TURING 图灵程序设计丛书 网络安全系列

WILEY

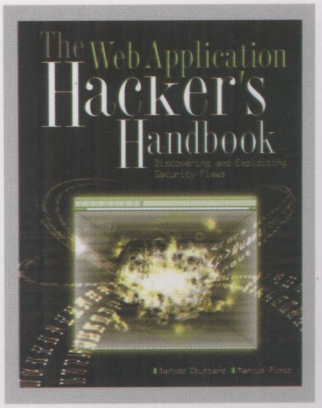
The Web Application Hacker's Handbook

Discovering and Exploiting Security Flaws

黑客攻防技术宝典

Web实战篇

[英] Dafydd Stuttard
Marcus Pinto 著
石华耀 等译



- 跟安全技术大师学习黑客攻防技术
- 全面分析Web应用程序安全漏洞
- 大量实例和代码片段

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书 网络安全系列

The Web Application Hacker's Handbook

Discovering and Exploiting Security Flaws

黑客攻防技术宝典

Web实战篇

[英] Dafydd Stuttard
Marcus Pinto 著
石华耀 等译

人民邮电出版社
北 京

图书在版编目（CIP）数据

黑客攻防技术宝典：Web实战篇 /（英）斯图塔德（Stuttard, D.），（英）平托（Pinto, M.）著；石华耀等译．—北京：人民邮电出版社，2009.8
（图灵程序设计丛书）
书名原文：The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws
ISBN 978-7-115-21077-7

Ⅰ.黑… Ⅱ.①斯…②平…③石… 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（2009）第105816号

内 容 提 要

本书是探索和研究Web应用程序安全缺陷的实践指南。作者利用大量的实际案例、屏幕快照和示例代码，详细介绍了每一种Web应用程序弱点，并深入阐述了如何针对Web应用程序进行具体的渗透测试。本书从介绍当前Web应用程序安全概况开始，重点讨论渗透测试时使用的技巧和详细步骤，最后总结书中涵盖的主题。每章后还附有习题，便于读者巩固所学内容。

本书适用于各层次计算机安全和Web开发与管理领域的技术人员。

图灵程序设计丛书

黑客攻防技术宝典：Web实战篇

◆ 著 [英] Dafydd Stuttard Marcus Pinto
译 石华耀 等
责任编辑 朱 巍

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京顺义振华印刷厂印刷

◆ 开本：800×1000 1/16
印张：32
字数：796千字 2009年8月第1版
印数：1－4000册 2009年8月北京第1次印刷

著作权合同登记号 图字：01-2008-3321号

ISBN 978-7-115-21077-7/TP

定价：69.00元

读者服务热线：(010)51095186 印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

本书是发现并利用Web应用程序安全漏洞的实用指南。这里的“Web 应用程序”是指通过使用Web浏览器与Web服务器进行通信，从而加以访问的应用程序。本书不仅分析了大量各种各样的技术，如数据库、文件系统与Web服务器，而且讨论了它们在Web应用程序中的使用情况。

如果你想了解如何运行端口扫描、攻击防火墙或以其他方式对服务器进行渗透测试，我们建议你阅读其他书籍。但是，如果你希望了解渗透测试员如何攻击Web应用程序、窃取敏感数据、执行未授权操作，那么本书可以满足你的需要。本书将就以上主题展开全面而详实的讨论。

本书概述

本书极其注重实用性。虽然我们提供了足够的背景信息与理论知识，以帮助读者了解Web应用程序中包含的漏洞；但是，渗透测试员在攻击Web应用程序时所需要实施的步骤及采用的技巧，才是我们讨论的重点所在。本书详细阐述了探查每一种漏洞所需采用的特定步骤，以及如何利用它执行未授权操作。我们还根据多年的工作经验，列出大量实例，说明在当今Web应用程序中存在的各种安全漏洞。

另一方面，安全意识就像一把双刃剑。开发者能够从了解攻击者所使用的方法中受益；相反，黑客也可以通过了解应用程序的防御机制而窥探它的受攻击面。除介绍安全漏洞与攻击技巧外，我们还将详细介绍应用程序为抵御攻击者而采用的应对措施。同时，Web应用程序渗透测试员还可以从本书中获得大量实用的建议，以帮助应用程序所有者强化他们的应用程序。

