; i <= numberOfColumns; i++) {
                System.out.print(rset.getObject(i) + "\t");
            }
            System.out.println();
        }
    }

    public static void main(String[] args) {
        Connection conn = null;

        try {
            System.out.println(Class.forName("org.postgresql.Driver"));
            conn = DriverManager.getConnection("jdbc:postgresql://localhost/Fotoagentur?user=postgres&password=.....");
        } catch (Exception e) {
            System.out.println("Fehler: " + e);
            System.exit(-1);
        }
        if (conn != null) {
            try {
                Statement sql_stmt = conn.createStatement();
                ResultSet rset = sql_stmt.executeQuery("select * from FotographenKomplett2");
                outputResultSet(rset);
                rset.close();
                conn.close();
            } catch (SQLException se) {
                System.out.println("Fehler: " + se);
            }
        }
    }
}
```

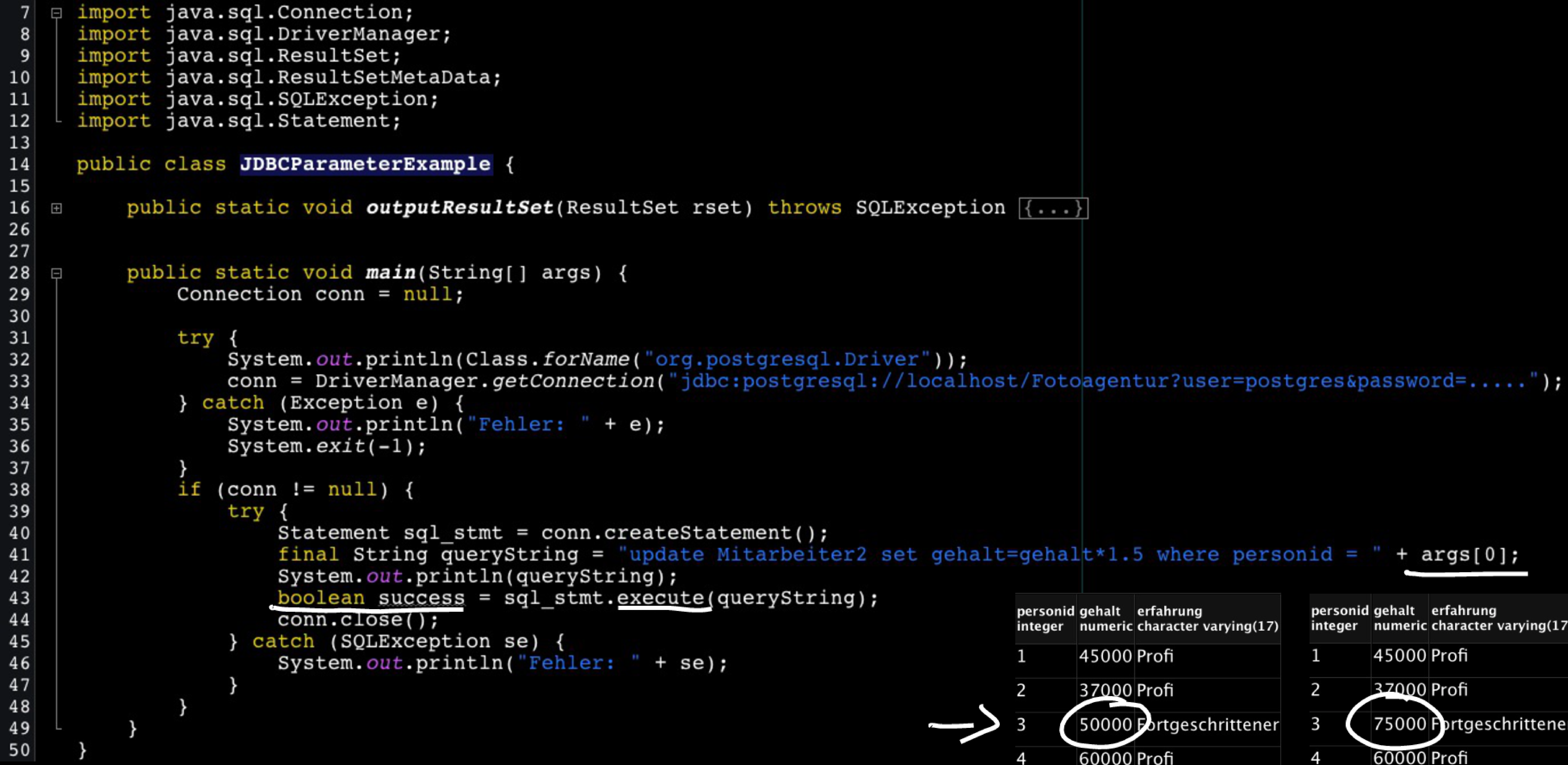
```
3       Mueller Peter   1963-10-09      50000   2
6       Wurst   Hans    1974-02-01      15000   1
7       Miese   Peter   1983-05-06      50000   2
42      Froehlich       Frida   1987-03-02      52000   2
77      Sorglos Lisa    1977-07-12      62000   3
34      Mueller Herta   1992-11-30      32000   1
BUILD SUCCESSFUL (total time: 0 seconds)
```

