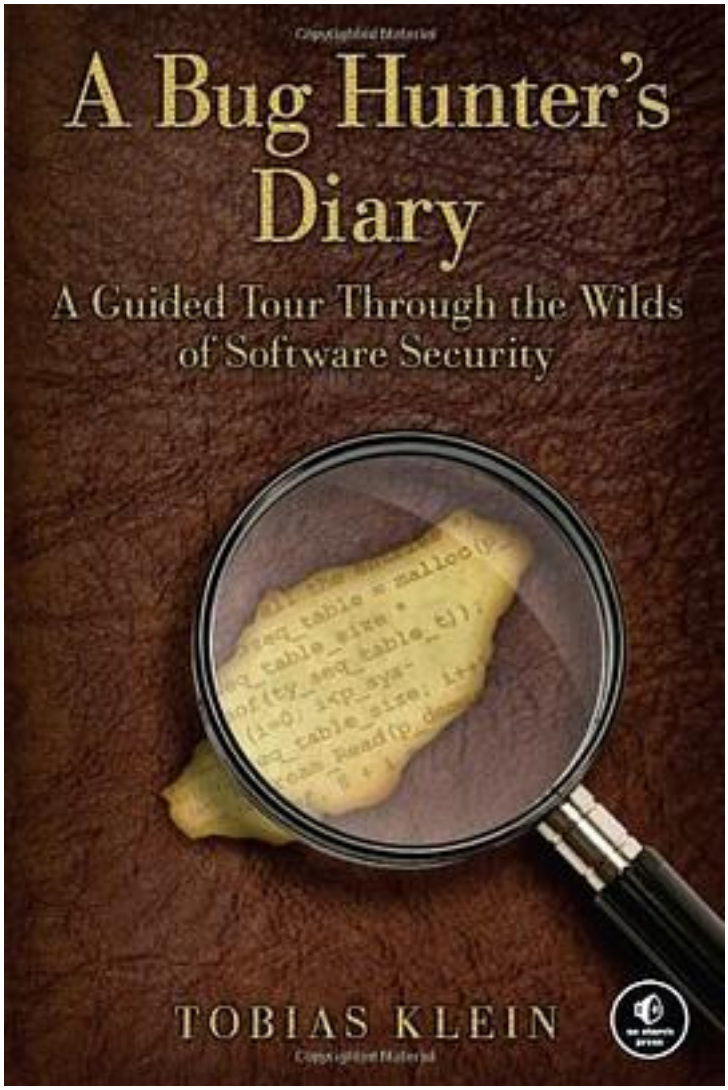
A Bug Hunter's Diary



A Bug Hunter's Diary_下载链接1_

著者:Tobias Klein

出版者:No Starch Press

出版时间:2011-11-11

装帧:Paperback

isbn:9781593273859

"Give a man an exploit and you make him a hacker for a day; teach a man to exploit bugs and you make him a hacker for a lifetime." -Felix 'FX' Lindner Seemingly simple bugs can have drastic consequences, allowing attackers to compromise systems, escalate local privileges, and otherwise wreak havoc on a system. A Bug Hunter's Diary follows security expert Tobias Klein as he tracks down and exploits bugs in some of the world's most popular software, like Apple's iOS, the VLC media player, web browsers, and even the Mac OS X kernel. In this one-of-a-kind account, you'll see how the developers responsible for these flaws patched the bugs-or failed to respond at all. As you follow Klein on his journey, you'll gain deep technical knowledge and insight into how hackers approach difficult problems and experience the true joys (and frustrations) of bug hunting. Along the way you'll learn how to: * Use field-tested techniques to find bugs, like identifying and tracing user input data and reverse engineering * Exploit vulnerabilities like NULL pointer dereferences, buffer overflows, and type conversion flaws * Develop proof of concept code that verifies the security flaw * Report bugs to vendors or third party brokers A Bug Hunter's Diary is packed with real-world examples of vulnerable code and the custom programs used to find and test bugs. Whether you're hunting bugs for fun, for profit, or to make the world a safer place, you'll learn valuable new skills by looking over the shoulder of a professional bug hunter in action.

