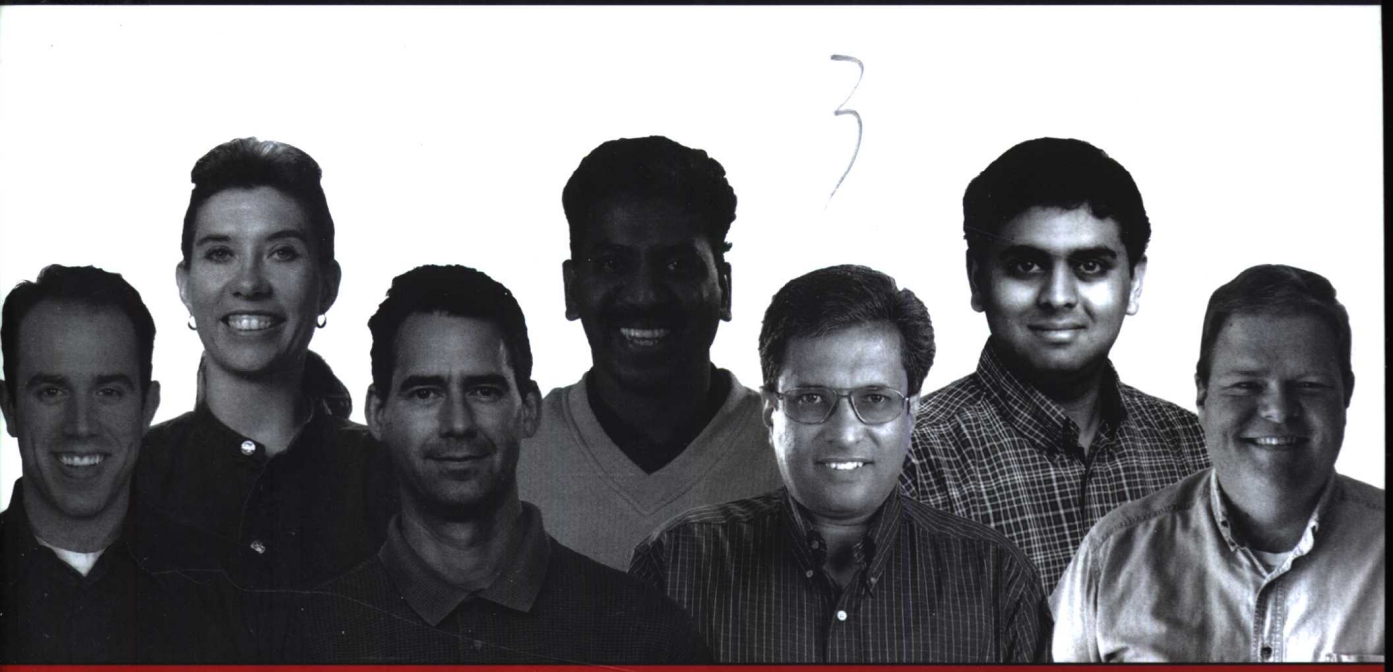
OGRAMMER TO PROGRAMMER™



# Professional Web Services Security

# Web 服务安全性高级编程

(美) Ben Galbraith
Whitney Hankison 等著
吴旭超 王 黎 译

清华大学出版社

# Web 服务安全性高级编程

(美) Ben Galbraith
Whitney Hankison
等著

吴旭超　王　黎
译

清华大学出版社

北　京

## 内 容 简 介

本书全面、系统地介绍了使用 Web 服务时所面临的安全性问题，从 Web 服务的角度指明当前系统中的安全漏洞以及相关的安全规范、解决方案和注意事项，并通过对 J2EE 和.NET 中具体实例的分析，介绍这些规范的实际应用。

本书适用于那些对 Web 服务体系结构有较好理解的 Web 服务开发人员，以及曾经在现有的任何平台上开发(部署)过 Web 服务的人员，同时，也适用于负责系统完整性的安全分析员。

EISBN：1-86100-765-5
Professional Web Services Security
Ben Galbraith, Whitney Hankison et al.


北京市版权局著作权合同登记号　图字：01-2002-6524

**图书在版编目(CIP)数据**

Web 服务安全性高级编程/(美)加尔布雷斯等著；吴旭超　王黎译. —北京：清华大学出版社，2003
书名原文：Professional Web Services Security
ISBN 7-302-07005-9

Ⅰ. W…　Ⅱ.①加…②吴…③王…　Ⅲ.互联网络—安全技术　Ⅳ.TP393.48

中国版本图书馆 CIP 数据核字(2003) 第 070816 号

**出 版 者**：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
**社 总 机**：010-62770175　　**客户服务**：010-62776969

**组稿编辑**：曹　康
**文稿编辑**：王晓娜
**封面设计**：康　博
**版式设计**：康　博
**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**：185×260　**印张**：33.75　**字数**：863 千字
**版　　次**：2003 年 9 月第 1 版　2003 年 9 月第 1 次印刷
**书　　号**：ISBN 7-302-07005-9/TP・5156
**印　　数**：1～4000
**定　　价**：68.00 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

