Broadview
www.broadview.com.cn

Microsoft®

安全技术大系

Hunting Security Bugs

安全漏洞追踪

【美】Tom Gallagher　Bryan Jeffries　Lawrence Landauer 著
钟力　朱敏　何金勇 译

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

安全技术大系

Hunting Security Bugs

安全漏洞追踪

[美]Tom Gallagher　Bryan Jeffries　Lawrence Landauer 著

钟力 朱敏 何金勇 译

電子工業出版社

Publishing House of Electronics Industry

北京•BEIJING

内 容 简 介

这是一本针对安全测试的书籍，同时也是一本十分适合信息安全研究人员的优秀参考书。本书共20章，其中前3章讨论了安全测试的基础，包括如何从攻击者的角度去思考测试方法，以及如何进行威胁建模和入口点查找。第4章至第19章则通过详细的示例与代码，分别深入地阐述了网络流量和内存数据的操控方法，包括缓冲区溢出、格式化字符串、HTML脚本、XML、规范化、权限、拒绝服务、托管代码、SQL注入和ActiveX再利用等安全漏洞追踪方法，以及在二进制代码条件下查找安全漏洞的逆向工程技术。第20章论述了合理报告安全漏洞的程序，并提出了一个负责的安全漏洞公开流程。最后，本书还提供了一个适于初学者的测试用例列表。

版权合同登记号　图字：01-2007-4584

图书在版编目（CIP）数据

安全漏洞追踪 /（美）盖弗（Gallagher,T.），（美）詹弗瑞斯（Jeffries,B.），（美）兰德（Landauer,L.）著；钟力，朱敏，何金勇译. —北京：电子工业出版社，2008.10
（安全技术大系）
书名原文: Hunting Security Bugs
ISBN 978-7-121-07371-7

I. 安…　II. ①盖…　②詹…　③兰…　④钟…　⑤朱…　⑥何…　III. 软件开发－安全技术　IV. TP311.52

中国版本图书馆CIP数据核字（2008）第140005号

责任编辑：江　立
印　　刷：北京智力达印刷有限公司
装　　订：北京中新伟业印刷有限公司
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
开　　本：787×980　1/16　印张：33.25　字数：686千字
印　　次：2008年10月第1次印刷
定　　价：80.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。
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。
服务热线：（010）88258888。

致　谢

本献给我的父母——非常感谢你们一直以来对我的支持和鼓励。
献给 Vy（Sara）Vu——感谢你为我所做的一切，你真的令人惊叹。

—Tom

感谢父母一直以来对我的关爱、支持和指导。
感谢朋友们对我不得不错过“Wing Dome”之夜的理解。
尤其要感谢我深爱的妻子 Kim，是她一直在那陪我度过所有的日日夜夜，
任劳任怨、尽其所能地帮助我；你是我的全部。

—Bryan

感谢和祝福一直关注安全的人们；
感谢 Katherine（GG）对我的高度信任、支持、祝福和信心；
感谢 Joy 和 Christopher 对我的鼓励和祝福；
感谢妈妈和 John 给我买了第一台计算机；
感谢微软公司所有为我提供这个机会的人。

—Lawrence

推荐序

当 Jesse James——美国西部著名的歹徒被问到他为什么抢劫银行时，他回答道："钱在那！"同样地，任何一个可能雇佣你作为安全测试员的现代公司，在它的内部网络上都有着非常重要的资产，同时心怀恶意的人将会试图进入内部网络并窃取那些资产。无论你测试的是哪种软件——内部使用的、外部网站的或现成的商业软件——总会有人有目的地攻击你的产品。改善应用程序的安全涉及设计人员、开发人员和测试人员，而且，安全测试人员的角色是不能被低估的。

有那么多关于软件安全的书，为什么要读这本书呢？我认识很多在微软公司和比较大的安全协会中能查找安全缺陷的人，但 Tom Gallagher 和 Lawrence Landauer 的工作我非常了解，他们是最优秀的和表达最清楚的人中的两位。在微软 Office 可信计算小组（The Microsoft Office Trustworthy Computing team）中，有一些在行业中最好的安全测试人员。Tom、Lawrence 和他们的朋友及合著者 Bryan Jeffries 都极富经验，并且知识渊博。在本书中他们提供的信息将会使你更深层次地认识安全测试。

