创教材 · 信息安全系列

Web 安全基础教程

佟 晖 陈晓光 张作峰◎主编

WEB ANQUAN JICHU JIAOCHENG

北京师范大学出版集团
BEIJING NORMAL UNIVERSITY PUBLISHING GROUP
北京师范大学出版社

新世纪高等学校规划教材 · 信息安全系列

Web 安全基础教程

● 佟 晖 陈晓光 张作峰◎主编

WEB ANQUAN JICHU JIAOCHENG

北京师范大学出版集团
BEIJING NORMAL UNIVERSITY PUBLISHING GROUP
北京师范大学出版社

图书在版编目（CIP）数据

Web 安全基础教程 / 佟晖等主编. —北京 ：北京师范大学出版社，2017.8

新世纪高等学校规划教材 · 信息安全系列

ISBN 978-7-303-22377-0

Ⅰ. ①W… Ⅱ. ①佟… Ⅲ. ①互联网络－安全技术－高等学校－教材 Ⅳ. ①TP393.408

中国版本图书馆 CIP 数据核字（2017）第 114358 号

营 销 中 心 电 话 010-62978190 62979006
北师大出版社科技与经管分社网 www. jswsbook.com
电 子 信 箱 jswsbook@163.com

出版发行：北京师范大学出版社 www.bnup.com
北京市海淀区新街口外大街 19 号
邮政编码：100875

印 刷：北京玺诚印务有限公司
经 销：全国新华书店
开 本：787 mm×1092 mm 1/16
印 张：12.25
字 数：277 千字
版 次：2017 年 8 月第 1 版
印 次：2017 年 8 月第 1 次印刷
定 价：29.80 元

策划编辑：赵洛育 责任编辑：赵洛育
美术编辑：刘 超 装帧设计：刘 超
责任校对：赵非非 责任印制：赵非非

主编简介

佟晖，女，硕士研究生，教授，硕士研究生导师。北京警察学院公安科技系副主任，北京警察学院学术委员会委员，北京市高等教育学会计算机教育研究会常务理事。先后承担国家以及省部级项目 10 余项，主编教材 4 部，发表论文 30 余篇。公安部高等教育教学名师、全国优秀人民警察。

陈晓光，男，硕士研究生。恒安嘉新（北京）科技股份公司执行总裁，资深安全专家，中国网络空间安全协会理事委员，腾讯守护者计划特聘专家。毕业于北京邮电大学信息安全国家重点实验室，长期从事网络与信息安全的技术研究、方案设计和产品推广工作。参与多项重大国家和行业标准、全国性安全系统工程和国家关键课题研究，拥有 CISSP、CISA、ISO 27001 LA 等安全资质。

张作峰，男，本科。具有十余年网络安全行业从业经验，主要研究方向为 Web 安全。具备行业内多项安全资质，目前为恒安嘉新（北京）科技股份公司安全攻防团队负责人，曾圆满的完成了北京奥运会、广州亚运会、上海世博会、十八大、二十国集团峰会、世界互联网大会等国家重要活动的网络安全技术保障任务。

本书编委会成员

主　编：佟　晖　陈晓光　张作峰

副主编：胡　兵　刘晓蔚　王文娟　李雅楠

撰稿人：（按姓氏笔画排序）

卜宁琳　于存楠　王兆龙　刘　书　齐　柏　纪鲁鹏　杜　爽　李　刚　李　欢
李旭敏　李艳梅　李雅楠　杨志学　杨　晨　肖祥勇　佟　晖　张小玲　张作峰
张冠廷　张瑜龙　武鸿浩　黄泽超　梁健芳　魏　喆

前言

“没有网络安全，就没有国家安全”。当前，网络安全已被提升到国家战略的高度，成为影响国家安全、社会稳定至关重要的因素之一。

面对严峻挑战，为实施国家安全战略，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，在“公安技术”一级学科下开设“网络安全与执法”专业，网络安全专门人才的培养逐渐步入正轨。

