
Arbeitsprotokoll

JDBC

INSY MARM,ROSC
4CHIT 1617

Martin Wölfer

Betreuer: ROSC

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

Inhaltsverzeichnis

1	Aufgabenstellung	1
2	Source-Code	1
2.1	JDBCClient.java	1
2.2	ArtikelAdmin.java	2
3	Screenshots	3
3.1	GUI	3
3.2	Artikel hinzufügen	4
3.3	Artikel ändern	5
3.4	Artikel löschen	6
4	SQL Injection	7

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;

3
5 import java.sql.Connection;
6 import java.sql.DriverManager;
7 import java.sql.PreparedStatement;
8 import java.sql.ResultSet;
9 import java.sql.SQLException;
10 import java.sql.Statement;
11 import java.util.ArrayList;
12 import java.util.List;

13 public class JDBCClient {

15     Connection con;

17     JDBCClient() throws SQLException{
18         //Initialize the connection with test user that has privileges
19         this.con = DriverManager.getConnection("jdbc:postgresql://localhost:5432/webshop","test","test")
20             ;
21     }
22     /**
23      * Makes an preparedStatement and then fills and ArrayList with Artikel
24      * @return List of all articles
25      * @throws SQLException
26      */
27     List<Artikel> getAllArticles() throws SQLException {
28         PreparedStatement pstmt = con.prepareStatement("SELECT * FROM artikel");
29         ResultSet rs = pstmt.executeQuery();

31         ArrayList<Artikel> rl = new ArrayList<>();
32         while(rs.next()){
33             int anr = rs.getInt("anr");
34             String abez = rs.getString("abez");
35             String ainfo = rs.getString("info");
36             Float preis = rs.getFloat("npreis");
37             int vstueckz = rs.getInt("vstueckz");
38             rl.add(new Artikel(anr,abez,ainfo,preis,vstueckz));
39         }
40         return rl;
41     }

42     /**
43      * Makes an preparedStatement and then inserts the desired article into the database with
44      * executeUpdate()
45      * @param a the desired article to be inserted into the database
46      * @throws SQLException
47      */
48     void addArticle(Artikel a) throws SQLException {
49         PreparedStatement pstmt = con.prepareStatement("INSERT INTO artikel(anr,abez,npreis,vstueckz,
50             info) values(?,?,?,?);");
51         pstmt.setInt(1, a.getAnr());
52         pstmt.setString(2, a.getAbez());
53         pstmt.setFloat(3, a.getPreis());
54         pstmt.setInt(4, a.getVstueckz());
55         pstmt.executeUpdate();
56     }
57 }

```

