JUST DO IT
HÖHERE ABTEILUNG FÜR INFORMATIONSTECHNOLOGIE

tgm
Die Schule der Technik

# Arbeitsprotokoll

# JDBC

INSY MARM,ROSC
4CHIT 1617

Martin Wölfer

Version 0.2
Begonnen am 17. November 2016
Beendet am 29. November 2016

Betreuer: ROSC

# Inhaltsverzeichnis

# 1 Aufgabenstellung

- relevanter sourcecode
- Screenshot(s)
- Beispiel für mögliche sql injection, die durch Prepared Statements verhindert wird.

# 2 Source-Code

## 2.1 JDBCClient.java

```
1  package webshop;
2
3
4  import java.sql.Connection;
5  import java.sql.DriverManager;
6  import java.sql.PreparedStatement;
7  import java.sql.ResultSet;
8  import java.sql.SQLException;
9  import java.sql.Statement;
10 import java.util.ArrayList;
11 import java.util.List;
12
13 public class JDBCClient {
14
15     Connection con;
16
17     JDBCClient() throws SQLException{
18         //Initialize the connection with test user that has priviliges
19         this.con = DriverManager.getConnection("jdbc:postgresql://localhost:5432/webshop","test","test")
               ;
20     }
21     /***
22     * Makes an preparedStatemenent and then fills and ArrayList with Artikel
23     * @return List of all articles
24     * @throws SQLException
25     */
26     List<Artikel> getAllArticles() throws SQLException {
27         PreparedStatement pstmt = con.prepareStatement("SELECT * FROM artikel");
28         ResultSet rs = pstmt.executeQuery();
29
30         ArrayList<Artikel> rl = new ArrayList<>();
31         while(rs.next()){
32             int anr = rs.getInt("anr");
33             String abez = rs.getString("abez");
34             String ainfo = rs.getString("info");
35             Float preis = rs.getFloat("npreis");
36             int vstueckz = rs.getInt("vstueckz");
37             rl.add(new Artikel(anr,abez,ainfo,preis,vstueckz));
38         }
39         return rl;
40     }
41
42     /***
43     * Makes an preparedStatement and then inserts the desired article into the database with
           executeUpdate()
44     * @param a the desired article to be inserted into the database
45     * @throws SQLException
46     */
47     void addArticle(Artikel a) throws SQLException {
48         PreparedStatement ptsmt = con.prepareStatement("INSERT INTO artikel(anr,abez,npreis,vstueckz,
               info) values(?,?,?,?,?)");
49         ptsmt.setInt(1, a.getAnr());
50         ptsmt.setString(2, a.getAbez());
51         ptsmt.setFloat(3, a.getPreis());
```

 

```
        ptsmt.setInt(4, a.getVstueckz());
53      ptsmt.setString(5, a.getAinfo());
        ptsmt.executeUpdate();
55  }

57  /**
    * Makes an preparedStatement and then updates the desired article with the values
59  * @param a the article to be updated
    * @throws SQLException
61  */
    void saveArticle(Artikel a) throws SQLException {
63      PreparedStatement ptsmt = con.prepareStatement("UPDATE artikel SET anr=?,abez=?,npreis=?,
            vstueckz=?,info=? WHERE anr=?");
        ptsmt.setInt(1, a.getAnr());
65      ptsmt.setString(2, a.getAbez());
        ptsmt.setFloat(3, a.getPreis());
67      ptsmt.setInt(4, a.getVstueckz());
        ptsmt.setString(5, a.getAinfo());
69      ptsmt.setInt(6, a.getAnr());
        ptsmt.executeUpdate();
71  }

73  /**
    * Delete an article based on the primary key anr
75  * @param anr primary key which defines an article so it can be deleted
    * @throws SQLException
77  */
    void delArticle(int anr) throws SQLException{
79      PreparedStatement ptsmt = con.prepareStatement("DELETE FROM artikel WHERE anr=?");
        ptsmt.setInt(1, anr);
81      ptsmt.executeUpdate();
    }
83 }
```

