Web渗透与漏洞挖掘

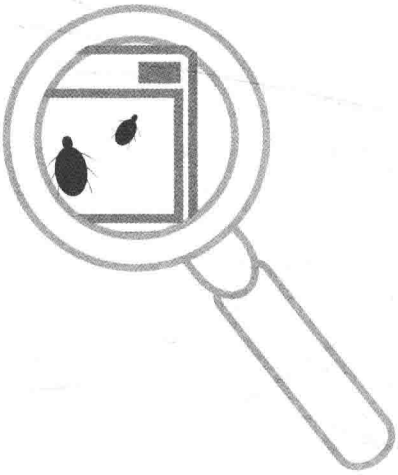
赵显阳 / 著

本书内容来源于实践，并可以举一反三延伸到更多领域。
相信可以引导对安全感兴趣的朋友步入更深层次的安全世界。

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渗透与漏洞挖掘

赵显阳 / 著



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

内 容 简 介

全书分为三部分。第一部分为漏洞基础知识，包括第 1 章和第 2 章。第 1 章详细介绍漏洞的基本概念、漏洞分类和挖掘方法；第 2 章对多个具体的漏洞进行分析，进一步阐明漏洞基础知识，是对第 1 章内容的巩固和深化。第 3 章是本书的第二部分，通过多个系统的漏洞实例，介绍漏洞挖掘的方法和步骤，使读者能够对漏洞挖掘的方法和过程有清晰的了解。本章是本书的核心内容，是对前述方法的具体应用，需要读者具有一定的开发语言和安全攻防知识基础。第 4~7 章为本书的第三部分，介绍漏洞利用的一些相关内容，涵盖的范围跨度比较大，包括基于漏洞进行的渗透测试、相关安全开发编程、无线及渗透过程中的常用工具介绍。

本书主要目标读者为 Web 应用程序渗透测试人员以及相关开发人员。相信读者通过阅读本书，能够提升在安全开发以及测试方面的能力，从而提升企业在安全方面的防护能力。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

Web 渗透与漏洞挖掘 / 赵显阳著. —北京：电子工业出版社，2017.9
ISBN 978-7-121-32532-8

Ⅰ. ①W… Ⅱ. ①赵… Ⅲ. ①计算机网络－网络安全－研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2017）第 202716 号

责任编辑：黄爱萍
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
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：720×1000　1/16　印张：13　字数：187 千字
版　　次：2017 年 9 月第 1 版
印　　次：2017 年 9 月第 1 次印刷
定　　价：59.00 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）88254888，88258888。

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。

本书咨询联系方式：（010）51260888-819，faq@phei.com.cn。

推荐序

第一次见到赵显阳是2008年在中关村软件园，那时他已经是一位高级安全工程师了。参加过中国科学院、北京机场、奥运会等众多项目的安全渗透测试服务，不仅具有丰富的Web渗透和漏洞挖掘经验，还精通Delphi等编程技术，是一位不可多得的全方位安全专家。

漏洞挖掘是一门艺术，同时也是对技术要求较高的安全领域的一项技能。本书详细阐述了作者挖掘各种漏洞的宝贵经验，很值得大家借鉴。信息安全技术发展到今天，漏洞研究、渗透测试和安全工具的编写已经成为一个信息安全高手必须具备的基本条件，本书作者正是从这些方面入手，将自己多年宝贵的安全实践经验融汇成珍贵的信息安全结晶，为大家提供踏上安全专家之路的捷径。

本书关于漏洞挖掘的章节主要讲述PHP产品代码漏洞，其中很多技巧和思路都非常具有代表性。现今绝大部分网站都由PHP驱动，因此研究PHP漏洞对整个互联网Web安全具有较大的覆盖范围，而且也可以举一反三应用到ASP、ASPX和JSP领域。在编程章节从多个角度展开了从漏洞研究到工具实现的过渡，为安全技术进阶铺平了道路。最后作者以常用的安全工具结尾，作为本书的画龙点睛之笔。对于有一定安全经验的工作者，非常建议从本书进阶。