来看看到目前为止已经在其他书中探讨过的主题，比如《黑客大曝光（Hacking Exposed）》和《Assessing Network Security》。这些书很好地揭示了网络黑客和从事网络安全评估的人所使用的技术。如果你的工作是开发更安全的软件，那么它们会是很有用的信息，能帮助你看到那些很容易受到黑客攻击的缺陷。但是，虽然掌握这种知识是好事，但它们并不能帮助你快速、有效、系统地查找安全问题。而这就是本书将要讨论的主题。

有些人的工作就是在其他人的产品中查找安全缺陷，其中一个最有创造性的人就是 Greg Hoglund。他的书《Exploiting Software》（2004 年，与 Gary McGraw 合著，Addison-Wesley 公司出版）对在此行业中对最优秀的、最具有创造性的人是如何查找漏洞的给予了一些很好的阐述。但 Greg 没有源代码，也没有询问开发人员，所以他采用了一个不同的方法。正如 Tom 简短的解释：安全行业的超级明星每年仅能发现和公布非常少的问题。当我在互联网安全系统的 X-Force 组（Internet Security System's X-Force）管理漏洞搜寻人员时，该组中最优秀的人每个月做得好的话能够发现一个或两个严重的安全问题。一个专业的软件测试人员不会奢侈到花费这么长时间来查找如此少的漏洞，同时，大多数阅读本书的人还要负责功能特性的测试，这会进一步地限制了他们的时间。你可以把本书作为一种资源来帮助你理顺和加强安全测试进程。

也许你更关心那些受公司防火墙保护的内部运行的软件。如果公司的网络相当大，那

么最安全的设想就是将内部网络当作一个半公开、半敌对的网络来对待。大多数的公司已经犯下了雇佣错误，同时内部安全的不足会允许心怀不满或恶意的雇员做许多坏事。尽管由内部人员发起的内部攻击比来自外部网络的攻击要少得多，但是他们攻击成功的可能性要大得多，并且能造成更严重的伤害。我也曾看到过一些内部的、在线交易应用程序的例子，它使大公司的网络变得不安全。如果攻击者找到了系统所在，那将会有很多问题。大网络之外具有一定熟练程度的攻击者想达到这个目的是极度困难且代价不菲的。

你为什么需要学习安全呢？由安全漏洞导致的损失已经非常严重。如果你正在为微软公司或者另外一家大的软件厂商工作，你就会看到安全问题对你的客户和公司的影响。对你和你的客户来说，花费时间修补已经售出的软件比在软件发行前发现漏洞的代价要昂贵得多。在经历了系统崩溃和其他一些损失后，如果厂商不在产品发行前找到并修补安全缺陷的话，客户几乎不可能从他们那再购买软件。

更糟的是，这种形势正变得更加具有挑战性。攻击者可利用的工具正变得更加完善且更容易使用。在 90 年代中期，需要非常专业的开发人员编写把缓冲区溢出变成可利用程序的汇编代码。近几年来，许多优秀的安全审计小组都有一个或多个人在渗透测试期间编写漏洞利用程序来攻击定制的软件。现在，一个点选式（point-and-click）的网站能产生针对多种操作系统的漏洞利用代码，克服了许多用户输入方面的限制，通常会很容易地把开发人员的错误变成可利用的条件。

在攻击者可得到的资源变得更加全面的时候，攻击者也变得越来越全面。很多年以前，闯入计算机的人一般不会破坏任何东西或他们可能仅仅恶作剧一下。因为互联网上并没有多少计算机，而且被侵入的计算机也没有什么有趣的东西，所以在攻击者中产生了一套道德规范。人们会写一些带有政治口号或者只会引起一点点小麻烦的病毒。真正有破坏性的病毒是非常罕见的。

