Web安全漏洞检测技术

蔡皖东◎编著

中国工信出版集团

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

Web 安全漏洞检测技术

蔡皖东　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书以常见的 Web 安全漏洞为对象，详细介绍了这些 Web 安全漏洞的漏洞成因、检测方法以及防范技术，这些漏洞都是 OWASP TOP 10 中所列举的主要风险，为学习和研究 Web 安全漏洞检测及防范技术提供了有价值的参考。

全书共 11 章，分别介绍了 Web 系统安全概论、Web 安全漏洞检测方法、SQL 注入漏洞检测技术、XSS 漏洞检测技术、缓冲区溢出漏洞检测技术、会话管理漏洞检测技术、服务器配置漏洞检测技术、传输保护弱点检测技术、漏洞检测工具及评价、Web 系统健壮性测试技术、移动互联网安全等内容，所涉及的漏洞基本涵盖了 OWASP TOP 10 中所列举的主要风险。

本书可作为从事相关工作科技人员的参考书，也可作为相关专业本科生和研究生的教材。

图书在版编目（CIP）数据

Web 安全漏洞检测技术 / 蔡皖东编著. —北京：电子工业出版社，2016.3

ISBN 978-7-121-28219-5

Ⅰ. ①W… Ⅱ. ①蔡… 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（2016）第 039751 号

策划编辑：窦 昊
责任编辑：窦 昊
印 刷：北京京师印务有限公司
装 订：北京京师印务有限公司
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：14.25 字数：328 千字
版 次：2016 年 3 月第 1 版
印 次：2016 年 3 月第 1 次印刷
定 价：58.00 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。

前　言

随着互联网技术的不断发展，计算机网络越来越显示出在社会信息化中的巨大作用。它已经成为当前知识经济和社会生活的基础设施，推动了企业信息化、新兴服务业、信息产业的快速发展，带动了国民经济发展和社会进步。

网络系统的开放性以及现有网络协议和软件系统固有的安全缺陷，使得任何一种网络系统都不可避免地、或多或少地存在着一定的安全隐患和风险。人们在享受网络所带来方便和效益的同时，也面临着网络安全提出的巨大挑战，如黑客攻击、病毒传播、非法联络、信息窃取等，威胁到网络信息安全，安全事件屡有发生，给国家安全、企业利益和个人权益带来极大的危害，并造成巨大的经济损失。

随着网民规模和网站数量的持续增长，Web 应用程序已经广泛应用到各个领域，如电子商务、社交网络、网上支付等。同时，Web 应用系统安全问题也越来越突出。根据有关组织调查，约 75%的 Web 安全问题发生在 Web 应用程序上，约 65%的 Web 网站存在较为严重的安全问题。Web 安全漏洞给攻击者造成可乘之机，威胁着 Web 系统安全。因此，Web 系统安全已成为互联网安全的重要组成部分，越来越受到人们的关注和重视。

Web 网站是一种开放的信息系统，它所面临的主要安全风险是来自黑客的外部攻击，包括分布式拒绝服务（DDoS）攻击、网络病毒攻击以及各种渗透式攻击等，给 Web 网站及应用系统安全带来极大的挑战。由于大多数的网络攻击都是利用了信息系统中的各种安全漏洞，包括各种软件漏洞、配置漏洞、结构漏洞以及管理漏洞等，因此及时检测并修复 Web 系统安全漏洞，对于保障 Web 系统安全性是十分重要的。Web 安全漏洞检测技术是一种重要的信息安全技术，成为当前信息安全技术的研究热点。

本书主要介绍 Web 安全漏洞检测及防范技术。全书共 11 章，第 1 章为 Web 系统安全概论，主要介绍 Web 网站系统结构、Web 系统安全态势、Web 安全漏洞分析、Web 系统安全技术等内容；第 2 章为 Web 安全漏洞检测方法，主要介绍静态检测技术、动态检测技术、Web 测试技术、漏洞扫描技术、检测性能评价等内容；第 3 章为 SQL 注入漏洞检测技术，主要介绍 SQL 注入漏洞分析、SQL 注入漏洞检测、SQL 注入漏洞防范等内容；第 4 章为 XSS 漏洞检测技术，主要介绍 XSS 漏洞分析、XSS 漏洞检测、XSS 漏洞防范等内容；