本书目标读者

本书的目标读者是Web应用程序渗透测试员，以及负责开发和管理Web应用程序的人，因为了解你的敌人有助于对他们进行有效防御。

我们希望读者熟悉核心安全概念，如登录和访问控制；并希望读者掌握基本的核心Web技术，如浏览器和HTTP。通过阅读本书提供的解释说明或其他参考资料，可以迅速弥补当前读者在这些领域的知识欠缺。

在介绍各种安全漏洞的过程中，我们将提供代码片断，说明应用程序为何易受攻击。这些示例都非常简单，不需要事先了解编写代码的语言就能够理解它们；但是，已经掌握阅读或编写代码的基础知识会更有用。

本书结构

总体而言，本书根据不同主题之间的依赖关系将内容组织在一起。如果你还不了解黑客是如何攻击Web应用程序的，应该从头至尾读完本书，以了解在后续有关章节中需要用到的背景信息和技巧。如果你在这方面已经拥有一定的经验，可以直接跳到特别感兴趣的任何章节或部分。必要时，我们将提供其他章节的交叉参考，以帮助你弥补理解上的欠缺。

本书前3章介绍一些背景信息，描述当前Web应用程序的安全状况，说明它将来的发展趋势。然后将介绍影响Web应用程序的核心安全问题，以及应用程序为解决这些问题所采取的防御机制。同时还将介绍当前Web应用程序所使用的关键技术。

本书的主要部分重点讨论核心主题——渗透测试员在攻击Web应用程序时使用的技巧。我们根据实施全面攻击所需要完成的关键任务组织材料，这些任务依次为：解析应用程序的功能，检查和攻击它的核心防御机制，探查特殊类型的安全漏洞。

最后3章对本书涵盖的各种主题进行简要总结：描述如何在应用程序源代码中查找漏洞；回顾能够帮助渗透测试员攻击Web应用程序的工具；详细介绍一种攻击方法，说明渗透测试员如何对一个目标应用程序实施全面而深入的攻击。

第1章描述当前在因特网上运行的Web应用程序的安全状况。尽管软件商常常保证Web应用程序是安全的，但绝大多数的应用程序并不真正安全；只要掌握一些技巧，就能够攻破它们。Web应用程序中的漏洞源于一个核心问题：用户可提交任意输入。这一章将分析造成当今应用程序安全状况不佳的关键因素，并说明Web应用程序中存在的缺陷如何使得组织的全面技术基础架构非常易于受到攻击。

第2章描述Web应用程序为解决“所有用户输入都不可信”这个基本问题而采用的核心安全机制。应用程序通过这些机制管理用户访问、控制用户输入、抵御攻击者。这些机制还为管理员提供各种功能，帮助他们管理和监控应用程序自身。应用程序的核心安全机制还是它的主要受攻击面，在对它们实施有效攻击前，渗透测试员必须了解这些机制的工作原理。

第3章简要介绍渗透测试员在攻击Web应用程序时可能遇到的关键技术，包括相关HTTP协议、客户与服务器端常用的技术以及各种数据编码方案。已经熟悉主要Web技术的读者可以跳过本章。

第4章描述渗透测试员在攻击一个新的应用程序时所需采取的第一步，即收集与应用程序有关的尽可能多的信息，以确定它的受攻击面，制定攻击计划。渗透测试员需要搜索并探查应用程序，枚举它的全部内容与功能，确定所有用户输入进入点并查明它所使用的技术。

第5章描述了存在漏洞的第一个区域。如果一个应用程序依靠在客户端实现的控件来保护它的安全，就可能造成这种漏洞。这种保护应用程序的方法往往存在缺陷，因为攻击者可轻易避开任何客户端控件。应用程序易于受到攻击的原因有两个：(1) 通过客户传送数据，认为这些数据不会被修改；(2)依赖客户端对用户输入进行检查。这一章将介绍一系列有用的技术，包括HTML、HTTP与JavaScript所采用的轻量级控件，以及使用Java applet、ActiveX控件和Shockwave Flash对象的重量级控件。