现今，有人控制了大量的计算机形成“僵尸”大军。为了获取金钱，有人编写复杂的间谍软件而不是病毒。如今攻击者的目标通常是金钱，社会上甚至存在着从商业网站偷取信用卡的市场需求。位于日本东京的一家安全公司——Little Earth Corporation——最近对一百多个商业网站进行了评估，发现具有严重安全问题的网站比安全网站要多得多。尽管开发操作系统和 Web 服务器的开发人员做了大量工作，但如果建立在那些安全平台上的软件是不安全的，那么客户的数据和公司的声誉就会存在风险。

为了充分保护你的客户，请阅读本书吧！

David LeBlanc
2006 年 4 月

译 者 序

本书是一本难得的面向安全测试的好书，凝聚了作者在该领域渊博的知识和丰富的经验。前三章是本书讨论内容的基础，第 1 章提出了安全测试的基本思路和方法，认为从攻击者的角度去思考如何进行安全测试，是目前最有效的方法；第 2 章讨论了威胁模型在安全测试中的关键作用，指出理解软件工作机制和数据流程图，列举数据的入口点和退出点，分析潜在的威胁和数据处理点，是威胁建模的重要内容；第 3 章则介绍了常见的入口点及其查找方法。第 4 章至第 19 章分别针对不同的主题进行深入的阐述，内容涉及如何对网络流量和内存等数据进行操控，缓冲区溢出、格式化字符串、HTML 脚本、XML、规范化、权限、拒绝服务、托管代码、SQL 注入和 ActiveX 再利用中的安全漏洞及其测试方法，以及怎样在二进制代码条件下进行逆向工程来查找安全漏洞。第 20 章讨论了合理报告安全漏洞的程序，并提出了一个负责的漏洞公开流程。最后，附录 A 和附录 B 给出了本书引用的相关工具列表和适于初学者的测试用例列表。

本书最大的特点就是“广”和“实”。它探讨了几乎所有的软件存在安全漏洞的地方，覆盖面非常宽；而且，对每一个主题都进行了深入的分析，给出明确的指导和具体的实例。该书不但能够很好地直接用于安全测试，同时对于从事信息安全研究的技术人员来说，也不失为一本优秀的参考书。

我们成立了一个 10 人组成的团队来翻译这本书。除前言和第 3 章由大家共同翻译之外，王中锋翻译了第 4、5、6 章，朱敏翻译了第 7、8 章，唐云翻译了第 9、12 章，何金勇翻译了第 10、11 章，阮强翻译了推荐序、致谢和第 13、14 章，李蒙翻译了第 15 章，张金祥翻译了第 16、17 章，张志鹏翻译了第 18、19 章，韦朋辉翻译了附录 A 和附录 B，我翻译了第 1、2、20 章，并对本书进行了全文校对。在这里，我十分感谢大家的辛勤劳动，正是由于每个人的努力付出，本书的翻译工作才得以顺利完成。在翻译过程中，我尽量兼顾每位成员所擅长的研究方向和工作经验，但由于本书非常全面，有些领域我们涉猎不深，再加上时间紧迫，水平有限，所以翻译难免有误，敬请读者谅解。另外，在本书的翻译过程中，得到了出版社的大力支持，在此表示衷心的感谢。

钟　力

2008 年 8 月 8 日

前　言

你可能想知道微软为什么要出版这样一本关于安全测试的书，因为加强软件安全是一件非常困难的事情。当然，微软已经遇到过相当多的软件安全问题，因而有大量的经验供测试人员参考。在2002年可信计算计划被提出之前，我们就已经在微软工作了。自微软实施该计划以来，我们已经看到微软在处理安全问题方面的重大改变。现在，安全问题已经不仅仅是安全专家的职责，已经成为了我们每一个人的责任。这本具有创见性的关于软件安全测试的书，源于我们在微软的工作经验以及为开发出用户购买后能持续安全可靠运行的软件而做出的努力。

应用软件的安全并不仅仅局限于使用安全技术的功能特征，以及像加密和账户管理这样的功能特征。我们必须认真考虑一个产品的每个功能特征的安全。鉴于此，在微软工作的每个项目管理人员、开发人员、测试人员和相关技术人员都有责任保证软件尽可能安全。本书认为安全是每个人的责任，并且重点向测试人员提供用来发现软件功能安全漏洞的信息，这些安全漏洞都可能是难以发现的。

