HZ BOOKS

Testing Web Security: Assessing the Security of Web Sites and Applications

网络与信息安全技术丛书

行之有效的安全测试技术

Web安全测试

(美) Steven Splaine 著

李昂 王梅蓉 金旭 等译

机械工业出版社
China Machine Press

网络与信息安全技术丛书

Web安全测试

（美） Steven Splaine 著

李 昂 王梅蓉 金 旭 等译

机械工业出版社
China Machine Press

本书分为五个部分：第一部分提供了本书的概述并阐明了本书的主要框架。第二部分为“测试计划”，并涉及围绕着计划测试效果的一些相关事项。第三部分“测试设计”是本书的重点，大部分内容为详细列举的各种各样的可选测试，这一部分包括了第3、4、5、6、7、8章。第四部分是“测试实施”，讲述如何最好地执行这些测试，即由谁来实际做这些工作、需要使用什么工具以及以什么顺序执行测试（排列测试优先级），这部分包括第9章和第10章。在全书的最后，还附有丰富的附录，提供了大量的背景知识。

本书使用了最新的材料，书中所列各种测试方法都有实际的步骤及具体的项目，因而操作性较强，是一本不可多得的好书。本书适合专业的网站安全评估人员阅读，对于各公司的CIO、系统管理员以及广大的网络技术研究者也很有参考价值。

Steven Splaine: Testing Web Security: Assessing the Security of Web Sites and Applications (ISBN:0-471-23281-5).

本书版权登记号：图字：01-2002-6223

图书在版编目（CIP）数据

Web安全测试 /（美）斯普莱恩（Splaine, S）著；李昂等译. -北京：机械工业出版社，2003.5
(网络与信息安全技术丛书)
书名原文：Testing Web Security Assessing the Security of Web Sites and Applications
ISBN 7-111-11908-8

I. W… II ①斯… ②李… III. 计算机网络-安全技术 IV. TP393.08

中国版本图书馆CIP数据核字（2003）第023800号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）
责任编辑：翟静华 姚 蕾
北京昌平奔腾印刷厂印刷·新华书店北京发行所发行
2003年5月第1版第1次印刷
787mm × 1092mm 1/16 · 17.25印张
印数：0 001-4 000册
定价：39.00元

译 者 序

Internet已经成为人类所构建的最丰富多彩的虚拟世界，在世界各地，用户的数目正在飞速增长。而Web作为Internet上最主要的服务，已经成为万众瞩目的焦点和Internet的象征。几乎所有的政府、公司、机构，甚至是个人都建立了自己的Web站点。据报道，现在Web的内容正以每天两百万页的速度增加。随着Internet及Web一同发展起来的还有安全问题，每天都在发生的黑客入侵及篡改网页等问题越来越引起了人们的关注，因为随着Web内容的增加、应用程序功能的丰富和用户的普及，安全问题已经不容忽视。

很多公司的管理者甚至一些技术人员都认为只要有一个防火墙保护就能保证网络的安全。其实不然，尽管建立防火墙是必不可少的安全措施，但防火墙不是万能的，在某些情况下它也会失效，例如：在网站上运行的应用程序有缺陷、防火墙配置不当或有心怀不满的内部人员。还曾经有人说过：只要有足够的时间，任何网站都可以被攻破。不幸的是，现在需要测试安全漏洞的网站的数目远远多于那些有足够经验完成这样一种测试的安全专家的人数，这意味着很多网站及其应用程序往往没有经过充分的测试，或者根本没有进行过测试。

因此，对网站的安全进行全面的测试评估和规划部署是一件非常必要的工作。本书作者Steven Splaine是一位经验丰富的网络安全专家，在本书中，他通过很多例子和详细的检查列表向读者介绍了全面的安全测试方法。本书不同于那些泛泛而谈的图书，本书介绍的方法具有极强的可操作性，相信各位读者看完全书后也会有自己的体会。

本书共分五个部分：第一部分介绍本书的框架；第二部分介绍测试计划；第三部分是本书的重点，作者在此用了六章的篇幅详细列举各种各样的可选测试；第四部分为测试实施，告诉读者如何进行实际操作；第五部分为附录，提供附加的背景知识。