第6～8章将主要介绍Web应用程序中最重要的防御机制——负责控制用户访问的机制。第6

章描述应用程序确认用户身份的各种功能，包括主登录功能和更加外围的与验证有关的功能，如用户注册、密码修改和账户恢复功能。验证机制在设计和执行方面都包含大量漏洞，攻击者能够利用它们获得未授权访问。这些漏洞包括明显的缺陷，如保密性不强的密码和易于受到蛮力攻击，以及验证逻辑中存在的更微妙的问题。这一章还将详细分析许多安全性至关重要的应用程序所采用的多阶段登录机制，并描述这些机制中频繁出现的新型漏洞。

第7章介绍会话管理机制。大多数应用程序通过有状态会话这个概念补充无状态的HTTP协议，帮助它们在不同的请求中确定每个用户的身份。当Web应用程序受攻击时，这个机制是一个主要的攻击目标；因为如果能够攻破它，就能够有效避开登录机制，伪装成其他用户，而不必知道他们的证书。这一章还将分析生成和传送会话令牌过程中存在的各种常见漏洞，并描述发现和利用这些漏洞所需采取的步骤。

第8章说明应用程序如何实施访问控制。应用程序主要依靠验证与会话管理机制来完成这项任务。本章将介绍各种破坏访问控制的技巧，以及探查和利用这些弱点的方法。

第9章介绍大量相关漏洞。如果应用程序以不安全的方式在解释型代码中插入用户输入，就会造成这种漏洞。我们首先说明SQL注入漏洞，讨论各种攻击方法，从最明显、最简单的方法到一系列高级利用技巧（如带外通道、推断和时间延迟）。对于每一种漏洞和攻击技巧，我们将描述3种常用数据库（MS-SQL、Oracle和MySQL）之间的相关差异，然后介绍其他几种注入漏洞，包括操作系统命令注入、Web 脚本语言注入、注入SOAP/XPath/SMTP/LDAP协议。

第10章介绍一种简单而重要的漏洞。如果应用程序以不安全的方式将用户输入提交给文件系统 API，就会造成这种漏洞，使得攻击者能够获取或修改Web服务器上的任意文件。我们将描述各种技巧，说明应用程序为防止路径遍历攻击而实施的防御机制。

第11章将介绍应用程序受攻击面的一个重要的、常被人们忽略的区域——实现其功能的内部逻辑。应用程序逻辑中的漏洞各不相同，它们比 SQL 注入与跨站点脚本之类的常见漏洞更难以辨别。为此，我们将列举一系列实例，它们中存在的逻辑缺陷使得应用程序易于受到攻击，借此说明应用程序设计者与开发者所做出的各种错误假设。根据这些各不相同的缺陷，我们将进行一系列特殊测试，以确定许多常常难以探测的逻辑缺陷。

第12章将介绍一种严重的漏洞。如果Web应用程序中存在的缺陷使得应用程序的恶意用户能够攻击其他用户，并以各种方式危及他们的安全，就会造成这种漏洞。跨站点脚本漏洞是其中最重要的漏洞，它非常流行，影响着因特网上绝大多数的Web应用程序。我们将详细介绍各种不同类型的XSS漏洞，并说明如何探查并利用即使是最难以辨别的漏洞。然后，我们将分析另外几种针对其他用户的攻击方法，包括重定向攻击、HTTP 消息头注入、框架注入、跨站点请求伪造、会话固定、利用ActiveX控件中的缺陷以及本地隐私攻击。

第13章并不介绍任何新的漏洞，而是描述一种渗透测试员攻击Web应用程序时需要掌握的技巧。由于每种应用程序都各不相同，大多数攻击都经过某种方式的定制（或自定义），以针对应用程序的特殊行为，以及发现对攻击有利的操纵方法。这些攻击还要求提出大量相似的请求，并监控应用程序的响应。手动执行这些请求非常费力，而且容易出错。要真正熟悉Web应用程序，必须尽可能自动实施攻击步骤，使定制攻击更加简单、快捷而高效。本章将详细描述一种正被证实的方法，以完成这项任务。

第14章分析应用程序如何在遭受攻击时泄露信息。当实施本书描述的其他各种攻击时，渗透测试员应该始终监控应用程序，以确定其他可供利用的信息泄露来源。我们将介绍如何分析应用程序的反常行为与错误消息，以深入了解应用程序的内部工作机制，并细化攻击。我们还将介绍如何利用存在缺陷的错误处理机制，从应用程序中获取敏感信息。