```java
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.ResultSetMetaData;
import java.sql.SQLException;
import java.sql.Statement;
import static jdbcexample.JDBCExample.outputResultSet;

public class JDBCParameterExample {

    public static void outputResultSet(ResultSet rset) throws SQLException {...}


    public static void main(String[] args) {
        Connection conn = null;

        try {
            System.out.println(Class.forName("org.postgresql.Driver"));
            conn = DriverManager.getConnection("jdbc:postgresql://localhost/Fotoagentur?user=postgres&password=.....");
        } catch (Exception e) {
            System.out.println("Fehler: " + e);
            System.exit(-1);
        }
        if (conn != null) {
            try {
                Statement sql_stmt = conn.createStatement();
                ResultSet rset = sql_stmt.executeQuery("select * from FotographenKomplett2 where id = " + args[0]);
                outputResultSet(rset);
                rset.close();
                conn.close();
            } catch (SQLException se) {
                System.out.println("Fehler: " + se);
            }
        }
    }
}
```

args[0] = 3

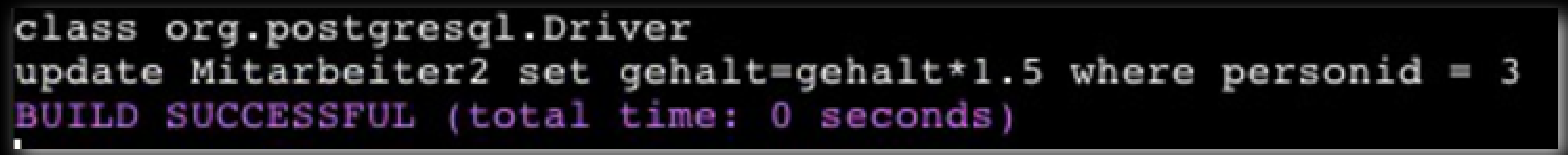


```
class org.postgresql.Driver
3        Mueller Peter    1963-10-09       50000    2
BUILD SUCCESSFUL (total time: 0 seconds)
```



```java
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.ResultSetMetaData;
import java.sql.SQLException;
import java.sql.Statement;

public class JDBCParameterExample {

    public static void outputResultSet(ResultSet rset) throws SQLException {...}


    public static void main(String[] args) {
        Connection conn = null;

        try {
            System.out.println(Class.forName("org.postgresql.Driver"));
            conn = DriverManager.getConnection("jdbc:postgresql://localhost/Fotoagentur?user=postgres&password=.....");
        } catch (Exception e) {
            System.out.println("Fehler: " + e);
            System.exit(-1);
        }
        if (conn != null) {
            try {
                Statement sql_stmt = conn.createStatement();
                final String queryString = "update Mitarbeiter2 set gehalt=gehalt*1.5 where personid = " + args[0];
                System.out.println(queryString);
                boolean success = sql_stmt.execute(queryString);
                conn.close();
            } catch (SQLException se) {
                System.out.println("Fehler: " + se);
            }
        }
    }
}
```

args[0] = „3“



