O'REILLY®

敏捷应用程序安全

Agile Application Security

Laura Bell Michael Brunton-Spall
Rich Smith Jim Bird 著
杨宏焱 刘恒屹 译

中国电力出版社

敏捷应用程序安全

Laura Bell, Michael Brunton-Spall,
Rich Smith, Jim Bird 著
杨宏焱 刘恒屹 译

Beijing • Boston • Farnham • Sebastopol • Tokyo O'REILLY®
O'Reilly Media, Inc. 授权中国电力出版社出版

中国电力出版社

图书在版编目（CIP）数据

敏捷应用程序安全 /（美）/劳拉·贝尔（Laura Bell）等著；杨宏焱，刘恒屹译. — 北京：中国电力出版社，2018.11

书名原文：Agile Application Security

ISBN 978-7-5198-2639-0

I. ①敏… II. ①劳… ②杨… ③刘… III. ①软件开发－安全技术 IV. ①TP311.522

中国版本图书馆CIP数据核字(2018)第261094号

北京市版权局著作权合同登记 图字：01-2018-7455号

出版发行：中国电力出版社
地　　址：北京市东城区北京站西街19号（邮政编码100005）
网　　址：http://www.cepp.sgcc.com.cn
责任编辑：刘 炽（liuchi1030@163.com）
责任校对：黄 蓓，李 楠
装帧设计：Karen Montgomery，张 健
责任印制：杨晓东

印　刷：北京天宇星印刷厂
版　次：2018年11月第一版
印　次：2018年11月北京第一次印刷
开　本：750毫米×980毫米　16开本
印　张：22.25
字　数：399千字
印　数：0001—3000册
定　价：78.00元

O'Reilly Media, Inc.介绍

O'Reilly Media通过图书、杂志、在线服务、调查研究和会议等方式传播创新知识。自1978年开始，O'Reilly一直都是前沿发展的见证者和推动者。超级极客们正在开创着未来，而我们关注真正重要的技术趋势——通过放大那些“细微的信号”来刺激社会对新科技的应用。作为技术社区中活跃的参与者，O'Reilly的发展充满了对创新的倡导、创造和发扬光大。

O'Reilly为软件开发人员带来革命性的“动物书”；创建第一个商业网站（GNN）；组织了影响深远的开放源代码峰会，以至于开源软件运动以此命名；创立了《Make》杂志，从而成为DIY革命的主要先锋；公司一如既往地通过多种形式缔结信息与人的纽带。O'Reilly的会议和峰会集聚了众多超级极客和高瞻远瞩的商业领袖，共同描绘出开创新产业的革命性思想。作为技术人士获取信息的选择，O'Reilly现在还将先锋专家的知识传递给普通的计算机用户。无论是通过书籍出版，在线服务或者面授课程，每一项O'Reilly的产品都反映了公司不可动摇的理念——信息是激发创新的力量。

业界评论

“O'Reilly Radar博客有口皆碑。”

——Wired

“O'Reilly凭借一系列（真希望当初我也想到了）非凡想法建立了数百万美元的业务。”

——Business 2.0

“O'Reilly Conference是聚集关键思想领袖的绝对典范。”

——CRN

“一本O'Reilly的书就代表一个有用、有前途、需要学习的主题。”

——Irish Times

“Tim是位特立独行的商人，他不光放眼于最长远、最广阔的视野并且切实地按照Yogi Berra的建议去做了：‘如果你在路上遇到岔路口，走小路（岔路）。’回顾过去Tim似乎每一次都选择了小路，而且有几次都是一闪即逝的机会，尽管大路也不错。”

——Linux Journal

目录

前言

软件正在改变这个世界。开发者成为了新的无冕之王。物联网意味着每个电灯泡中都会有一台计算机存在。

这种说法也表明软件开发越来越占据了统治地位，世界上大多数人距离某台计算机不会超过 1 米，在任何时候我们都生活在计算机辅助类物品或环境的影响下。

但随之而来的却是某种危机。在过去，安全通常是银行业和政府系统才需要真正考虑的事情。但由于计算机无处不在，通过系统滥用的可行性增加了，从而诱发了系统滥用，增加了系统所要面对的风险。