本书分为 5 篇，共 17 章，内容包括 Web 安全基础介绍、Web 安全测试方法、Web 常见漏洞介绍、Web 安全实战演练、日常安全意识。附录部分为相关课程设计了大纲框架图。同时提供了课时分配供参考。本书编写特点：一是注重理论与实战的结合。以安全理论知识为本，结合实战以及教学视频，将实际问题分解映射到相关理论，既便于课堂讲解，也便于学生自学。二是实战操作步骤详尽，图文并茂。三是取材上既考虑了传统的、经典的技术，又引入大量新的、有代表性的技术。

本书可以作为普通高等院校网络空间安全学科和公安高等院校网络安全与执法专业学生的教学用书和参考书，也适合广大网络安全爱好者自学。本书帮助读者掌握 Web 安全知识和网络安全技术，树立良好的网络安全防范意识，为从事相关工作奠定坚实基础。

在此出版之际，对关心和支持我们编写与出版工作的所有朋友表示衷心的感谢。感谢恒安嘉新（北京）科技股份公司（下文简称为“恒安嘉新”）金红总经理对编写工作的支持和指导。感谢北京师范大学出版社赵洛育主任的大力帮助。感谢恒安嘉新的专家和北京警察学院的老师将日常教学与工作实践相结合，反复斟酌，数次修改，确保了知识点的条理清楚、语言的生动形象和技术的科学实用。

由于水平有限，书中难免有不妥之处，加之网络攻防技术纵深宽广，发展迅速，在内容取舍和编排上，难免考虑不周全，诚请读者批评指正。

编者

2017 年 5 月

目录

第 1 篇　Web 安全基础介绍

第 2 篇　Web 安全测试方法

第 3 篇 Web 常见漏洞介绍

第1篇

Web安全基础介绍

第1章

Web安全简介

1.1 最新安全事件[①]

近年来，全球大规模网站被黑、数据泄露事件频繁发生，掌握大量个人信息的政府机构、大型零售企业、金融机构，以及移动应用服务提供商成为信息窃取的重要目标。在网络智能飞速发展的今天，黑客利用工控设备、交通工具系统存在的漏洞入侵系统，进而执行一些恶意操作的事件日益增多。本节中介绍发生在我们身边的网络安全事件。

- 据外媒报道，黑客利用成本不足20美元的工具可黑掉汽车系统。可实现的功能包括关闭头灯、关闭警报系统、关闭车窗、关闭ABS系统或紧急刹车系统。根据最新的研究，利用大约1亿辆大众汽车共同存在的漏洞，可以让小偷远程通过无线信号打开大众汽车的车门。这种新的攻击手法几乎适用于所有1995年后生产的大众汽车。
- 波兰航空公司LOT的地面操作系统遭遇黑客袭击，致使系统瘫痪长达5小时，至少10个班次的航班被取消，1400多名乘客滞留机场。据悉，这是民航公司全球首次遭遇操作系统被黑。若黑客攻击的是飞行系统，攻击者可通过劫持飞机上的娱乐系统或IFE，并重写飞机的推进管理计算机中的代码，能向飞机下达爬升的命令，并让飞机短暂改变航向。更为严重的事情是，还可以推论出如何在35000英尺的高空中关闭飞机发动机，而且在驾驶舱内不会有警示灯的提示。众所周知，一旦飞机偏离航向或关闭发动机，造成的后果难以想象。
- 浙江省温州电视广播中心系统遭黑客攻击，黑客通过技术方式将反动信息植入网络机顶盒，在四十几万用户收看电视时，弹出带有反动图文信息的画面。
- 台湾地区一用户报警称自己在家的一举一动被发布在网上直播，原来是黑客利用漏洞攻破了安装在家里的网络摄像机，进而监控用户的一举一动。
- 台湾第一银行旗下20多家分行的41台ATM机遭遇黑客攻击，ATM机有不明吐钞情况，被盗8327余万新台币。