我们相信，本书不仅对系统管理员、安全测试人员会有很大的帮助，而且对于网站设计开发人员、各公司主管网络技术的经理也有较大参考价值。希望本书的翻译出版能为提高国内迅速发展的Web网站的安全水平做出一点贡献。

全书由李昂、王梅蓉、金旭、陈长春、郭龙永、王冶、李鹃君、常欣、李桦、时丁、李海涛、文静、李祥、刘海宁、丁镇兴等进行翻译，前导工作室全体工作人员共同完成了本书的翻译、录排、校对等工作。本书最后由宋涛统稿。由于时间仓促，且译者的水平有限，在翻译过程中难免会出现一些错误，请读者批评指正。

宋 涛

2003年1月

序

现在，越来越多的企业使用基于Internet或基于内联网的应用程序，人们逐渐意识到自己已经暴露在新的或渐增的系统质量风险中，尤其是在性能方面和安全方面存在隐忧。Steven Splaine的新书：《The Web Testing Handbook》提供给读者建议和技术来测试性能，并考虑其他很多重要的有关网站测试的问题，例如实用性。而在本书中，Steven关注的是最关键的问题——网站测试。

相当多的用户甚至于网站应用程序的测试人员都认为：要解决Web安全问题，仅需买个防火墙并接上各种连线就行了。在本书里，Steven认为这是“防火墙神话”，而我在自己的测试、咨询和培训工作中，曾见过相信这种神话的受害者。本书不仅有助于打破这种神话，而且也提供了可以采取的实用步骤，这些步骤可以使你在网络上发现并解决安全问题。客户端、服务器端、Internet、内联网、外部的黑客及其入侵方法、软件、硬件、网络和社会工程，这些内容都是本书要讨论的问题。如何进行一个渗透性测试？怎样评估每个潜在的安全漏洞的特有风险等级，并正确地测试它们？当面对一个现有的系统或创建一个新系统时，应如何监控发生的每件事情？而这一桩桩一件件的事情，每件都可能引发各式各样的麻烦。本书会成为我下一个网站测试项目的重要资源。如果你正在负责一个网站系统的安全或正在测试一个网站系统的安全性，我相信本书定会对你有所帮助。

Rex Black

Rex Black咨询公司（Bulverde, Texas）

前　言

随着Internet的不断发展，越来越多的企业把他们充满宣传材料只起推广作用的站点逐步改造成了担负重要任务的网站。设计网站是为了获得新的利润和整合现有的系统。实现这些整体目标的人所面临的最严峻的挑战之一，就是确保这些新的店面免遭攻击和不当使用。

不幸的是，现在需要测试安全漏洞的网站数目远远多于那些有足够经验完成这种测试的安全专家的人数。这意味着很多网站及其应用程序往往没有经过充分的测试，或者根本没有进行过测试。实际上，这些企业在玩“黑客轮盘赌”的游戏，仅仅希望自己走运罢了。

没有足够的专家进行网站及其应用程序的安全测试，其中一个重要原因是缺少入门级的书。现在面市的图书不是面向高层的，就是面向底层的。前者偏重战略性，定位于高级管理人员和首席架构师，他们设计系统的高度实用性。而后者则极端技术化，定位于实现这些设计的有经验的开发人员和网络工程师。

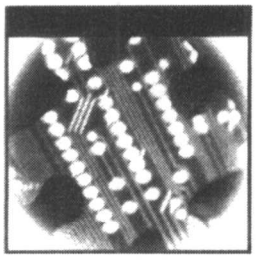
本书是一本简明易懂、易于按步操作的书，任何初涉安全测试领域的人都可以轻松读懂。我的第一本书《The Web Testing Handbook》（与Stefan Jaskiel合著，2001）的读者会发现我在本书中保留了第一本书的列表格式。因为我发现这种列表格式是如此地广受欢迎，所以希望保留这种列表格式会使安全测试人员更容易确保开发人员和网络工程师实现一个系统，而这个系统恰恰能够满足用户和设计者所构想的明确的或暗含的安全目标。

