软件项目管理世界经典教材丛书·影印版

Microsoft Press

编写安全的代码 2

(第2版)

Writing Secure Code (Second Edition)

Michael Howard,
David LeBlanc

网络时代保护应用程序代码安全的实战策略和技术

- 安全的原则，实战策略和技术
- 成功阻击黑客攻击的要领
- 解决最为棘手的安全问题

“微软员工必读。”

——比尔·盖茨

清华大学出版社

软件项目管理世界经典教材丛书

编写安全的代码
(第2版)

(影印版)

[美] Michael Howard, David LeBlanc

清华大学出版社
北京

内 容 简 介

本书的两位作者是曾经击败过世界上最难缠的恶意黑客的代码武士，他们在书中披露了经过实战考验的保护代码安全的各种绝招。比尔·盖茨将此书钦定为“微软员工必读”。

本书分为五大部分。第 I 部分介绍了为什么要保护系统安全，使之免遭攻击，以及设计这种系统的原则和分析技术。第 II 部分和第 III 部分是本书的重点，分别介绍了几乎适用于任何一种应用程序的关键性安全编码技术，以及网络应用程序和.NET 代码安全技术。第 IV 部分讲述了一些特殊的、在一般的图书中很少讨论的安全问题。第 V 部分包括 5 个附录，分别介绍危险的 API 以及安全措施核对清单等。

本书告诉您应用程序怎么会不安全，为什么人们不愿意构建安全的系统，最重要的是如何构建安全的系统。本书是软件设计、开发、测试、系统管理等人员必读的教材，也是软件学院、计算机专业或软件公司首选的软件安全教材。

Writing Secure Code, Second Edition(ISBN 0-7356-1722-8)
Michael Howard,David LeBlanc

北京市版权局著作权合同登记号：图 01-2003-0832 号

图书在版编目(CIP)数据

编写安全的代码=Writing Secure Code：Second Edition/(美)霍华德，(美)勒布朗克著.—2 版(影印本).—北京：清华大学出版社，2003
(软件项目管理世界经典教材丛书)
ISBN 7-302-06461-X

Ⅰ.编… Ⅱ.①霍… ②勒… Ⅲ.电子计算机—安全技术 Ⅳ.TP309

中图版本图书馆 CIP 数据核字(2003)第 018868 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
http://www.tup.tsinghua.edu.cn
责任编辑：郭福生 杨志娟
印 刷 者：北京牛山世兴印刷厂
发 行 者：新华书店总店北京发行所
开 本：787×960 1/16 **印张**：49.5
版 次：2003 年 4 月第 1 版 2003 年 4 月第 1 次印刷
书 号：ISBN 7-302-06461-X/TP·4863
印 数：0001～2000
定 价：72.00 元

前　言

在 2002 年 2、3 月份，Windows 所有正常的安全特性都停止了工作。在此期间，整个开发组的注意力都转向如何提高此产品的下一版本即 Windows .NET Server 2003 的安全上。众所周知，“Windows 安全运动”的目标是使开发组全体成员了解最新的安全编码技术，以找出设计和代码缺陷，改进测试代码和文档。在此运动期间，本书的第 1 版是 Windows 开发组全体成员的必读教材，而第 2 版收录了在这场运动中以及在针对微软其他产品的后续安全运动中的许多新发现，这些产品包括 SQL Server、Office、Exchange、Systems Management Server、Visual Studio .NET、.NET 公共语言运行库，等等。

Windows 安全运动(以及许多其他的安全运动)的原动力，来自比尔·盖茨 2002 年 1 月 15 日的名为 Trustworthy Computing (值得信赖的计算)的备忘录，其中概括说明了一种关于向用户提交新型计算机系统的高级策略，这种新型系统将更安全、更可靠。自从有了那个备忘录以来，我们两人已经与微软公司内外的数千名开发人员交谈过或合作过，而他们均异口同声地告诉我们同一件事情：“我们要做正确的事情——我们要开发安全的软件——但我们知道的还不够。”那种愿望和不确定性，直接道明了本书的目的：向他们传授学校里从来就学不到的技术——如何设计、生成、测试和注解安全的软件。所谓“安全的软件”，并不是指安全码或实现安全特性的代码，而是指为抵挡恶意攻击而设计的代码。安全的代码也是健壮的代码。

本书的目标是要绝对的切实可行，这反倒使您认识到您的代码**可能会**受到攻击。更确切地说就是，如果您创建的应用程序要在一台或多台计算机上运行，而这台或这些计算机已经连接到一个网络上，或已连接到最大的网络 Internet 上，那么您的代码就可能会受到攻击。

系统安全受到损害后会造成各种严重后果，包括产量下降、客户信誉受损以及财产损失。例如，如果攻击者能够损害应用程序的安全(如使之无法使用)，您的客户就会转用其他的产品。在使用基于 Internet 的服务时，大多数人都不是很有耐心。如果您的服务不可用，许多客户就会弃您而去，投奔您的竞争对手。

对于众多软件开发商来说，真正的问题是安全不像开发过程那样盈利作用显而易见。因此，管理层不愿意花钱去培训开发人员编写安全的代码，在攻击得逞之前，他们不想在安全技术上投资。而一旦攻击得逞，则为时已晚——损失已然造成。事后的修补工作，无论是在财力上还是在信誉上，都要付出高昂的代价。

历史证明，保护财产使之免遭盗窃和攻击是上策。我们的祖先早就制定了对盗窃、损坏或侵占他人财产者进行惩罚的法律。的确，人们都明白属于私人的动产和财物应当受到保护。这些道德准则也适用于数字世界，因此，作为开发人员，我们的部分职责就是创建可保护数字资产的应用程序和解决

