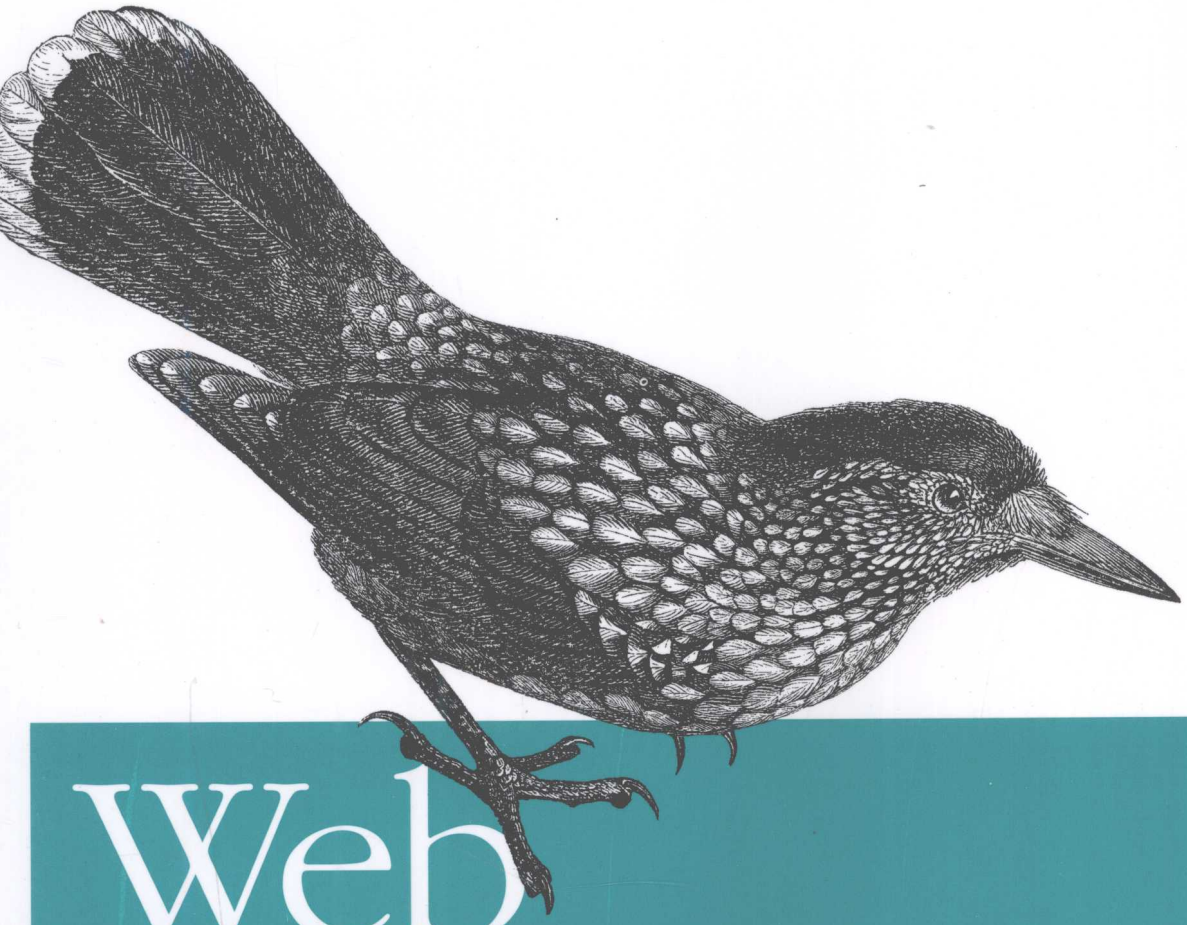
Web Security Testing Cookbook



Web 安全测试

Paco Hope & Ben Walther 著
傅鑫 等译

O'REILLY®

清华大学出版社

Web安全测试

*Paco Hope & Ben Walther*著

傅鑫 等译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo

O'Reilly Media, Inc.授权清华大学出版社出版

清华大学出版社

北京市版权局著作权合同登记

图字：01-2009-5237号

图书在版编目（CIP）数据

Web安全测试 /（美）霍普（Hope, P.），（美）沃尔瑟（Walther, B.）著；傅鑫等译.
—北京：清华大学出版社，2010.3
书名原文：Web Security Testing Cookbook
ISBN 978-7-302-21968-2
I. W… II.①霍… ②沃… ③傅… III. ①互联网络－安全技术 IV. ①TP393.408
中国版本图书馆CIP数据核字（2010）第018843号