第 5 章为缓冲区溢出漏洞检测技术，主要介绍缓冲区溢出漏洞分析、缓冲区溢出漏洞检测、缓冲区溢出漏洞防范等内容；第 6 章为会话管理漏洞检测技术，主要介绍 Cookie 基本特性、会话管理漏洞分析、会话管理漏洞检测、会话管理漏洞防范等内容；第 7 章为服务器配置漏洞检测技术，主要介绍服务器配置漏洞分析、服务器配置漏洞检测、服务器配置漏洞防范等内容；第 8 章为传输保护弱点检测技术，主要介绍安全套接层协议 SSL、传输保护弱点分析、传输保护弱点检测、传输保护弱点防范等内容；第 9 章为漏洞检测工具及评价，主要介绍三种静态检测工具 YASCA、Pixy、Rips 及其检测性能评价，四种动态检测工具 WVS、AppScan、Nikto、W3af 及其检测性能评价，静/动态工具性能对比等内容；第 10 章为 Web 系统健壮性测试技术，主要介绍 Web 系统测试技术、测试系统组成、系统健壮性测试等内容；第 11 章为移动互联网安全，主要介绍移动互联网安全威胁与对策等内容。

本书以常见的 Web 安全漏洞为对象，通过实例分析方式，系统而具体地介绍漏洞成因、检测方法以及防范技术等，这些漏洞都是 OWASP TOP 10 中所列举的主要风险，为学习和研究 Web 安全漏洞检测及防范技术提供了有价值的参考，使读者能够对这些 Web 安全漏洞有比较全面和深入的了解，有助于在实际工作中避免和防范 Web 安全漏洞。

由于 Web 安全漏洞检测技术比较复杂，很难覆盖 Web 安全漏洞及其检测技术的方方面面，书中难免存在不足和疏漏之处，欢迎广大读者批评指正。

最后，感谢西北工业大学专著出版基金对本书的大力资助。

作　者

于西北工业大学

目　录

第1章

Web 系统安全概论

1.1 引言

互联网技术的不断发展，越来越显示出计算机网络在社会信息化中的巨大作用。它已经成为当今社会经济活动和社会生活的基础设施，推动了工业信息化、新兴服务业、信息产业的快速发展，带动了国民经济发展和社会进步。

2015 年 1 月，中国互联网络信息中心（CNNIC）发布了第 34 次中国互联网络发展状况统计报告，截至 2014 年 12 月底，中国网民规模达到 6.49 亿，全年共计新增网民 3117 万人，互联网普及率为 47.9%。中国网民规模和互联网普及率如图 1.1 所示。

图 1.1 中国网民规模和互联网普及率

截至 2014 年 12 月底，中国手机网民规模达 5.57 亿，较 2013 年底增加 5672 万人，如图 1.2 所示。网民中使用手机上网人群占比由 2013 年的 81.0%提升至 85.8%。

图 1.2　中国手机网民规模及其占网民比例

截至 2014 年 12 月底，我国域名总数为 2060 万个，其中“.CN”域名总数年增长为 2.4%，达到 1109 万，在中国域名总数中占比达 53.8%；中国网站总数为 335 万个，年增长 4.6%，参见图 1.3。

图 1.3　中国网站数量

中国网页的总数量为 1899 亿个，年增长了 26.6%，如图 1.4 所示。其中，静态网页数量为 1127 亿个，占网页总数的 59.36%；动态网页数量为 772 亿个，占网页总数的 40.54%。

图 1.4　中国网页数及其增长率

由于网络系统的开放性，以及现有网络协议和软件系统可能存在着某些安全缺陷或漏洞，任何一种网络信息系统都将面临着一定的安全风险，人们在享受网络所带来方便和效益的同时，也面临着网络安全提出的巨大挑战，如黑客攻击、病毒传播、非法联络、信息窃取等，威胁到网络信息安全，安全事件屡有发生，给国家安全、企业利益和个人权益带来极大的危害，并造成了巨大的经济损失。