```

53     pstmt.setInt(4, a.getVstueckz());
    pstmt.setString(5, a.getAinfo());
    pstmt.executeUpdate();
55 }
57 /**
 * Makes an preparedStatement and then updates the desired article with the values
 * @param a the article to be updated
 * @throws SQLException
59 */
61 void saveArticle(Artikel a) throws SQLException {
63     PreparedStatement pstmt = con.prepareStatement("UPDATE artikel SET anr=?, abez=?, npreis=?,
        vstueckz=?, info=? WHERE anr=?");
    pstmt.setInt(1, a.getAnr());
65     pstmt.setString(2, a.getAbez());
    pstmt.setFloat(3, a.getPreis());
67     pstmt.setInt(4, a.getVstueckz());
    pstmt.setString(5, a.getAinfo());
69     pstmt.setInt(6, a.getAnr());
    pstmt.executeUpdate();
71 }
73 /**
 * Delete an article based on the primary key anr
 * @param anr primary key which defines an article so it can be deleted
 * @throws SQLException
75 */
77 void delArticle(int anr) throws SQLException {
79     PreparedStatement pstmt = con.prepareStatement("DELETE FROM artikel WHERE anr=?");
    pstmt.setInt(1, anr);
81     pstmt.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, addAbesz, addAinfo, addPreis, addVstueckz, addButton, delButton);
```

3 Screenshots

3.1 GUI

Artikel Admin

geführte Artikel

ANr	Bezeichnung	Informationen	Preis	verfügbar
1	Der Pate	Guter Film	5.0	3
22222	Buch		35.0	42
100016	Mathematik-Buch	unnötige Investition	10.0	2
11226	Apfel	Grüner Apfel	0.99	100
12174	Buch	Ein Buch aus Papier	9.99	100
13260	Schokolade	Lecker Schokolade	10.0	100
13261	Metro 2033	Roman in der Postapokalyptischen Welt	15.0	127
13622	Suicide squad	Guter Film	20.0	127
14956	Guter Film		4.99	100
1616	Harry Potter and the Sorcerer's Stone	mit Steelbook	30.0	10
1820	Büroklammer	aus Gold	100.0	1
203816828	Er ist wieder da	Die Verfilmung des Buches -er ist wieder da-	9.99	100
203816829	Mein Kampf	Autobiografie, Die Urheberrechte endeten ...	9.99	100
2303	Gartenschlauch	Ein guter Gartenschlauch	9.99	7
73408	Mineralwasser	Erfrischendes Hochquellwasser	0.99	7
73409	Der letzte Zauberer	Erlebe die Geschichte von Gandalf den letzten	14.99	8

ANr Artikelbezei Info Preis verfügbar Speichern Löschen

Abbildung 1: Alle Artikel werden angezeigt

3.2 Artikel hinzufügen

Artikel Admin

geführte Artikel

ANr	Bezeichnung	Informationen	Preis	verfügbar
100	Warioqueille	Gute Qualität	0.99	10
161	Star Wars	Der 5te Teil der Saga	10.99	5
162	Star WarsIV	Episode 4 der Saga	12.99	3
1701	Tron Legacy	2010	19.9	1
17011702	hdmi-kabel	10m	20.5	5
170117023	Total War der Film	Die ferilmung der bekannten Spielreihe TTW	17.5	5
170117024	Total War Guide	Guide zum Spiel TTW	15.0	25
22	Ex_Machina		12.99	24
303	Jaws	Film	19.9	200
45	Erben des Imperiums	Star Wars	14.9	1
77	GameOfThrones	sehr lang	9.99	2
3	Test2	Das ist ein weiterer Test	500.0	1
10001	HDMI-Kabel Mit GoldFassung	H1131!	9.99	7
0	Schlagring	Aus Eisen - demoliert	9.99	0
12300230	eh die	eh die	69.0	12
100041	Supreme Jacke ist scheiße	warm und toll juhu	420.69	34

123123123 TestArtikel Das ist ein Ti 20.00 20 Speichern Löschen

Abbildung 2: Artikelinformationen werden eingetragen

Artikel Admin

geführte Artikel

ANr	Bezeichnung	Informationen	Preis	verfügbar
101	Star wars	Der 5te Teil der Saga	10.99	5
162	Star WarsIV	Episode 4 der Saga	12.99	3
1701	Tron Legacy	2010	19.9	1
17011702	hdmi-kabel	10m	20.5	5
170117023	Total War der Film	Die ferilmung der bekannten Spielreihe TTW	17.5	5
170117024	Total War Guide	Guide zum Spiel TTW	15.0	25
22	Ex_Machina		12.99	24
303	Jaws	Film	19.9	200
45	Erben des Imperiums	Star Wars	14.9	1
77	GameOfThrones	sehr lang	9.99	2
3	Test2	Das ist ein weiterer Test	500.0	1
10001	HDMI-Kabel Mit GoldFassung	H1131!	9.99	7
0	Schlagring	Aus Eisen - demoliert	9.99	0
12300230	eh die	eh die	69.0	12
100041	Supreme Jacke ist scheiße	warm und toll juhu	420.69	34
123123123	TestArtikel	Das ist ein Testartikel der gut funktioniert!!	20.0	20

ANr Artikelbezeic Info Preis verfügbar Speichern Löschen