Web 服务拥有众多优势，吸引了很多商家。与其他技术相比较，Web 服务具有一些特定的优势，比如集成性，它使 Web 服务能够适用于电子商务。它们的开发速度较快、成本较低、便于部署，并且提供了更多的灵活性和互操作性。然而，伴随着这些优点也出现了一些安全上的风险，当今大多数管理人员对此异常关注。在用于 Web 服务体系结构时，为 Web 设计的安全体系结构是有限的，因而迫切需要有新的标准。这些问题的解决方案正在形成，新的标准正在创建，以便使 Internet 世界快速适应安全性体系结构。

本书主要关注这些正在形成的、旨在解决大部分安全威胁的安全性标准，从 Web 服务的角度指明当前系统中的安全漏洞。最后，本书通过一系列案例来描述可能出现的问题，并解释可用来解决这些问题的各种技术、标准以及工具包。

## 本书主要内容

本书由 3 个部分组成：

### 1. 概念

这一部分简要地介绍了有关 Web 服务的所有内容，推动这些服务发展的商业因素，以及这些服务对安全性的需求。

### 2. 原理

原理部分是本书的关键内容。它介绍了安全性问题中所涉及的各种概念，以及特定于 Web 服务的安全性标准的演变，并对每个内容都作了详细的论述。

### 3. 应用

最后，在应用部分中，我们分别展示了针对 J2EE 和.NET 的两个 Web 服务示例。

## 本书读者对象

本书适用于那些对 Web 服务体系结构有较好理解的 Web 服务开发人员，以及曾经在现有的任何平台上开发(或者部署)过 Web 服务的人员。本书对熟悉 J2EE 或者.NET 平台的读者的帮助最大，因为我们分别对这两个平台的实际案例进行了具体分析。即使用户不熟悉这些平台，仍然可以通过本书了解 Web 服务中的安全体系结构和原理，并从中获益。

读者如果想了解一些实践信息，使自己的 Web 服务具备足够的安全性，本书将是最合适的选择。本书也适用于负责系统完整性的安全分析员。

# 使用要求

要运行本书中的示例，您需要具备以下程序，具体情况取决于个人所使用的工作平台：

- JDK 1.4.1 或 Visual Studio .NET Framework
- Apache Jakarta Tomcat 4.0.6(截止本书编写之日，Tomcat 4.1.2 与 Axis 共同运行时还存在一些小故障)或 Internet Information Server(IIS)
- Apache Axis 1.0
- Apache XML Security 1.0.4
- Verisign TSIK 1.5

如需完整的示例源代码 ，请从 http://www.wrox.com/ Web 站点下载。

# 用户支持

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)向我们反馈意见。请确保反馈信息提到本书的书名。

## 如何下载本书的示例代码

当您访问 Wrox 公司站点(地址为 http://www.wrox.com/)时，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 列中的 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文件都是使用 WinZip 压缩过的文档。保存文件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(WinZip、PKUnzip 及其他)被设置为使用原有文件夹名。

## 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省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。您的反馈信息将被检查，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 Advanced Search 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的封面图解下面。

## E-Mail 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 位数字和问题所在的页码。
- 邮件正文中应包括读者的名字、联系信息和问题。

我们将不返回您的无用邮件，因为我们仅仅需要有用的详细资料，以便节约您和我们的时间。当您发送一个电子邮件信息时，它将经过下面一系列支持：

- 用户支持：首先，您的信息将被递送到我们的用户支持人员手中，并由他们阅读。他们有一些被频繁提到的问题的文件，可以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。
- 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。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。

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，对于超出此范围的问题，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，我们除了提供一对一的支持系统外，还通过邮件列表、论坛和新闻组等方式进一步体现了 Programmer to Programmer™(程序员为程序名而著)的理念。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订阅一个邮件列表：

(1) 登录 http://p2p.wrox.com/站点。
(2) 从左边的主菜单栏选择一个合适的列表。
(3) 单击希望加入的邮件列表。
(4) 按照说明订阅并填写自己的邮件地址和密码。
(5) 回复您收到的确认邮件。
(6) 使用订阅管理程序加入更多的邮件列表并设置自己的邮件首选项。

## 本系统提供最好的支持的原因

您可以加入整个邮件列表，也可以只接收每周的邮件摘要。如果您没有时间和工具来接收邮件列表，可以直接查找我们的在线文档。独特的 Lyris 系统可以将一些没有用的垃圾邮件删除，并保护您的电子邮件地址不被侵扰。当存在加入和离开列表以及任何有关列表的其他常见问题时，请发送邮件到 listsupport@p2p.wrox.com。

# 目　　录