第15章介绍在以C和C++等代码语言编写的应用程序中存在的一些重要漏洞。这些漏洞包括缓冲区溢出、整数漏洞和格式化字符串漏洞。这个主题涉及的内容非常广泛，我们将重点讨论如何在Web应用程序中探查这些漏洞，并分析一些实例，了解造成这些漏洞的原因，以及如何对它们加以利用。

第16章介绍一个常被忽略的Web应用程序安全领域。许多应用程序采用一种分层架构，无法正确隔离这些层面可能会导致应用程序易于受到攻击，使得攻击者能够利用在其中一个组件中发现的漏洞迅速攻破整个应用程序。共享主机环境带来另外一些严重的威胁；有时，攻击者可以利用一个应用程序中存在的缺陷或恶意代码攻破整个环境及其中运行的其他应用程序。

第17章描述各种攻击技巧，说明如何通过攻击Web服务器进而攻击其中运行的Web应用程序。Web 服务器中存在的漏洞主要包括服务器配置方面的漏洞以及Web服务器软件中的安全漏洞。这个主题属于本书的讨论范围，因为严格来讲，Web 服务器是技术栈的另一个组件。但是，大多数Web服务器都与在它们之中运行的Web应用程序关系密切。因此，本书介绍针对Web服务器的攻击，因为攻击者常常可以利用它们直接攻破一个应用程序，而不是首先间接攻破基础主机，然后再攻击Web应用程序。

第18章描述另外一种查找安全漏洞的方法。这种方法与本书其他章节讨论的方法截然不同。许多时候，我们都可以对应用程序的源代码进行审查，并且不必得到应用程序所有者的协助。通常，审查应用程序的源代码可以迅速确定一些漏洞，但在运行的应用程序中探查这些漏洞可能极其困难，或者需要耗费许多时间。我们将介绍一种代码审查方法，并简要说明如何对以各种语言编写的代码进行审查，以帮助读者在编程经验不足的情况下进行有效的代码审查。

第19章详细介绍本书描述的各种工具。我们将分析这些工具的优缺点，讨论一些全自动工具能否有效地发现Web应用程序中存在的漏洞，并提供一些提示和建议，说明如何充分利用工具包。

第20章综合介绍本书描述的所有攻击步骤与技巧。我们将根据渗透测试员在实施攻击时所需完成的任务之间的逻辑依赖关系来组织这些步骤与技巧，并对它们进行排序。如果你已经阅读并理解书中描述的各种漏洞和攻击技巧，就可以把这个方法当作一个完整的清单和工作计划，对Web应用程序实施渗透测试。

需要的工具

本书着重讨论渗透测试员在攻击Web应用程序时所采用的实用技巧。阅读本书后，你将了解每项攻击任务的细节、它们涉及的技术以及它们为什么有助于探查和利用各种漏洞。下载某个工具，使用它攻击一个目标应用程序，并根据它的输出结果了解应用程序的安全状况，这些内容并不是本书讨论的重点。

也就是说，当实施我们描述的步骤与技巧时，你会发现一些有用、有时甚至是必不可少的工具。所有这些工具都可以在因特网上找到，建议你下载并试用本书介绍的每一个工具。

同步网站内容

本书的同步网站（www.wiley.com/go/webhacker）提供一些掌握各种攻击技巧所需要的有用资源，该网站主要包括以下内容：

- 本书列出的一些脚本的源代码；
- 本书讨论的所有工具和其他资源的链接；
- 攻击一个常见应用程序的步骤列表；
- 每章结束部分提出的问题的答案；
- 包含本书描述的许多漏洞的一个攻击挑战。

其他说明

Web应用程序安全是一个有趣而流行的主题。对我们而言，撰写本书是一种享受。我们希望，在学习本书描述的各种攻击技巧和了解如何防御这些攻击手段的过程中，你能够找到乐趣。

此外，我们在此提出严正警告。在许多国家，未经所有者许可而攻击他们的计算机系统的做法属非法行为。如果未经他人同意，执行我们描述的绝大多数技巧可能会触犯法律。

本书作者为专业的渗透测试员，他们代表客户对Web应用程序实施攻击，以帮助强化应用程序的安全。近年来，许多安全专业人士与其他人由于未经许可而尝试或主动攻击计算机系统，从而犯罪，其职业生涯也因此结束。我们强烈要求你仅在法律许可的范围内使用本书提供的信息。