以获取经济利益为目的的黑客经济兴起，网络侵权和犯罪活动屡禁不止，手法日益翻新，包括篡改网站内容、攻击网络服务器、传播盗版数字作品、窃取网银账号、组建僵尸网络等，直接危害了网络安全和社会和谐。

不法分子利用互联网传播黄色信息、邪教信息、虚假新闻、政治攻击、垃圾邮件等有害信息，严重扰乱了人们的思想，特别给青少年的身心健康带来极大的损害。

国内外敌对势力利用互联网进行非法联络，通过加密邮件、即时通信、语音通信、社交网络、P2P 通信等手段进行秘密联络，策划和实施恐怖活动，直接威胁着国家安全和社会稳定。

网络间谍利用互联网盗窃国家机密信息、企业内部信息和个人隐私信息，网络窃密和泄密事件不断发生。尤其是海外间谍机关利用木马技术有预谋性地窃取国家的政治、军事和经济情报，直接危害了国家安全和利益。根据国家安全保密部门统计，在我国每年发生的泄密案件中，70%是海外间谍机关通过互联网和木马来窃取的，并且有逐年增长的趋势，对国家安全和利益造成极大的危害。

随着网民规模和网站数量的持续增长，Web 应用程序已经广泛应用到各个领域，如电子商务、社交网络、网上支付等。同时，Web 应用系统安全问题也越来越突出。根据有关组织调查，约 75%的 Web 安全问题都是发生在 Web 应用程序上，约 65%的 Web 网站存在较为严重的安全问题。Web 安全漏洞给攻击者造成可乘之机，威胁着 Web 系统安全。因

此，Web 系统安全已成为互联网安全的重要组成部分，越来越受到人们的关注和重视。

根据第 34 次中国互联网络发展状况统计报告，2014 年，总体网民中有 46.3%的网民遭遇过网络安全问题，我国个人互联网使用的安全状况不容乐观。在安全事件中，电脑或手机中病毒或木马、账号或密码被盗情况最为严重，分别达到 26.7%和 25.9%，在网上遭遇到消费欺诈比例为 12.6%，参见图 1.5。

