1 Prepared Statement

Have a look at the following method.

```
public boolean isLoginOK(String _user, String _pwd) throws Exception {
     boolean isOK = false;
     conn = createConnection(CONN_STRING);
     String select = "SELECT COUNT(*) FROM member
                      WHERE user = ‘” + _user +
                            “’ AND passwort = ‘” + _pwd + “’”;
     Statement stmt = conn.Statement(select);
     ResultSet rs = stmt.executeQuery();
     if(rs.next() && rs.getInt(1) == 1)  {
            isOK = true;
     }
     conn.close();
     return isOK;
}
```

a) Its developer worked semiprofessional. Why so? What are the problems/disadvantages in comparison to an appropriate „prepared statement“ (overview)?

b) If you see also a security-problem in a) then write down what exactly a hacker could give as input in order to get the method returning TRUE (without knowing the user a/o password). If you do not see a security problem, forget b).

c) Change the code to reach a professional state.