[①] 最新安全事件详见教程配套视频。

- 2016 年 3 月，一类名为“密锁”的敲诈型恶性病毒在国内突然爆发，该类病毒通过电子邮件传播，一旦用户点击带毒附件，计算机中的各类文档、隐私文件都将被病毒“上锁”，如不按黑客要求付款，将永远无法恢复正常。2016 年上半年手机安全报告数据显示，全国感染手机病毒用户超 2 亿人次，并呈上升趋势。感染用户中有 72%的用户使用公共 WiFi，移动支付，这给用户的财产安全构成进一步威胁。
- 武汉一家汽车销售公司的会计，被“董事长”拉入一个克隆的微信群，被骗 85 万元。根据调查，用户平时使用微信时若点击了钓鱼网站，不法分子利用获取的信息可克隆微信群等，进而实施诈骗。
- 辽宁警方揭秘了朋友圈投票的真相。诈骗团伙利用投票活动，获取报名者的个人信息，进而将信息出售。利用获取到的详细信息，团伙可进一步实施诈骗行为。
- 高考结束，不少同学和家长都通过网站查询报考学校和专业。高校网站也成为黑客攻击的重要目标。黑客入侵高校网站后，在访问量较高的院系网站挂木马，用户点击后木马会感染系统，进而获取照片、账号等敏感信息。
- 2016 年 8 月，DOTA2 论坛被黑，近 200 万用户详细信息被窃取，其中包括用户名、邮件地址、用户识别码、密码、IP 地址。

1.2　黑客、白客、灰客

黑客，源自英文 hacker，曾指热心于计算机技术、水平高超的计算机专家，尤其是程序设计人员，现在逐渐区分为白帽子、灰帽子、黑帽子等。

白客（白帽子）是正面的黑客。白客检测到系统漏洞后，不会恶意利用漏洞、窃取系统数据，而是公布漏洞，提醒网站管理员及时修复，防止网站系统被其他人（如黑帽子）攻击。

灰客（灰帽子）与白帽子相似。灰客擅长攻击技术，精通攻击与防御，但不轻易造成破坏。通常灰客将黑客行为作为一种业余爱好来做，希望通过黑客行为来警告系统管理员网络或系统存在漏洞，以达到警示别人的目的。

与白帽子相对的就是黑帽子，即传统意义的黑客。在发现系统漏洞后，会利用攻击技术窃取网站信息，滥用资源，恶意攻击，蓄意破坏。黑帽子的主要目的是要入侵系统，找到有价值的数据，通常有黑色产业链，以此非法获取利益。

1.3　网站入侵的途径

网站被入侵，大部分原因是网站（系统）存在漏洞，包括主机（服务器）漏洞、中间件（apache、weblogic……）漏洞、应用服务（数据库、FTP 文件服务、Web 应用……）漏洞等。本书着重介绍攻击者利用 Web 漏洞攻击网站。漏洞产生原因是多方面的。首先，很

多开发人员没有安全意识，开发的代码中出现漏洞。其次，系统上线之后的服务器环境可能会有变化，本来没有问题的代码可能就变得有问题。另外，管理员密码泄露、一些配置性错误等都会存在安全问题。当然，即便目标系统不可被直接入侵，攻击者也可以通过 C 段服务器（同网段服务器）间接对目标主机进行渗透，或利用社会工程学收集信息以达到入侵系统的目的。如图 1-1 所示为对漏洞的大致分类。

