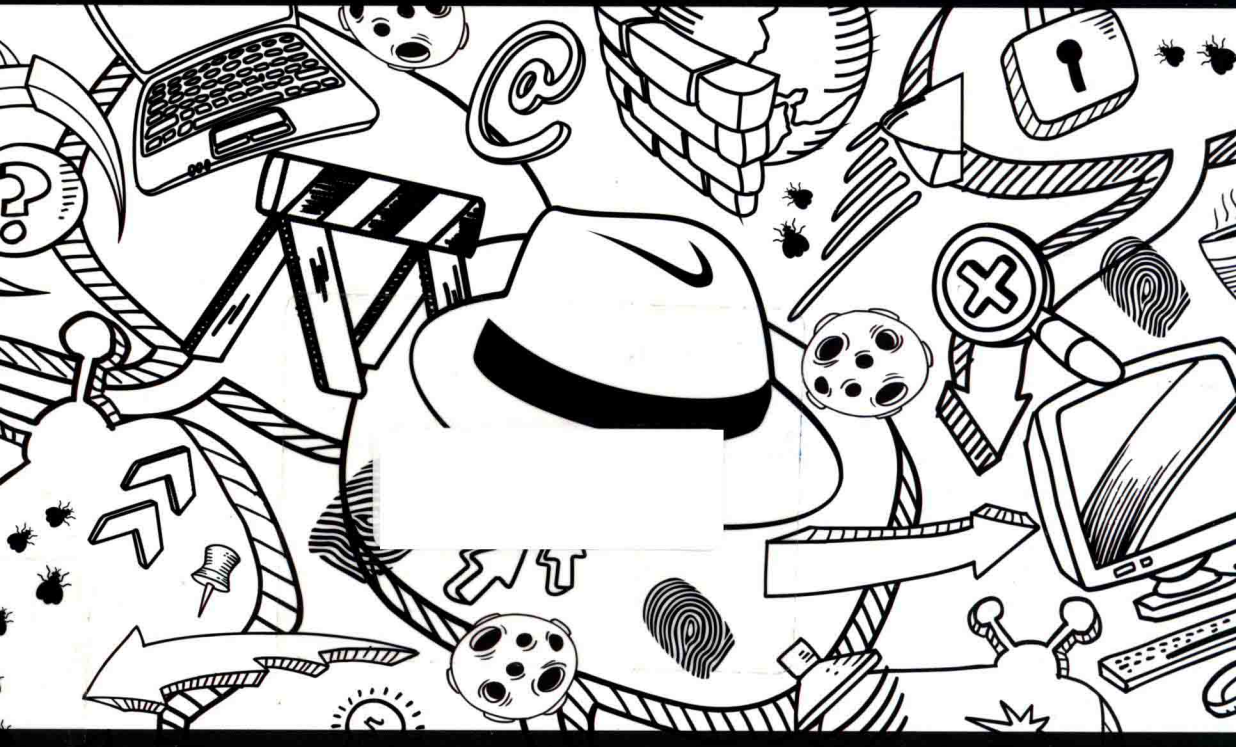
Broadview
www.broadview.com.cn

安全技术大系

白帽子讲Web扫描



Web 2.0爬虫 · 扫描设计 · 漏洞审计 · 云扫描 · 企业扫描 · 扫描反制

刘潇 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

安全技术大系

白帽子讲Web扫描

刘漩 编著

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

内 容 简 介

Web 扫描器是一种可以对 Web 应用程序进行自动化安全测试的工具，它可以帮助我们快速发现目标存在的安全风险，并能够对其进行持续性安全监控。

本书详细讲述了 Web 扫描器的概念、原理、实践及反制等知识，笔者凭借多年的安全工作经验，站在安全和开发的双重角度，力求为读者呈现出一个完整的 Web 扫描知识体系。通过对本书的学习和实践，可以让你快速建立自己的 Web 扫描体系，提高安全基础能力。