Steven Splaine

目　录

第四部分 测试实施

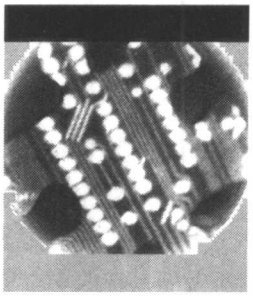
第五部分 附 录



第一部分

本书概述

第1章 概　述



以下这些严峻的统计数字和事实可以形象地说明评估网站及其应用程序的需要是多么迫切。由计算机安全学会（Computer Security Institute，CSI）协同旧金山联邦调查局开展的2002计算机犯罪和安全调查中提供了以下的统计数字（可以从www.gocsi.com免费获得）。

- 90%的被调查者（主要是大公司和政府机构）在过去12个月中探测到有计算机安全漏洞。
- 74%的被调查者称其Internet连接遭受频繁攻击，而40%的被调查者探测到有来自外部的系统渗透。
- 75%的被调查者估计他们过去所受的攻击的一部分可能来自于心怀不满的雇员。

以下清单列举了在过去四年半里向CERT（Computer Emergency Response Team，美国计算机应急响应小组）协调中心（www.cert.org）报告过的与安全相关的事件的数目：

- 2002（第一季度和第二季度）——43 136
- 2001——52 658
- 2000——21 756
- 1999——9 859
- 1998——3 734

2002年2月，路透社(www.reuters.com) 报道了“黑客进攻”造成CloudNine通信（英国最老的ISP之一）退出运营的事件。CloudNine公司得出的结论是，恢复遭受黑客进攻的系统所需的成本太高，以致于公司无法负担。于是CloudNine公司选择了把所有客户让给他们的竞争对手。

2002年5月，CNN财经在线（www.money.cnn.com）报道，一个美国大汽车制造商的财会部门警告13 000人要小心自己的身份信息被盗，因为他们发现“黑客”冒充其雇员企图盗取顾客的信用报告。

1.1　本书的目的

安全领域，尤其是网络安全，是一个非常复杂和广泛的知识领域。而安全失效的后果可能是极其严重的。从业者经过多年学习研究只会意识到：他们知道的越多，还需要知道的也就越多。实际上，这种挑战看起来是如此令人望而生畏，以致于很多人选择避开这个问题，并且拒绝对他们所做的系统的安全负责。当项目组里的很多成员不对系统安全进行测试时，“我们并不负责安全问题——其他人负责”是最常见的借口。当然，当问到到底是谁负责时，最常听到的回答是“我不知道”。而这意味着安全测试是不完整的或根本没有。

第二个有效安全测试的障碍是很多老板和高级经理所持有的幼稚想法：他们保护其内部网及其应用程序所做的仅需购买一个防火墙设备，并把它插入组织与Internet连接的地方。尽管防火墙无疑是网站不可缺少的防护，但它决不应该成为一个组织保护其网站设施的惟一防护。大多数复杂的防火墙所提供的防护会因以下几种情况而失效：在网站上运行的设计有缺陷的网站应用程序、防火墙配置不当或工作在内部的心怀不满的雇员。

防火墙神话

以下两组真实对话形象生动地举例说明了“防火墙神话”。Anthony 是一家欧洲的软件测试咨询公司的主管，而Kevin是佛罗里达一家大型销售公司的拥有者。

Anthony：我们刚刚雇人装了三个顶尖的防火墙，所以现在我们十分安全了。

安全测试员：有没有人测试过它们是否正确地配置了？

Anthony：没有，我们为什么那样做呢？

Kevin：我们正在整个公司安装新的无线通信网络。

安全测试员：你们对数据传输加密了吗？

Kevin：我不知道。这有什么区别吗？根本没人会攻击我们，即使有，我们的防火墙也会保护我们。

本书有两个目的。一是提高负责网站安全的经理们的警惕性，即防火墙应成为安全解决方案的一部分，而非全部。这有助于他们设计和规划需要哪些工作来测试入侵者用以危害网站的所有可能方法。二是为数目日趋增长的一类人提供指导，他们初涉安全领域，但仍被期望能够评估网站的安全。尽管什么书也代替不了多年的经验，但本书还是提供了成百组可供选择采用的测试样例的描述和清单。这些组测试可以收入网站测试计划中，从而使得测试工作更加全面。出于实用性考虑，本书的每部分还推荐了一些工具用以自动执行测试任务，从而加速测试进程。

