<<Web安全设计之道>>

图书基本信息

书名：<<Web安全设计之道>>

13位ISBN编号：9787115211965

10位ISBN编号：7115211965

出版时间：2009-10

出版时间：人民邮电出版社

作者：杨云，刘君 编著

页数：338

前言

.NET框架是微软公司为了满足广大用户的需求而开发的一种通用平台，它带给我们方便、快捷的应用服务。
但是在实际环境中，网络入侵和安全隐患也成了不容忽视的问题，这使得开发人员和软件用户更加关注系统的安全性。

安全工作在企业级软件开发中被戏称为“亡羊补牢”，大家印象中的安全工作都是在问题发生后才采取措施。
本文旨在从根本上纠正这一做法，通过对.NET平台安全问题的了解，做到风险早避免，问题早处理，在应用程序开发的全生命周期中严把安全关，保证系统正常、稳定地运行。

本书为两组人群编写。

（1）.NET应用程序的设计和开发人员，他们应该了解.NET安全的特点和局限性，以便在设计和编码过程中进行相应考虑。
本书的每一章节都使用了大量实例，帮助开发人员理解安全的服务配置和代码编写。

（2）应用系统的用户，这些应用系统是基于.NET平台进行开发和部署的。
通过本书，读者可以清晰地分辨哪些行为是危险的，而这些行为我们是每天都会遇到的.比如，通过最常见的数据加密和身份验证，了解.NET平台安全运行的机制，就可以减少在系统操作过程中的低级错误，排除安全隐患。

我们希望读者具有基本C#或Visual Basic.NE7.编程经验，相关技术可以参考作者所著.NET开发系列书籍。

本书由杨云、刘君主编，参加编写的还有：刘小鹿、谢晓锋、蔡芳、胡建、陈雪郊、刘扬、杜华富、胡浩、成梅花、王磊、李渝乎、王宇晟、王春中、冉剑、陈代勇、陈佳佳、陈家云、李广平等。
在编写过程中，人民邮电出版社和作者所在院校领导对此给予了大力支持和帮助，东北大学的乔建忠教授对本书进行了审阅，在此表示感谢。
最后，还要感谢家人在写作过程中的理解和支持，那是我们工作的持续动力和精神支撑。

本书部分代码可在http：llwww.ptpress.com.ell处下载。
如有问题，可以访问作者博客：http：Naspnet.spaces.1ive.com／。

由于水平有限，书中难免存在不足之处，欢迎广大读者批评指正（电子函件：book better@sina.tom）。
另外，如果想要发表关于本书的评论，可发电子邮件或者在博客上留言。

<<Web安全设计之道>>

内容概要

随着Web应用程序日益广泛的应用，基于Web环境的安全性也越来越成为人们关注的问题，.NET框架的安全性给使用.NET平台编程的所有开发人员和用户带来了解决安全问题的福音。
本书作者总结了多年项目实施和管理经验，在此基础上加以提炼，试图用最简明易懂的方式介绍.NET框架下的安全问题以及应对措施。
本书内容涉及Web应用程序安全、代码安全、数据库安全通信、数据验证、身份验证、组件安全、会话安全以及安全日志的设计等，并用典型实例作为引导，介绍各种安全类库和安全编程，带领读者进入神秘而妙不可言的.NET安全世界。
本书适合.NET平台下的开发人员、项目经理及系统管理人员阅读。