作者介绍:

Tobias Klein
德国著名信息安全咨询与研究公司NESO安全实验室创始人，资深软件安全研究员，职业生涯中发现的软件安全漏洞无数，更曾为苹果、微软等公司的产品找出不少漏洞。除本书外，还出版过两本信息安全方面的德文作品。

张伸
不合格码农。爱咖啡，爱葡萄酒。爱听布鲁斯，也爱吃巧克力。不小资，不文青，只是喜欢收藏图书和CD。慢生活，每天听相声才能入睡。twitter和新浪微博：@loveisbug。

目录:

A Bug Hunter's Diary_下载链接1_

标签

安全

软件开发

security

漏洞挖掘

信息安全

计算机安全

计算机

调试

评论

还行

八个defect的发掘过程，比侦探小说还要引人入胜，妙趣横生

作者有那么点啰嗦，但讲得真心清楚，作为小白也能看

细读了前两张以及最后的附录，bug查找这事儿就好比警察查案，100个案子可能有100种不同的思路和方法，最好还是自己亲自上阵debug，以不变应万变。只是看别人的diary，估计仍旧无法掌握真谛。

由浅入深，故事一样，太好看了！

再棒的经历或者电子重复太多次也会变得很乏味

主要讲的是Memory Error，我比较关注的是Web-specific Vulnerabilities；对关键技术的描述值得借鉴

趣味读物

看的电子版，很不错，据说国内有人已经在翻译了。。。主要介绍了以查看源代码的方式挖掘安全漏洞，也有以fuzzing的方法，过程很是详细。不足之处在于讲的漏洞类型不是很多，而且偏老。。。现在比较流行的use-after-free\dobule free等内存bug没有

A Bug Hunter's Diary_下载链接1_

书评

对于苦逼的IT男而言，对下面这个场景应该感到亲切。发出去的软件版本出现了bug，事情很紧急，于是大佬召集所谓一堆专家头脑风暴寻求解bug的思路，各路专家你一言我一语各抒己见，最终在众人齐心协力下，终于在最后关头定位出了根因。没有解不了的bug，只有不努力的coder。 然而...

这本书能告诉你怎么写代码可以避免一些常见的安全漏洞，它是作者寻找各种平台与知名软件漏洞的实践日记。不要以为这些都离你很远，恰恰是开发人员造就了各种漏洞。如果有些在写代码时就可以避免，为什么不这么做呢。
这本书读起来不会觉得艰深晦涩，但还是需要掌握一些基础知...

Mark Dowd et al The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities (Addison-Wesley, 2007) Fuzzing Michael Sutton et al Fuzzing: Brute Force Vulnerability Discovery

---
Although no formal documentation exists that describes the standard bug-hunting process, common techniques do exist. These techniques can be split into 2 categories: static and dynamic. In static analysis, also referred to as static code analysis, the sour...

作者简介 Tobias
Klein，安全问题研究员，创办NESO安全实验室，NESO是一家位于德国海尔布伦的信息安全咨询、研究公司。身为安全漏洞研究人员，Tobias发现了许多安全漏洞，并帮助修复它们。他也出版了另外两本信息安全领域的著作，由海德堡的出版商dpunkt在德国发行。 ...

地铁里看完的第一章，捉虫子，这个最原始的概念让我对今天的工作又燃起了激情。感觉这是个好的开始，可以重新培养地铁看书的习惯。
里面的空指针、缓冲区溢出等信息，让我冒出一头冷汗，太久太久没接触这些东西了，能不能看懂？但还是从中慢慢感受到力量充实进来，process ...

我看过了 我看...

[A Bug Hunter's Diary_下载链接1_]