Broadview
www.broadview.com.cn

SYNGRESS®

安全技术大系

你的Web应用程序难道安全吗?

Hacking The Code:
ASP.NET Web Application Security

拒绝黑客——ASP.NET Web应用程序安全性剖析

[美] Mark M. Burnett 著
良 忠 译

- 设计、开发和审查安全的ASP.NET Web应用程序
- 学习防护程序的开发技巧
- 完整的C#和VB.NET代码实例

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

拒绝黑客

——ASP.NET Web 应用程序安全性剖析

Hacking the Code

ASP.NET Web Application Security

[美] Mark M. Burnett 著

良 忠 译

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书详细介绍了 ASP.NET Web 应用程序面对的各种威胁和攻击，并有针对性地提供了完美解决方案。运用本书介绍的安全技术基本上可以抵御到目前为止出现的各种黑客攻击，如账号劫持、社会工程、跨站点脚本、暴力攻击等。

对于 ASP.NET Web 程序开发人员而言，本书可谓是一本非常实用的参考书，同时也适合网络管理员参考学习。

版权贸易合同登记号　图字：01-2004-3565

图书在版编目（CIP）数据

拒绝黑客：ASP.NET Web 应用程序安全性剖析 /（美）伯内特（Burnett, M. M.）著；良忠译.
—北京：电子工业出版社，2005.2
（安全技术大系）
书名原文：Hacking the Code ASP.NET Web Application Security
ISBN 7-121-00405-4

Ⅰ. 拒…　Ⅱ. ①伯… ②良…　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（2004）第 128954 号

责任编辑：孙学瑛
印　　刷：北京智力达印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：23.25　字数：422 千字
印　　次：2005 年 2 月第 1 次印刷
印　　数：4000 册　　定价：48.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

译者的话

对于 Web 应用程序来说，若安全措施脆弱，或存在潜在的安全漏洞，无异于敞开大门不设防的银行；对于用户来说，在不安全的网站上输入用户名和密码，实际上使自己的隐私置入危险之中；对于黑客来说，各种安全隐患则成为他们的有力攻击目标。随着网络应用的进一步深入，网络安全的重要性也日益凸现。有人将各种网络攻击比做“洪水猛兽”也毫不为过。抵御这种“洪水猛兽”的根本途径是堵塞各种安全漏洞，构筑坚固的 Web 应用程序。

本书正是这样一本为脆弱的 ASP.NET Web 应用程序提供完美解决方案的参考书籍。本书讲解了 ASP.NET Web 应用程序可能受到的各种威胁，并提供了理想的解决方案。对于重要的安全技术，本书还提供了典型的案例。本书的最大特点是其务实性，即先提出问题（安全威胁），再有针对性地给出解决方案（安全技术），并对各种可能性进行提纲挈领式的总结。

当然，黑客技术与安全技术永远是“攻”与“防”的两个对立面，它们的技术也在不断地发展。即使充分运用了本书介绍的安全技术，也不可能一劳永逸，因为攻击技术无时无刻不在更新。何况，应用程序在升级过程中，由于种种原因，也可能引入新的攻击点，无形中扩大了攻击面。因此，阅读此书时，我们要理解其精髓，在安全维护中做到举一反三。

由于译者水平有限，且时间仓促，错误在所难免，希望广大读者不吝指正。我的 E-mail 地址是：web_zhou@21cn.com。

译　者

作　者

Mark Burnett（微软 MVP） 他是一位独立安全顾问和自由作家，也是一位基于 Windows 的 IIS Web 服务器的安全专家。Mark 是 *Maximum Windows Security* 一书的合作者，也是 *Stealing the Network: How to Own the Box*(Syngress Publishing, 1-9311836-87-6)和 *Dr. Tom Shinder's ISA Server and Beyond: Real World Security Solutions for Microsoft Enterprise Networks*(Syngress Publishing, ISBN: 1-931836-66-3)撰稿人之一。他是 Syngress 出版社 *Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle*(ISBN: 1-931836-69-8)一书的撰稿人和技术编辑。Mark 曾在多次安全会议上发表演讲，并在 *Windows & .NET, Information Security, Windows Web Solutions, Security Administrator* 杂志上发表多篇技术文章，还经常给 SecurityFoucs.com 投稿。Mark 还在自己的 Web 站点 IISSecurity.info 上发表文章。

撰 稿 人

Joshua Skillings Trade West Systems, LLC 公司（这是一家致力于为金融业开发应用程序的咨询公司）的一位高级软件工程师。Joshua 毕业于布里汉杨大学，获得计算机科学专业的学士学位。他是 BYU ACM 俱乐部的主席。自从.NET Beta 2 发布以来，他就一直使用.NET，并且使用.NET 框架开发了各种游戏、掌上电脑应用程序、Web 网站和安全工具。他与妻子和两个孩子生活在犹他州的桑迪。