目　录

第1章 Web应用程序安全与风险

Web应用程序安全无疑是当务之急，也是值得关注的话题。对相关各方而言，这一问题都至关重要。这里的相关各方包括因特网业务收入日益增长的公司、向Web应用程序托付敏感信息的用户，以及通过窃取支付信息或入侵银行账户偷窃巨额资金的犯罪分子。可靠的信誉也非常重要，没人愿意与不安全的Web站点进行交易，也没有组织愿意披露有关其安全方面的漏洞或违规行为的详细情况。因此，获取当前Web应用程序安全状况的可靠信息不可小视。

本章简要介绍Web应用程序的发展历程及它们提供的诸多优点，并且列举我们亲身体验过的在目前Web应用程序中存在的漏洞，这些漏洞表明绝大多数应用程序还远远不够安全。本章还将描述Web应用程序面临的核心安全问题（即用户可提交任意输入的问题），以及造成安全问题的各种因素。最后讨论Web应用程序安全方面的最新发展趋势，并预测其未来的发展方向。

1.1 Web应用程序的发展历程

在因特网发展的早期阶段，万维网（World WideWeb）仅由Web站点构成，这些站点基本上是包含静态文档的信息库。随后人们发明了Web浏览器，通过它来提取和显示那些文档，如图1-1所示。这种相关信息流仅由服务器向浏览器单向传送。多数站点并不验证用户的合法性，因为根本没有必要这样做；所有用户同等对待，收取同样的信息。创建一个Web站点所带来的安全威胁主要与Web服务器软件的（诸多）漏洞有关。攻击者入侵Web站点并不能获取任何敏感信息，因为服务器上保存的信息可以公开查看。所以攻击者往往会修改服务器上的文件，以歪曲Web站点的内容，或者利用服务器的存储容量和带宽传播“非法软件”。

如今的万维网与早期的万维网已经完全不同，Web上的大多数站点实际上是应用程序（见图1-2）。它们功能强大，在服务器和浏览器之间进行双向信息传送。它们支持注册与登录、金融交易、搜索以及用户创作的内容。用户获取的内容以动态形式生成，并且往往能够满足每个用户的特殊需求。它们处理的许多信息属于私密和高度敏感的信息。因此，安全问题至关重要：如果人们认为Web应用程序会将他们的信息泄露给未授权的访问者，他们就会拒绝使用这个Web应用程序。

Web应用程序带来了新的重大安全威胁。应用程序各不相同，所包含的漏洞也各不相同。许多应用程序是由开发人员独立开发的，还有许多应用程序的开发人员几乎对他们所编写的代码可

能引起的安全问题一无所知。为了实现核心功能，Web应用程序通常需要与内部计算机系统建立连接。这些系统中保存着高度敏感的数据，并能够执行强大的业务功能。十年前，如果需要转账必须去银行，让银行职员帮助你完成交易。而今天，你可以访问银行的Web应用程序，自己完成转账交易。进入Web应用程序的攻击者能够窃取个人信息，进行金融欺诈或执行针对其他用户的恶意行为。