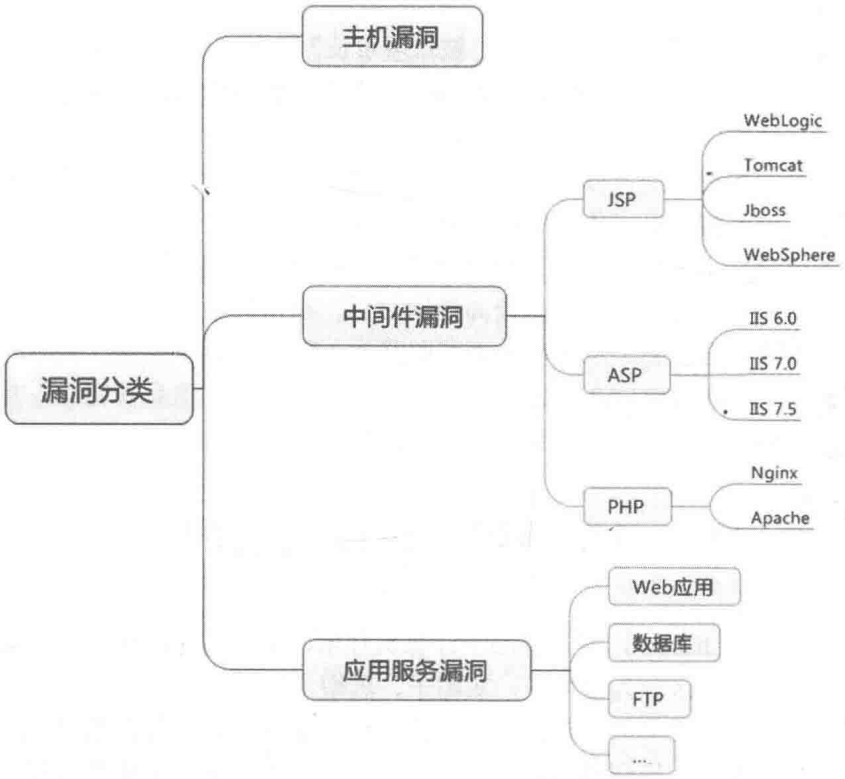

图 1-1　漏洞分类

攻击者在渗透服务器时，直接对目标下手一般有三种手段，当了解攻击者的手段之后，防御也就变得简单了。图 1-2 显示了 Web 应用的风险点，攻击者入侵服务器可能就是从这些点下手的。黑客如何利用漏洞攻击网站，具体细节将在后面的章节介绍。

- C 段渗透：攻击者通过渗透同一网段内的一台主机对目标主机进行 ARP 等手段的渗透。
- 社会工程学：社会工程学是高端攻击者必须掌握的一个技能，渗透服务器有时不仅仅只靠技术。详细内容请参照第 15 章“社会工程学”。
- Services：很多传统的攻击方式是直接利用应用服务存在的漏洞，例如溢出，至今一些软件仍然存在溢出漏洞。像之前的 MySQL 就出现过缓冲区溢出漏洞。当然，对这类服务还有其他入侵方式，这些方式也经常用于内网的渗透中，在后面的章节中都会一一讲述。

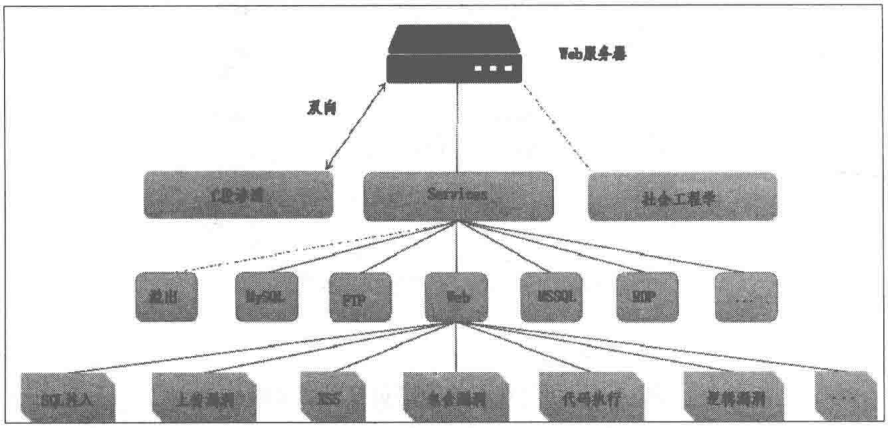

图 1-2　Web 应用存在的风险点

1.4　实战演练（网站入侵）

本节通过一个简单的例子来了解黑客是如何攻击网站的。

演示案例：

目标网站：127.0.0.1

被攻击的原因：

- 管理员登录账号存在弱口令漏洞，攻击者可利用暴力破解工具获取账号，登录系统，进而获取用户信息。
- 用户信息管理页面上传头像对文件类型未做限制，攻击者可上传 WebShell，进而获取网站服务器控制权限。