石祖文

安全伞科技创始人 国家漏洞库特聘专家

2017年7月7日

前　言

随着国内互联网行业的快速发展，针对互联网行业的 Web 攻击行为大量增加，根据“乌云”发布的漏洞统计数据来看，近年与 Web 相关的漏洞的数量保持在两位数的增长速度。因此，大家对 Web 安全的关注也日益增加。

本书通过对多个实例的分析，详细阐述了对 Web 漏洞的挖掘及利用过程。全书按照从简单到复杂、从基础到进阶的先后顺序进行组织。第 1 章对安全知识进行介绍，使读者对漏洞的概念和分类体系，以及然后对常用的漏洞挖掘方法等有一个整体的了解。第 2 章针对近几年爆发的一些典型漏洞进行详细分析，阐述漏洞产生和利用的细节情况；第 3 章通过一些未公布的漏洞实例梳理漏洞挖掘的思路和过程，这要求读者熟练掌握安全基础知识；第 4 章介绍如何基于漏洞实现渗透的过程，而在渗透过程中所需要的编程技术和相关工具则在第 5~7 章进行详细介绍。

本书主要目标读者为 Web 应用程序渗透测试人员以及相关开发人员。与现有的其他资料相比，本书对已公布的漏洞或基础知识涉及较少，注重对未知漏洞的挖掘和利用，将笔墨主要集中在使读者如何通过已经掌握的安全基础知识去发现漏洞，从而提升相关能力水平。为了便于读者理解漏洞的细节信息，书中提供了部分代码片段，需要读者具有一定的编程基础和安全经验。

相信读者通过阅读本书，能够提升在安全开发以及测试方面的能力，从而提升企业在安全方面的防护能力。作为一名网络安全研究人员，对 Web 应用的安全测试是一种必备能力、一种生活乐趣，同时也是一份责任。希望读者通过学习书中描述的思路和

此为试读，需要完整PDF请访问：www.ertongbook.com

方法能够提升漏洞分析和挖掘的能力，但也提醒各位，请不要利用书中讲述的技术攻击他人。

赵显阳

2017 年 7 月

轻松注册成为博文视点社区用户（www.broadview.com.cn），扫码直达本书页面。

- **提交勘误**：您对书中内容的修改意见可在 提交勘误 处提交，若被采纳，将获赠博文视点社区积分（在您购买电子书时，积分可用来抵扣相应金额）。
- **交流互动**：在页面下方 读者评论 处留下您的疑问或观点，与我们和其他读者一同学习交流。

页面入口：*http://www.broadview.com.cn/32532*

目　录

1

第 1 章
安全知识

1.1 什么是漏洞

漏洞是指一个系统存在的弱点或缺陷，系统对特定威胁攻击或危险事件的敏感性，或进行攻击威胁的可能性。漏洞可能来自应用软件或操作系统设计时的缺陷或编码时产生的错误，也可能来自业务在交互处理过程中的设计缺陷或逻辑流程上的不合理之处。这些缺陷、错误或不合理之处可能被有意、无意地利用，从而对一个组织的资产或运行造成不利影响，如信息系统被攻击或控制、重要资料被窃取、用户数据被篡改、系统被作为入侵其他主机系统的跳板等。从目前发现的漏洞来看，应用软件中的漏洞远远多于操作系统中的漏洞，特别是 Web 应用系统中的漏洞更是占信息系统漏洞中的绝大多数。

1.2 Web 漏洞的分类

1. SQL 注入

SQL 注入就是通过把 SQL 命令插入到 Web 表单，递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令的目的。