责任编辑：龙啟铭
封面设计：Jan Davis 张 健
责任校对：徐俊伟
责任印制：杨 艳
出版发行：清华大学出版社 **地 址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn **邮 编**：100084
社 总 机：010-62770175 **邮 购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京鑫海金澳胶印有限公司
经 销：全国新华书店
开 本：178×233 **印 张**：18.5 **字 数**：404 千字
版 次：2010 年 3 月第 1 版 **印 次**：2010 年 3 月第1 次印刷
印 数：1～3000
定 价：39.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103 产品编号：029772-01

O'Reilly Media, Inc.介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly Media, Inc.授权清华大学出版社翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc.是世界上在 Unix、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时也是联机出版的先锋。

从最畅销的*The Whole Internet User' Guide & Catalog*（被纽约公共图书馆评为20世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly Media, Inc.一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly Media, Inc.是最稳定的计算机图书出版商 —— 每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly Media, Inc.具有深厚的计算机专业背景，这使得O'Reilly Media, Inc.形成了一个非常不同于其他出版商的出版方针。O'Reilly Media, Inc.所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly Media, Inc.还有许多固定的作者群体 —— 他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly Media, Inc.依靠他们及时地推出图书。因为O'Reilly Media, Inc.紧密地与计算机业界联系着，所以O'Reilly Media, Inc.知道市场上真正需要什么图书。

《Web安全测试》的好评

“Paco和Ben理解并解释了curl和HTTP的概念，既轻松却又不失技术性和准确性。他们使这本书成为每个想要了解组成Web应用的‘程序块’并进而了解如何对这些程序块进行安全测试的人的理想指南”

——Daniel Stenberg，cURL的设计者

“我喜爱美味的食物，但我不是个很好的厨师。这就是我依赖于食谱的原因。食谱能快速地给像我这样的厨师带来不错的结果。它们也给了我一个起点，使我可以在此基础上进行试验，学习和改进。《Web安全测试》对我这样的安全测试新手也起到了同样的功效。”

对免费工具的描述，包括Firefox及其安全测试扩展，WebScarab以及许多其他工具，使我能够快速上手。我感谢这个列表，更要感谢书中有关工具在不谨慎使用时可能出现的反作用的警告。

有关编码的解释揭开了我在URL及cookie中见到的那些古怪字符串的面纱。

作为测试人员，我熟悉使用大文件来阻塞应用，但恶意XML和ZIP文件则是下一个发展阶段。“billion laughs”攻击将成为经典。

随着AJAX在Web应用中变得越来越流行，这里介绍的测试秘诀对所有测试人员来说都将是至关重要的，因为应用中将存在比之前多得多的潜在安全漏洞。

“贯穿整本书的精彩的真实示例，使理论生动起来，并使攻击引人入胜。”

——Lee Copeland，StarEast和StarWest测试会议的议程主席，《A Practitioner s Guide to Software Test Design》的作者

“测试Web应用安全通常是一件费时而重复性的过程，遗憾的是它通常是手动完成的。其实并不需要这样，而这本书将教给你简单，高效和可重用技术的关键，它可以帮助你在黑客之前发现问题。”

——Mike Andrews，《How to Break Web Software》的作者

“最后，这是一本供测试人员使用的普通意义上的手册，它讲授安全测试的机制。与其‘秘诀’使用方法不相符的是，这本书实际上武装了测试人员，使他们能够找出甚至连某些最著名的安全工具也无法发现的漏洞。”

——Matt Fisher，Piscis有限责任公司的创始人和CEO

“如果你想知道你的公司是否存在应用安全问题，那么一些失败的安全测试就是最令人信服的证据。Paco和Ben使你从最好的免费Web应用安全工具入手，其中包括许多来自OWASP的工具，而他们的简单秘诀同时完美地适用于开发人员和测试人员。”

——Jeff Williams，Aspect Security的CEO，兼OWASP的主席

“无论你的编程人员有多优秀，严格的测试将始终是生产安全的软件这个过程中的一部分。Hope和Walther将安全测试从黑客手中夺回，并归还到遵守纪律的专业人士的领域。”

——Brain Chess，Fortify Software的创始人/首席科学家

作者简介

Paco Hope是Cigital公司的一名技术经理，《Mastering FreeBSD and OpenBSD Security》（由O'Reilly出版）的合著者之一。他也发表过有关误用、滥用案例和PKI的文章。他曾被邀请到会议就软件安全需求、Web应用安全和嵌入式系统安全等话题发表演讲。在Cigital，他曾担任MasterCard International在安全策略方面的主题专家，而且曾协助一家世界500强的服务业公司编写软件安全策略。他也为软件开发和测试人员提供软件安全基础方面的培训。他还曾为博彩业和移动通信行业中的几家公司提出过软件安全方面的建议。Paco曾在威廉玛丽学院主修计算机科学和英语，并从弗吉尼亚大学获得计算机科学方面的理学硕士学位。

