Universität Leipzig, Institut für Informatik
Abteilung Datenbanken
Prof. Dr. E. Rahm,
V. Christen, Dr. A. Groß

Ausgabe: 24.04.2017
Besprechungen: 08.05.2017 (Mo)
10.05.2017 (Mi)
15.05.2017 (Mo)
17.05.2017 (Mi)

Datenbanksysteme II

SS 2017 – Übungsblatt 2

1. Stored Procedure

a) Erstellen Sie analog zu Aufgabe 2d) des ersten Übungsblatts eine SQL Stored Procedure, welche den Freundschaftsgrad zweier Benutzer eines sozialen Netzwerks aktualisiert. Dazu sollen die Parameter *uid1, uid2* und *Fgrad* übergeben werden.

b) Erweitern Sie die obige Lösung derart, dass anstelle der Nutzer-IDs die Benutzernamen (*name1, name2*) als Eingabeparameter dienen, d.h. die Nutzer-IDs müssen auf Basis der Namen ermittelt werden. Nehmen Sie an, dass Nutzer eindeutig durch ihren Benutzernamen gekennzeichnet werden.

c) Skizzieren Sie den Aufruf dieser Stored Procedure aus einem Java-Programm mittels JDBC.

2. SQL-Injection

Es sei folgendes Szenario zum Thema „Soziales Netzwerk“ gegeben.

Eine Webapplikation bietet Ihnen die Möglichkeit unter Eingabe der uid oder des Namens die Daten eines Benutzers zu ermitteln. Die notwendigen Parameter werden mittels Http-GET Request übermittelt.

a) Welche Anfragen sind bzgl. SQL- Injections kritisch zu bewerten, wenn Sie den Parameter durch das Ersetzen eines Patterns, z.B. $$$, an die Anfrage binden. Begründen Sie Ihre Antwort und definieren Sie ein mögliches Angriffsszenario.

i) Parameter: uid=7

```
SELECT n.uid, n.name  FROM Nutzer n
    WHERE n.uid=$$$
```

ii) Parameter: name=Hans

```
SELECT n.uid, n.name  FROM Nutzer n
    WHERE n.name='$$$'
```

b) Wie können Sie das Problem generell vermeiden, wenn Ihre Middleware in Java implementiert ist?

3. PHP

a) Skizzieren Sie das Code-Skelett eines HTML-Formulars welches die Eingabe einer Nutzer-ID ermöglicht. Nach dem Abschicken des Formulars soll serverseitig das PHP-Skript `listFriends.php` ausgeführt werden.

b) Innerhalb des Skriptes sollen mittels eines Prepared Statements (PDO) alle Freundschaftsbeziehungen des übergeben Nutzers ermittelt und tabellarisch ausgegeben werden. Skizieren sie das PHP-Skript `listFriends.php`. Verwenden Sie hierzu das Datenbankschema aus Aufgabe 2 des ersten Übungsblatts.

4. JDBC vs. PHP

a) Vergleichen sie die Verwendung von Prepared Statements in PHP und in JDBC durch die Identifikation analoger Funktionen. Verwenden sie dabei für PHP das *PDO*-Modul

b) Was ist der Vorteil von DB-Modulen wie *PDO* gegenüber der Nutzung datenbanksystemspezifischer Module wie *mysqli*?

Hinweis: Im Rahmen der praktischen Übungen werden weitere Übungsaufgaben zu den Themen JDBC und PHP zur selbstständigen Bearbeitung angeboten.