2. XSS（跨站脚本攻击）

跨站脚本攻击(Cross Site Scripting，缩写为 XSS)，为了不与层叠样式表(Cascading Style Sheets）的缩写 CSS 混淆，故将跨站脚本攻击缩写为 XSS。XSS 是一种经常出现在 Web 应用中的计算机安全漏洞，其允许恶意 Web 用户将代码植入到提供给其他用户使用的页面中，这些代码包括 HTML 代码和客户端脚本。攻击者利用 XSS 漏洞进行非法访问控制——例如同源策略（Same Origin Policy）。这种类型的漏洞由于被黑客用来编写危害性更大的网络钓鱼（Phishing）攻击，所以广为人知。对于跨站脚本攻击，黑客界的共识是：跨站脚本攻击是新型的“缓冲区溢出攻击”，而 JavaScript 是新型的“ShellCode”。

3. 文件上传

文件上传漏洞是指用户上传一个可执行的脚本文件，并通过此脚本文件获得了执行服务器端命令的能力。这种攻击方式是最为直接和有效的，有时几乎不具有技术门槛。

“文件上传”本身没有问题，有问题的是文件上传之后服务器怎么处理、解释文件。如果服务器的处理逻辑做得不够安全，则会有严重的不安全隐患。

4. 文件下载

可以下载网站所有的信息数据，包括源码、网站的配置文件等信息。

5. 目录遍历

如果 Web 设计者设计的 Web 内容没有恰当的访问控制，允许 HTTP 遍历，攻击者就可以访问受限的目录，并可以在 Web 根目录以外执行命令。

6. 本地文件包含（Local File Include）

这是 PHP 脚本的一大特色，程序员们为了开发方便常常会用到包含。比如把一系

列功能函数都写进 fuction.php 中，之后当某个文件需要调用时就直接在文件头中写上一句<?php include("fuction.php");?>，然后调用内部定义的函数。

本地包含漏洞是 PHP 中一种典型的高危漏洞。由于程序员未对用户可控的变量进行输入检查，导致用户可以控制被包含的文件名，当被成功利用时可以使 Web Server 将特定文件当成 PHP 脚本执行，从而导致用户获取一定的服务器权限。

7. 远程文件包含

服务器通过 PHP 的特性（函数）去包含任意文件时，由于要包含的文件来源过滤不严，可以包含一个恶意文件，而我们可以构造这个恶意文件达到渗透系统的目的。几乎所有的 CGI 程序都有这样的 Bug，只是具体的表现方式不一样罢了。

8. 全局变量覆盖

register_globals 是 PHP 中的一个控制选项，可以设置成 Off 或者 On，默认为 Off，决定是否将 EGPCS（EGPCS 是 Environment、GET、POST、Cookie、Server 的缩写）变量注册为全局变量。

如果打开 register_globals，客户端提交的数据中含有 GLOBALS 变量名，就会覆盖服务器上的$GLOBALS 变量。

9. 代码执行

由于开发人员编写源码时没有针对代码中可执行的特殊函数入口做过滤，导致客户端可以提交恶意构造语句，并交由服务器端执行。Web 服务器没有过滤类似 system()、eval()、exec()等函数是该漏洞攻击成功的最主要原因。

10. 信息泄露

由于代码编写不严谨或应用固有的功能，造成网站服务器信息被非法获取，但这只是一个低危漏洞。

11. 弱口令

弱口令的危害就犹如你买了一个高级保险箱，什么刀斧工具都破坏不了它，但遗憾的是你把钥匙挂在了门上。常见的弱密码出现在个人邮箱、网游账号、系统口令等环境。

12. 跨目录访问

开发人员没有正确地限制能够访问存储系统的网页路径。通常，跨目录攻击的受

此为试读，需要完整PDF请访问：www.ertongbook.com

害者大多是社交网站，或者是全球性的 Web 服务器。因为在同一个 Web 服务器上可能为不同的用户或部门分配不同的目录。例如，每个 MySpace 用户都有一个个人的网络空间。此时，如果使用 Cookie 或者 DOM 存储，就可能产生跨目录攻击。

13. 缓冲区溢出

缓冲区溢出是一种非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击会导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权进而进行各种非法操作。

