1 Zugriffsrechte

1.1 SQL-Injection

```
1  String sql = "UPDATE FEEDBACK SET INTERACTION_END=" + d.getTime()
2  + ", MINEOPINION=" ...
3  ...
4  + sanitizeString(myChoiceReason.getValue())
5  ...
```

Listing 1.1: Code gegen SQL-Injection

UPDATE FEEDBACK SET
INTERACTION_END="22102012",
MINEOPINION="5",... MYEXPLANATION='mir gefällt dieses Buch',
got you where 1=1;
where participant='Markus';

Um die Gefahr einer Sql-Injection zu minimieren ⇒ Berechtigungen beschränken

1.2 Benutzerrechte

Identifikation: durch Benutzername
Attribute:

- Authentifizierungsmethode (intern, extern)
  extern: in einem externen System z.B. Passwortserver
- Passwort zur Authentifizierung (verschlüsselt gespeichert)
- Voreingestellte Tabelspaces für temporären und dauerhaften Speicher
- Tabelspace Kontingent (Quota, Speichereinschränkung)
- Status des Benutzerkontos (gesperrt, freigeschaltet)
- Status des Passworts (aktuell, abgelaufen)

```
CREATE USER <benutzername> IDENTIFIED BY <passwort>
(DEFAULT TABLESPACE <tablespace>);
```

Listing 1.2: Erstellen eines Users

```
ALTER USER <benutzername> IDENTIFIED BY <passwort>;
```

Listing 1.3: Ändern eines Users

```
DROP USER <benutzername> CASCADE; --CASCADE: Rechte, etc auch loeschen
```

Listing 1.4: Löschen eines Users

Systemrechte:

- Create Table
- UNLIMITED TABLESPACE
- CREATE USER
- CREATE INDEX
- DROP ANY VIEW
- ALTER USER
- CREATE SESSION

Objecktrechte für Tabellen:

- ALTER
- DELETE
- UPDATE
- SELECT
- INDEX
- REFERENCE
- INSERT
- EXECUTE

```
GRANT CREATE SESSION TO <benutzername>;
GRANT CREATE TABLE TO <benutzername>;
GRANT UNLIMITED TABLESPACE TO <benutzername>;
```

Listing 1.5: Tabellen anlegen

1.3 Rollen - Sammlung von Rechten

```
CREATE ROLE <rollenname> [IDENTIFIED BY <passwort> || NOT IDENTIFIED];
```

Listing 1.6: Definieren von Rollen