PROGRAMMER TO PROGRAMMER™

Professional ASP.NET Security

ASP.NET 安全性高级编程

Russ Basiura
Richard Conway 等著
王晓娜 黄开枝 译

清华大学出版社

ASP.NET 安全性高级编程

Russ Basiura
Richard Conway 等著

王晓娜 黄开枝 译

清华大学出版社
北 京

北京市版权局著作权合同登记号：01-2002-0947

内 容 简 介

随着 Internet 在各行各业的应用和普及，安全问题越来越受到 Web 应用程序开发人员的关注。为了帮助您全面掌握 ASP.NET 应用程序安全性问题的解决方案，本书深入探讨了各种安全攻击类型以及相应的 ASP.NET 安全对策。具体内容包括常规的安全攻击类型和可以实现的多种安全措施、在 ASP.NET 安全架构中的身份验证和授权、包括.NET Passport 和 Windows 授权在内的多种不同授权方式、代码访问安全性、Web 服务安全性、IIS 和 ASP.NET 安全性配置等。通过阅读本书，可大大提高您的安全意识和预防 Internet 攻击的能力。

本书适合那些具有一定的 ASP.NET 和.NET Framework 编程经验并需要自己开发各种安全选项，以确保 ASP.NET 应用程序安全的中高级 ASP.NET 开发人员。

EISBN：1-86100-620-9
Professional ASP.NET Security
Russ Basiura，Richard Conway et al

图书在版编目(CIP)数据

ASP.NET 安全性高级编程/(美)巴兹拉等著；王晓娜，黄开枝译. —北京：清华大学出版社，2003
书名原文：Professional ASP.NET Security
ISBN 7-302-06493-8

Ⅰ. A… Ⅱ. ①巴…②王…③黄… Ⅲ. 主页制作—程序设计—安全技术 Ⅳ. TP393.092

中国版本图书馆 CIP 数据核字(2003)第 022926 号

出 版 者：清华大学出版社(北京清华大学学研大厦，邮编 100084)
http://www.tup.com.cn
责任编辑：徐燕萍
封面设计：康博
版式设计：康博
印 刷 者：北京密云胶印厂
发 行 者：新华书店总店北京发行所
开　　本：787×1092 1/16　**印张**：27.75　**字数**：710 千字
版　　次：2003 年 4 月第 1 版　2003 年 4 月第 1 次印刷
书　　号：ISBN 7-302-06493-8/TP・4879
印　　数：0001～4000
定　　价：56.00 元

出版者的话

近年来，国内计算机类图书出版业得到了空前的发展，面向初级用户的应用类软件图书铺天盖地，但是真正有深度和内涵的高端图书不多。已经掌握计算机和网络基础知识的人们，尤其是 IT 专业人士迫切需要“阳春白雪”。IT 图书市场呼唤精品！

为了满足这种市场需求，清华大学出版社从世界出版业知名品牌 Wrox 出版公司引进了受到无数 IT 专业人士青睐，被奉为 IT 出版界经典之作的 Professional 系列丛书。这套讲述最新编程技术与开发环境的高级编程丛书，从头到尾都贯穿了 Wrox 出版公司“由程序员为程序员而著(Programmer to Programmer)”的出版理念，每一本书无不是出自软件大师之手。实际上，Wrox 公司的图书作者都是世界顶级 IT 公司(如 Microsoft，IBM，Oracle 以及 HP 等)的资深程序员，他们的作品既深入研究编程机理，传授最新编程技术，又站在程序员的角度，指导程序员拓展编程思路，学习实用开发技巧，从而风靡世界各地，被 IT 专业人士和程序员视为职业生涯中的必读之作。

为了保证该系列丛书的质量，清华大学出版社迅速组织了一批位于 IT 开发领域前沿的专家学者进行翻译，经过编辑人员的进一步加工整理后，现陆续奉献给广大读者。

读者可以从 www.wrox.com 网站下载所需的源代码并获得相关的技术支持。同时，也欢迎广大读者参与 p2p.wrox.com 网站上的在线讨论，与世界各地的编程人员交流读书感受和编程体验。