本书没有阐述这些漏洞应该如何修补。其他的一些书，如Michael Howard和David LeBlanc所写的《Writing Secure Code》（微软出版社，2002年）是一本从编写代码的角度阐述如何修补和防止安全漏洞的优秀参考书。

微软因为发布了含有安全缺陷的软件而经历了一些惨痛的教训，后来微软不得不通过安全更新来修补这些缺陷。本书描述了现在许多软件中存在的安全问题，并包含了一些已经带来损失的漏洞信息，以及我们在产品发布前自己发现的一些漏洞信息。我们希望你能从我们的经验中学到知识，从而在发布自己的软件时防止产生类似的安全漏洞。

在本书中，我们把能够被另外一名用户控制的数据称为“攻击者已控数据（Attacker Controlled Data）”。我们这么做，是要让你不仅意识到应用程序所操作的数据有可能来自攻击者，还应该树立攻击者的意识，认识到你也能控制这些数据。我们鼓励你不但要像攻击者那样带有恶意的想法去思考，而且在测试软件时还要扮演攻击者，攻击你自己的系统，以此来帮助公司发现软件的安全漏洞。

本书的目的就是为了促进你的测试工作，能够开发出更好的软件，而不是让你攻击其他人的软件，或者利用攻击者的恶意想法或技术去分析不属于你测试范围的软件。本书是一本为白帽黑客而写的书。

软件安全一直在快速地发展。未来我们将面临今天所不知道的危险攻击。但是无论如

何，本书讨论的以攻击者的角度、采用攻击者的方法进行安全测试的步骤，并不会发生太大的改变。

本书的读者对象

软件测试人员是此书的主要读者。下面列出的这些读者朋友因其工作性质，都能从本书中受益：

- **软件测试人员**：测试人员有责任全面了解他们所测试的功能特征工作原理的技术细节。软件测试时会用到这些技术细节。我们为测试人员展示了如何利用功能特性的测试知识来完成安全测试。我们在微软的测试机构工作过，曾经花费了几年的时间与软件测试人员在一起，帮助他们更好地理解如何在已进行功能特性测试的地方进行安全测试。在撰写本书的过程中，我们已向功能特性测试人员和安全专家寻求了反馈意见。
- **软件开发人员**：尽管此书并没有介绍如何构建和编写安全代码的知识，但它的确介绍了如何攻击软件。软件开发人员应该对这方面比较感兴趣，因为准确地理解攻击是如何进行的，开发人员就能更好地保护他们的应用软件。软件开发人员也能学到特定测试领域的知识，然后要求安全测试人员开发适用于这些测试领域的代码。
- **学生**：现在许多学校是不会讲授如何进行安全测试的相关知识。如果学生毕业以后，从事软件和信息技术领域的工作，可能会因为没有接受过安全测试的教育而感到手足无措。阅读此书的学生能够在设计、写作和配置安全软件等方面获取更多的技能。这些技能有助于他们找到工作并胜任工作。
- **渗透测试人员**：专业的渗透测试人员（也被称为安全测试专家）对于此书所要讨论的许多主题也许已经十分了解。很可能，书中一大段文章可以引起渗透测试人员探寻未知领域的兴趣。这本书包含了客户端和服务器应用程序。我们从该领域专家那里获知了信息和建议，这些专家可以是我们所讨论的某些技术的提出者，也可以是专注于安全测试技术的专家。

本书的组织结构

你可以按照章节顺序阅读此书。然而，本书中的许多章节都可以独立成篇。前三章介绍了此书的背景信息，是其他章节的基础。第 4 章“成为恶意的客户端”和第 5 章“成为恶意的服务器”解释了网络流量是如何被操控的，我们平时所讨论的许多攻击行为都需要

操控网络流量。第 8 章“缓冲区溢出及堆栈/堆操纵”和第 9 章“格式化字符串攻击”一并阐述了攻击者是如何通过直接操控内存来执行任意代码的。第 18 章“ActiveX 再利用攻击”和第 19 章“其他再利用攻击”阐述了各种各样的再利用攻击。在书的最后，你会看到一系列工具（附录 A）和一份安全测试用例列表（附录 B），其中包含了一些适用于初学者的基本测试用例。

