答：

(1).1-3的作法有以下的安全问题：

a. SQL注入：拼接的SQL字符串改变了设计者原来的意图，执行了如泄露、改变数据等操作，甚至控制数据库服务器， SQL Injection与Command Injection等攻击包括在内

b. 登录信息提示：用户登录提示信息会给攻击者一些有用的信息。

c. 传输层保护不足：在身份验证过程中没有使用SSL / TLS，因此暴露传输数据和会话ID，被攻击者截听，或使用过期或者配置不正确的证书。

(2)改进：

a. 不要信任用户的输入，对用户的输入进行校验；不要使用动态拼接SQL；不要使用管理员权限的数据库连接；数据库机密信息不要明文存储 加密、hash。

b. 异常信息不要直接返回给用户。

c. 使用有效的证书来传输身份验证时的数据

(3)其他方法：

a. 通过Shiro框架(Java安全框架,执行身份验证、授权、密码和会话管理)进行认证

b. 通过拦截器、过滤器进行验证

c. 通过AOP进行验证：可在控制层或业务层进行；如实现接口，使用JDK动态代理；如没有实现接口，使用CJLIB代理（需引入一个库文件）

d. 在每一个方法中调用Session对象，对什么进行验证，判断是否为合法用户