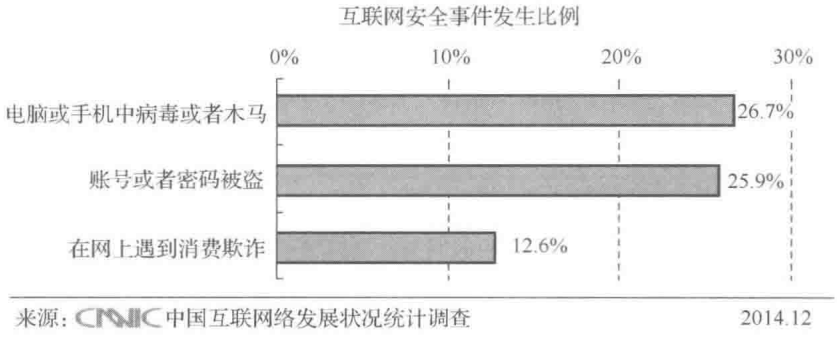


图 1.5　互联网安全事件发生情况

1.2　Web 网站系统结构

Web 系统安全性与 Web 网站系统结构密切相关。根据 Web 网站的性质和系统架构，通常将 Web 网站分为静态网站和动态网站两种。

1．静态网站

静态网站是指以静态网页发布内容的网站，一般不具备网站交互式功能。静态网站由两个部分组成。

（1）Web 服务器：以静态页面形式发布网站内容，网站内容全部由 HTML 代码格式的静态页面组成，所有的内容包含在网页文件中，一般不需要建立数据库。

（2）Web 客户端：支持 HTTP 协议的通用浏览器，如 IE 浏览器等。用户使用浏览器，通过 URL 地址来访问 Web 网站。

2．动态网站

动态网站是指网站内容可以根据不同情况动态变化的网站，主要用于实现网站交互功能，如用户注册、信息发布、产品展示、订单管理等。

动态网站一般采用三层结构来构建，在系统结构上，由 Web 服务器、数据库系统、Web 客户端等三个部分组成（参见图 1.6）。

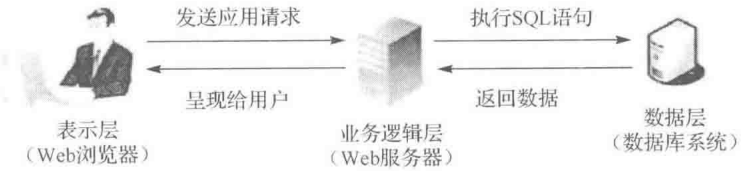


图 1.6　Web 应用系统三层架构

（1）Web 服务器：以动态页面形式发布网站内容，动态网页并不是独立存在于服务器的网页文件，而是根据浏览器发出的不同请求，返回不同的网页内容，动态网页中通常包含有服务器端脚本程序，页面文件名常以.JSP、.PHP 和.ASP 等为后缀。

（2）数据库系统：提供网站数据的存储和查询功能，有无数据库系统是区别动态网站和静态网站的主要特征。

（3）Web 客户端：支持 HTTP 协议的通用浏览器，如 IE 浏览器等，用户使用浏览器，通过 URL 地址来访问 Web 网站。

从应用逻辑上，一个 Web 应用系统由表示层、业务逻辑层和数据层组成（参见图 1.6）。

（1）表示层：表示层位于最上层，主要为用户提供一个交互式操作的用户界面，用来接收用户输入的数据以及显示请求返回的结果。它将用户的输入传递给业务逻辑层，同时将业务逻辑层返回的数据显示给用户。

（2）业务逻辑层：业务逻辑层是三层架构中最核心的部分，是连接表示层和数据层的纽带，主要用于实现与业务需求有关的系统功能，如业务规则的制定、业务流程的实现等，它接收和处理用户输入的信息，与数据层建立连接，将用户输入的数据传递给数据层进行存储，或者根据用户的命令从数据层中读出所需数据，并返回到表示层展现给用户。

（3）数据层：数据层主要负责对数据的操作，包括对数据的读取、增加、修改和删除等操作。数据层可以访问的数据类型有多种，如数据库系统、文本文件、二进制文件和 XML 文档等。在数据驱动的 Web 应用系统中，需要建立数据库系统，通常采用 SQL 语言对数据库中的数据进行操作。

Web 应用系统的工作流程如下：表示层接收用户浏览器的查询命令，将参数传递给业务逻辑层；业务逻辑层将参数组合成专门的数据库操作 SQL 语句，发给数据层；数据层执行 SQL 操作后，将结果返回给业务逻辑层；业务逻辑层将结果在表示层展现给用户。

动态网站主要用于支持复杂的 Web 应用系统，也最容易产生安全漏洞，成为 Web 系统安全防护的重点。

在 Web 应用系统开发中，常用的编程语言和开发环境有 JSP、PHP 和 ASP 等，在使用它们来开发 Web 应用系统时，存在一定的安全问题需要引起重视。

1．JSP 技术

JSP（Java Server Page）是一种功能强大的 J2EE 技术，用于开发动态 Web 页面内容，

如 HTML、XML、DHTML 和 XHTML 等。JSP 技术将 Web 页面中的静态内容和动态内容进行区分，并提供一种简单而有效的方式，将动态数据加载到静态内容中。JSP 提供两种对处理逻辑的封装机制：Java Beans/Enterprise Java Beans（EJB）组件和标签库。Java Beans 组件以约定的格式定义一系列相对独立的属性，并提供直接获取和设置这些属性的方法，提高了代码的可重用性；标签库对处理逻辑进行封装，包括客户动作、方法、监听以及验证逻辑等，并提供类似 HTML 标记格式的标签来调用这些处理逻辑，实现页面表现和处理逻辑的分离。JSP 提供一组标准的标签库，还可以根据 JSP 规范来开发自定义的标签，对现有的标签库进行扩展。

