

USE Prepared Statement instead of Statement

Scenario:

Consider the following SQL command

Method `userExists (String username)`

We use the following SQL command. It looks very nice since we look if a user with that name exists, and if exists accept connection.

You can use either *Statement* or *Prepared Statement*.

EXAMPLE JAVA CODE

Assume we have a table called *Users* and have two tuples..

```
>> Select Name from Users
```

Name

```
----  
firat  
moser
```

```
String in = "firat' OR 'a' = 'a";
```

```
PreparedStatement ps = conn.prepareStatement("Select * from users where  
name=?");  
ps.setString(1,in);  
rs = ps.executeQuery();
```

or

```
ResultSet rs = conn.createStatement().executeQuery("Select * from users  
where name='"+in+"'");
```

```
while (rs.next())  
{  
    System.out.println ("Tuple...");  
}
```

If the user enters a username like **'YungTing' OR 'a' = 'a'** see what will happen..

The statement will return two tuples, yet prepared statement will not return any tuple.