14. Cookies 欺骗

Cookies 能够让网站服务器把少量数据储存到客户端的硬盘，或从客户端的硬盘读取数据。当你浏览某网站时，由 Web 服务器置于你硬盘上一个非常小的文本文件，它可以记录你的用户 ID、密码、浏览过的网页、停留的时间等信息。当你再次来到该网站时，网站通过读取 Cookies 得知你的相关信息，就可以做出相应的动作，如在页面显示欢迎你的标语，或者让你不用输入 ID、密码就可以直接登录等。

从本质上讲，它可以看作是你的身份证。但 Cookies 不能作为代码执行，也不会传送病毒，为你所专有，且只能由提供它的服务器来读取。保存的信息片断以“名/值对”（Name-Value Pairs）的形式储存，一个“名/值对”仅仅是一条命名的数据。Cookies 欺骗就是修改其中保存的信息，从而实现某些特殊的目的。

15. 反序列化

如果服务端程序没有对用户可控的序列化代码进行校验，而是直接进行反序列化使用，并且在程序中运行一些比较危险的逻辑（如登录验证等），那么就会触发一些意想不到的漏洞。比如经典的有 Weblogic 反序列化和 Joomla 反序列化漏洞。

16. CSRF（跨站请求伪造）

攻击者通过用户的浏览器注入额外的网络请求，破坏一个网站会话的完整性。浏览器的安全策略是允许当前页面发送到任何地址，因此也就意味着当用户在浏览其无法控制的资源时，攻击者可以控制页面的内容来控制浏览器，发送其精心构造的请求。

17. 命令注入

系统对用户输入的数据没有进行严格过滤就运用，并且使用 bash 或 cmd 执行。

1.3　漏洞挖掘常用的方法

1. SQL 注入

对于注入漏洞，通常我们在 URL 后加单引号即可判断是否有注入漏洞。如 http://www.isafe.cc/list.asp?id=1 后加单引号，即 http://www.isafe.cc/list.asp?id=1'，这时服务器会把 1'代入数据库查询，然后页面报错，而对于不同的数据库错误信息也不一样。

对于不报错的页面，可以使用 and 1=1 和 and 1=2，并根据页面返回内容判断是否有注入。如果 and 1=1 和 and 1=2 返回的页面内容不同，则可以断定存在注入。比如，第一次提交的 URL http://www.isafe.cc/list.asp?id=1 and 1=1 页面有返回内容，而第二次提交的 URL　http://www.isafe.cc/list.asp?id=1 and 1=2 页面没有完整的内容，则可以断定存在 SQL 注入。

对于有些特定的 Web 页面后端查询，比如 Update、Delete、Insert 等，可以使用 Sleep 等函数（数据库不同则函数不同）进行 SQL 注入，比如提交 URL http://www.isafe.cc/list.asp?id=1 and sleep(5)，如果页面等待几秒钟才返回，则可以断定存在 SQL 注入。

SQL 注入一般有基于报错的注入、基于布尔值的注入和基于时间的注入。

2. XSS（跨站漏洞）

跨站漏洞一般出现在 Web 浏览器端，分为反射型、存储型等，跨站可用来盗取其他用户的 Cookie，虽然没有 SQL 注入危害大，但也被业界评为高危漏洞，一般在 URL 后加入<script>alert("www.isafe.cc");</script>，如果页面有弹框，则表示存在跨站漏洞。

3. 文件上传

文件上传漏洞一般视情况而定，有些是中间件的漏洞如 apache、nginx、iis 等。对于 apache 上传 1.php.bak 这样的文件是可以作为 PHP 文件执行的（某些版本），对于 nginx 上传 1.jpg 文件，访问 http://www.isafe.cc/upload/1.jpg/1.php 就可以执行 PHP 代码。对于 iis 6.0 上传 1.asp、1.jpg 这样的文件可以被作为 ASP 来执行，建立 1.asp 文件夹，在 1.asp 文件下的任意后缀文件都可以作为 ASP 来执行。有些是代码过滤不严谨造成的任意文件上传，有些代码对文件上传根本不过滤，对应过滤的文件也可以