技术编辑

James C. Foster 计算机科学全球安全开发公司的副主任。他一直负责开发和实施管理、教育、信息化、咨询和外包服务。在加入 CSC（Computer Sciences Corporation）之前，Foster 是 Foundstone 公司的研发部主任，负责产品的全部方面并配合研发，包

括合作战略和国际化市场拓展。在 Foundstone 公司之前，Foster 是 Guardent 公司的高级顾问和研究科学家（该公司于 2004 年由 Verisign 以 1.35 亿美元的价格收购），还是 Information Security 杂志的临时撰稿人（该杂志于 2003 年由 TechTarget 以内部保密价格收购）。他经常受邀为相关安全问题出谋划策，成为 USAToday，Information Security 杂志，Baseline，Computer World，Secure Computing 和 MIT Technologist 的嘉宾。James 为 *Snort 2.0 Intrusion Detection* (Syngress, ISBN: 1931836744)、*Special Ops Host and Network Security for Microsoft, Unix, and Oracle* (Syngress, ISBN: 1931836698)、*Hacking Exposed, Fourth Edition, Advanced Intrusion Detection, Anti-Hacker Toolkit Second Edition* 和 *Anti-Spam Toolkit* 书籍的合作者或撰稿人。James 曾在耶鲁、哈佛和马里兰大学接受教育，分别获得科学副学士、理学士和 MBA 学位。现在，他是宾夕法尼亚沃顿商学院的职员。

致　谢

感谢以下人员为本书的付梓而给予的热心帮助。

如今，Syngress 书籍由 O'Reilly & Associates 公司在美国发行。ORA 的工作人员具有高涨的热情以及崇高的职业道德，感谢他们将 Syngress 书籍推入市场而付出了时间和精力，他们是：Tim O'Reilly，Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikert, Opol Matsutaro, Lynn Schwartz, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop, Tim Hinton, Kyle Hart, Sara Winge, C.J. Rayhill, Peter Pardo, Leslie Crandell, Valerie Dow, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett 和 Rob Bullington。特别要感谢 John Chodacki，感谢他对 Safari 提供的帮助。

感谢 Elsevier Science 中辛勤工作的团队。他们包括：Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna, Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Rosie Moss, Chris Hossack 和 Krista Leppiko，感谢他们使本书技术具有世界前瞻性。

感谢 STP 发行人员 David Buckland, Daniel Loh, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua 和 Joseph Chan，是他们的热情工作让读者早日见到了本书。

感谢 Acorn Publishing 的 Kwon Sung 给予的支持。

感谢 Woodslane 的 David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Geoff Ebbs, Hedley Partis, Bec Lowe 和 Mark Langley，他们负责本书在澳大利亚、新西兰、巴布亚新几内亚、斐济、汤加、所罗门岛和库克岛范围内发行本书。

感谢 Global Publishing 和 Winston Lim 为在菲律宾发行 Syngress 书籍而提供的帮助和支持。

目　录

Chapter 1

第 1 章
管理用户

本章提供的解决方案：

- 建立用户证书
- 管理密码
- 重新设置丢失或被窃取的密码
- 授权用户

☑ 编码标准快速参考

☑ 代码审查快速参考

☑ 常见问题

1.1 引言

用户通常是 Web 应用程序的庞大组成部分，也是 Web 应用程序的安全性焦点。实际上，大多数 Web 应用程序的安全性都是为了保护用户和他们的私有信息。

每个 Web 应用程序都有不同的危险和敏感度级别。必须在组织中评估这种危险，以此确定对用户安全性的关注程度。如何构建 Web 应用程序将在很大程度上影响用户如何分享安全性。用户可能不会像程序员所希望的那样认真考虑安全性，但作为一个安全性专业人员，其工作就是确保数据受到适当的保护。

请考虑某杂志的在线文章档案，经过认证的订阅者可阅读该文件。拥有者希望保护他们的版权内容，因此他们需要用户经过认证才能获得对某篇文章的访问权限。然而，读者不会在站点上保存个人信息，并且他们也可能不注意安全性，甚至可能和朋友共享注册信息，允许朋友获得访问受保护文章的权限。

可能更为普遍的情况是，用户比 Web 站点操作员更关注安全性。许多公司对安全性都没有足够的重视，直到产生了难以补救的问题。在 2001 年 3 月，美国联邦调查局（FBI，Federal Bureau of Investigation）和国家基础设施保护中心（NIPC，National Infrastructure Protection Center）发布了一份报告，指出许多电脑黑客正以电子商务和电子银行的 Web 站点为目标，窃取信用卡信息，并且企图向站点所有者敲诈钱财。电脑黑客一般利用众所周知的 Windows 漏洞，如果站点管理员经常保持对安全补丁的更新，则所有这些漏洞将不会产生任何问题。NIPC 报告声明，电脑黑客已经从 40 家公司中窃取了 100 多万的信用卡号。显然，这些公司没有注意严格地采取安全性措施来处理敏感的用户信息。缺乏这方面的细致工作，将导致用户的私有信息处于危险之中。

