

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 \Rightarrow Berechtigungen beschränken

1.2 Benutzer und Benutzerrechte

Identifikation: durch Benutzername

Attribute:

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

```

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

```

Listing 1.2: Erstellen eines Users

```

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

```

Listing 1.3: Ändern eines Users

```

1 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

Objektrechte für Tabellen:

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

```

1 GRANT CREATE SESSION TO <benutzername>;
2 GRANT CREATE TABLE TO <benutzername>;
3 GRANT UNLIMITED TABLESPACE TO <benutzername>;

```

Listing 1.5: Tabellen anlegen

1.3 Rollen - Sammlung von Rechten

```

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

```

Listing 1.6: Definieren von Rollen

```

1 DROP ROLE <rollenname> [CASCADE]; --Rollen koennen auf Rollen basieren
2 [GRANT <rollenname> to <schema>;
3 GRANT CONNECT TO student_role;]

```

Listing 1.7: Löschen von Rollen

Rechte der Rolle **CONNECT**:

- ALTER SESSION
- CREATE CLUSTER, CREATE DATABASE, CREATE SEQUENZ, CREATE SYNONYM, CREATE SESSION, CREATE TABLE, CREATE VIEW
- LINK

with admin option: Rechte dürfen weitergegeben werden

1.3.1 Rechte vergeben / entziehen

Rechte gewähren GRANT; Rechte entziehen REVOKE

```
1 GRANT CREATE TABLE, ALTER TABLE TO "0815";  
2 REVOKE CREATE TABLE, ALTER TABLE  
3 ON [<besitzer>] <object>  
4 FROM <benutzer- oder rollenname>;
```

Listing 1.8: Gewähren und löschen von Objektrechten

Der Benutzer der Berechtigungen mit GRANT vergibt kann diese mit REVOKE auch wieder entziehen!

Ein Benutzer bekommt die Rechte:

- durch Vereinigung der Rechte aller Rollen bei Anmeldung
- Liste der Default-Rollen mittels ALTER USER ändern
ALTER USER alfons [DEFAULT ROLE PETOMOTOMGR, PETOMOTouser
—— ALL]
ALL
- SET ROLE Petomotouser IDENTIFIED BY 'passwort'; während einer Session
- Alle Rollen abwählen: SET ROLE NONE;

2 Systemtabellen