

无懈可击



[无懈可击_下载链接1](#)

著者:杨云

出版者:清华大学

出版时间:2012-1

装帧:

isbn:9787302269281

《无懈可击:全方位构建安全Web系统》对常见的web安全问题，依照分类的方式讲解每一个知识点，告诉读者如何开发安全高效的web系统，如何使自己的系统免受黑客的攻击。《无懈可击:全方位构建安全Web系统》内容是作者多年项目实施和管理经验的总结，在此基础上加以提炼，试图用最简明易懂的方式介绍网站开发的安全问题以及应对措施；内容涉及界面ui安全、代码安全、中间件安全、session安全等，并用典型实例作为引导，介绍各种安全类库和安全编程。《无懈可击:全方位构建安全Web系统》适合网站开发人员、应用程序设计和开发人员使用，也适合网站系统的管理维护人员阅读和参考。

作者介绍:

目录: 第一部分第1章 网站安全技术概述 1. 1 代码安全性的含义 1. 1. 1 代码与代码的安全域 1. 1. 2 代码的安全策略 1. 2 可靠的安全架构第2章 类库与安全类 2. 1 安全类的总体架构 2. 2 System. Security 2. 3 System. Security. Cryptography 2. 4 System. Security. Principal 2. 5 System. Security. Policy 2. 6 System. Security. Permissions 2. 7

System. Web. Security 2. 8 JSP的安全类第3章 ASP. NET 4. 0的安全组件 3. 1
登录控件 3. 2 登录状态控件 3. 3 密码维护控件 3. 4 创建用户向导控件 3. 5
页面访问控件第二部分第4章 存储的安全 4. 1 对数据的攻击方式 4. 2 Hash算法 4. 3
利用操作系统的接口加密 4. 4 加密XML文件 4. 4. 1
DpapiProtectedConfigurationProvider类 4. 4. 2
RsaProtectedConfigurationProvider类 4. 5 保护视图数据 4. 5. 1 开启视图保护开关
4. 5. 2 加密视图信息 4. 5. 3 用户独立视图 4. 6 数据保护 4. 6. 1 对称加密算法
4. 6. 2 非对称加密算法 4. 6. 3 证书加密第5章 让ASP. NET/JSP与数据库安全通信
5. 1 数据库与注入隐患 5. 1. 1 攻击原理 5. 1. 2 攻击方式 5. 1. 3 防范方法 5. 2
一个注入实例 5. 3 加固SQL参数与存储过程 5. 4 正确连接数据库 5. 4. 1
数据库身份验证 5. 4. 2 数据库授权 5. 4. 3 数据库安全配置 5. 4. 4 加密敏感数据
5. 4. 5 安全处理出错数据 5. 4. 6 正确安装数据库第6章 把住用户输入关 6. 1
需要验证的数据 6. 2 几种常见验证方案 6. 2. 1 图片和附加码数据验证 6. 2. 2
Web表单数据验证 6. 2. 3 Web窗体数据验证 6. 3 信息过滤第三部分第7章
编写安全中间件 7. 1 脆弱的中间件 7. 2 如何设计中间件 7. 3 设计中间件的权限 7. 4
一个中间件的实例 7. 5 强签名与反编译 7. 6 如何操作存储系统第8章
ASP. NET角色机制 8. 1 ASP. NET安全管道 8. 1. 1 HTTP请求处理流程 8. 1. 2
安全HTTP管道 8. 1. 3 过滤器 8. 2 角色安全认证 8. 2. 1
IIS和ASP. NET用户认证流程 8. 2. 2 ASP. NET用户认证 8. 2. 3
使用ASP. NET管理工具添加用户 8. 2. 4 角色管理系统 8. 2. 5
使用Membership/Role API添加用户 8. 3 窗体验证 8. 4 混合认证 8. 4. 1
基于IIS的Windows身份验证 8. 4. 2 基于活动目录的Windows身份验证第9章
构建可靠Session 9. 1 Session的概念 9. 2 安全Session的运行 9. 3 如何创建Session
9. 4 利用加密连接加固Session 9. 5 使用权标 9. 6 合理配置Session 9. 7
正确处理链接 9. 8 利用数据库保存Session第10章 安全的Provider模式 10. 1
ASP. NET的MemberShip Provider 10. 2 实现自定义的MembershipProvider类 10. 3
安全使用SiteMap第11章 保护错误信息 11. 1 安全处理ASP. NET系统错误 11. 1. 1
错误异常处理机制 11. 1. 2 错误异常组成 11. 2 异常处理程序的设计 11. 2. 1
错误异常的引发 11. 2. 2 错误异常的处理 11. 2. 3 错误异常的捕获 11. 2. 4
设计自定义错误异常 11. 2. 5 错误异常的性能 11. 2. 6 显示安全的错误信息 11. 3
监控自己系统的安全状态 11. 3. 1 Web系统安全监控 11. 3. 2 记录错误信息
11. 3. 3 日志组件第12章 Web系统与钓鱼技术 12. 1 反射型XSS漏洞 12. 2
保存型XSS漏洞 12. 3 重定向漏洞 12. 4 本站点请求漏洞第四部分第13章
程序间的访问策略 13. 1 代码信任技术概述 13. 2 资源访问安全 13. 3
完全信任和部分信任 13. 4 代码访问安全配置 13. 5 ASP. NET策略文件 13. 6
ASP. NET安全策略 13. 7 开发部分信任Web应用程序 13. 8 部分信任级的配置方法
13. 9 部分信任的Web应用程序处理策略 13. 10 自定义策略 13. 11 沙箱保护策略
13. 12 中度信任程序 13. 13 中度信任的限制第14章 正确加固IIS 14. 1
配置安全的操作系统 14. 2 安全配置IIS 14. 3 使用IIS 14. 4 IIS安全设置 14. 4. 1
角色设置 14. 4. 2 页面和控件设置 14. 4. 3 监控Web系统安全 14. 4. 4
安全密钥配置 14. 4. 5 安全日志配置第15章 代码漏洞检测软件 15. 1 检测HTTP协议
15. 1. 1 Fiddler工具 15. 2 黑盒技术 15. 3 二进制代码分析 15. 4
数据库安全扫描参考文献
· · · · · (收起)

[无懈可击 下载链接1](#)

标签

计算机

网站

安全

security

Web安全

Web

JavaScript

评论

[无懈可击_下载链接1](#)

书评

[无懈可击_下载链接1](#)