敏捷开发技术越来越被大多数组织所快速采用。通过响应式改变以及开发成本的明显降低，它们以一种敏捷的方式提供了理想的、能够不断迭代直到软件大版本被构建出来的标准。

但是，从历史观点来说，安全和敏捷从来不是天生的一对。

在前面提到的政府、经济和银行系统中，安全专家正在忙得不可开交，他们正在努力构建、测试和加固这些系统，以应对层出不穷的各种威胁。而且，我们经常可以在技术博客和晚间新闻中看到的最有趣、最刺激的东西，也主要集中在职业黑客团队所做的漏洞研究、Exploit 开发和特技攻击上。

你可能听过几个最新的漏洞，比如心血漏洞（Heartbleed）、阻塞漏洞（Logjam）及破壳漏洞（Shellshock），也可能知道几个能够越狱最新 iPhone 和 Android 设备的团队。

但除了最终出现的那个带有好听的、媒体友好名字的防御措施或方法之外，你还记得任何一个防御者或者建设者的名字吗？

安全专家在敏捷开发方面的知识和经验已经落伍了，在我们这个行业中已经出现了一个惊人的鸿沟。

同样地，敏捷开发团队拒绝和摆脱了过去的羁绊。没有详细的需求说明、没有系统建模、没有传统的瀑布切换和控制门。但问题是，敏捷团队将洗澡水和婴儿一起泼出去了。那些有时候既缓慢又不灵活的实践，在过去也曾经证明过是有价值的。它们的存在是有原因的，敏捷团队丢弃了它们，很容易就忽略和丢掉了它们的价值。

这意味着敏捷团队是尽可能地不考虑安全问题。有一些敏捷实践让系统更安全，但那通常是一个意外惊喜而不是故意设计。很少有敏捷团队会意识到他们系统面临的威胁；不理解他们正处于风险之中；不跟踪或者不会控制这些风险；对有人会攻击他们的系统缺乏理解。

本书的读者对象

我们不知道你是一个敏捷团队的领导者，还是一个想知道更多安全知识的开发者，也可能是一个安全行业的从业者，发现整个开发团队已经不是你曾经认识过的样子，你想学习更多。

这本书的目标是针对这三种主要的读者。

敏捷开发者

你活着、呼吸着，所以敏捷。你从你的 Kaizen 中知道你的 Scrum，在你的反馈循环中进行测试驱动开发。无论你是不是一个 Scrum 大师，开发者、测试者、敏捷开发讲师、产品的业主，还是客户代理，你都需要理解敏捷开发的实践和价值。

本书将帮助你学习什么是安全，存在什么样的威胁，以及安全从业者用于描述所发生的事情的语言。我们会帮助你理解如何建模威胁，度量风险，从理论上构建安全软件，安全地安装软件，以及理解运营中来自于某个在线服务的安全问题。

安全从业者

无论你是否是一个风险管理者、一个信息安全专家，还是一个安全运营分析家，你应该理解安全。你可能关心如何使用在线服务，无时不刻不在思考各种威胁、风险以及缓解措施，你甚至发现过新漏洞并利用它们进行过提权。

这本书会帮助你理解敏捷团队是如何真正对软件进行开发的，这个地球上的这类团队正在谈论什么，以及他们口中的冲刺和故事是什么。你将学习查看 chaos 中的模板，以及帮助你和团队进行交流并影响他们。本书将告诉你可以从哪些地方介入或者做出努力，这也是对一个敏捷团队最具价值和最能发挥作用的地方。

敏捷安全从业者

从风险到冲刺，你无一不知。无论你是一个帮助团队做好安全的工具创建者，还是一个负责对团队提建议的顾问，本书都适合你。抛开本书的主要内容，去理解本书作者的意图，也就是正在增长的良好实践。本书将有助于了解在你领域内的其他人，以及我们正在组织中处理这个问题时出现的想法和概念。这会提高、扩展你对相关域的理解，以及为你提供一个继续研究学习的目标。

本书主要内容

你可以按从头到尾的顺序来逐章阅读本书。实际上我们也推荐你以这种方式阅读；我们努力编写本书，希望在每一章都包含对所有读者有用的内容，哪怕一个小小的冷幽默或趣闻轶事！

但实际上，我们也认为有的章对你来说会比其他章更有用。大致将本书分成三个部分。

第一部分：基础

敏捷和安全是非常宽的领域，我们不知道你掌握了什么。尤其当你是来自其中某一个领域时，你可能不知道另一个领域的知识。

如果你是敏捷专家，我们建议你先阅读第 1 章，“安全概述”，以确保你具备基本的安全知识。

如果你不是，或者你还刚刚开始接触敏捷开发，那么在我们开始介绍敏捷之前，我们建议你阅读第 2 章，“敏捷促进者”。这一章介绍了我们认为的基本实践是什么，以及我们将从什么样的基础开始。