通过各种方法绕过上传。文件上传视情况而定，有各种各样可利用的方法。

4. 文件下载

下载系统上的任意文件，如数据库配置文件、密码文件 Shadow 等，Web 层面会提供下载附件或软件的功能，一般形式如 http://www.isafe.cc/download.php?filename=/files/document.doc，Web 后端会根据 filename 参数在指定的目录中读取文件的内容返回给浏览器，如果修改 filename 为 http://www.isafe.cc/download.php?filename= ../../../../../../../etc/passwd 这样的形式，则可以跨越指定的目录访问系统的任意文件。

5. 代码执行

远程代码执行多见于 PHP、Java 等脚本语言中，PHP 中的 Eval、System、Assert、Popen 等函数如果对外界传入的参数直接使用，则会造成远程代码执行，我们在找漏洞的时候只要定位到相关函数，观察相关函数的参数来源即可。

2

第 2 章

漏洞研究

2.1 Apache 文件名解析漏洞

Apache 是一个 Web 服务器，可以提供 Web 服务，配合 Java 中间件、PHP 实现动态网页访问。

Apache 和 PHP 通过接口接入后，Apache 接收用户的请求，并把请求传送给 php.exe，php.exe 程序执行完成后，把结果发送给用户，如图 2-1 所示。

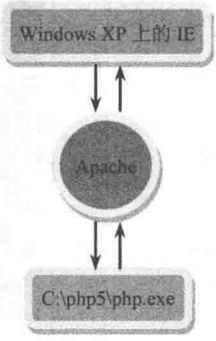


图 2-1

在 Apache 将文件内容交给 PHP 的时候，Apache 会从右到左对文件名进行判断，确保只有.php 的后缀文件得到解析，当文件名是 test.php.bak 时，按照 httpd.conf 中的定义，.bak 是不可识别的文件后缀，那么 Apache 会提取.bak 左边的后缀.php，判断 PHP 是否可以识别，来识别文件程序执行。当 Apache 和 PHP 以 fastcgi 方式结合时，则不存在该问题。

我们以 Apache 2.2.17 为例，打开网站 http://192.168.1.106:2217/phpinfo.php，如图 2-2 所示。

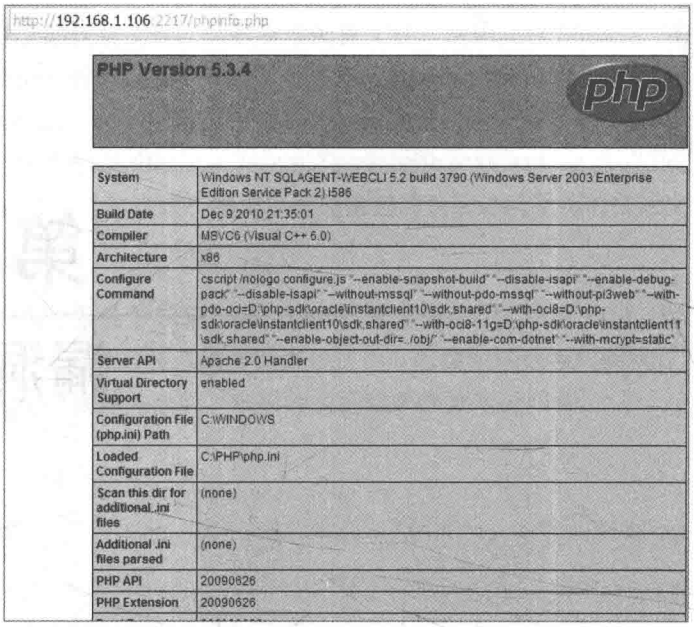


图 2-2

这是正常访问，我们把 phpinfo.php 重命名为 phpinfo.php.bak 再用 IE 访问 http://192.168.1.106:2217/phpinfo.php.bak，如图 2-3 所示。