Ben Walther是Cigital公司的一名顾问，Edit Cookies工具的开发者之一。他同时参与标准质量保证和软件安全方面的工作。他日复一日地设计和执行测试——因此他理解忙碌的QA领域对简单秘诀的需求。他也曾对开放式Web应用程序安全项目（OWASP）的成员就Web应用测试工具发表过演讲。在Cigital，他测试包括从财务数据处理到投币自动信贷机在内的系统。Ben具有康奈尔大学信息科学方面的理学学士学位。

封面介绍

封面上的图像是一只星鸦。有关这种迷人的鸟的更多信息，请参见“前言”。

封面图像是Frank Deras独创的照片。

目录

序

Web应用遭受着格外多的安全攻击。其原因在于，网站及在网站上运行的应用在某种意义上是所有公司和组织的虚拟正门。Web自1993年以来的发展令人瞠目结舌，就其被广泛采用的速度而言，甚至超过了电视和电力技术。

Web应用在软件开发中所扮演的角色不断成长并且越来越重要。事实上，评论家日前称我们已经进入了Web 3.0时代（参见*http://www.informit.com/articles/article.aspx?p=1217101*）。问题在于，安全性确实没能跟上这种发展步伐。目前，我们在加固Web 1.0应用的安全方面仍有很多的问题，以致于还没有开始加固Web 2.0的安全，更别提Web 3.0了。

在继续之前，我有一些话不吐不快。Web应用是很重要而且正在不断发展的一类软件，但它们并不是唯一的软件类型！事实上，考虑到遗留应用，嵌入式设备以及世界上的其他代码，我相信Web应用只占到所有软件的一小部分。因此，当世人将所有对软件安全的注意力全部倾注在Web应用上时，我感到担忧。有大量其他类型的重要软件并不依赖于Web。这就是我自称是软件安全人员而不是Web应用安全人员的原因。

无论如何，Web应用安全和软件安全确实存在许多共同的问题和缺陷（这一点也不奇怪，因为前者是后者的子集）。一个共同的问题是将安全作为一项功能，或者某种“东西”。安全并不是某种“东西”，它是系统的一项属性。这意味着再多的身份验证技术、神奇的加密技术或者面向服务架构（SOA）Web服务安全API都无法自动地解决安全问题。事实上，与任何其他方面相比，安全与测试及保障都有着更多的关联。

打开这本书，哦，我们确实需要一种有效的Web应用安全测试方法么？要知道，许多由安全专家为Web应用测试所设计的“测试”都不具有任何测试严密性。原来测试本身就

是一门学科，背后有整套的学问。Paco和Ben带给我们的是对测试线索的深入了解。这真是一对珍贵的组合。

所有称职的测试人员都理解，关于测试的一项关键要素是：测试结果必须能够用于指导行动。差的测试结果会给出像“bigjavaglob.java文件中存在XSS问题”这样含糊的报告。开发人员怎么会知道如何去修复这个问题呢？这里缺少的是适当地说明XSS是什么（当然，它指的是跨站式脚本），指出在成千上万行代码的文件中问题可能出现的位置，以及如何做才能修复它。本书中包含了大量技术信息，足以供像样的测试人员向真正起作用的开发人员报告可用于指导行动的结果。

但愿本书中的内容不仅能够被安全人员采用，而且也能够被Web应用的测试人员所采用。事实上，质量保证（QA）人员会高兴地看到，本书正好面向测试人员，书中采用了回归测试、覆盖率以及单元测试等术语。以我的经验来看，就测试而言，测试人员做得要比安全人员好得多。使用得当的话，本书可以将安全人员改造成更优秀的测试人员，将测试人员改造成更优秀的安全人员。

本书的另一重要特点在于，它明确地将重点放在工具和自动化上。与现代安全人员一样，现代测试人员也使用工具。本书包含了大量基于实际工具的真实例子，其中许多工具都可以从网上免费下载。事实上，本书适用于指导正确的工具使用方法，因为书中描述的许多开源工具都没有自带内置的手册或入门指导。我喜欢实践性的资料，而这本书在实际动手方面做到了极致。

一种过度乐观的软件开发方法必然会创造出令人吃惊的东西，但是从安全角度而言，它同样也会使我们陷入困境。简单地说，我们会忽视去考虑自己的软件在遭到故意和恶意攻击时会发生什么。攻击者就在大门口，每天都在探查我们的Web应用。

