Broadview
www.broadview.com.cn

安全技术大系

漏洞战争

软件漏洞分析精要

林桠泉 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

漏洞战争

软件漏洞分析精要

林桠泉 著

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

内 容 简 介

本书系统地讲解软件漏洞分析与利用所需的各类工具、理论技术和实战方法，主要涉及 Windows 和 Android 系统平台。全书根据不同的软件漏洞类型划分，比如堆栈溢出、沙盒逃逸、类型混淆、UAF、内核漏洞等，同时又针对当前流行的移动安全，加入 Android 平台上的漏洞分析与利用。以精心挑选的经典漏洞为例，以分享漏洞的分析技巧和工具为主，对这些漏洞的成因、利用及修复方法进行详细讲解，旨在“授之以渔”。本书最大的特点是以各种类型的经典漏洞作为实战讲解，摒弃空头理论，几乎是“一本用调试器写出来的书”。

本书适合计算机相关专业的本科及研究生，信息安全爱好者，软件安全及移动安全相关的安全从业人员，软件开发与测试人员、黑客等阅读。

图书在版编目（CIP）数据

漏洞战争：软件漏洞分析精要 / 林桠泉著. —北京：电子工业出版社，2016.6
（安全技术大系）
ISBN 978-7-121-28980-4

Ⅰ. ①漏… Ⅱ. ①林… Ⅲ. ①软件可靠性 Ⅳ. ①TP311.53

中国版本图书馆 CIP 数据核字（2016）第 125946 号

策划编辑：刘　皎
责任编辑：郑柳洁
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：787×980　1/16　　印张：37.75　　字数：960.36 千字
版　　次：2016 年 6 月第 1 版
印　　次：2016 年 6 月第 1 次印刷
定　　价：119.00 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

独乐乐，与人乐乐，孰乐？

不断向底层钻研的技术深度，创造性的广度思维，契而不舍地执着追求是成为优秀的安全研究员所必备的基础素质，无疑riusksk全都具备。

单论技术本身，问世间，是否此山最高，没有人能说的清楚。但是我在书目中还看到了许多超出技术的其他元素:有精益求精、追求完美的极客精神；有循序渐进、耐心引导的导师身影；有架构明晰，逻辑严谨的整体设计感；最能打动我的，其实是那份炽热的分享精神，毫无保留地去帮助那些还在摸索中学习的朋友。

一代宗师除了不断修炼自己之外，还需要将自己的智慧发扬传承，我在书中看到了这样的影子。

《0day安全：软件漏洞分析技术》作者，北京子衿晨风科技有限公司CEO

failwest

前　言

为什么写这本书

不知道大家是否曾有过这样的经历：

- 无法读懂网上很多软件漏洞分析文章，不理解里面的漏洞成因和漏洞利用技巧。
- 即使读懂某篇软件漏洞分析文章，自己仍无法独立完成相同漏洞的分析。如果文章中所使用的测试环境与软件版本跟自己使用的不一样，则顿时更不知如何入手。
- 很多软件漏洞分析文章贴出存在漏洞的汇编代码，指出导致漏洞的原因，即“结论式分析”，但如何定位到此段代码并无解释，看完之后，仍不知如何快速定位，缺乏可借鉴的思路。

带着这些问题，相信读者会在本书中找到想要的答案。

再来聊下本书的一些写作经历，开始写作本书始于2012年5月，最初是“爱无言”找到我，说大家合作写一本关于软件漏洞案例分析的书，因为那段时间我在博客上每周都会分享一两篇软件漏洞分析的实际案例，而当时国内还没有专门写软件漏洞案例的专著（几年前出版的《0Day安全：软件漏洞分析技术》主要偏向堆和栈溢出及内核方面的漏洞分析，实际案例较少，且“爱无言”也是作者之一）。

就这样，两人开始谋划，写书的念头就此产生。

后来，我又拉了两位朋友加入，然后几人列出大纲目录，但最后因为种种原因，只剩下我一人独自完成本书创作，中途也多次想放弃，但庆幸的是，历时3年半，终于2015年12月完稿，共历时4年后出版。

就这样，一本原为“合著”的书就写成了“专著”。

由于朋友的退出，以及写作速度较慢，中途停写半年，已原本打算放弃。后来，有一天，编辑“皎子”找我聊了一些出书的想法。

就这样，一本原打算沉留箱底的“残卷”再次被“激活”。

之后的写书经历还算顺利，又历时一年左右完稿，比较符合预期，遗留心底多年的梗总算可以释怀了。

相信一些读者看完本书目录之后会有一些疑问，也相信其中一些疑问也是我在定位本书方向时考虑的，所以有必要在此谈一谈。

Q：本书与《0day安全：软件漏洞分析技术》有何区别？

A：0day安全一书主要是讲Windows平台下堆栈溢出和内核提权的漏洞分析技术，还涉及部分格式化字符串漏洞，从基础讲起，最后是实例分析。本书则完全是以真实的漏洞为实例以分享漏洞分析时的一些技巧，以漏洞类型的不同来分享不同的漏洞分析技巧，可以说是“用调试器写出来的一本书”，而且综合考虑当前热门的移动安全，特意加入Android平台上的漏洞分析章节，从Java层、Native层和内核层等方向分享不同的调试分析方法。从难度而言，本书比《0day安全：软件漏洞分析技术》一书更难，可以将本书当作进阶版，搭配学习。