作者简介

杨云，微软指定培训中心讲师，微软最有价值专家（Microsoft MVP）。
长期从事微软ASP．NET技术培训，为微软新闻组和多家报纸杂志撰写文章。

参加多项大型微软．NET项目。
如企业级应用系统开发、电信系统开发、政府办公自动化架构等。
主要研究方向是ASP．NET安全部署技术、设计模式。

<<Web安全设计之道>>

书籍目录

章节摘录

（2）加载时，除非控件拥有受信任的签名，否则，运行库仅授予控件与工.ocalIntranet命名权限集关联的权限。
在控件拥有受信任签名的情况下，会被授予与LocalIntranet权限集关联的权限，同时因为控件拥有受信任签名，还可能被授予其他一些权限。
（3）运行时，每当调用方（在此情况下为寄宿的控件）访问公开受保护资源的库或调用非托管代码的库时，该库就会提出安全要求，导致对调用方的权限进行检查，查看调用方是否被授予了适当权限。
这些安全检查可防止控件在客户端执行未经授权的操作。
2.基础知识　　每种以公共语言运行库为目标的应用程序必须与运行库的安全系统进行交互。
当应用程序执行时，运行库将自动对它进行计算，然后赋予其一个权限集。
根据应用程序获得的权限不同，应用程序或者正常运行，或者发生安全性异常。
特定计算机上的本地安全设置最终决定代码所收到的权限。
这些设置会因计算机而异，所以无法确保代码将收到运行所需的足够的权限。
这与非托管开发领域不同，在非托管开发领域，不必担心运行代码所需权限。
每个开发人员都必须熟悉下面的代码访问安全性操作。
编写类型安全代码：若要使代码受益于代码访问安全性，必须使用生成可验证为类型安全代码的编译器。
强制性语法和声明式语法：与运行库安全系统的交互使用强制性安全调用和声明式安全调用执行。
声明式调用使用属性执行，强制性调用在代码中使用类的新实例执行。
有些调用只能强制性地执行，有些调用只能以声明方式执行，还有一些调用可以这两种方式中的任一种方式执行。
为代码请求权限：请求将应用到程序集范围，代码通知运行库在此范围内运行它所需的权限，运行库在代码加载到内存中时计算安全请求。
代码使用请求通知运行库运行所需权限。
使用安全类库：类库使用代码访问安全性指定所需权限。
3.通过部分受信任的代码使用类库　　系统一般不允许通过低于完全信任级别（该信任级别是运行库代码访问安全系统授予的）的应用程序调用共享托管库，除非库编写器通过使用AllowPartiallylYustedCallersAttribute类明确允许调用。
因此，应用程序编写器必须注意在部分受信任的上下文中不能使用的库。
默认情况下，在本地：Intranet或Internet区域中执行的所有代码都是部分受信任的。
如果您的代码不会在部分受信任的上下文中执行或被部分受信任的代码调用，那么您就不需要关心本小节中的信息。
但是，如果编写的代码必须与部分受信任的代码交互或在部分受信任的上下文中运行，则应该考虑以下因素。
必须用强名称对库进行签名，这样该库就可以被多个应用程序共享。
强名称允许代码放置在全局程序集缓存中，并允许使用者验证特定的移动代码。
默认情况下，具有强名称的共享库自动为完全信任执行隐式LinkDemand，无须库编写器执行任何操作。

媒体关注与评论

黑客入侵、挂马、网页篡改……网络系统安全的种种问题令人困扰，是否有方法能彻底解决这些安全问题呢……　　互联网上黑与白的较量已经持续了多年，双方都在不断地博弈。
目前病毒的发展方向已经从普通桌面软件转移到了网站上，这些黑客利用网站本身的各类漏洞植入非法脚本甚至木马程序。
提高网站自身的安全性是当务之急，是网络程序员务必要思考的问题。
这本书教会了大家如何开发出高质量的安全网站，值得推荐！
——瑞星 西南分公司 首席网络安全顾问 顾明凯　　我觉得系统安全的本质就是意识和技术不断学习提高的过程。
这本书叙述清晰，语言简练，把安全技术讲解得朴实无华，实在是一本不可多得的安全力作。
——上海交通大学 计逢机网络安全博士 张涛　　这本书很实用，内容很经典，是安全编码技术方面一本难得的好书。
年轻时如果有这样一本书，也许我会少走不少弯路。
——前淘宝及支付宝（中国）网络安全工程师 刘明德　　安全问题，我想现在上到政府机关，下到中小公司，没有敢不重视吧？
这本书，我觉得使用NET技术的人员，应该人手一册。
——中国杀毒网 安全顾问 张庆生

编辑推荐

黑客入侵、挂马、网页篡改……网络系统安全的种种问题令人困扰，是否有方法能彻底解决这些安全问题呢……《Web安全设计之道：.NET代码安全、界面漏洞防范与程序优化》为你解决。

<<Web安全设计之道>>

版权说明