攻击过程：

攻击过程如图 1-3～图 1-11 所示。

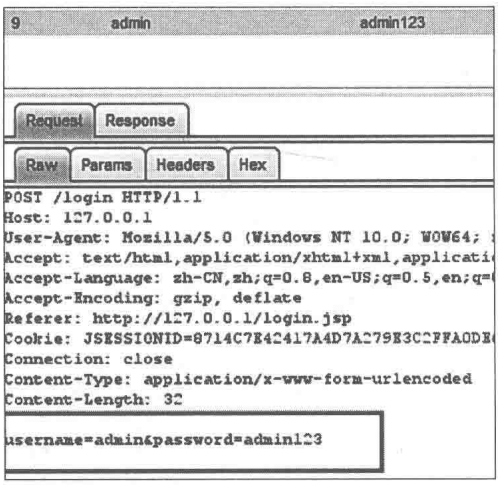

图 1-3　使用暴力破解工具获取管理员登录账号

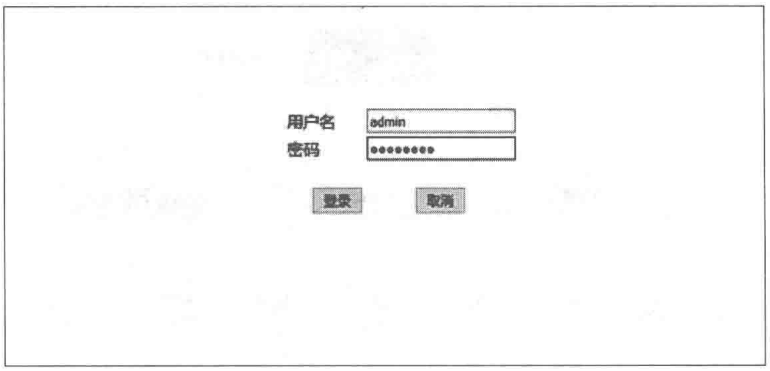

图 1-4　利用获取的管理员账号登录网站

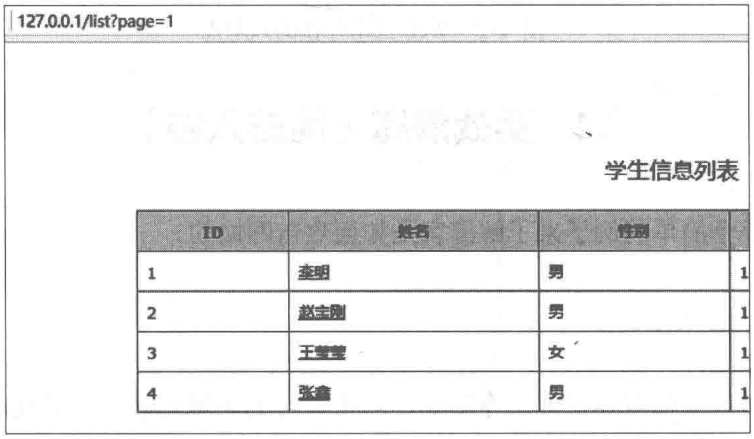

图 1-5　成功登录网站后台