Q：本书列举的许多漏洞实例网上早有分析文章，为何还写这本书？

A：著书的宗旨在于“授人以鱼，不如授人以渔”。如果读者经常看网上的漏洞分析文章，就会发现一个常见现象：它们大多是“结论性分析”，而非“思路性分析”。换句话说，就是贴出存在漏洞的汇编代码，然后直接给出漏洞成因的结论，至于如何定位到漏洞代码，并没有给出分析思路。正因为如此，即使你看懂了Vupen漏洞军火商写的分析文章，也不代表你看完后就能独立分析出来，甚至在调试之后，你还会发现Vupen在一些文章里留有“坑”，故意省略或写错某些关键内容，如果没有自己实际调试一遍是很难发现这些问题的。

相信有一定软件漏洞分析经验的朋友会注意到，*软件漏洞分析的大部分时间是花费在寻找和定位漏洞代码，而非分析存在漏洞的代码*。对于有一定编程经验和漏洞基础的读者，如果直接给一段漏洞代码，可能很容易就看出来，但像Adobe和Windows这些复杂的软件或系统，在千千万万的代码行中找到漏洞代码是有一定难度的。因此，本书的重点是讲授如何快速地定位漏洞代码，针对不同漏洞类型采取不同的分析技巧，以帮助大家快速地分析出漏洞成因，制定检测、防御与修复方案。书中的漏洞实例分析技巧是可以长期运用和延伸的，这才是本书的核心价值。

Q：如何借助本书提升自身的软件漏洞分析能力？

A：本书主要面向有一定软件漏洞基础的读者，如果缺乏这方面的基础，且有一定C语言和汇编语言基础，建议提前看看《0day安全：软件漏洞分析技术》一书。软件漏洞分析是一门实践性比较强的安全领域分支，需要许多实际动手的调试经验，因此建议大家在看本书时，一边看一边动手调试，以加深理解，就像骑自行车一样，熟练之后，哪怕十年未碰，也依然会骑。本书在分析漏洞时，也尽量以思路性地描述为主，以讲解分析漏洞时的思考方式和常用技巧，包括工具和方法论，因此大家在阅读时，应该掌握书中介绍的思考方式、工具运用及分析技巧，毕竟单个漏洞案例本身是会过时的，但技巧性的东西总是可以借鉴和扩展。

记得大一上第一节历史课时，老师说过这样一句话，如果在未来的某一天，你在和朋友闲聊时，

能够运用到历史课上学到的知识，哪怕一句话作为谈资，那这历史课就算没白学。同样地，我也希望未来大家在分析软件漏洞时，本书能够提供一些帮助，哪怕是一个分析技巧，一个工具使用，我也觉得这4年的付出算值了。

纵观近五年，各种APT攻击事件频发，包括知名企业，甚至国家级单位都曾遭受到漏洞攻击。每年都有一款产品的漏洞被频繁用于网络攻击，比如2012年的Office漏洞（还记得经典的CVE-2012-0158吗？），2013年的Java漏洞，2014年的Internet Explorer漏洞，2015年Adobe Flash漏洞。PC端上的软件漏洞一直在逐年增加，虽然厂商在不断地推出各种安全机制，但漏洞利用技术的发展从未间断，Exploiter们依然生存得很好。同时，互联网早已步入移动化时代，伴随着PC软件漏洞攻击事件的频发，移动端的漏洞攻击也在逐年增长。因此，笔者结合PC端（Windows）与移动端（Android）平台上的漏洞案例，历时近4年，将自身的实战经验整理成本书。

求学之路

经常有人问我："一个医学生为什么会转行做安全？"，通常我都会这么回答："因为小说看多了"。

大一时，由于喜欢看黑客小说，比如《黑客传说》《地狱黑客》《指间的黑客》，就去图书馆找一些黑客书籍学习，每天中午都不休息，几乎天天都泡在图书馆看书，甚至翘课去看计算机书。

大四才买计算机，在此之前一直都只能去网吧、学校机房或者借用舍友的计算机。当年就用诺基亚3100手机看完了《Windows程序设计》、《Windows核心编程》和《Windows环境下32位汇编语言程序设计》。后来就网购实体书来看，这样比在网吧看电子书更实惠。

大学期间，经常给《黑客防线》杂志投稿，一方面可以提高个人技术，一方面可以用稿费作为生活补贴，后来就用稿费加上我哥的经济支持，买下了第一台属于自己的计算机，本书就有一半内容是在那台计算机上完成的。