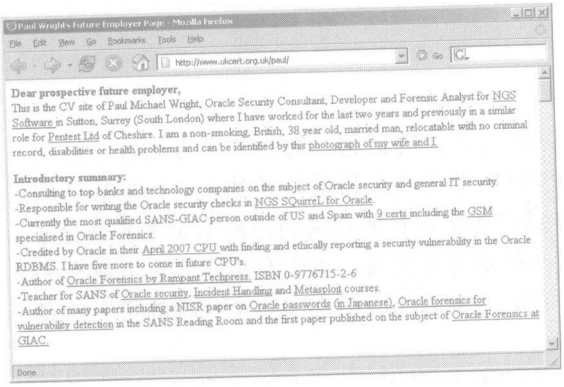


图1-1　包含静态信息的传统Web站点

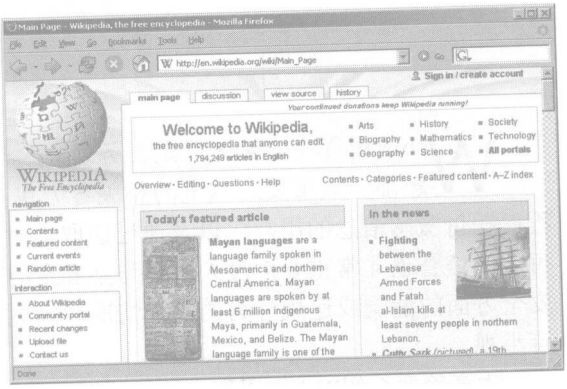


图1-2　典型的Web应用程序

1.1.1　Web应用程序的常见功能

创建Web应用程序的目的是执行可以在线完成的任何有用功能。近些年出现的一些Web应用程序功能有：

- 购物（Amazon）
- 社交网络（MySpace）
- 银行服务（Citibank）
- Web搜索（Google）
- 拍卖（eBay）
- 博客（Blogger）
- Web邮件（Hotmail）
- 交互信息（Wikipedia）

除公共因特网外，许多组织内部也广泛采用Web应用程序执行一些关键业务功能，包括访问人力资源服务、管理公司资源等。硬件设备（如打印机）和其他软件（如Web服务器和入侵检测系统）也往往利用Web应用程序提供管理界面。

在Web应用程序之前出现的许多应用程序已被移植到这种技术之中。商业应用程序，如以前需要使用专用的“厚客户（thick-client）”应用程序才能访问的ERP（Enterprise Resource Planning，企业资源计划）软件，现在通过Web浏览器就可以访问。软件服务，如最初需要一台独立的电子邮件服务器进行传送的电子邮件，如今也可通过如Outlook Web Access之类的Web界面访问。文字处理器和电子表格等传统的桌面办公应用程序都已经通过Google Apps和Microsoft Office Live移

植到Web应用程序中，这种趋势仍将持续。

大多数计算机用户所需要的客户端软件仅仅是一个Web应用程序，这样的时代即将来临。到那时，用户使用一组共享的协议和技术即可执行各种功能，但随之也会出现各种常见的安全漏洞。

1.1.2 Web应用程序的优点

Web应用程序越来越流行的原因显而易见。若干技术因素已经与主要的商业动机相结合，从而引发了因特网使用方式上的重大变革。

- HTTP是用于访问万维网的核心通信协议，它是轻量级的，无需连接。这一点提供了对通信错误的容错性。应用HTTP，许多传统客户-服务器应用程序中的服务器无需再向每一个用户开放网络连接。HTTP还可通过代理和其他协议传输，允许在任何网络配置下进行安全通信。
- 每个Web用户都在其计算机上安装了浏览器。Web应用程序为浏览器动态部署用户界面，不必像以前的Web应用程序那样需要分配并管理独立的客户端软件。界面变化只需在服务器上执行一次，就可立即生效。
- 如今的浏览器功能非常强大，可构建内容丰富并且令人满意的用户界面。Web界面使用标准导航和输入控件，可保证用户即时熟悉这些功能，而不需要学习如何使用各种应用程序。应用程序可通过客户端脚本功能将部分处理交由客户端完成，必要时，可使用厚客户组件任意扩展浏览器的功能。
- 用于开发Web应用程序的核心技术和语言相对简单。即使是初学者，也可使用现有的各种平台和开发工具，开发出强大的应用程序，还有大量开源代码和其他资源可供整合到定制的应用程序中。

1.2 Web应用程序安全

与任何新兴技术一样，Web应用程序也会带来一系列新的安全方面的漏洞。这些常见的缺陷也在“与时俱进”，出现了一些开发人员在开发现有应用程序时未曾考虑到的攻击方式。由于安全意识的加强，一些问题已经得到解决。新技术的开发也会引入新的漏洞。Web浏览器软件的改进基本上消除了某些缺陷。

在整个发展过程中，不时有报道知名Web应用程序被攻破的消息。情况似乎并未好转，也没有迹象表明这些安全问题已经得到解决。可以说，如今的Web应用程序安全领域是攻击者与计算机资源和数据防御者之间最重要的战场，在可预见的将来，这种情况可能仍将持续。

1.2.1 “本站点是安全的”

人们普遍认识到，对Web应用程序而言，安全确实是个“问题”。查询一个典型的应用程序的FAQ页面，其中的内容会向你保证该应用程序确实是安全的。例如：

本站点绝对安全。它使用128位安全套接层（Secure Socket Layer, SSL）技术设计，可防止未授权用户查看您的任何信息。您可以放心使用本站点，我们绝对保障您的数据安全。