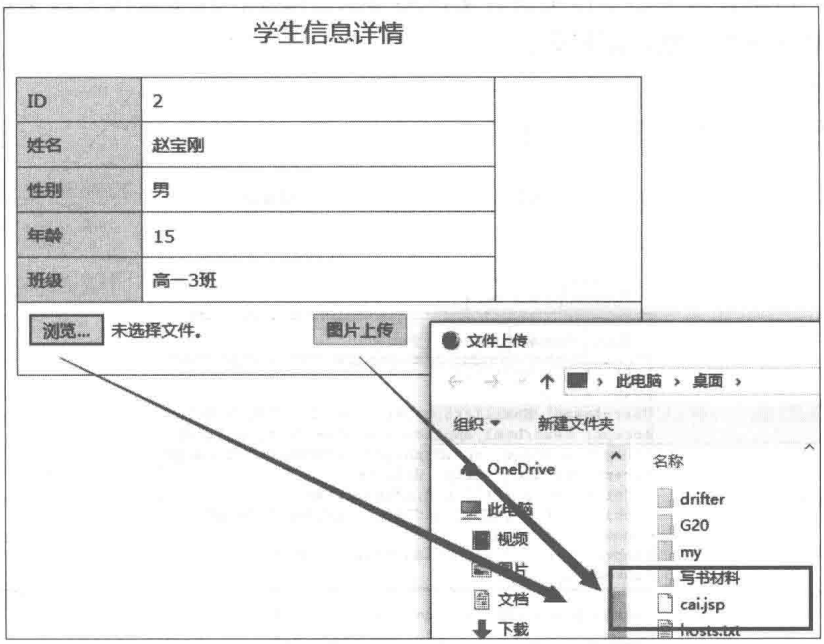

图 1-6　在学生信息管理上传头像处上传 WebShell

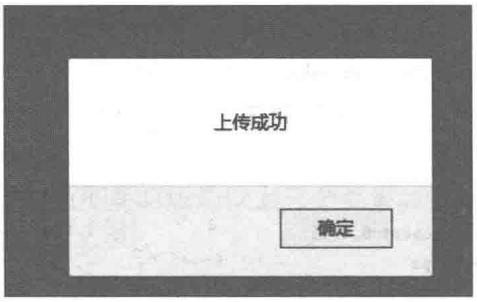

图 1-7　WebShell 上传成功

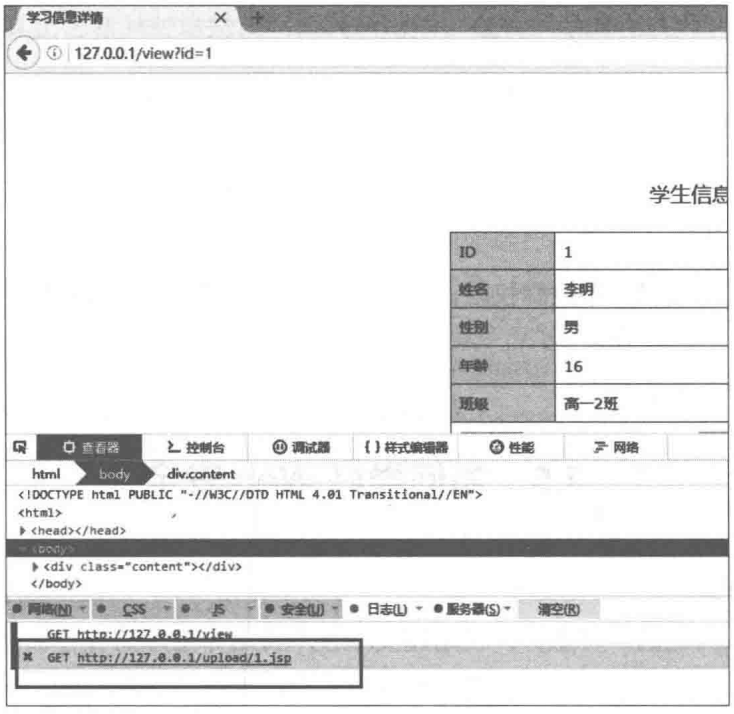

图 1-8　获取后门链接地址

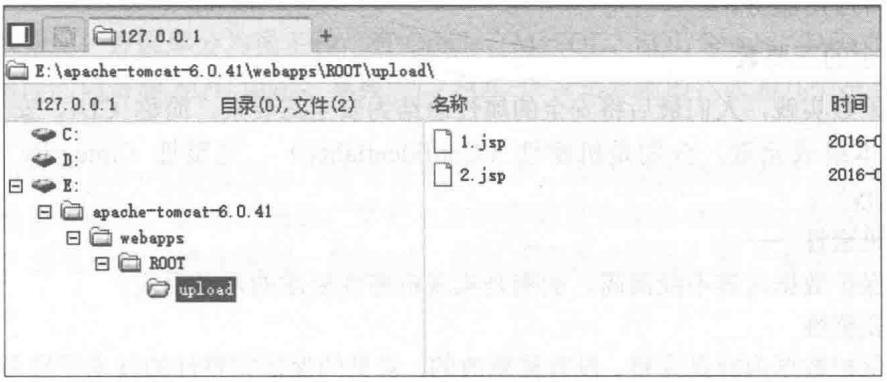

图 1-9　利用连接工具访问网站服务器