```
class org.postgresql.Driver
update Mitarbeiter2 set gehalt=gehalt*1.5 where personid = 3
BUILD SUCCESSFUL (total time: 0 seconds)
```

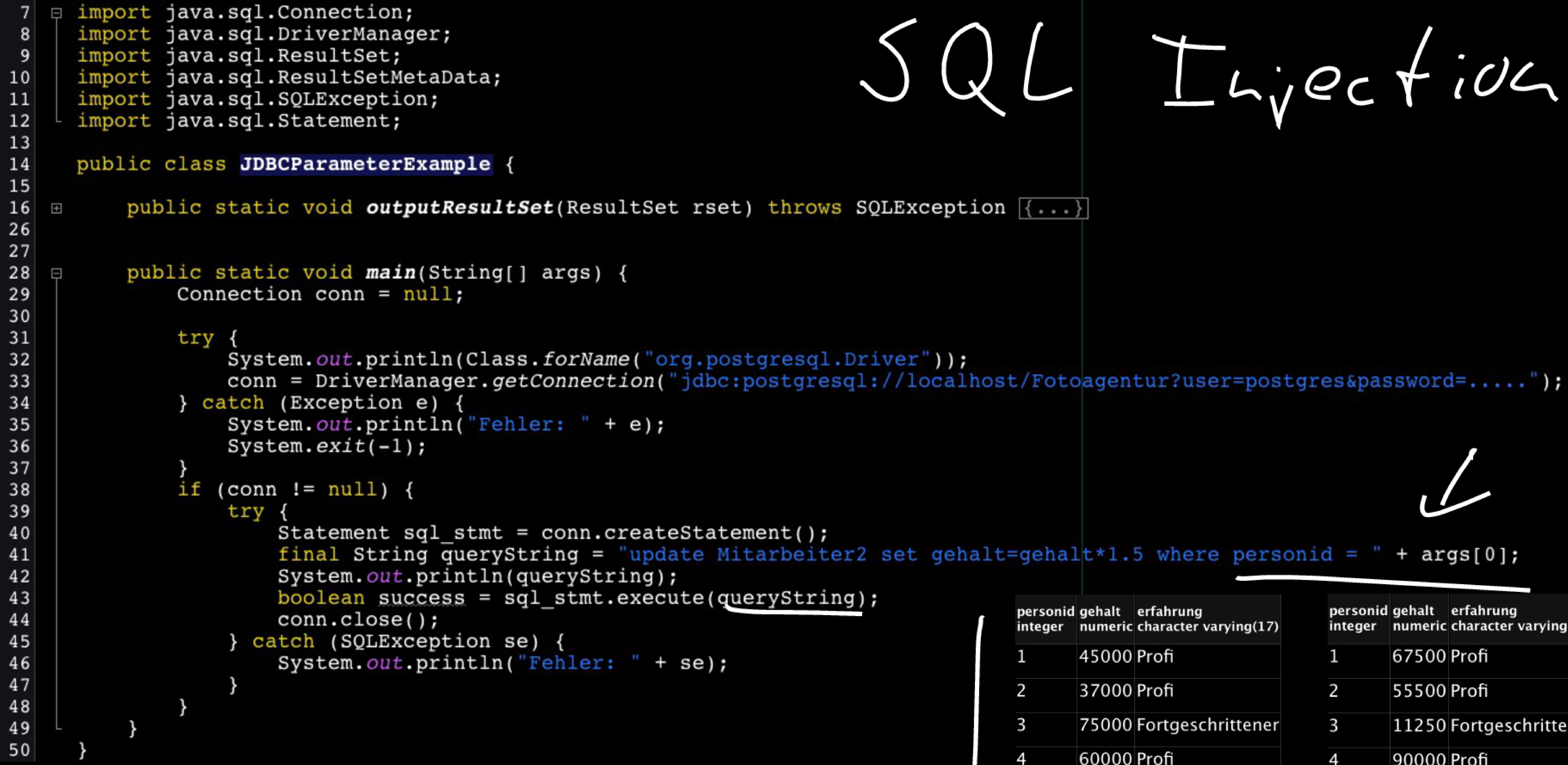
personid integer	gehalt numeric	erfahrung character varying(17)
1	45000	Profi
2	37000	Profi
3	50000	Fortgeschrittener
4	60000	Profi
5	55000	Fortgeschrittener
6	15000	Anfaenger