图书在版编目（CIP）数据

白帽子讲 Web 扫描 / 刘漩编著. —北京：电子工业出版社，2017.7
（安全技术大系）
ISBN 978-7-121-31477-3

Ⅰ. ①白… Ⅱ. ①刘… Ⅲ. ①网络安全－安全技术 Ⅳ. ①TN915.08

中国版本图书馆 CIP 数据核字（2017）第 096978 号

责任编辑：张 玲
印 刷：北京中新伟业印刷有限公司
装 订：北京中新伟业印刷有限公司
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：15.5 字数：320 千字
版 次：2017 年 7 月第 1 版
印 次：2017 年 7 月第 1 次印刷
印 数：3000 册 定价：65.00 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

非常荣幸受刘漩的邀请为本书写推荐序。

刘漩是安全宝第一位安全工程师，也是早期 WAF 规则的主要维护者。这六年多来，他一直在 Web 安全的最前线与黑客做斗争，从防御到漏洞挖掘，都有着丰富的经验，也正是因为如此，他眼中的扫描技术更为系统化。

纵观网络安全的发展历史，扫描器是最早出现的工具，从著名的开源实现 Nmap，到国人为之骄傲的流光 FluXay，都是端口扫描的利器。而 Web 安全领域里的扫描器虽然原理类似，但实现却更为复杂，需要考虑扫描频率、扫描深度、爬虫对于 HTML 的解释能力，还要不断地积累 POC。

记得我最早使用过的扫描器是 IBM 的 AppScan，其爬取能力很强，但扫描速度却奇慢无比，基本上对 URL 要尝试所有扫描特征，最后还需要从大量的漏洞中去伪存真。

扫描器也是百度安全团队最早开发的工具之一，百度公司有数百个产品线，每天的发布量数不胜数，如果没有一个高效的漏洞扫描，安全几乎无从谈起。无论是新上线的业务，还是当出现 0day 时的大规模临检，扫描已经成为例行化工作。扫描结合被动的 URL 发现，目前已经成为最大的漏洞来源，同时扫描与工单系统联动，完成派单、巡检、复检也成为现代安全管理自动化流程的一部分。

扫描已经成为所有互联网业务中必不可少的安全工作。这本书将系统化地为读者讲解扫描原理与实现方法，我相信无论你是甲方安全工程师，还是乙方安全服务人员，阅读本书后都将受益匪浅。

百度云安全技术总监，百度云加速总负责人

冯景辉

序

我的安全路

本人第一次接触安全是在大学期间，有一次无意中读到室友买的一本《黑客防线》杂志，立刻就被里面的黑客技术深深吸引。从那以后，我就开始疯狂学习安全知识，而那时候大学还没有设立类似的课程，只能靠自己独立钻研。一方面我借助安全杂志学习入侵实践知识，另一方面则“泡”在图书馆里翻阅各类与安全相关的书籍补充理论知识，成长非常快。

但在大学毕业的时候，我却并没有选择进入自己感兴趣的安全类公司，反而进入了一家大型跨国公司，在里面做了一年的软件测试工作，感觉这段经历对我最大的改变就是，养成了喜欢用自动化方式去解决一些重复工作的习惯。

后来我还是希望遵从内心，决定找一份与安全相关的工作。在辞职前，我成功地入侵了公司的内部网络，拿到公司域控的管理权限，并在服务器的桌面上留下了善意的修复建议，目的只是为了证明自己的安全能力。

有着大公司的背景及对安全工作的执着追求，我顺利地加入了瑞星公司，在这里开始进一步学习安全的知识。得益于瑞星宽松的工作环境和浓厚的安全氛围，在完成本职工作之余，我开始进行更多的学习和研究，同时也接触到很多新的安全产品。也是在那段时间，我写了自己第一款移动端的手机防火墙软件，不过此时我对安全的理解更多的是攻防学习和漏洞研究，所掌握的知识并不成体系。

再后来我加入安全宝创业。安全宝算是我最有感情的一家公司，它让我从零开始踏上一个公司的安全建设之路，对安全工作进行系统的规划，以闭环的方式来推进和完善每个工作流程，然后通过攻防对抗实践进行迭代式的改进。其实对于企业来讲，攻防对抗仍然可以作为企业安全建设中最有价值的应用实践之一。