Abbildung 3: Artikel wurde hinzugefügt

3.3 Artikel ändern

Artikel Admin

geführte Artikel

ANr	Bezeichnung	Informationen	Preis	verfügbar
161	Star Wars	Der 5te Teil der Saga	10.99	5
162	Star WarsIV	Episode 4 der Saga	12.99	3
1701	Tron Legacy	2010	19.9	1
17011702	hdmi-kabel	10m	20.5	5
170117023	Total War der Film	Die ferilmung der bekannten Spielreihe TTW	17.5	5
170117024	Total War Guide	Guide zum Spiel TTW	15.0	25
22	Ex_Machina		12.99	24
303	Jaws	Film	19.9	200
45	Erben des Imperiums	Star Wars	14.9	1
77	GameOfThrones	sehr lang	9.99	2
3	Test2	Das ist ein weiterer Test	500.0	1
10001	HDMI-Kabel Mit GoldFassung	H1131!	9.99	7
0	Schlagring	Aus Eisen - demoliert	9.99	0
12300230	eh die	eh die	69.0	12
100041	Supreme Jacke ist scheiße	warm und toll juhu	420.69	34

ANr Artikelbezeik Info Preis verfügbar Speichern Löschen

Abbildung 4: Artikelinformationen werden bearbeitet

Artikel Admin

geführte Artikel

ANr	Bezeichnung	Informationen	Preis	verfügbar
100	vvaioquelle	Gute Qualität	0.99	10
161	Star Wars	Der 5te Teil der Saga	10.99	5
162	Star WarsIV	Episode 4 der Saga	12.99	3
1701	Tron Legacy	2010	19.9	1
17011702	hdmi-kabel	10m	20.5	5
170117023	Total War der Film	Die ferilmung der bekannten Spielreihe TTW	17.5	5
170117024	Total War Guide	Guide zum Spiel TTW	15.0	25
22	Ex_Machina		12.99	24
303	Jaws	Film	19.9	200
45	Erben des Imperiums	Star Wars	14.9	1
77	GameOfThrones test	sehr lang	9.99	2
3	Test2	Das ist ein weiterer Test	500.0	1
10001	HDMI-Kabel Mit GoldFassung	H1131!	9.99	7
0	Schlagring	Aus Eisen - demoliert	9.99	0
12300230	eh die	eh die	69.0	12
100041	Supreme Jacke ist scheiße	warm und toll juhu	420.69	34

ANr Artikelbezeik Info Preis verfügbar Speichern Löschen

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

Artikel Admin

gefürhte Artikel

ANr	Bezeichnung	Informationen	Preis	verfügbar
101	Star wars	Der 5te Teil der Saga	10.99	5
162	Star WarsIV	Episode 4 der Saga	12.99	3
1701	Tron Legacy	2010	19.9	1
17011702	hdmi-kabel	10m	20.5	5
170117023	Total War der Film	Die ferilmung der bekannten Spielreihe TTW	17.5	5
170117024	Total War Guide	Guide zum Spiel TTW	15.0	25
22	Ex_Machina		12.99	24
303	Jaws	Film	19.9	200
45	Erben des Imperiums	Star Wars	14.9	1
77	GameOfThrones	sehr lang	9.99	2
3	Test2	Das ist ein weiterer Test	500.0	1
10001	HDMI-Kabel Mit GoldFassung	H1131!	9.99	7
0	Schlagring	Aus Eisen - demoliert	9.99	0
12300230	eh die	eh die	69.0	12
100041	Supreme Jacke ist scheiße	warm und toll juhu	420.69	34
123123123	TestArtikel	Das ist ein Testartikel der gut funktioniert!!	20.0	20

Abbildung 7: anr wird eingegeben zum löschen des Artikels

ANr	Bezeichnung	Informationen	Preis	verfügbar
1	Der Pate	Guter Film	5.0	3
22222	Buch		35.0	42
100016	Mathematik-Buch	unnötige Investition	10.0	2
11226	Apfel	Grüner Apfel	0.99	100
12174	Buch	Ein Buch aus Papier	9.99	100
13260	Schokolade	Lecker Schokolade	10.0	100
13261	Metro 2033	Roman in der Postapokalyptischen Welt	15.0	127
13622	Suicide squad	Guter Film	20.0	127
14956	Guter Film		4.99	100
1616	Harry Potter and the Sorcerer's Stone	mit Steelbook	30.0	10
1820	Büroklammer	aus Gold	100.0	1
203816828	Er ist wieder da	Die Verfilmung des Buches -er ist wieder da-	9.99	100
203816829	Mein Kampf	Autobiografie, Die Urheberrechte endeten ...	9.99	100
2303	Gartenschlauch	Ein guter Gartenschlauch	9.99	7
73408	Mineralwasser	Erfrischendes Hochquellwasser	0.99	7
73409	Der letzte Zauberer	Erlebe die Geschichte von Gandalf den letzten	14.99	8

Abbildung 8: Artikel wurde anhand der anr gelöscht

4 SQL Injection

Beispiel:

Passworteingabe funktioniert 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 lediglich 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

1	Alle Artikel werden angezeigt	3
2	Artikelinformationen werden eingetragen	4
3	Artikel wurde hinzugefügt	4
4	Artikelinformationen werden bearbeitet	5
5	Artikel wurde geändert	5
6	Auch in der Datenbank	6
7	anr wird eingegeben zum löschen des Artikels	6
8	Artikel wurde anhand der anr gelöscht	7