7	50000	Fortgeschrittener

vorher

personid integer	gehalt numeric	erfahrung character varying(17)
1	45000	Profi
2	37000	Profi
3	75000	Fortgeschrittener
4	60000	Profi
5	55000	Fortgeschrittener
6	15000	Anfaenger
7	50000	Fortgeschrittener

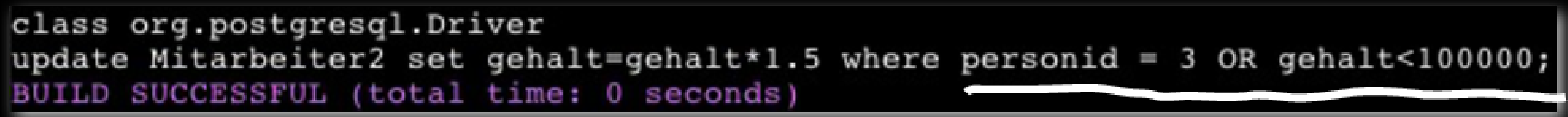
nachher

SQL Injection

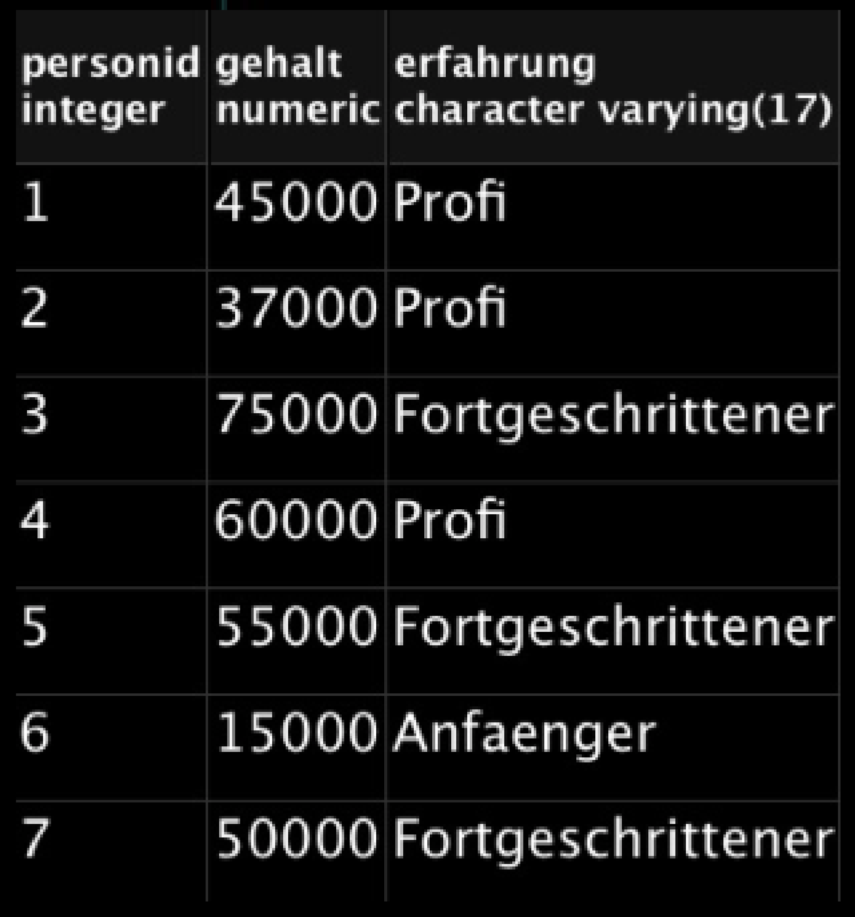