之后我加入百度。虽然还是以乙方的视角做着安全服务工作，但甲方的工作氛围和技术培训也让我对攻防的理解更加全局化，更加工程化，也更加体系化。此时，我对扫描的看法也发

生了变化：扫描作为攻击的一种方式，它应该更贴近真实的攻击；而真实的攻击其实是一种全视角、持续性、动态化的入侵行为，它会对目标进行全视角的信息和资产收集，然后通过持续性的漏洞测试及动态的情报能力发现其中的脆弱点。因此，如果我们想重塑扫描的价值，那么就应该以攻击者的视角，同时将更多的安全能力融入扫描中，并以攻击的全流程来对其进行改进和扩充，从而最终实现扫描的情报化、插件化、智能化。

我的安全观

我眼中的 Web 安全

还记得自己刚刚加入百度，小哥（程岩）在面试我的时候，问了一个问题，我至今依然记忆深刻：每个 Web 安全人员都有自己的安全体系，你眼中的 Web 安全是什么样子的？

当时我也是第一次被问到这么宏观的问题，第一感觉就是问题很大，一时不知从何说起，现在我还记得自己当时的回答：我眼中的 Web 安全包含着我做的所有内容，比如漏洞挖掘、漏洞分析、漏洞攻击和规则防御等。它们都是围绕漏洞的生命周期进行展开的，可以按照时间顺序将它们划分为 4 个阶段，如下。

- **漏洞的感知**：我们需要从各个方面和渠道去关注 Web 漏洞，获取最新的漏洞资源和信息，如漏洞监控、漏洞预警或漏洞挖掘等。
- **漏洞的分析**：获取漏洞资源后，我们就需要对漏洞进行分析和研究，弄清楚漏洞的原理及成因，而这主要体现在两方面，一方面是可以构造出漏洞的 POC，并补充到扫描器中，对漏洞实现自动化检测和验证；另一方面则是深入理解漏洞原理后，能够写出对应的漏洞匹配特征，制作漏洞签名，并给 WAF 升级进行防护。
- **漏洞的响应**：这里主要分为两部分，一部分是对内的响应，也就是自身的漏洞响应，对漏洞进行快速排查和修复；另一部分则是对外的响应，也就是对互联网的全网客户进行响应，评估漏洞对其影响，以及协助修复，并对全网的安全态势进行监控。
- **漏洞的沉淀**：按照漏洞的描述、原理、场景，以及修复策略等相关信息，对每个漏洞进行编号和积累，形成有价值的漏洞知识库。

现在回想起来，对于当时的回答，我其实并不满意，只能算是勉强应付下来。但事后自己却想得更多了，这个问题属于主观题，或许它没有标准的答案，也没有所谓的对与错，但它却

可以让每个人按照自己的角度、自己的工作、自己的理解，重新去思考和审视自己的知识体系。从那以后，这个问题也就一直伴随着我，它也是我作为面试官必问的题目之一。因为我相信在不同的阶段，每个人对它的理解肯定是不一样的。

三个基础的安全认知

1. 木桶原理

盛水的木桶是由多块木板箍成的，盛水量也是由这些木板决定的。若其中一块木板很短，则此木桶的盛水量就被限制，该短板就成了这个木桶盛水量的限制因素，若要此木桶盛水量增加，只有换掉短板或将其加长才行，这就是木桶原理。它表达的意思就是，一个水桶无论有多高，它盛水的高度取决于其中最短的那块木板。在信息安全领域中，目标系统就好比盛水的木桶，它的安全性完全取决于系统中最薄弱的那个环节。

举个例子，我们在给企业进行渗透测试服务时，发现弱口令的安全问题仍然是企业的一个重灾区，这些企业虽然在安全方面做了很多工作，而且也部署了一些安全设备，但往往却因为一个简单的弱口令导致整个系统被入侵和攻破，所以我们需要审视系统中的薄弱点，并进行加强。