前　言

在 Web 应用程序和 Web 服务时代，应用程序安全正变得越来越重要。如果我们不能加倍关注如何维护一个应用程序的安全，那么我们连最简单的 Web 应用程序也不能部署。只有理解和使用我们所拥有的安全特性，并理解对安全的威胁，我们才能设计应用程序，使危及它们安全的可能性降至最小。

最近，安全问题因一些高配置网站的安全漏洞而受到人们的高度重视，无论怎样夸大保障应用程序安全的重要性都不为过。对一个公司来说，安全漏洞会造成非常严重的后果：不仅电脑黑客可能破坏或者干扰我们的应用程序，而且更严重的是机密信息可能会受到损坏(或者是落入了坏人之手，或者是被破坏或者被删除了)。同样，世界上的某些地区在法律上都要求确保个人信息是安全的。例如，欧盟(European Union，EU)的公司以及 EU 国家中的公司贸易都有一个法定义务，那就是采用合理方法来保障个人信息安全。

在某些方面，保障 Internet 应用程序的安全变得越来越复杂，因为现在并没有利用最初预期的方式使用 Internet。Internet 的设计意图是使我们能够向其他人发布信息；我们正在使用它处理金融和商业事务。因此，开发人员和系统管理员全面负责保障一个应用程序的安全(尽管我们所使用的技术给了我们极大的帮助)；World Wide Web 没有固有的安全特性。

Windows 2000 和 Internet 信息服务(Internet Information Services，IIS)本身具有完善的内部安全特性，并且使用这些安全特性是实现安全的一个重要部分。可是，Microsoft 利用许多复杂的安全特性(例如代码访问安全性和基于角色的安全性)设计了 ASP.NET 和.NET Framework，并且利用这些安全特性也是保障安全的关键组成部分。这就意味着，开发人员和系统管理员都要负责保护 Web 应用程序的安全。如果要有效地利用这些资源，那么我们需要掌握它们的工作方式。

简而言之，保障 ASP.NET 应用程序安全有两个关键方面。系统管理员的责任是：创建驻留我们的应用程序的合适环境。包括安装和配置代理服务器、创建非军事区、配置 IIS 等(我们将在附录 A 和 B 中讨论这类问题)。当然，开发人员需要详尽理解这类问题，但是他们重点关注的是别的方面：即实现一个应用程序内部的安全特性。这是保障 ASP.NET 应用程序安全的第二个方面，并且包括实现身份验证(识别特殊用户)、授权 (允许特殊用户访问特定资源)、确保我们没有为黑客提供任何可供利用的漏洞等等。尽管我们研究了诸如配置 IIS 和使用代理服务器之类的问题，但是保障 ASP.NET 应用程序安全的这些特性是本书介绍的重点。

本书主要内容

在本书中，我们明确和全面研究了 ASP.NET 开发人员所关心的安全问题的各个方面。在开发 ASP.NET 时，我们可以利用.NET Framework 提供的复杂环境，其中包括许多只能通过 ASP 3.0 才能够获得的安全特性。

我们首先将研究一些更一般的安全问题：我们应该针对什么类型的安全威胁来保护我们自己、这些安全威胁可以采用什么形式以及我们应该采用什么类型的策略才能对付它们。在第 2 章，我们转而讨论一般的策略，这些策略用于确保我们的 Web 应用程序或者 Web 站点有适当的安全措施，以保护它不会受到来自客户端机器的潜在攻击。在这个讨论中，我们研究了可能会攻击我们站点的不同类型的攻击(例如跨站点脚本处理、SQL Injection 攻击以及内容吸入)，以及我们能够用于预防这类攻击的方法(或者至少减少这类攻击的可能性)。

在第 3、4 和第 5 章，我们继续研究了一般的安全策略，同时讨论了如何安全存储秘密或者其他机密信息、 保护对数据库和其他数据源的访问，以及开发和实现强健的密码策略。