```java
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.ResultSetMetaData;
import java.sql.SQLException;
import java.sql.Statement;

public class JDBCParameterExample {

    public static void outputResultSet(ResultSet rset) throws SQLException {...}


    public static void main(String[] args) {
        Connection conn = null;

        try {
            System.out.println(Class.forName("org.postgresql.Driver"));
            conn = DriverManager.getConnection("jdbc:postgresql://localhost/Fotoagentur?user=postgres&password=.....");
        } catch (Exception e) {
            System.out.println("Fehler: " + e);
            System.exit(-1);
        }
        if (conn != null) {
            try {
                Statement sql_stmt = conn.createStatement();
                final String queryString = "update Mitarbeiter2 set gehalt=gehalt*1.5 where personid = " + args[0];
                System.out.println(queryString);
                boolean success = sql_stmt.execute(queryString);
                conn.close();
            } catch (SQLException se) {
                System.out.println("Fehler: " + se);
            }
        }
    }
}
```

args[0] = “3 OR gehalt<100000;“

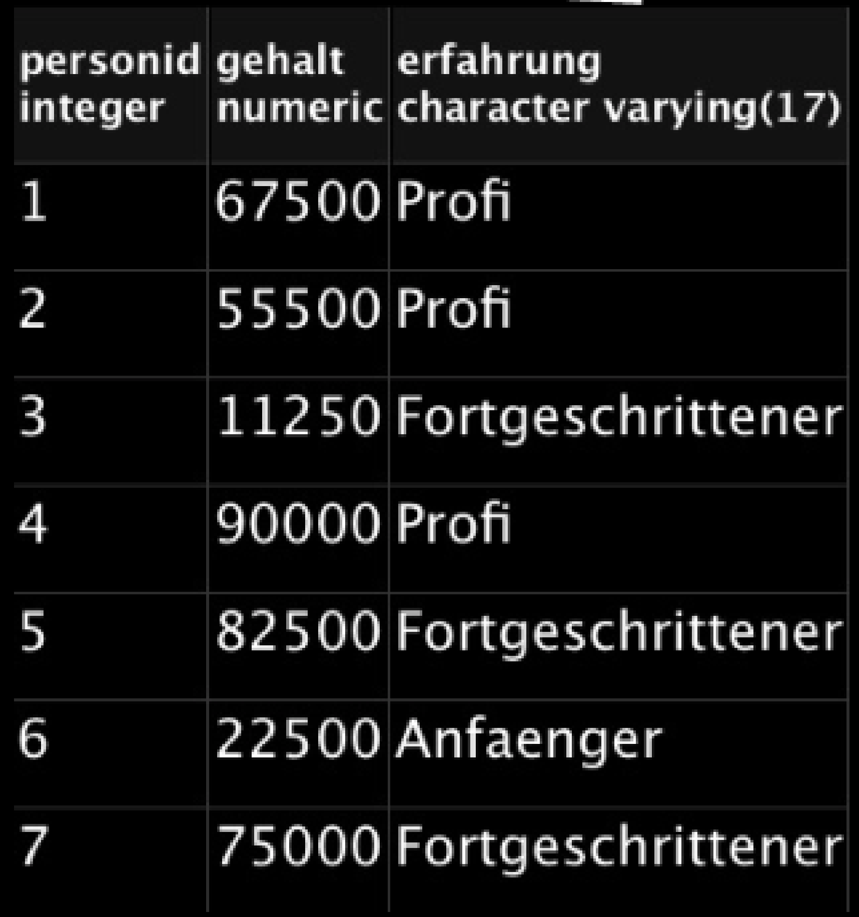


```
class org.postgresql.Driver
update Mitarbeiter2 set gehalt=gehalt*1.5 where personid = 3 OR gehalt<100000;
BUILD SUCCESSFUL (total time: 0 seconds)
```



personid integer	gehalt numeric	erfahrung character varying(17)
1	45000	Profi
2	37000	Profi
3	75000	Fortgeschrittener
4	60000	Profi
5	55000	Fortgeschrittener
6	15000	Anfaenger
7	50000	Fortgeschrittener

vorher



personid integer	gehalt numeric	erfahrung character varying(17)
1	67500	Profi
2	55500	Profi
3	11250	Fortgeschrittener
4	90000	Profi
5	82500	Fortgeschrittener
6	22500	Anfaenger
7	75000	Fortgeschrittener

nachher

Prepared Statements

```
DEALLOCATE        updateMitarbeiter2;
```

```
Abfrage war erfolgreich nach 19 ms. Keine Zeilen geliefert.
```

```
PREPARE           updateMitarbeiter2 (int) AS
     UPDATE            Mitarbeiter2 SET gehalt=gehalt*1.5
     WHERE             personid=$1;
```

```
Abfrage war erfolgreich nach 13 ms. Keine Zeilen geliefert.
```

```
EXECUTE showFotograph(3);
```

id integer	name character varying	vorname character varying	geburtsdatum date	gehalt numeric	erfahrung integer
3	Mueller	Peter	1963-10-09	50000	2

showFotograph ist hier ein zweites prepared statement, das einfach den Inhalt der Tabelle Mitarbeiter2 für eine bestimmte personid ausgibt. Um das eigentlich update für personid=3 auszuführen, muss ich natürlich EXECUTE updateMitarbeiter2(3) aufrufen.