2. 攻防不对称，安全是相对的

攻防不对称其实很好理解，防御方需要保护的是一个整体，而攻击方却可以通过审视这个整体，选择其中一个薄弱的环节进行持续的攻击。在这个对抗的过程中，其实很多内容都是不对称的，如下。

- **技术不对称**：攻击方可以针对目标使用的某个软件或组件进行深入的漏洞挖掘，然后通过新的 0day 漏洞完成攻击和入侵，而防御方却无法对系统每个部分的漏洞都有所了解。
- **成本不对称**：攻击方可以选择成本低廉、破坏力强的 DDoS 拒绝服务攻击，而防御方却需要消耗巨大的成本进行整体的防御。
- **信息不对称**：攻击方可以选择通过人员、社交、无线等与企业有依赖关系的入口制订攻击路径，而防御方却无法覆盖所有的关联入口。

因此不论是安全产品，还是安全设计，它们的目标从来都不是绝对安全的，而只追求相对

安全。但这个认知绝不是用来找借口或是逃避安全责任的，而是用来提醒我们：安全是一个动态的过程，当前的安全工作仍然还有提升的空间；攻防其实只是一种成本的博弈对抗，只需要在允许的成本范围内进行适度、有效的防御即可；在攻防不对称的情况下，我们可以选择用攻击驱动的方式进行防御。

3. 纵深防御

我们知道，当今所有的信息安全技术其实都是以“用户是好人”为信任前提，只有当确认他干了坏事之后，才会把他定义为“坏人”，然后开始对其进行响应或防御。只有当某个用户已被证明产生了危害后，才将其定位为黑客或攻击者，开始对他进行应急处置，这种防御方式显然存在天然的滞后性，也势必会导致安全人员处于被动、挨打的局面。

为了能够改变这种被动、滞后的劣势，就需要拉伸防御的纵深。其实一个完整的攻击并不是由单点完成的，它通常会由一系列的环节关联组成，属于一个持续、连贯的过程。因此，我们可以在攻击过程中的每个必要环节点设置防御，从而做到提前感知和防御，利用这种层层设防、联动防御的方式，就可以化被动为主动，在攻击产生危害之前对其进行应急响应和处置。

安全其实是一个动态、整体的概念，正如道哥所说，互联网本来是安全的，自从有了研究安全的人之后，互联网就变得不安全了；而研究安全的人归根结底可以分为攻与防两个大分支，不过这里所说的攻防不是单纯的攻击入侵与技术防御，它们会结合技术、业务、流程、人员、制度和管理，形成一个广义的攻防概念，并一起构成了安全这个整体。因此我们看待安全的时候需要从攻与防两个不同的角度来整体审视和博弈均衡，同时攻击和防御也会在不断碰撞和对抗的过程中得到发展和变化。攻击通常会选择系统相对薄弱的环节来实施，防御则需要从各个角度及不同维度进行整体防御，补齐系统的各个短板，但攻防它又是不对称的，因此我们需要利用纵深防御的理念，将完整的攻击链条进行拆分和细化，在每个环节进行深度分析和防御，从而建立起立体化的安全防御体系。

前言

随着互联网的高速发展，Web 应用在其中所扮演的地位也越来越重要，因为很多业务都选择使用 Web 的形式来提供服务，但随之而来的 Web 安全问题也日渐凸显出来，企业往往会因此遭受巨大的损失，此时很多企业都会在 Web 应用上线前或运行中对其进行相应的安全测试来保证安全性，减少由于安全问题造成的损失。

通常而言，Web 应用的安全测试技术主要有：黑盒测试和白盒测试，还有一种灰盒测试，它是介于黑盒和白盒之间的。这里我们主要说一下黑盒测试，它又被称为动态调试，这种方法主要是测试应用的功能点。它不需要分析内部代码，也不需要测试代码实现的逻辑。在黑盒测试过程中，只需要通过网页爬虫模拟正常用户访问 Web 应用的全部路径，然后基于探测的路径生成安全测试用例即可。在该过程中，被测站点往往被视为一个黑盒，此时不用关心其内部如何运行，用何种语言编写，只需依赖于 Web 应用的可用性。因此，黑盒测试常常是安全人员首选的测试方法，同时它具有实施性强、兼容性好，以及测试效率高等特点，因而得到了广泛的应用。