## 2.2 ArtikelAdmin.java

Hier wurde lediglich ein löschen Button hinzugefügt welcher nur auf das `anr` input-Feld zugreift. Wenn der Button gedrückt wird, wird jedoch auch aus der Liste welche alle in der GUI vorhandenen Artikel besitzt der gewünschte mit der anr definierten Nummer Artikel aus der Liste genommen:

```
1   final Button delButton = new Button("Loeschen");
    delButton.setOnAction(new EventHandler<ActionEvent>() {
3       @Override
        public void handle(ActionEvent e) {
5           int anr = Integer.parseInt(addAnr.getText());
            for(int i = 0; i < data.size(); i++){
7               if(data.get(i).getAnr() == anr){
                    data.remove(i);
9               }
            }
11          try {
                db.delArticle(anr);
13          } catch (SQLException e1) {
                e1.printStackTrace();
15          }
            addAnr.clear();
17      }
    });
```

Und dieser Button muss noch hinzugefügt werden zu der GUI

```
hb.getChildren().addAll(addAnr, addAbez, addAinfo, addPreis, addVstueckz, addButton,delButton);
```

# 3 Screenshots

## 3.1 GUI

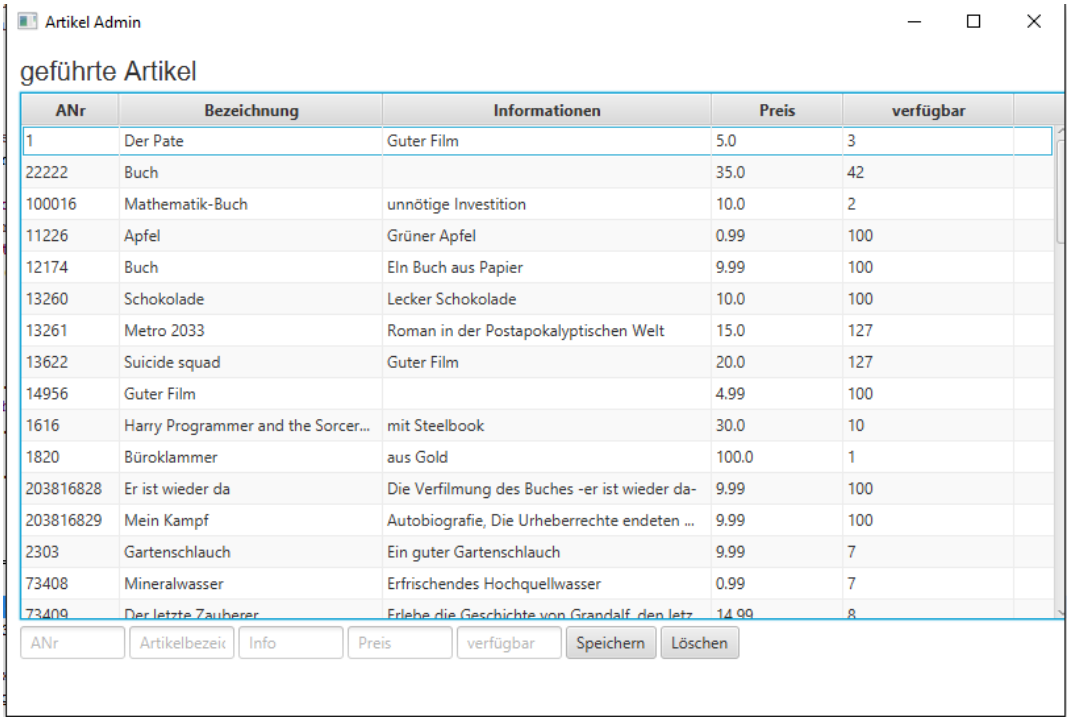


Abbildung 1: Alle Artikel werden angezeigt

## 3.2 Artikel hinzufügen

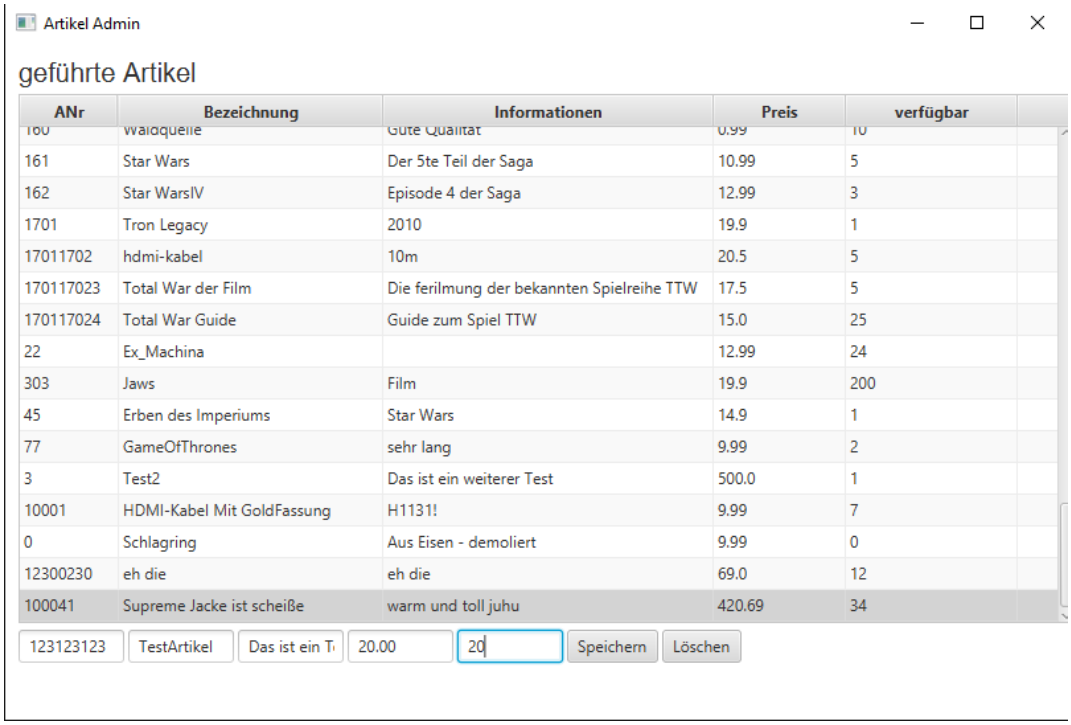


Abbildung 2: Artikelinformationen werden eingetragen

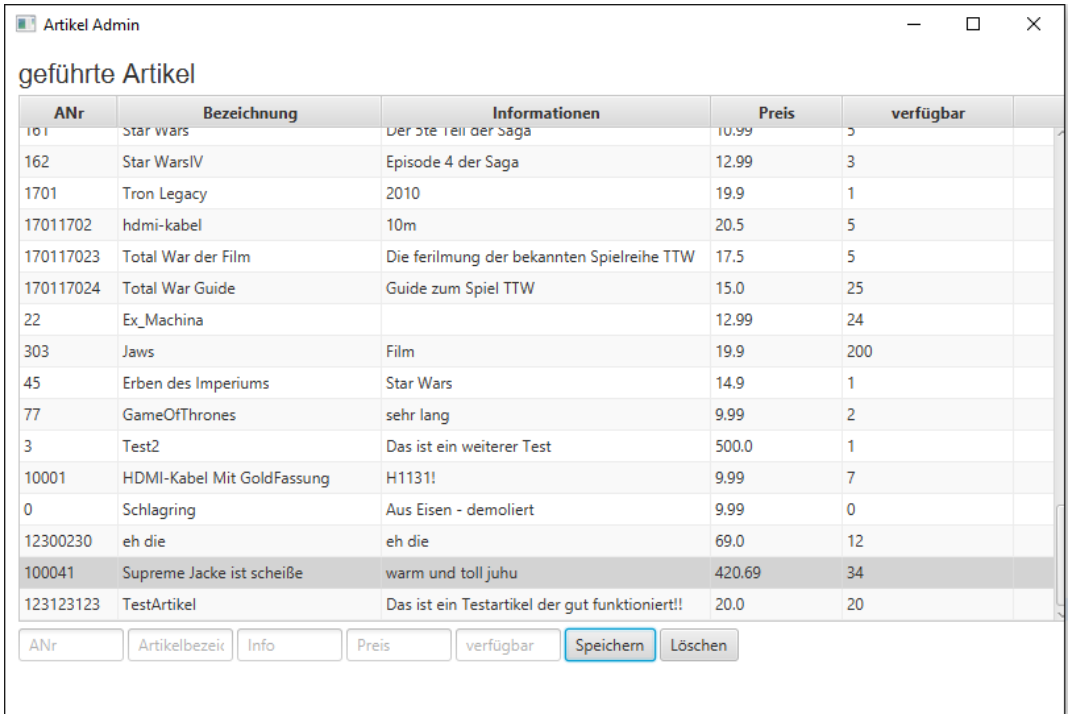


Abbildung 3: Artikel wurde hinzugefügt

## 3.3 Artikel ändern

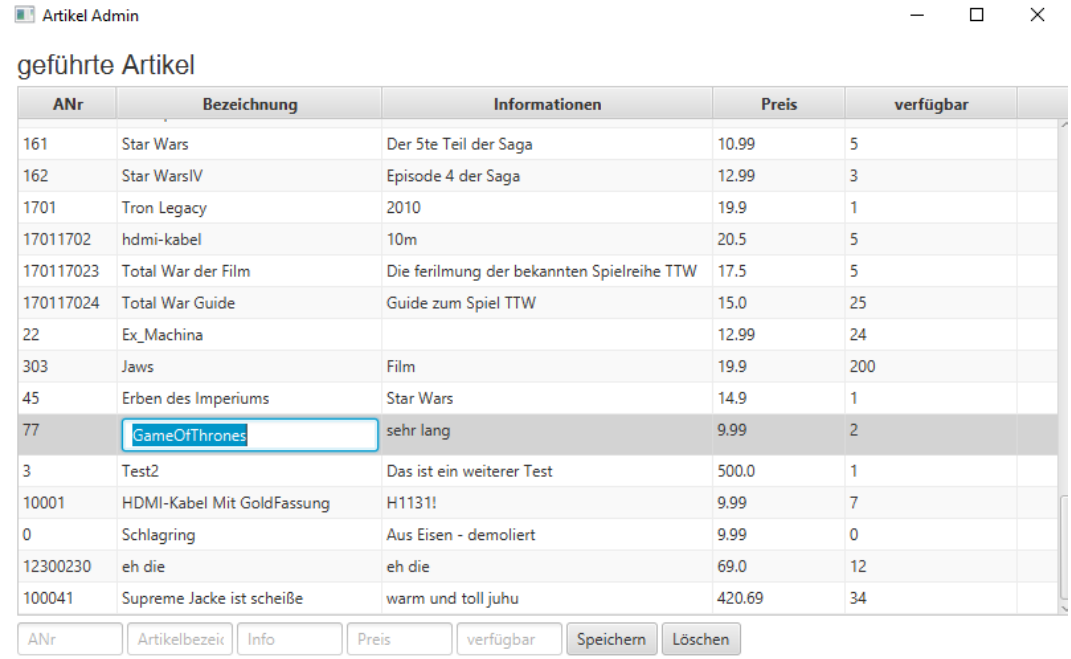


Abbildung 4: Artikelinformationen werden bearbeitet

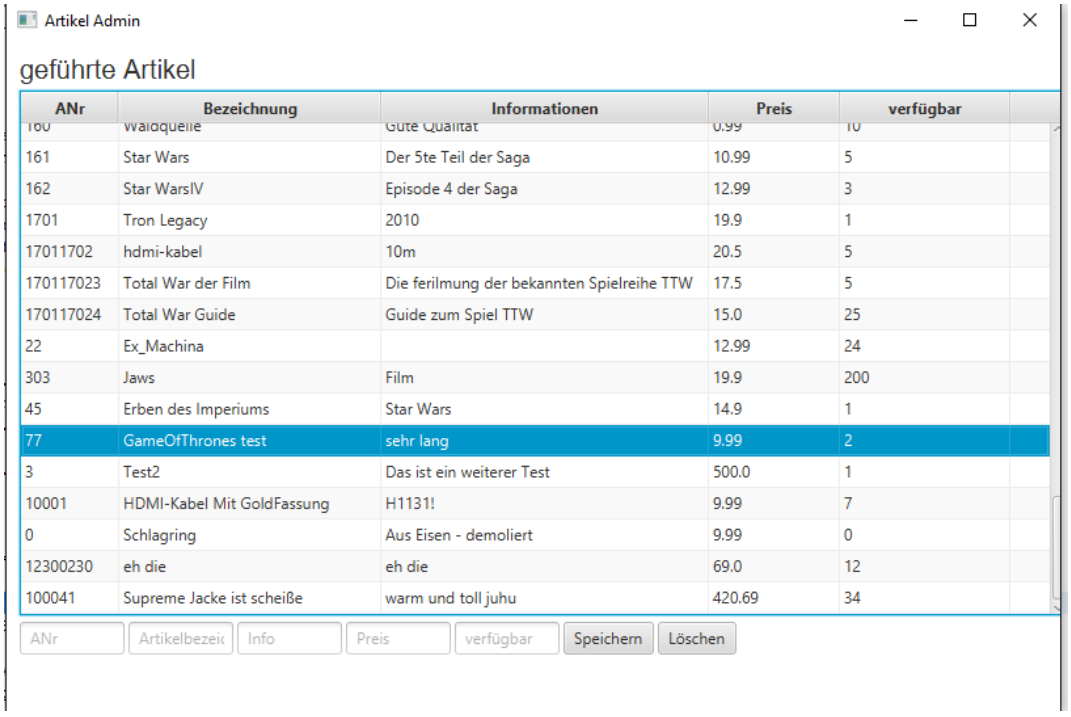


Abbildung 5: Artikel wurde geändert

```
100031 | Das Buch                                | 15.99 |       25 | Gutes Buch bitte kaufen
 10004 | hologram                                | 47.44 |        2 | holo
  1001 | fussball                                | 160.00 |       2 | nicht lieferbar
 10011 | HDMI-Kable                              |  9.99 |        7 |
   101 | Harry Potter und der Stein der Weisen   | 30.99 |        4 | Harry Potter - Blue Ray
   102 | Per Anhalter durch die Galaxis          | 19.99 |       10 | Per Anhalter durch die Galaxis als Buch
   103 | Currygewürz                             |  5.99 |        2 | Dieses Currygewürz besteht aus feinsten Gewürzen aus Indien