在对一个安全应用程序的访问的管理中，我们区分了验证用户(识别一个特殊用户是谁)和授权访问特定资源(我们不希望所有用户访问应用程序中的所有资源)。在第 6 章，我们研究了在 ASP.NET 中实现身份验证和授权方案的一般方法。

从第 7～11 章，我们详细研究了如何为 ASP.NET 应用程序实现不同种类的身份验证方案：使用 Windows 身份验证、使用 Microsoft 的.NET Passport 作为身份验证方案、实现一些标准窗体身份验证方案并定制它们以及开发我们自定义的身份验证方案。

然后，我们在第 12 章探讨了各种授权方案，例如限制特殊用户访问站点的特定区域或者特定资源。

.NET Framework 实现了一个全新的安全范例，用于管理对特定代码段的访问。这被称为代码访问安全性(Code Access Security)。如果一本有关 ASP.NET 安全的书没有研究保护应用程序的强大的新方法，那么这本书就是不完整的，所以在第 13 章中我们详细研究了在实现安全解决方案中利用代码访问安全的高级方式。

.NET Framework 中的新内容还有 XML Web 服务，它也是通过 Internet 提供功能，因而也具有某些类型的安全漏洞。理解这些安全漏洞，并能够实现安全特性以防止它们被攻击是很重要的。所以，我们在第 14 章中研究了 Web 服务安全性。

最后，我们详细研究了如何在.NET Framework 中实现假冒(Impersonation)以及如何利用它。

作为开发人员，我们不仅有必要理解如何在应用程序中实现安全解决方案，还需要理解如何确保应用程序环境是安全的。包括：配置 IIS、.NET Framework 安全设置、利

用 Windows 安全特性等等。我们在附录 A 和 B 中研究了这些问题。

学习本书的条件

要运行本书中的示例，您必须具备：

- 一个合适的操作系统：带有 Service Pack 2 的 Windows 2000 (Professional、Server 或者 Advanced Server 版) 或者 Windows XP Professional Edition
- .NET Framework SDK
- 本书中的一些示例需要 SQL Server 或者 MSDN

本书中的一些示例是使用 Visual Studio .NET IDE 开发的。因此，虽然 VS.NET IDE 不是绝对必需的，但还是建议您安装它。

建议您还要从 http://www.wrox.com 上下载本书示例的源代码(参见下面的“用户支持和反馈”一节)。不管您是从这些源文件中粘贴代码还是亲自输入代码，源代码都提供了一种有价值的方式，可以检查您代码中的错误。

用户支持和反馈

我们一贯重视读者的意见，并想知道每位读者对本书的看法，包括读者喜欢和不喜欢的内容，以及读者希望我们下一次完善的地方。您可以通过发送电子邮件(地址为 feedback@wrox.com)来向我们反馈意见。请确保在反馈信息中提到本书的ISBN和书名。

源代码和更新

在学习本书中的示例时，可以手动输入所有代码，也可以使用我们为本书提供的源代码。许多读者都愿意选择前者，这主要是因为手动输入代码有利于读者熟练掌握所需的编码技巧。

无论您是否希望手动输入所有示例代码，手边有一份本书源代码的副本是非常有用的。如果您喜欢手动输入示例代码，仍然可以使用我们的源代码来检验应当获得的结果——如果您认为自己可能存在输入错误，示例源代码可以帮助您验证错误，得到正确结果。如果您不喜欢手动输入示例代码，那就需要从我们的站点下载本书源代码。总之，源代码有利于您更新和调试书中的示例程序。

从 Wrox 公司站点(地址为 http://www.wrox.com)中可以下载本书所使用的所有源代码。登录这个站点之后，通过 Search 工具或书名列表，可以方便地定位需要的书目。

然后，单击 Code 栏中的 Download 超链接，或者单击本书的详细信息页面中的 Download Code 超链接，就可以下载相应的示例代码。

从我们的站点上下载的可用文件都是使用 WinZip 压缩过的文档。把附件保存到本地磁盘上的文件夹中后，需要使用一个解压缩程序(例如 WinZip 或 PKUnzip)来解压缩文件。在解压缩文件时，通常将代码解压缩到每一章所在的文件夹中。在解压缩的过程中，应确保解压缩程序已经选中 Extract to 选项(或对等选项)下面的 Use folder names 选项(或者实现相同功能的选项)。