在求学这条道路上，我一直是一个人默默地前行着，就连一块生活了几年的舍友也不知道我在学习安全方面的知识，我买的一堆计算机书籍一直藏在宿舍衣柜最里面。在此过程中，自己走过很多弯路，甚至多次差点放弃，但很庆幸最后还是坚持下来了，并直至今日，依然在安全这条道路上前行着……

面试经历

在圈内朋友的建议下，我在大五（医学五年制）上学期开始找安全相关的工作，最终顺利拿到安恒和腾讯的offer。当初投简历给安恒时，安恒的副总裁看完简历后直接发了offer，我有点受宠若惊，也特别感谢安恒的信任，但最终还是选择了腾讯。面试腾讯的经历，我觉得是个有趣的过程，值得与大家分享。

那年我还在厦门市第二医院骨伤科实习，门诊部刚好不是特别忙，我在给一位腰椎患者做完针灸后，就接到来自腾讯安全中心的面试电话。然后趁主任不在，偷偷躲到门诊部后面的楼梯口进行电话面试，整个面试过程还算比较顺利，第2天腾讯安全中心就来电说希望我到深圳总部面试。

到了深圳总部后，腾讯安全中心的主管面试了我，虽然聊了一个半小时，但没有问我多少问题，聊完后直接被带去HR那里面试。

HR面试我时，并非以常规的话题开场，我们是以腰椎间盘突出的话题开场的，也算是一次别开生面的面试经历。

回到厦门后，我跟带教老师说明了转行情况，之后有上手术台的机会，我都会主动让给其他同班同学，让他们有更多上台练手的机会，而我自己自然有更多的时间去专研安全技术。

加入腾讯

腾讯是我的第一家雇主，也是目前我唯一工作过的公司，从我毕业一直工作到现在。在公司我见证了腾讯安全应急响应中心（TSRC）的成立与发展，帮助完善各种流程和标准，作为早期主要的漏洞审核者，我也从广大白帽子身上学到很多东西，包括各种漏洞挖掘与利用技术，涉及各个安全领域，如Web安全、驱动安全、应用软件安全、移动安全等，正是TSRC给了我更多学习的机会，使得我在安全技术上能够更加全面地发展。除此之外，我在公司也做一些安全研究工作，并研发出Android与iOS应用安全审计系统，已投入公司日常运营使用。

至今，我依然觉得工作能够与兴趣结合在一起，是一件既幸福又幸运的事，而选择腾讯依然是我当年的明智之举。

著书感言

本书是我写的第一本书，也可能是最后一本技术书籍，只有自己经历了著书过程，才知道写书的不易。特别是类似本书这种以漏洞实例进行调试分析的书，写起来特别费时，也更需要有持之以恒之的毅力。如果说单纯写书用掉1年时间，那么我用来调试的时间大约是3年，因此可以说这是“一本用调试器写出来的书”。

“开头容易，收尾难”是个人著书的真实感受，很多人一时兴起写了开头，最后很难坚持下去，导致夭折了不少著作。

本书结构

本书共12章，可以分为三大部分。

基础篇（第1章）：主要介绍一些软件漏洞相关的基本概念，以及常用工具及漏洞分析方法，最后向读者推荐一些相关的学习站点和书籍，方便读者做进一步地学习和交流。

实战篇（第2~11章）：是本书最主要的部分，根据不同的漏洞类型挑选不同的经典案例，用不同的漏洞分析技巧，向读者介绍比较高效的分析方法，剖析各种常见的软件漏洞类型、原理、利用和修复的实战技术。同时，紧跟当前热门的移动互联网安全问题，增加了Android平台的漏洞分析，以保持内容与时俱进。

展望篇（第12章）：对未来的软件漏洞发展趋势做出预判，相信未来的主要战场会更集中在移动终端、云计算平台、物联网三大方向上，并对现有的这些方向的漏洞案例进行简要介绍。

致谢

感谢我父母的养育之恩，是他们在背后默默地支持我前行。

感谢我的兄长在生活和工作上对我的帮助与支持。

感谢我的女朋友，正是她的督促和支持才让我能够准时完稿，并且书中有些截图是经过她后期制作的，以便使得图片的印刷效果更好。

感谢我的姑母长期以来对我生活上的关心与照顾。

感谢我的公司腾讯，它所营造的良好氛围，使我的技术水平和在职场的发展都更上一层楼。同时也感谢在工作中一直给予我帮助和鼓励的同事和领导，由于人数较多，就不一一列举。

感谢王清先生为本书作序，他所著书籍一直是软件安全行业的经典。

感谢博文视点的编辑皎子、郑柳洁及她们的团队，正是他们的努力才使得本书最终能够与大家见面。

感谢各位圈内的朋友，他们包括但不限于（排名不分先后）：wushi、爱无言、仙果、wingdbg、instruder、kanxue、lake2、harite、h4ckmp、dragonltx、非虫、monster、gmxp、古河、冰雪风谷、KiDebug、KK……

由于作者水平有限，书中难免有误，欢迎各位业界同仁斧正！

2016年3月27日 于深圳

目　录