   111 | Baseballschläger                        | 420.00 |       5 | Nix
  1111 | HDMI-Kabel                              |  9.99 |        7 |
   120 | foo                                     | 420.20 |      999 | this is a very valuable item
   121 | bar                                     | 20.32 |      999 | this is a very valuable item
   122 | baz                                     | 20.32 |      999 | this is useless
   140 | Immun aktiv Kapseln                     | 29.99 |        7 | Staerkt das Immunsystem
   141 | Peter Pan und die Schluempfe            | 10.99 |       10 | Peter Pan trifft auf die blauen Helden
   142 | Peter Pan der Film                      | 14.99 |       10 | Peter Pan verfilmt
153631 | HDMI                                    |  9.99 |        7 |
   160 | Waldquelle                              |  0.99 |       10 | Gute Qualität
   161 | Star Wars                               | 10.99 |        5 | Der 5te Teil der Saga
   162 | Star WarsIV                             | 12.99 |        3 | Episode 4 der Saga
  1701 | Tron Legacy                             | 19.90 |        1 | 2010
17011702 | hdmi-kabel                            | 20.50 |        5 | 10m
170117023 | Total War der Film                   | 17.50 |        5 | Die ferilmung der bekannten Spielreihe TTW
170117024 | Total War Guide                      | 15.00 |       25 | Guide zum Spiel TTW
    22 | Ex_Machina                              | 12.99 |       24 |
   303 | Jaws                                    | 19.90 |      200 | Film
    45 | Erben des Imperiums                     | 14.90 |        1 | Star Wars
     3 | Test2                                   | 500.00 |       1 | Das ist ein weiterer Test
 10001 | HDMI-Kabel Mit GoldFassung              |  9.99 |        7 | H1131!
     0 | Schlagring                              |  9.99 |        0 | Aus Eisen - demoliert
 12300230 | eh die                               | 69.00 |       12 | eh die
100041 | Supreme Jacke ist scheiße               | 420.69 |      34 | warm und toll juhu
    77 | GameOfThrones test                      |  9.99 |        2 | sehr lang
(65 Zeilen)
```