1.2 本书的测试方法

测试方法可以用很多种方式分类，白盒黑盒法是最常用的方法之一。黑盒测试（也称行为测试）把待测的系统看作是测试者不可见的黑盒。因此，所有测试必须经由系统外部接口执行（例如，应用程序的网页），并且测试需基于系统被明确或暗含的要求所规定的表现而设计。白盒测试技术的测试者可以访问源代码并能看到盒内系统的内部工作情况。这就是为什么白盒测试有时也称为透明盒、玻璃盒、半透明的或结构性的测试。访问源代码有助于测试者了解系统是如何工作的，并使他们可以设计测试运行特定程序的执行路径。输入数据可通过内部或外部接口提交。测试结果无需仅仅基于外部输出，它们也可以从检测内部数据存储中推测出（例如应用程序数据库的记录或操作系统的注册表项）。

通常，这两种方法在寻找缺陷上并不见得一种本来就比另一种更有效率。这取决于特定的测试项目的特定环境（例如，是谁来做测试，他们是测试开发人员还是最终用户），一种方法可能比另一种更容易或实现起来代价更低。Beizer(1995)、Craig等 (2002)、Jorgensen(2002)和Kaner等 (1999)提供了关于黑盒和白盒测试技术更多的信息。

灰盒测试技术可以被看成是一种混合方法。换句话说，测试者仍将把系统看作黑盒来测试，但是这些测试是基于其通过使用类白盒的调查技术所获得的知识来设计的。灰盒测试者使用从检测系统内部结构所获得的知识可以设计出更准确、更有侧重点的测试，这比用传统黑盒测试所探测得到的缺陷率要更高。而同时，灰盒测试者也能够不用像白盒测试者那样在测试时消耗资源设施，而完成这些测试。

灰盒测试

灰盒测试结合了黑盒和白盒两种测试的基本元素。它包括源于有关应用程序内部工作机制及其互动环境的知识的一些方法和工具。这种额外的知识可以用于黑盒测试中以改进测试效率、寻错和析错效率。

来源：Nguyen(2000)

只要可能，本书就会采用灰盒方法来进行安全测试。通过先介绍用于创建或部署待测系统所涉及到的技术，并随后解释每种技术设计或实施方案潜在的缺陷（或漏洞），读者就能够以资源友好的黑盒方式来创建更有效的测试。

本书对有关特定平台和特定威胁的测试执行细节只进行简短的描述，例如如何保护Win2000/IIS v5.0服务器站点免受尼姆达（Nimda）病毒的威胁（这种特定威胁的更多细节，可参考CERT对策CA-2001-26，www.cert.org）。本书所讲的不是现存的成千上万种不同的安全威胁的详尽细节（仅在2002年上半年，CERT协调中心记录了报告到的2 148个漏洞），而是一般性的可预见的测试，并可以被读者根据个别的情况和特定的需要而自己配置更改的。而且，本书并

未涉及到如何利用一个安全漏洞（这种信息对于滥用安全者似乎更为有用，而非安全测试者），并努力避免推荐如何去修复一个安全漏洞，因为绝大部分的修复会随着各个组织的不同情况而不同,并且这种决策和随后的实施通常是安全设计者应做的。

1.3　本书的组织

尽管大多数的读者可能喜欢按顺序阅读，但本书的组织方式允许读者以任意顺序阅读任意章节。这取决于读者的背景和目的，某些读者也许会跳过某些章节。例如，经常测试网站应用程序的实用性，非常精通于撰写测试计划的测试经理，就可以跳过有关测试计划部分而侧重于介绍新测试类型的章节，这些完全可以写入他或她的测试计划。而网站应用程序开发员，他或她可能不关心有关测试网站物理安全的章节（因为其他人负责这些），而对有关网站应用程序安全的章节更感兴趣。