勘误表

我们已经尽最大努力确保本书中的文本和代码没有错误，但是错误仍然在所难免。如果您发现本书存在错误，例如拼写错误或不正确的代码段，请反馈信息给我们，我们将不胜感激。勘误表的发送可以节约其他读者学习本书的时间，而且能够帮助我们提供更高质量的信息。请将您的反馈信息以电子邮件的形式发送到 support@wrox.com，它们将被检查，如果正确，将被粘贴到本书的勘误页面上，或者在本书的后续版本中使用。

要在我们的站点上找到勘误表，请访问 http://www.wrox.com/，并通过 Search 工具或者书名列表轻松定位本书页面。然后单击 Book Errata 超链接即可，该链接位于本书的详细信息页面中。在这个页面中，您可以看到所有已经由编辑检查并提交的勘误内容。通过单击 Submit Errata 链接，您也可以通知我们您已经发现的勘误内容。

技术支持

如果您希望直接向详细了解本书的专家咨询本书中的问题，可以发送电子邮件到 support@wrox.com，要求在邮件的主题栏中带上本书的书名和 ISBN(国际标准图书编号)的后 4 位数字。一封典型的电子邮件应包括下面的内容：

- 在主题栏中必须有本书的书名、ISBN 的后 4 位数字(本书后 4 位数字是 6209)和问题所在的页码。
- 正文部分应包括读者的名字、联系信息和问题。

我们将不返回无用邮件，因为我们仅仅需要有用的详细资料，以便可节约您和我们的时间。当您发送一封电子邮件信息时，它将经过下面一系列支持：

- 客户支持：首先，您的信息将被递送到我们的客户支持人员手中，并由他们阅读。对于一些被频繁提到的问题将被归档，并将立即回答有关本书或者 Web 站点的任何常见问题。

- 编辑支持：接着，一些有深度的问题将被送到对本书负责的技术编辑手中，他们在程序设计语言或者特定的产品上有着丰富的经验，能够回答相关主题的详细技术问题。问题一旦得到解决，编辑会及时将勘误表发送到我们的 Web 站点上。
- 作者支持：最后，如果编辑不能回答您的问题(这种情况很少发生)，他们将请求本书的作者。我们将尽量保护作者免受干扰，以便不影响其写作。然而，我们也非常高兴转寄给他们一些特殊的问题。所有 Wrox 公司的作者都为他们的书提供技术支持。作为回应，他们将发送电子邮件给用户和编辑，进而使所有的读者受益。

注意：

Wrox 公司的支持过程仅仅对那些与我们出版的书目内容直接相关的问题提供支持，对于超出常规书目支持的问题，您可以从 http://p2p.wrox.com/论坛中的公共列表中获得支持信息。

p2p.wrox.com 站点

为了便于作者和其他人讨论，特将编程人员加入到 P2P 站点的邮件列表中，而且我们独符的系统将 programmer to programmer™(由程序员为程序员而著)的编程理念与邮件列表、论坛、新闻组以及所有其他服务内容(一对一的邮件支持系统除外)相联系。如果您向 P2P 发送一个问题，相信它一定会被登录邮件列表的 Wrox 公司作者和其他相关专家所检查到。无论您是在阅读本书，还是在开发自己的应用程序，都可以在 p2p.wrox.com 站点中找到许多对自己有所帮助的邮件列表。

按照下面的步骤可以预订一个邮件列表：

(1) 登录 http://p2p.wrox.com/站点，并从左边的菜单栏选择一个适当的类别。

(2) 单击您希望加入的邮件列表。

(3) 按照说明订阅并填写自己的邮件地址和密码。

(4) 回复您收到的确认邮件。

(5) 使用预订管理程序加入更多的邮件列表并设置自己的邮件首选参数。

目　　录