JSP 技术继承了 Java 语言独立于系统运行平台的特点，其动态 Web 页面和组件可以移植在各种操作系统平台上，由相应的 Web 服务器编译执行，并通过各种浏览器进行访问。JSP 技术对 HTTP 请求的响应是多线程的，并且 JSP 引擎不会重复编译已经编译过的 JSP 页面。因此，使用 JSP 开发的 Web 应用系统具有较快的响应速度，与 CGI 技术相比，其性能更好。

在 JSP 规范中，定义了一种嵌套语言，整合了脚本语言、标记语言和描述语言，对处理逻辑进行封装，以实现页面表现和处理逻辑的分离。由于 JSP 技术的优良性能，越来越多的 Web 应用系统使用 JSP 技术来开发，这也使得 JSP 安全问题变得越来越突出。

在使用 JSP 开发应用程序时，可能产生的安全问题如下。

（1）用户以 HTTP 请求的方式访问 JSP 应用服务器资源，如果由 JSP 引擎编译得到的 Servlet 不安全，就会对整个 Web 服务器系统构成很大的安全威胁。

（2）JSP 规范允许与任何一种编程语言相协同，而内嵌的编程语言可能造成 JSP 安全问题。常见的内嵌编程语言是 Java 语言，而 Java 代码的安全漏洞将成为 JSP 安全漏洞的来源之一。

（3）JSP 通过可扩展的标签来分离页面表现和处理逻辑，同时也支持 HTML/XML 等标记语言，这些标签和标记也可能存在一定的安全隐患。

（4）JSP 页面嵌套的脚本语言可能也带来安全问题，例如，使用 Javascript 直接传递数据时可能造成数据泄露。

（5）JSP 技术体系结构比较复杂，其中包含一些交互组件和子系统，这些子系统和组件本身的安全漏洞也是 JSP 安全漏洞的来源之一，包括常用的 Web 容器、数据库等各个子系统之间的交互过程可能产生一些安全问题。

2．PHP 技术

PHP 作为一种 Web 应用程序开发脚本语言，具有方便、快捷、开源等特点，在 Web 应用程序开发中得到了广泛的应用。随着 PHP 功能的不断完善，PHP 已从最初的一种简单的网页开发工具，已发展成为能够处理复杂 Web 应用程序的模块化开发语言，广泛应用于复杂 Web 应用程序的开发。

LAMP（Linux+Apache+MySQL+PHP）架构成为非常流行的 Web 应用程序开发架构。PHP5 开始引入面向对象的概念，并提供异常处理等机制，进一步提升了 PHP 语言的开发能力。

PHP 语言得以流行的主要原因是它具有如下几个重要特点。首先，PHP 是一种开源的编程语言，这就为开发 Web 应用程序节约了大量成本，同时相关的开源社区还提供对 PHP 的功能维护和版本更新，不断推动 PHP 技术的发展和应用。其次，PHP 的官方网站和开源社区都提供在线手册等资料，开发人员能够很容易地得到这些在线资源，可以方便地进行学习和交流。第三，PHP 语言具有平台无关性，可以支持多种操作系统和 Web 服务器平台，特别适合于 LAMP 架构。第四，从 PHP5 版本以后，开始支持面向对象编程，大大降低了开发可重用代码的难度。

由于 PHP 语言具有简单易学、入门快捷等特点，开发人员经过大致的学习后就开始使用 PHP 语言来开发 Web 应用程序。由于对 PHP 语言缺乏深入的了解和准确的掌握，所开发出来的 Web 应用程序中可能存在一些安全缺陷和漏洞。

在使用 PHP 开发应用程序时，可能产生的安全问题如下。

（1）PHP 允许授权用户对文件系统进行访问，通过编写 PHP 脚本，很容易实现对系统中的重要目录和配置文件进行读取或修改，也可以操纵打印机等设备。如果用户授权不合理，则可能导致用户对系统目录或文件进行非法操作，同时也为攻击者获取和篡改系统目录和文件提供了便利。

（2）PHP 提供对 Web 服务器的良好支持，这一特性使得 PHP 用户可以方便地获取或提升自身权限，从而允许以高权限对服务器执行操作。恶意用户可以通过提升 PHP 用户的权限，对服务器实施攻击。

