安全性

猿眼电影订票系统采用B/S架构，客户端软件主要是Web页面。

**准则**

1)   确保最薄弱环节的安全

2)   纵深防御,避免单点失效

3)   失效安全：进入安全状态、阻止信息非授权访问

4)   最小化准则：范围最小化、权限最小化

5)   通过冗余和多样性降低风险

6)   验证所有输入

**安全性可分为: 数据或功能访问控制安全和页面访问控制安全。**

**数据或功能访问控制安全**

数据或功能访问安全性可保证在预期的安全性情况下，不同授权的用户只能访问特定的功能，或者只能访问有限的数据。例如，普通用户可进行输入数据、创建新账户等操作而不能随意删除数据或账户，只有管理员才能删除数据或账户。

**页面访问控制安全**

(1)页面登录。B/S 架构软件必须测试登录用户名和密码的有效性、输入大小写的敏感性、用户登录是否有次数限制; 而且要测试是否可以不登陆而直接浏览某个页面、IP地址登录是否有限制等;

(2) 超时限制。如果用户登陆系统后在一定时间 内没有进行任何页面操作，应进行超时判断，强制用户 重新登陆后才能正常使用系统。

(3) 日志文件。日志文件是保证 Web 应用系统安全性的重要的工具。B/S 架构软件需要测试日志文件 记录信息的完整性、各类操作的可追踪性。在服务器后台，还要检测服务器的日志记录是否正常进行。

(4) SSL。为保证信息在Internet 上传输的安全性，B/S架构软件会采用SSL技术。如果使用了SSL，测试人员需要测试加密的正确性、检测信息的完整性，确定是否有相应的替代页面。当用户进入或离开安全 站点的时候，是否有相应的提示信息。

**安全性测试技术手段**

为确保数据访问安全而进行的**安全功能测试**和为保证页面访问安全而进行的**安全漏洞测试**。安全功能测试基于软件的安全功能需求说明，测试软件的安全功能实现是否与安全需求一致; 安全漏洞测试则站在攻击者的角度，以发现软件的安全漏洞为目的。