<<Web应用系统安全设计与检测>>

图书基本信息

书名：<<Web应用系统安全设计与检测>>

13位ISBN编号：9787506666176

10位ISBN编号：7506666170

出版时间：2012-1

出版时间：中国标准出版社

作者：张晓梅　等编著

页数：247

<<Web应用系统安全设计与检测>>

内容概要

本丛书从电子政务的固有特点出发，结合编著单位丰富的实践经验，围绕电子政务信息安全保障的重点领域，介绍了信息安全的实用技术方法。

本书为丛书的Web应用系统安全设计与检测分册，按照web应用系统的生命周期详细阐述了Web应用系统的常见安全问题、安全设计与实验方法及检测技术，便于读者在项目实施过程中参考。

本书可供各级政府以及安全服务机构、第三方测评机构从事信息化、网络与信息安全的管理和技术人员使用，也可供其他行业相关人员参考。

<<Web应用系统安全设计与检测>>

书籍目录

章节摘录

版权页： 插图： 问题2：未及时安装程序补丁 不安装最新补丁将无法保证及时修补软件本身存在的安全漏洞。
问题3：未开启日志审计功能 未开启日志审计功能，这会导致Web服务器不能对应用层面的关键操作进行有效记录和跟踪。
因此建议启动审计日志，并根据安全需要，对安全审计范围、日志文件的存放位置等作必要的配置。
如果必要，还应该选用适当的日志查阅分析工具对日志文件进行定期分析。
问题4：服务器中保留有调试等无关文档 在服务器目录下保留有调试用、测试用文档，可能造成系统实现细节等信息的泄露。
6.WebLogic安全配置问题 问题1：采用默认运行方式 WebLogic在默认情况下是以开发方式运行的。
这种方式的安全限制比较宽松，存在较为严重的安全隐患。
问题2：Sockets最大打开数量设置不当或未限制 Sockets最大打开数目设置不当的话，容易受到拒绝服务攻击，超出操作系统文件描述符限制。
问题3：未禁止Send Server header Send Server header会返回用户WebLogic服务器主机名和版本号，泄露敏感信息，存在一定的安全隐患。
问题4：采用默认的错误提示页 如果没有定义默认错误网页，则当应用程序出错时会显示内部出错信息，有暴露系统和应用敏感信息的风险。
问题5：生产环境中存在源代码 生产环境中存在源代码是严重安全隐患，源代码可能因为误操作而泄露给攻击者，进而帮助攻击者了解系统，制订进一步攻击计划，应杜绝此类情况的机会。
问题6：未设置账号锁定策略 不设定账号锁定将导致服务器难以抵抗账号字典的攻击。
问题7：用户权限设置不当 存在共用账号，或未根据最小权限原则为不同账号分配相应角色，存在系统资源遭到非授权访问的安全隐患。
问题8：安全审计配置不当 审计功能没有启用，会导致无法回溯追踪安全事件。
而审计日志保存方式配置不当，将导致日志信息的丢失。
问题9：未及时安装补丁程序 WebLogic应用服务器的各版本都存在安全漏洞，应该需要及时安装厂商提供的安全补丁，删除用户不需要的组件。
2.3.2 数据库管理系统的配置管理安全隐患 多数Web应用系统都会涉及数据处理，并将包含敏感信息在内的各种数据存储在数据库中。
数据库管理系统也作为Web应用系统的重要组成部分，其安全隐患可能导致敏感信息泄露或被篡改，攻击者也经常利用此类漏洞攻击Web应用系统。

版权说明