方案。

您将会注意到，本书内容中包括一些基本的问题，在学校课程里介绍“设计和构建安全的系统”这一主题时，应当讲述过这些内容。您可能会认为，设计是设计师或程序经理们的事情，但作为开发人员和测试人员，您也需要了解设计能够抵御攻击的系统结构的有关过程。

众所周知，无论您花费多少时间和精力，所开发出来的软件总是会存在一些弱点，这只是因为您无法预测未来的安全问题。我们知道，对于 Windows .NET Server 2003 来说，同样会存在一些弱点；但我们也知道，按照本书中所建议的方法，可以减少弱点的总数，大大增加发现和利用代码中弱点的难度。

本书读者对象

在设计应用程序，或生成、测试以及注释解决方案时，您需要本书。如果您的应用程序是基于 Web 的或基于 Win32 的，您也需要本书。如果您正在学习或开发基于 Microsoft .NET 框架的应用程序，您还需要本书。总之，如果您的工作涉及到应用程序开发，您会在本书中找到许多值得学习的内容。

即使您正在编写不在 Microsoft 平台上运行的代码，本书中的许多内容依然非常有用。除了个别几章是完全针对 Microsoft 平台以外，同一类型的问题日渐与平台无关。即便有时某种东西似乎仅适用于 Windows，但其通常有更加广泛的应用。例如，Everyone 用户的“完全控制”访问控制列表和 UNIX 系统上设置给 World Writable 的文件，其实是同一问题，而跨网站的脚本问题是普遍存在的。

本书组织结构

本书分为五个部分。第 I 部分(第 1～4 章)，“当前的安全问题”，概括说明了为什么要保护系统安全使之免遭攻击，以及设计这种系统的原则和分析技术。

本书的主要内容集中在第 II 部分和第 III 部分。第 II 部分，“安全的编码技术”，包括第 5～14 章，概括介绍了几乎适用于任何一种应用程序的重要的编码技术。第 III 部分，“更安全的编码技术”，包括 4 章(第 15～18 章)，重点介绍了网络应用程序和.NET 代码。

第 IV 部分，“特殊的安全问题”，包括 6 章(第 19～24 章)，讲述了一般的图书中很少讨论的主题，如测试、进行安全代码审查、隐私策略以及安全的软件安装等问题。第 23 章介绍了放在其他各章都不太合适的一些一般原则。

第 V 部分，“附录”，包括 5 个附录，分别介绍危险的 API、我们所听到的未考虑安全问题的一些荒谬的借口以及分别针对设计人员、开发人员和测试人员设计的安全措施核对清单。

与其他关于安全的图书的作者不同，我们不仅告诉您应用程序怎么会不安全，而且告诉您为什么

人们不愿意构建安全的系统。本书是绝对实用的，也是绝对切实可行的。本书解释了系统怎么会受到攻击，人们常犯的错误，以及最重要的、如何构建安全的系统。(顺便说一句，请注意页边的图标，它们表示与安全有关的奇闻轶事。)

安装和使用范例文件

通过连接到站点 http://www.microsoft.com/mspress/books/5957.asp，可以从 Web 上下载本书的 Companion Content 页下载范例文件。要访问范例文件，请单击该页右侧 More Information 菜单框中的 Companion Content 链接，打开 Companion Content 页，此页中包括下载范例文件的链接，也可以连接到 Microsoft Press Support 站点。下载链接可打开一个包含有许可协议的可执行文件。要想把范例文件复制到硬盘上，请单击运行可执行文件的链接，然后接受显示的许可协议。默认情况下，范例文件将被复制到【我的文档】\Microsoft Press\Secureco2 文件夹下。在安装过程中，可以改变目标文件夹。

系 统 要 求

尽管可以使用包括 Visual C++ 6.0 在内的大多数编译器来编译本书中用 C/C++编写的大多数范例，但还是要求您安装 Microsoft Visual Studio .NET。用 Perl 编写的范例已经使用 ActiveState Perl 5.6 或 ActivateState Visual Perl 1.0 (可从 http://www.activestate.com 下载)测试过。VBScript 和 JScript 代码已经用 Windows Scripting Host 测试过，Windows 2000 及其以后的版本中包含 Windows Scripting Host。所有 SQL 范例都使用 SQL Server 2000 进行了测试。而 Visual Basic .NET 和 Visual C#应用程序均是使用 Visual Studio .NET 编写和测试的。

本书中的所有应用程序(两个例外)，均可以在符合建议的操作系统要求的、运行 Windows 2000 的计算机上运行。第 7 章的 Safer 范例和第 11 章的 UTF8 MultiByteToWideChar 范例，必须在 Windows XP 或 Windows .NET Server 上才能正确运行。编译代码时必须使用比符合编译器要求的机器更加健壮的机器。

支 持 信 息

为了降低书的成本，减轻读者负担，对于因内容很少而不值得单独配盘的图书，我们将其范例代码或练习文件放在我们的网站上，供读者下载。敬请访问以下网址：*http://www.wenyuan.com.cn*，查找本书的有关链接。

如果您对本书或配书文件有任何建议、意见或想法，请通过以下电子邮件与清华大学出版社计算机应用编辑二室客户服务部取得联系：

service@wenyuan.com.cn

或致函：

北京 100084-157 信箱

读者服务部

邮编：100084

亦可致电：010-62792098-220。

请注意，上述地址并不提供软件产品的支持。

目　录

第 I 部分　当前的安全问题

第 II 部分 安全的编码技术

第 III 部分 更安全的编码技术