```java
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.ResultSet;
import java.sql.ResultSetMetaData;
import java.sql.SQLException;

public class JDBCPreparedStatementExample {

    public static void outputResultSet(ResultSet rset) throws SQLException {...}

    public static void main(String[] args) {
        Connection conn = null;

        try {
            System.out.println(Class.forName("org.postgresql.Driver"));
            conn = DriverManager.getConnection("jdbc:postgresql://localhost/Fotoagentur?user=postgres&password=.....");
        } catch (Exception e) {
            System.out.println("Fehler: " + e);
            System.exit(-1);
        }
        if (conn != null) {
            try {
                PreparedStatement preparedStatement = conn.prepareStatement("select * from FotographenKomplett2 where id = ?"

                preparedStatement.setInt(1, 6);
                ResultSet rset = preparedStatement.executeQuery();
                outputResultSet(rset);

                //irgendwann später dann:
                preparedStatement.setInt(1, 42);
                ResultSet rset2 = preparedStatement.executeQuery();
                outputResultSet(rset2);

                rset.close();
                conn.close();
            } catch (SQLException se) {
                System.out.println("Fehler: " + se);
            }
        }
    }
}
```

```java
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.SQLException;

public class JDBCPreparedStatementExample2 {

    public static void main(String[] args) {
        Connection conn = null;

        try {
            System.out.println(Class.forName("org.postgresql.Driver"));
            conn = DriverManager.getConnection("jdbc:postgresql://localhost/Fotoagentur?user=postgres&password=.....");
        } catch (Exception e) {
            System.out.println("Fehler: " + e);
            System.exit(-1);
        }
        if (conn != null) {
            try {
                PreparedStatement preparedStatement = conn.prepareStatement("update Mitarbeiter2 set gehalt=gehalt*1.5 where personid = ?");

                preparedStatement.setInt(1, 6);
                preparedStatement.execute();

                //irgendwann später dann:
                preparedStatement.setInt(1, 42);
                preparedStatement.execute();


                conn.close();
            } catch (SQLException se) {
                System.out.println("Fehler: " + se);
            }
        }
    }
}
```

```
class org.postgresql.Driver
BUILD SUCCESSFUL (total time: 0 seconds)
```

```java
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.SQLException;

public class JDBCPreparedStatementExample2 {

    public static void main(String[] args) {
        Connection conn = null;

        try {
            System.out.println(Class.forName("org.postgresql.Driver"));
            conn = DriverManager.getConnection("jdbc:postgresql://localhost/Fotoagentur?user=postgres&password=.....");
        } catch (Exception e) {
            System.out.println("Fehler: " + e);
            System.exit(-1);
        }
        if (conn != null) {
            try {
                PreparedStatement preparedStatement = conn.prepareStatement("update Mitarbeiter2 set gehalt=gehalt*1.5 where personid = ?");

                preparedStatement.setInt(1, 6);
                preparedStatement.execute();

                //irgendwann später dann:
                preparedStatement.setInt(1, 42);
                preparedStatement.execute();

                //irgendwann später dann:
                preparedStatement.setString(1, "3 OR gehalt<100000;");
                preparedStatement.execute();


                conn.close();
            } catch (SQLException se) {
                System.out.println("Fehler: " + se);
            }
        }
    }
}
```

```
class org.postgresql.Driver
Fehler: org.postgresql.util.PSQLException: ERROR: operator does not exist: integer = character varying
  Hinweis: No operator matches the given name and argument type(s). You might need to add explicit type casts.
  Position: 58
BUILD SUCCESSFUL (total time: 0 seconds)
```