本书所讲的 Web 扫描器，属于黑盒测试的范畴，在 Web 应用安全测试中起着至关重要的作用，同时它的价值也是显而易见的。

- 对于企业建设来说，它可以帮助企业快速建立起常态、持续的安全扫描和监控体系，尽早发现安全问题并修复，从而节省人力成本和避免安全损失。
- 对于安全测试来说，它可以通过自动化的方式提高测试人员的效率及业务的覆盖面。
- 对于安全技术来说，Web 扫描器早已作为安全人员的必备工具，因此我们有必要了解其原理和思路，然后通过持续的安全研究和对漏洞库的积累打造属于自己的安全扫描器，提高安全能力。

因此，对于 Web 扫描器的学习和研究显得尤为重要。

本书适用的目标读者

- 甲方安全人员。
- 渗透测试人员。
- 安全测试人员。
- 安全开发人员。
- 技术负责人员。
- Web 扫描器开发人员。
- 对 Web 扫描器感兴趣的安全从业人员。

为什么写这本书

我还记得，在 2014 年年中的时候，我受邀参加上海的 QCon 大会，并在安全分会场上做了一场关于云 WAF 的演讲，会后博文视点的编辑找到了我，希望我可以写一本关于云 WAF 的书，经过慎重考虑，主要由于工作和时间的诸多不确定性，没敢贸然答应，此事只好作罢。

然而，时至今日，写书的想法却在心中越发强烈起来，我也深知写书不易，尤其是写一本技术类的书籍更难，它需要耗费大量的精力和时间去研究、调试、测试，以及论证。本书没有选择以云 WAF 为主题，主要是因为现阶段它与公司的业务过于密切，而且由于近年来我的工作角色的转变，已基本没有负责 WAF 相关的事情，所以最终放弃了，但也因此有了新的选择。

在安全宝被百度全资收购后，我有幸加入了百度安全，转而负责公司对外的企业安全服务。由于工作的需要，我经常会去拜访企业客户。在这个过程中，发现甲方客户其实很少会像 BAT 那样把安全当成一种习惯来执行，大多数都是事后出现安全问题才会想到使用渗透测试或 APP 测试这类服务来帮助排查和解决问题。至于 Web 扫描器那就更惨了，几乎快被人遗忘了，主要是因为很多甲方人员用扫描器来检测漏洞的时候，经常不能发现高危的安全问题，时间一久就开始对 Web 扫描器的价值产生质疑。

其实 Web 扫描就好比日常生活中的健康体检，你需要对安全进行长期的监控和检测，只有把扫描当成一种习惯，同时真正建立起企业专属有效的扫描体系，把安全当成一种习惯来对待，

你才能优于攻击者提前发现安全问题。

为了改变人们对扫描的一些误解，重新认识扫描特有的价值，所以，我决定写一本关于Web 扫描的安全书籍。在写书之初，我就开始对之前自己所写的扫描类文章进行重构和整理，希望可以借此将更多有价值的内容呈现出来，同时让读者有更多的收益或启示。

扫描器环境

操作系统：Debian 8 x64 账号：imiyoo/anquanbao

扫描测试：LNMP 1.2+ Wavesp 1.5

语言环境：Python 2.7.9

本书涉及的代码均以 Python 来实现，至于为什么选择 Python 语言？理由如下：

- Python 简单易学，上手很快，而且跨平台，可移植性强。
- 除了内置的库外，还有大量的第三方库，减少重复“造轮”工作。

约定

本书所提到的扫描器特指 Web 扫描器，为了便于内容简洁和避免读者误解，所以书中会统一使用扫描器来代替 Web 扫描器；同时阅读本书需要读者有一定的安全和开发基础，本书对一些比较基础的名称和技术并没有做太多的解释，读者可以通过百度等搜索引擎自行查阅。