（3）数据库是 PHP 应用中的重要组件，一些敏感或保密的信息可能存储在数据库中，因此数据库信息安全也是 PHP 安全问题的来源之一。PHP 提供对数据库的良好支持，但 PHP 本身并没有提供对数据库的安全保障机制，因此在编写 PHP 脚本时，需要针对数据库连接、查询、权限控制等制定相应的安全策略，防范 SQL 注入攻击。

3. ASP 技术

ASP（Active Server Page）是一种脚本语言编写环境，运行在服务器端，以解释方式来执行。ASP 脚本通过整合 HTML 语言、脚本命令和 Active X 组件，可以用于开发交互性强、功能强大的 Web 应用系统。一个 ASP 应用由若干个对 ASP 脚本的调用组成，每个 ASP 脚本调用的过程大致如下：客户端使用浏览器访问 ASP 脚本，浏览器向服务器发出 HTTP 请求，服务器判断出该请求是针对 ASP 脚本后，通过 ISAPI 接口调用引擎，对 ASP 脚本文件进行解释执行，将处理结果以 HTML 静态内容形式返回给浏览器，最终通过浏览器展示在客户端上。

根据 ASP 应用组成及运行原理，ASP 应用可能产生的安全问题如下。

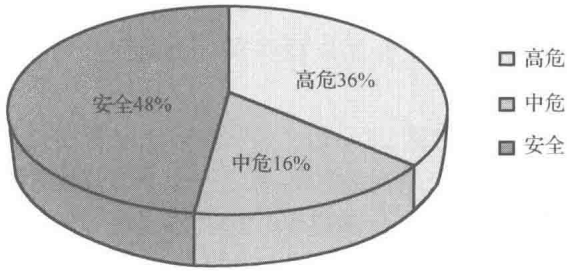
（1）在 ASP 应用开发时，在程序设计上可能存在安全漏洞。如果将用户名和口令在 ASP 文件中进行硬编码，可能造成信息泄露。在 ASP 文件中，仅仅使用简单的判断语句对用户身份和 HTTP 请求对象进行验证，攻击者有可能绕过这种安全验证机制。另外，如果在 ASP 应用程序发布前缺乏足够的调试，则可能会暴露应用文件、数据库路径和目录结构等信息。

（2）ASP 作为一种 Web 应用程序开发技术，通常需要与数据库进行交互。数据库文件的命名和存储有一定的规律性，可能给攻击者提供了猜测数据库信息的机会，而程序中对数据源的硬编码可能导致数据库信息的泄露。

（3）由于缺乏对 HTTP 请求中 URL 字符串的验证，容易遭受远程注入攻击。在请求的 URL 中，包含 ASP 文件路径和文件名，即使对请求该文件进行验证，仍可能得到该页面，从而导致系统信息的泄露。

1.3 Web 系统安全态势

根据 360 安全检测平台对互联网中部分网站安全状况的监测数据，在随机抽取的 93233 个网站中，存在高危漏洞的网站有 33753 个（约占 36%），中危漏洞的网站有 14917 个（约占 16%），比较安全的网站有 44567 个（约占 48%），网站漏洞危险级别分布图如图 1.7 所示。由此可见，目前大部分网站存在着漏洞，严重威胁着网站的安全。



数据来源：360互联网安全中心

图 1.7　网站漏洞危险级别分布

开放 Web 应用安全项目（Open Web Application Security Project，OWASP）是一个开放的非营利组织，主要致力于协助政府、企业和组织开发和维护可信的 Web 应用程序，OWASP 发布的 10 种 Web 安全应用风险排名（即 TOP 10），在业界具有较大的权威性和影响力。OWASP TOP 10 最初于 2003 年发布，并于 2004 年、2007 年、2010 年和 2013 年分别发布了修改版本。在 TOP 10 2007 年及以前的版本中，主要专注于查找最常见的漏洞。而在 TOP 10 2010 年及以后的版本中，主要围绕风险来组织，明确描述了威胁代理、攻击向量、