书中绝大部分章节在开始处都有一个高度概括的概要，在结尾处会总结一些精炼的测试技巧。有些章节也包含了一些走查，你可以在自己的计算机上尝试这些步骤。

系统需求

你需要配置以下的硬件和软件来编译和运行书中提到的代码实例。

- Microsoft Windows XP with Service Pack 2, Microsoft Windows Server 2003 Service Pack 1 或更高补丁版本
- Microsoft Visual Studio 2003 标准版或 Microsoft Visual Studio 2003 专业版或以后版本
- 600 MHz 奔腾或兼容处理器（推荐 1GHz 奔腾处理器）
- 192 MB 内存（推荐 256 MB 或更高）
- 显示器（800 × 600 或更高的分辨率）至少采用 256 色（推荐 1024 × 768，16 位色）
- 微软鼠标或其兼容设备

技术更新

因为书中涉及的相关技术是不断更新的，更新的内容将被放在微软出版社的技术更新网页上，地址如下：

http://www.microsoft.com/mspress/updates/

定期访问该页面可以获取 Visual Studio 2005 和其他技术方面的更新。

代码实例及附带内容

本书包含了一些预先设计好的代码实例、附带工具和程序。书中讨论的所有代码实例和附带内容能在以下地址下载：

http://www.microsoft.com/mspress/companion/0-7356-2187-X/

本书技术支持

我们已尽最大努力来确保本书及附带内容的正确性。微软出版社通过以下网址为本书及附带内容提供技术支持：

http://www.microsoft.com/learning/support/books

问题与评论

如果你对本书及附带内容有任何评论、问题或建议，或者你的问题在上述网址中没有找到解答，请发 E-mail 至 bn@phei.com.cn。

致谢

我们非常感谢为本书内容提供了想法、技术见解和其他反馈意见的人士。以下人士慷慨地贡献了他们的时间无偿审阅了此书的部分章节，这些人士是：Atin Bansal、Srijan Chakraborty、Shawn Farkas、Stephen Fisher、Greg Foltz、Raul Garcia、Greg Hartrell、Eric Jarvi、Chris Jeuell、Hidetake Jo、Akhil Kaza、Ariel Kirsman、Alex Krawarik、Secure Windows Initiative Team 的 John Lambert、Web Services Team 的 John Lambert、Ivan Medvedev、Bala Neerumalla、Maurice Prather、Walter Pullen、Yong Qu、David Ross、Micky Snir、Peter Torr、Ambrose Treacy、Don Willits 和 Oleh Yuschuk。

以下人士的付出应受到特别的赞誉：微软安全响应中心（Microsoft Security Response Center）的 Christopher Edwards 认真审阅了本书，并对第 20 章“报告安全漏洞”提供了反馈，Jason Geffner 校对了第 17 章“观察及逆向工程”并提出了一些合理的建议。Sean Hunt 和 Mark Iler 超出我们预期地审阅了本书的更多章节并提供了反馈意见。Alan Myrvold 认真地审阅了本书几乎每一页，他同时也提出了很多评论和建议，提供了一些附加的信息资源。

本书谈到了两个由微软员工编写但未公开的工具，他们慷慨地允许我们把这些工具提供到本书的对应网址上。其中，MITM 由 Jiri Richter 开发、ObjSD 由 Vikram Subramanian 开发。这两个工具都十分有用。再次感谢他们允许我们公开这两个工具。同样感谢 Mark Russinovich 对 Sysinternals 工具问题的解答，以及对进程浏览器工具的细致修改。

特别感谢 Imran Akhtar、Matt Cohen、 Grant George、David Hansen、 David LeBlanc、

Mark Mortimore、Tara Roth 和 Matt Thomlinson，他们全力支持了我们的测试活动，为本书提出了宝贵建议。David LeBlanc 更是帮助我们描述了安全测试的重要性。感谢 Ben Ryan(策划编辑)、Kathleen Atkins（项目编辑）、Christina Palaia（文字编辑）、William Teel（美工）和 Chris Weber（技术编辑），为了使本书更易懂、语法更准确、技术更精确，他们做了大量的工作。

目　录