由于时间关系，书中所涉及的相关资源暂无法全部上传，后面会陆续上传到笔者的 GitHub 上，读者可以在 https://github.com/imiyoo2010 上获取。

导读

全书共分为 9 章，内容之间有一定的关联性，所以建议大家最好从头到尾地阅读和学习。

第 1 章为扫描器基础，主要介绍扫描器的一些基础和必备知识，帮助读者更快地进入扫描器的世界并开始进行有目标的学习。

第 2 章和第 3 章分别为 Web 爬虫基础和 Web 爬虫进阶。爬虫作为 Web 扫描器的重要组成

部分，内容非常多，这里分两章来介绍，Web 爬虫基础主要介绍 Web 爬虫的一些必要的理论知识；Web 爬虫进阶则重点关注功能原理和代码实现，并对业界流行的 Web 2.0 爬虫进行思考和实践。

第 4 章为应用指纹识别，它也是 Web 扫描器必备的一个功能组成部分，主要介绍应用指纹识别的原理及实践。

第 5 章为安全漏洞审计，它是 Web 扫描器的核心，也是本书的重点内容之一，主要分为通用漏洞审计和 Nday/0day 漏洞审计，通过对漏洞进行场景化分析，由浅入深地介绍安全漏洞审计的原理和实践。

第 6 章为扫描器进阶，主要从整体的角度来设计和实现 Web 扫描器。

第 7 章为云扫描，主要介绍云扫描的知识及相关技术的具体实践。

第 8 章为企业安全扫描实践，主要介绍企业常用的扫描场景及实践。

第 9 章为防御，主要介绍扫描器的常见防御方式和手段。

致谢

我相信每一本书的完成都少不了身边亲人和朋友的支持，需要感谢的人太多了。

感谢我的老婆，为我生了一个聪明可爱的小子，并一直操劳着这个家，让我有足够的时间和精力来写作，老婆辛苦了，我爱你。

感谢我的父母，他们不计回报地付出和关爱着我，只求我健康成长。

感谢我所在的公司百度，百度是一家以技术为导向的公司，宽松的工作环境和良好的技术氛围，让我很快地成长起来。

感谢博文视点的编辑及其团队，在书籍出版的过程中，他们给了我很多专业的意见和帮助。

特别感谢冯景辉为本书写推荐序，他是一个充满激情且令人敬佩的领导，能邀请到他为本书写序，我十分荣幸。在公司内部我们都喜欢称他为冯老板，他敏锐的洞察力和成熟的方法论，以及对问题抽丝剥茧的能力，让我们受益良多。

还有感谢那些在背后给我支持和帮助的朋友、同事，以及领导，他们分别是：刘文杰、石

祖文、王胄、周永成、刘焱、耿志峰、李婷婷、程岩、马哲超、陈燕。

最后感谢所有对本书做出贡献的人，没有你们，这本书不会这么快面世。

谢谢你们！

本书的写作大部分是我利用业余时间来实践和完成的，匆忙中难免会有一些问题或错误，欢迎各位读者提出意见和建议，笔者不胜感激。

刘　漩

2017 年 2 月 27 日

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/31477*

目录

第 1 章　扫描器基础……1

1.1　什么是 Web 扫描器……1
1.2　扫描器的重要性……2
1.3　扫描器的类型……3
1.4　常见的扫描器（扫描器的示例）……4
1.5　扫描器评测……8
1.6　漏洞测试平台……9
1.7　扫描环境部署……9
1.7.1　测试环境……9
1.7.2　开发环境……12

第 2 章　Web 爬虫基础……19

2.1　什么是 Web 爬虫……19
2.2　浏览器手工爬取过程……19
2.3　URL……21
2.4　超级链接……22
2.5　HTTP 协议（Request/Response）……23
2.5.1　HTTP 请求……23
2.5.2　HTTP 响应……24
2.6　HTTP 认证……25
2.6.1　Basic 认证（基本式）……26
2.6.2　Digest 认证（摘要式）……27
2.7　HEAD 方法……29
2.8　Cookie 机制……29
2.9　DNS 本地缓存……31
2.9.1　浏览器缓存……31
2.9.2　系统缓存……32