Abbildung 6: Auch in der Datenbank

## 3.4 Artikel löschen

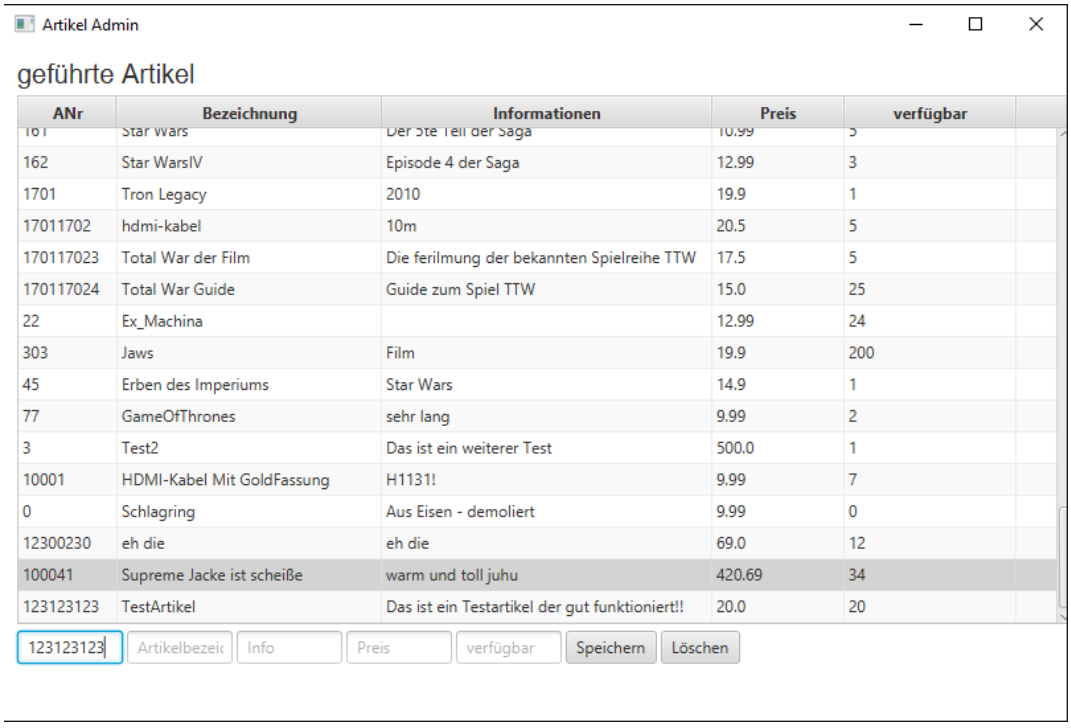


Abbildung 7: anr wird eingegeben zum löschen des Artikels

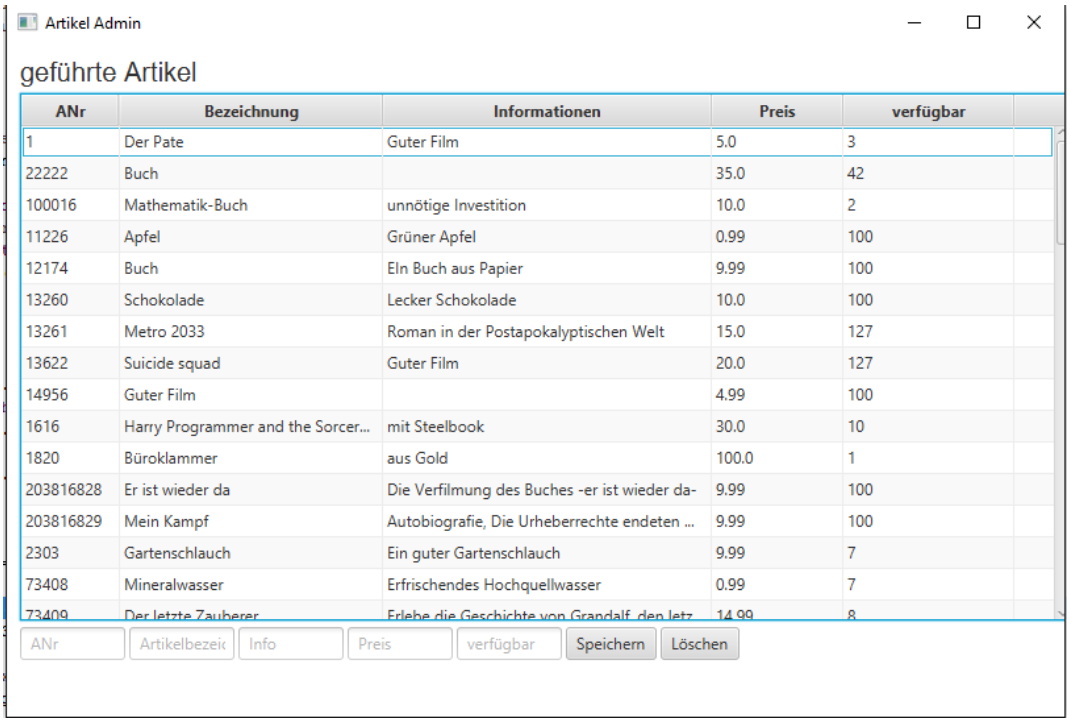


Abbildung 8: Artikel wurde anhand der anr gelöscht

# 4 SQL Injection

Beispiel:

Passworteingabe funtkioniert über input Feld welches simpel in Klartext ein Wort übernimmt und ihn der Datenbank überprüft ob es mit dem Passwort dort übereinstimmt. Annahme: **Keine PreparedStatements!**

Um nun diese Eingabe sehr leicht überbrücken zu können muss man jediglich folgendes eingeben:
`'' OR 1=1`

Was es bewirkt: In der Überprüfung steht etwas in der Art wie:
`SELECT ... FROM ... WHERE pwd = pwd;`.

Nun wenn man etwas wie oben beschrieben eingibt ergibt sich folgender SQL Query:
`SELECT ... FROM ... WHERE pwd = '' OR 1=1;`

Was dazu führt dass das Passwort immer richtig ist.

PreparedStatements funktionieren indem diese genau wissen welche Werte sie entgegen nehmen werden, z.B. werden dann wenn die Eingabe ein String ist, wird wirklich die Eingabe wie ein String behandelt und nicht wie ein SQL Statement

# Abbildungsverzeichnis