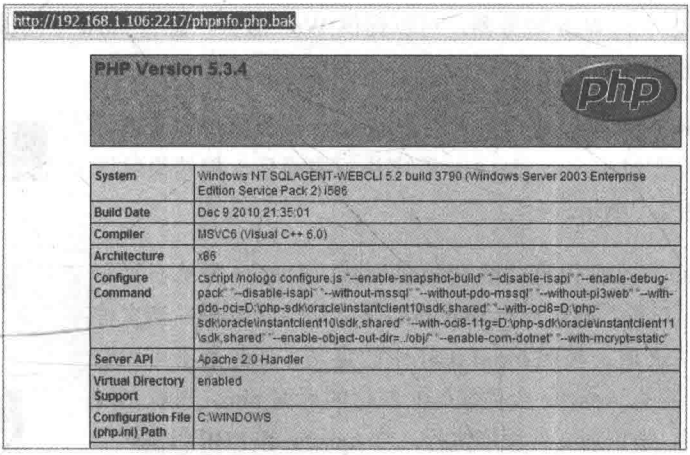


图 2-3

当 phpinfo.php.bak 执行后，有人会问那不就是发送 phpinfo.php.gif 文件就可以得到 webshell 了吗？答案是否定的。如图 2-4 所示。

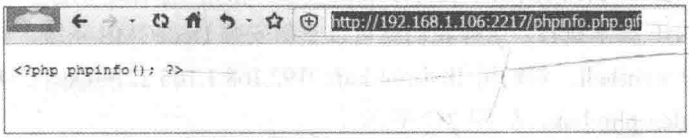


图 2-4

后缀为.jpg 和.jpeg 都不能解析，为什么呢？因这些后缀是 Apache 的已知类型，但后缀是.lock 就可以执行，后缀是.xx 也可以。如图 2-5 和图 2-6 所示。

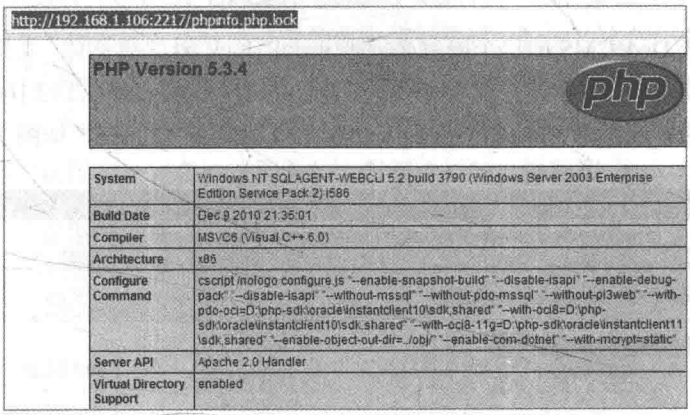


图 2-5

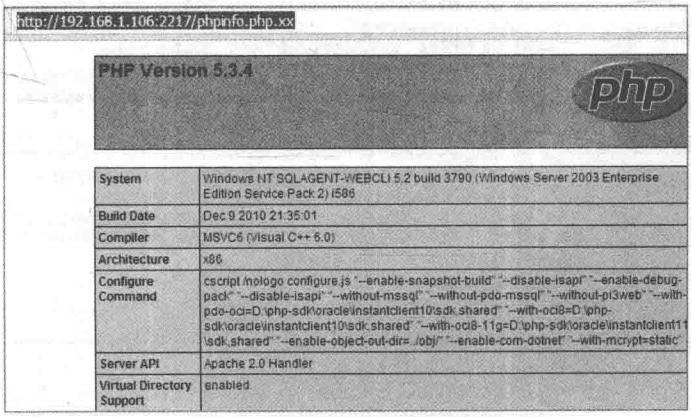


图 2-6

此为试读，需要完整PDF请访问：www.ertongbook.com