软件安全就是建立安全的软件，并使之在遭到恶意攻击时仍然能够正常运转的实践。本书的主题就是软件安全最重要的实践之一——安全测试。

—— Gary McGraw

前言

Web应用无处不在，存在于每个行业。从零售业到银行，人力资源，再到博彩，每一项都存在于Web上。现在，小到个人博客，大到至关重要的金融应用，所有这一切都建立在某种类型的Web应用之上。如果我们要想顺利地将应用移至Web上，或者要在Web上建立新的应用，我们必须能够有效地测试这些应用。但是，只需功能测试就已足够的那些日子一去不返了。今天，Web应用面临着无处不在且不断增长的安全威胁，这种威胁来自于黑客、内部人员、罪犯以及其他人员。

这本书讲述如何测试Web应用，并特别关注安全。我们是需要测试Web软件的开发人员、测试人员、设计师、质量经理和顾问。无论遵循哪种质量或开发方法论，将安全添加到我们的测试日程中都需要使用一种新的方式来进行测试。我们还需要专门工具来促进安全测试。在本书的所有秘诀中，我们都将利用Web应用的共有特性。我们将尽可能多地利用我们所知道的对Web应用而言始终正确的事情，或者通常正确的事情。这种普遍性使得本书中的秘诀具有通用性，并且很可能满足你的需求。此外，这意味着你将开发具有通用性的工具，这些工具可用来测试多种应用。

本书的目标读者

这本书面向的是主流开发人员和测试人员，而不是安全专家。每个参与到Web应用开发之中的人都能从本书中找到有价值的内容。负责为组件编写单元测试的开发人员将会欣慰地看到，这些工具能够精确地关注于单个页面、功能或表单。必须测试整个Web应用的QA工程师们将会特别感兴趣于那些能够轻松地成为回归测试套件中一部分的测试用例的自动化和开发。本书中的秘诀主要是利用免费工具，使之容易被采用，使读者在努力之余无需提交购买申请或投入大量资金。

我们为本书选择的工具以及我们选出作为秘诀的任务都是与平台无关的。这意味着两件非常重要的事情：它们总能够运行在你的桌面电脑上，而不管你的PC上运行着哪种操作系统（Windows，MacOS，Linux，等等），此外，它们总能与你的Web应用协同工作而不论你的应用采用了哪种技术。它们同样适用于ASP，PHP，CGI，Java和任何其他Web技术。有些情况下，我们会提到某种环境所特有的任务，不过通常这只是锦上添花，而并非秘诀的重点所在。因此，这本书的读者可以是使用任意Web平台的任意开发人员或测试人员。要利用书中的这些技术，你不需要拥有特殊工具（除了我们在本书中谈到的免费工具）或特殊环境。

利用免费工具

有许多免费的测试工具可用于帮助开发人员或测试人员测试他们的应用中基本功能的安全。这些工具不仅免费，而且往往可定制程度高，非常灵活。在安全方面，最好的工具往往是免费的，这种现象可能要比QA中任何其他专业领域都要更为突出。即使在商业软件已经变得成熟且功能强大的网络安全领域，商业软件对抗唾手可得且免费的工具也花费了很久时间。即使是现在，也没有哪位网络管理员完全使用商业工具来完成工作。免费工具仍然能够很好地发挥适当的功能。

不过，在很多情况下，免费工具都缺少帮助文档。这正是本书将要填补的缺口：向你演示如何很好地利用这些工具，这些工具你可能已经有所耳闻，但是却没有好的文档讲述如何以及为何使用它们。我们认为主流开发人员和测试人员正与免费且唾手可得的工具擦肩而过，因为他们不懂得如何使用这些工具。

使用免费工具有效地测试Web应用的另一障碍是人们对如何将工具结合起来执行好的安全测试普遍缺乏了解。知道TamperData可以用来绕过客户端检查是一回事，而使用TamperData开发出好的跨站式脚本测试则是另一回事。我们希望能够使你不仅限于生成好的Web应用测试，而且能够生成好的安全测试用例并从这些测试中获取可靠的结果。

最后，由于许多开发和QA机构没有太多的工具和培训预算，所以本书将重点放在免费工具上，这意味着你在尝试这些秘诀的时候无需为昂贵的工具申请演示版许可证。

关于封面

封面上的鸟是一只星鸦（*Nucifraga columbiana*），它作为Web应用安全测试过程的吉祥物是再贴切不过的了。星鸦设法撬开尚未成熟的松果以取出松子。它们的喙的结构适合于伸进那些小角落和缝隙将食物取出。作为安全测试人员，我们设法使用专门工具撬开