无论问题在于 Web 站点操作员还是用户，控制 Web 站点的安全性都应该从管理用户的基本点着手。

1.1.1 理解威胁

本章介绍的主要威胁如下所述。

- **暴力攻击（brute-force attack）**：这些攻击通过尝试所有可能的字符组合，以发现用户证书。首先尝试使用字典单词、常用密码或可预测的字符组合，优化暴力攻击。
- **账户劫持（account hijacking）**：这种威胁包括接管合法用户的账户，有时甚

至会拒绝合法用户访问自己的账户。

- **社会工程（social engineering）**：这是使用软技巧（而不是软件和硬件技术）获得敏感信息（例如，密码）的过程，这些信息可用于影响系统的安全性。
- **垃圾邮件（spamming）**：我们都很熟悉这种威胁。它是将大量无用电子邮件发送给用户或 Web 站点，从而堵塞因特网，有时甚至会引起服务器崩溃。

1.2　建立用户证书

用户安全性首先在于用户名和密码的选择。可由站点或用户选择用户名和密码，通过这种方式来向用户说明安全的重要性。在这一节中，将学习如下内容：

- 实施强密码（strong password）
- 避免使用易于猜测的证书
- 防止证书获取（credential harvesting）
- 返回安全错误消息
- 限制空闲的账户

技　巧

应该总是同时需要用户名和密码。有时候，我们会碰到一些只需要密码就可以登录系统的 Web 应用程序。但是，请考虑如下情况：若用户改变密码，但发现选中的代码已经被占用。此时，该用户就获得了另一个用户的证书。应该总是要求用公共证书（用户名）来标志用户，同时用私有证书（密码）来验证用户。

1.2.1　实施强密码

小结：使用技术性方法和策略来确保强用户密码

威胁：暴力攻击、账户劫持

如果密码是应用程序安全的中心机制，则必须确保用户具有强密码。建立一种策略，确保密码足够复杂，防止某些人很容易地猜出这些密码。可以通过如下方式创建可靠的密码策略：

- 实施最小长度为 8 位字符的密码。
- 不限制密码的最大长度。
- 需要多种字符集，包括小写字母、大写字母、数字和标点符号。

- 允许用户在他们的密码中使用任意键盘字符，包括空格。
- 不允许字典单词。
- 不允许密码中出现用户名。

技 巧

当用户无法提供满足复杂性需求的密码时，可能会被拒绝。为了避免这个问题，可以同时考虑字符集长度和数量，把它们作为密码复杂性的两个因素。较长但都是小写字母的密码和较短但有多个字符集的密码同样有效。一般情况下，在密码中添加 2～4 个字符和添加 1 个数字或标点符号一样有效。带有大小写字母和标点符号的 6 位字符密码在复杂性上大概等同于都是小写字母的 8 位字符密码。

许多流行的 Web 站点并不强制要求最小密码长度，或者强制要求了一个最小密码长度，但因为长度过短，无法保证安全性。图 1-1 显示了一个 Web 站点，该站点允许最小密码长度为 3 个字符，并且限制最大长度为 25 个字符。该密码的最小长度过短，而虽然 25 个字符是一个长密码，但完全不需要强加这种限制。

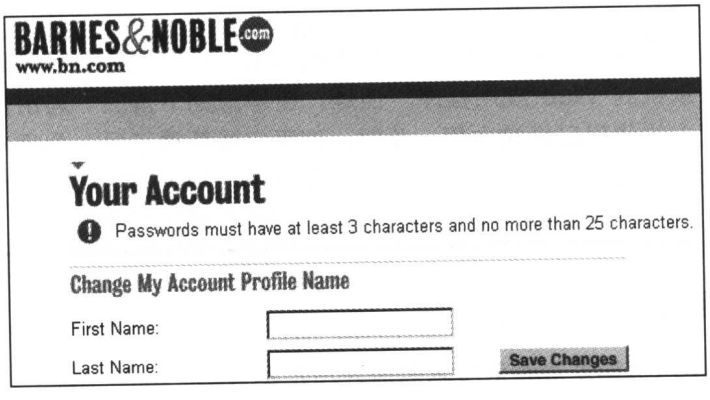

图 1-1 弱密码策略的示例

技 巧

要求长密码的另一个优点是，它减少了用户在密码中可以采用的字典单词数量。可在字典中找到的密码很容易被破解，应该避免这种情况。设置最小长度为 8 位字符的密码可避免使用 3～7 个字母的单词，在英语字典中大概有 50 000 个这样的单词。这将减少 50 000 个容易被破解的密码。