2.10 页面解析……33
2.11 爬虫策略……34
2.11.1 广度优先策略……34
2.11.2 深度优先策略……34
2.11.3 最佳优先策略（聚焦爬虫策略）……35
2.12 页面跳转……35
2.12.1 客户端跳转……36
2.12.2 服务端跳转……37
2.13 识别 404 错误页面……38
2.14 URL 重复/URL 相似/URL 包含……39
2.14.1 URL 重复……39
2.14.2 URL 相似……39
2.14.3 URL 包含……39
2.15 区分 URL 的意义……40
2.16 URL 去重……40
2.16.1 布隆过滤器（Bloom Filter）……41
2.16.2 哈希表去重……41
2.17 页面相似算法……42
2.17.1 编辑距离（Levenshtein Distance）……42
2.17.2 Simhash……43
2.18 断连重试……43
2.19 动态链接与静态链接……43
第 3 章 Web 爬虫进阶……44
3.1 Web 爬虫的工作原理……44
3.2 实现 URL 封装……45
3.3 实现 HTTP 请求和响应……47
3.4 实现页面解析……58
3.4.1 HTML 解析库……58
3.4.2 URL 提取……59
3.4.3 自动填表……66
3.5 URL 去重去似……67
3.5.1 URL 去重……67
3.5.2 URL 去似去含……73

3.6 实现 404 页面识别 ……75
3.7 实现断连重试 ……77
3.8 实现 Web 爬虫 ……78
3.9 实现 Web 2.0 爬虫 ……83
第 4 章 应用指纹识别 ……94
4.1 应用指纹种类及识别 ……94
4.2 应用指纹识别的价值 ……95
4.3 应用指纹识别技术 ……96
第 5 章 安全漏洞审计 ……102
5.1 安全漏洞审计三部曲 ……102
5.2 通用型漏洞审计 ……103
5.2.1 SQL 注入漏洞 ……103
5.2.2 XSS 跨站漏洞 ……111
5.2.3 命令执行注入 ……120
5.2.4 文件包含漏洞 ……129
5.2.5 敏感文件泄露 ……136
5.3 Nday/0day 漏洞审计 ……146
5.3.1 Discuz!7.2 faq.php SQL 注入漏洞 ……147
5.3.2 Dedecms get webshell 漏洞 ……150
5.3.3 Heartbleed 漏洞（CVE-2014-0160） ……153
5.3.4 PHP multipart/form-data 远程 DDoS（CVE-2015-4024） ……157
第 6 章 扫描器进阶 ……160
6.1 扫描流程 ……160
6.2 软件设计 ……163
6.3 功能模块 ……164
6.4 软件架构 ……165
6.5 数据结构 ……166
6.6 功能实现 ……167
6.6.1 IP/端口扫描和检测（端口模块） ……167
6.6.2 端口破解模块 ……170
6.6.3 子域名信息枚举 ……172
6.6.4 文件、目录暴力枚举探测（不可视 URL 爬取） ……175

6.6.5 扫描引擎……176
6.7 扫描报告……180
6.8 扫描测试……182
第 7 章 云扫描……185
7.1 什么是云扫描……185
7.2 云扫描架构……185
7.3 云扫描实践……187
7.3.1 Celery 框架……188
7.3.2 扫描器 Worker 部署……189
7.3.3 云端调度……193
7.4 云扫描服务……199
第 8 章 企业安全扫描实践……202
8.1 企业为什么需要扫描……202
8.2 企业扫描的应用场景……202
8.2.1 基于网络流量的扫描……202
8.2.2 基于访问日志的扫描……208
8.2.3 扫描的应用场景比较……217
第 9 章 关于防御……218
9.1 爬虫反制……218
9.1.1 基于 IP 的反爬虫……218
9.1.2 基于爬行的反爬虫……221
9.2 审计反制……223
9.2.1 云 WAF……223
9.2.2 云 WAF 的价值……223
9.3 防御策略……225
附录 A……227
附录 B……229