

软件工程系统安全

1.系统安全性

(1) 身份验证

- 系统有管理员验证机制，在进行敏感操作前（如添加新书籍、知识，对数据库进行改动）要求用户提供有效的凭据（如用户名和密码）来验证其身份。

(2) 日志记录

- 系统采用了日志记录敏感操作，记录下每个修改的操作类型、修改对象名、更改前的状态。

(3) 完整性安全

- 系统存放内部书籍名和知识库名时，编号及名称不能相同。

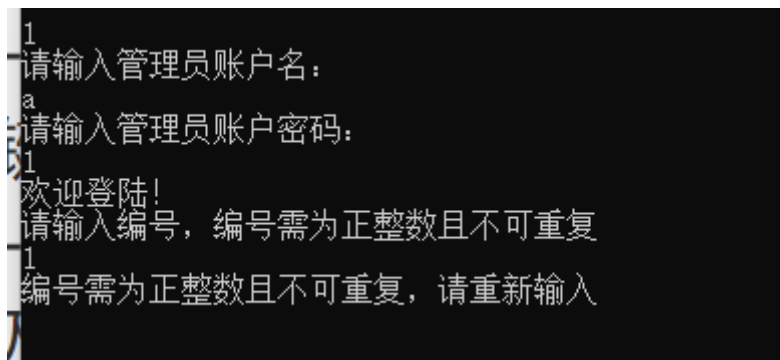
2.风险评估

系统敏感信息并未加密，因此有泄露管理员密码信息，从而导致数据库被攻击的风险。

也因此存在直接修改数据库的风险

3.防护措施

- 输入破坏完整性的重复编号、书籍名时，显示“不可重复，请重新输入”，防止数据读取冲突。



```
1 请输入管理员账户名：
a 请输入管理员账户密码：
1 欢迎登陆！
1 请输入编号，编号需为正整数且不可重复
1 编号需为正整数且不可重复，请重新输入
```

- 软件为个人应用级的硬盘应用，虽然程序内没有较好措施加密，但在操作系统上可设置一些操作。如：部署到系统管理员账户上，只有管理员可读写数据文件，且隐藏数据文件夹。程序入口放在访客账户上，只可读文件。这样就相当于借用部署平台的加密措施，防护了程序。