第 3 章，“迎接敏捷革命的到来”，介绍敏捷软件开发的历史，以及它的不同实现方式。对于安全专家和没有敏捷开发经验的人来说，这也是他们最感兴趣的部分。

第二部分：敏捷和安全

我们建议每个人都开始阅读第 4 章，“在现有的敏捷生命周期中工作”。

在这一章中，试图将我们想到的安全实践和真实的敏捷开发生命周期联系到一起，同时解释说明为什么要将它们联系起来。

第 5~7 章，学习需求和漏洞管理、风险管理，这些更全面的实践将从一个方面支撑起开发中的产品管理和总体方案。

第 8~13 章包括了安全软件开发生命周期的各个组成部分，从评估、代码评审、测试到运行安全。

第三部分：最后组装

第 14 章，介绍合规性，以及它和安全有何关系，如何在敏捷开发或 DevOps 环境中实现合规。

第 15 章，介绍安全的文化体系。没错，你可以实现本书介绍的所有实践，前面的章节介绍了你能够使这些改变持续的各种工具。然而敏捷开发都是关于人的，有效的安全持续也是这样：安全其实是改变内心的文化，这一章会提供一些我们在真实世界中找到的有效案例。

对于一个公司，要改变它的安全性，它需要安全专家和开发人员相互支持和尊重，他们需要密切合作以构建安全持续。它不仅仅是一堆工具或一系列实践，还需要这个组织的彻底改变。

第 16 章，介绍敏捷安全对不同的人意味着什么，并归纳出要让团队敏捷和安全，我们每个人应该干什么和不应该干什么。

本书约定

本书常用到的排版方式约定如下：

斜体（*Italic*）

表示新出现的术语、URL、email 地址、文件名及扩展名。

等宽字体（`Constant Width`）

在代码清单中使用，或者在段落中用于表示程序中的对象，如变量名、函数名、数据库、数据类型，环境变量、语句和关键字。如果在代码行后出现 ↵ 字符，表示这一行后面是下一行。

加粗的等宽字体（**`Constant width bold`**）

表示命令或需要用户输入的其他文本。

倾斜的等宽字体（*`Constant Width Italic`*）

表示文本应该由用户自己提供的内容替换，或者根据上下文改变。

表示提示或建议。

表示一般的注意事项。

表示警告或提醒。

O'Reilly Safari

Safari（过去叫 Safari 图书在线）是一个针对企业、政府、教育机构和个人的会员制培训和参考平台。

成为会员将可以从数据库中查找和浏览数以千计的图书、培训视频、学习路径、交互式教程和组织好的播放列表，这些资料的来源遍及 250 个出版社，如 O'Reilly Media、

Harvard Business Review、Prentice Hall Professional、Addison-Wesley Professional、Microsoft Press、Sams、Que、Peachpit Press、Adobe、Focal Press、Cisco Press、John Wiley & Sons、Syngress、Morgan Kaufmann、IBM Redbooks、Packt, Adobe Press、FT Press、Apress、Manning、New Riders、McGraw-Hill、Jones & Bartlett、Course Technology 等。

更多信息，请访问：*http://oreilly.com/safari*。

联系我们

请把你对本书的意见和疑问发给出版社：

美国：

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472

中国：

北京市西城区西直门南大街2号成铭大厦C座807室（100035）
奥莱利技术咨询（北京）有限公司

本书有一个专属网页，我们会在上面列出勘误、示例，以及其他附加信息。你可以通过以下地址访问它：http://*bit.ly/agile-application-security*。

如果是评论或者讨论和本书相关的技术问题，那么请发邮件到 *bookquestions@oreilly.com*。

关于我们出版社的其他书籍、教程、会议和新闻，请访问我们的网站 *http://www.oreilly.com*。

我们的Facebook：*http://facebook.com/oreilly*。

我们的Twitter：*http://twitter.com/oreillymedia*。

我们的 YouTube：*http://www.youtube.com/oreillymedia*。

致谢

首先要感谢三位了不起的编辑：Courtney Allen、Virgnia Wilson 和 Nan Barber。没有你们和其他 O'Reilly 团队的成员，我们无法完成本书。

我们还要感谢技术评审的耐心和真知灼见，分别是：Ben Allen、Geoff Kratz、Pete McBreen、Kelly Shortridge 和 Nenad Stojanovsk。

最后还要感谢我们的朋友和家人，忍受我们再次从事这样一个疯狂的项目。