为使读者更容易选择他们所感兴趣的章节，本书分为五部分。第一部分由本章构成，旨在提供本书的概述和介绍本书的主要框架。

第2章“测试计划”，构成第二部分“计划测试效果”，并涉及到了围绕着计划测试效果的有关的一些事项。

第三部分“测试设计”是本书的重点，其大部分内容为详细列举的各种各样的可选的测试。当测试组评估什么应当作为测试一个网站及其相关应用程序的安全测试效果的一部分时，这些是他们应该考虑的。因为这些测试要求测试者有不同的技能，所以可能不同的测试组会选取不同的测试组合。出于这种考虑，这些测试已基于要求测试者必要的技术和背景而归类。这部分包括以下各章：

第3章：网络安全

第4章：系统软件安全

第5章：客户端应用程序安全

第6章：服务器端应用程序安全

第7章：潜在的攻击：防范很少考虑的安全威胁

第8章：入侵者混淆、探测和响应

在讨论了需要什么测试后，第四部分“测试实施”，讲了有关如何最好的执行这些测试，即谁来实际做这些工作，需要使用什么工具，以及以什么顺序执行测试（排列测试优先级）。这部分包括以下各章：

第9章：评估和渗透选择

第10章：风险分析

为支撑这10章，附录提供了附加的背景知识。尤其是有关现在大多数网站所采用的网络技术的基础知识的简短介绍（出于这种考虑：本书部分读者可能不熟悉有关创建网站的部分内容）。前20个重要的安全漏洞的概略清单［由SANS学会（The Systems Administration, Networking and Security Institute，系统管理、网络与安全学会）拟定］和一些测试发布模板的样例（安全测试组可采用其作为基础，改写配置自己的测试文档）。

最后，资源部分不单包括本书所引用的参考书目和网站的清单，也列出了其他一些参考书，对网站安全感兴趣的读者在扩展自己知识方面会觉得有用的。

1.4 本书所用的术语

以下两节介绍了本书中用来描述人或名称的一些术语，即那些试图利用网站漏洞的人、安全测试员力图阻止的那些人以及安全测试员给他们起的更通常的叫法。

1.4.1 黑客、破解者、脚本玩家及心怀不满的内部人员

术语“计算机黑客”（computer hacker）最初指的是某人真正了解计算机内部（硬件软件）是如何工作的，并能依靠他提出的通过系统或者扩展系统的原有功能的天才办法（入侵程序）来解决问题。在这个意义上，大众传媒重新定义了这个术语，指试图非法访问计算机或计算机网络的人。

从业者区分那些试图非法访问的人的技术等级时，使术语变得更加模糊。术语“破解者”（cracker）常用来指有能力编写他或她自己的入侵程序的攻击者。而术语“脚本玩家”（script kiddie）则常用来指主要依靠别人编写的入侵程序的人（这种程序通常以脚本或可执行程序的形式传播）。当要把心怀不满的雇员归类时，情况变得更不明朗。他们无需非法访问就可以实现其恶意的目的，因为他们可以合法地访问系统。

不是所有的攻击者看起来都一样。除了他们不同的技术水平，从他们所遵守的不同规范也可以区分他们。大略地讲，基于他们的行为和意图，攻击者通常可以分为以下以颜色编码的三个群体。

白帽黑客 这些人获得网站拥有者或网站存取产品的拥有者的授权去查明站点或产品是否有足够的保护，以避开已知的安全漏洞或常见的安全缺口。他们也称为“合法黑客”，或“虎队”、“红队”的一部分。

灰帽黑客 有时也被称为怪客（wacker），灰帽黑客主动攻击一种新产品或新技术来寻找产品的安全漏洞，是为了扩展自己的知识，或为了满足自己的好奇心。尽管他们常说的目的是为了提高新技术的质量，或他们的知识并未对任何人造成直接损害，但他们的手法有时是滋事捣乱的。例如，某些这种攻击者并不通知产品的拥有者新发现的安全漏洞，直到他们有时间创建并公布一种给其他人用以容易地利用这个漏洞的工具。