O'REILLY®

TURING 图灵程序设计丛书

Web安全开发指南

掌握白帽子的Web安全技能，从源头消除安全隐患，打造安全无虞的Web应用

Security for Web Developers

[美] John Paul Mueller 著

温正东 译

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

Web安全开发指南

Security for Web Developers

[美] John Paul Mueller 著
温正东 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Tokyo
O'Reilly Media, Inc.授权人民邮电出版社出版

人民邮电出版社
北 京

图书在版编目（CIP）数据

Web安全开发指南 / (美) 约翰·保罗·米勒 (John Paul Mueller) 著 ; 温正东译. -- 北京 : 人民邮电出版社, 2017.6
（图灵程序设计丛书）
ISBN 978-7-115-45408-9

Ⅰ. ①W… Ⅱ. ①约… ②温… Ⅲ. ①互联网络－安全技术－指南 Ⅳ. ①TP393.408-62

中国版本图书馆CIP数据核字(2017)第083702号

内 容 提 要

本书分为5大部分，共17章，详细介绍了Web安全开发的必备知识，旨在让前端开发人员、设计师、产品经理等前端开发相关人士了解新形势下的安全技能，涉及从最新的智能手机到老旧的台式计算机等各种设备，并且不限定平台。具体内容包括：制订安全计划，运用成功的编码实践，创建有用及高效的测试策略，实现维护周期，查找安全资源。

本书适合所有Web开发领域的专业人士阅读。

◆ 著 [美] John Paul Mueller
译 温正东
责任编辑 岳新欣
执行编辑 赵瑞琳
责任印制 彭志环

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京市昌平百善印刷厂印刷

◆ 开本：800×1000 1/16
印张：17
字数：402千字 2017年6月第1版
印数：1－3 500册 2017年6月北京第1次印刷
著作权合同登记号 图字：01-2017-7589号

定价：69.00元

读者服务热线：(010)51095186转600 印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字20170147号

译者介绍

温正东

华南理工大学计算机硕士，曾任华为公司IT工程师，现为富途证券Web运营和基础架构组负责人。

微信连接

回复“Web开发”查看相关书单

微博连接

关注@图灵教育 每日分享IT好书

QQ连接

图灵读者官方群I：218139230
图灵读者官方群II：164939616

图灵社区
iTuring.cn

在线出版，电子书，《码农》杂志，图灵访谈

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。无论是通过图书出版、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*

献给那些帮我恢复身体健康的医学专家——他们聆听了我的疾苦并找到了解决方法。是的，我确实需要听从他们的建议。身体健康是一件非常棒的礼物。

前言

勒索软件、病毒、分布式拒绝服务（distributed denial-of-service，DDoS）攻击、中间人攻击、安全漏洞，这些词都会勾起参与应用程序管理的人噩梦般的回忆。现在已经到了这样的地步：在处理关乎应用程序或其相关数据安全的问题时，任何人都会变得风声鹤唳、极其保守。你肯定不希望承担应用程序安全相关的责任，但这是在所难免的。

任何一种安全失误所造成的灾难性后果都会困扰你的余生，让你承受极大的压力。与大多数错误不同的是，你不能将这种错误隐藏起来，因为它会出现在所有人都能看到的行业媒体上。虽然你的名字不会成为安全事故的代名词，但安全问题仍会给你带来很多麻烦，比如官司缠身、失业等。那么应该如何处理这个问题呢？

逃避并不能解决问题，至少不是长期的解决方案。本书并不打算介绍我们可能会遇到的每一种安全威胁或解决它们的方法，而是提供独立解决任何一种安全问题所需要的指导原则和工具，让你看到成功的希望。本书的真正目的是教你如何将事情做对，从而可以安心地睡个好觉。

本书预览

本书会提供处理应用程序安全问题所需的资源。是的，你还会在书中看到一些关于平台的信息，因为浏览器是在特定的平台上运行的。此外，你可能会看到使用桌面端应用程序时出现的一些安全问题，因为这些问题在这两种应用领域中都存在。但是，不论这些应用程序在什么地方运行，本书会聚焦于 Web 应用程序的安全性。你在本书中读到的内容不仅会涉及最新的智能手机，而且会涉及老旧的台式计算机等各种设备。本书会将内容分解为以下几个部分，每个部分都会协助你在安全性建设的道路上走好相应的一步。

- 第一部分

  无计划不成事。但在计算机行业中，一些最严重灾难的发生恰恰是由于糟糕的计划，而不是没有计划。这一部分会帮助你为公司创建良好的安全计划，即一个考虑到所有最新的用户设备和用户需求的计划。此外还将讨论第三方支持的必要性，因为我们不得不面对这样的事实：在复杂的环境下确实很难独自创建出安全的应用环境。这些内容有助于定位正确的第三方支持，并确保你能收获自己想要的价值。

- 第二部分
  如今的应用程序开发都会依赖第三方代码库、API 和微服务。这一部分将有助于你思考编码问题。你不会读到太多涉及位或字节层面的内容，但会找到将这些元素成功集成到应用程序中的一些技巧。这一部分会帮助你驾驭应用程序，而不是被它们所驾驭。

- 第三部分
  测试应用程序安全性的方法有很多种。比如，你可以创建自己的测试套件或者使用其他人创建的套件。第三方程序也能为你做测试。也许你想要知道怎样才能最好地整合不同的测试策略，以确保整个应用程序被完整覆盖。这一部分可以回答你所有关于现代化测试策略的问题，并介绍如何让工作更有效率。

- 第四部分
  应用程序在某个时间点被发布到生产环境中，并且运行良好。一些应用程序会以这样的方式持续运行多年而不需要适当的维护。不幸的是，现代的应用程序开发需要不断更新，因为黑客在不停地想出新的策略来入侵系统。而你所使用的所有第三方库、API 和微服务的更新则让情况变得更加混乱。这一部分将为你提供一张走出“更新迷宫”的地图，以便应用程序的各部分能够按照你最初的设想保持正常运行。

- 第五部分
  安全威胁在持续地演变，这意味着你需要一些方法来持续跟进。第一种方法是跟踪这些安全威胁。当然，如果你跟踪每一种威胁，那将一事无成。这一部分描述了你能用来避免信息泛滥的一些技巧。第二种方法是接受额外的培训。事实上，整个公司都需要一些培训来了解最新的安全问题和处理它们的技术。这一部分还以一种所有公司都能采用的方式探讨了安全培训的要求，即使是只有一个人的公司或者创业公司也同样适用。

阅读须知

本书的读者可以是拥有任何头衔的人，比如网页设计师、前端开发人员、UI 设计师、用户体验设计师、交互设计师、美术总监、内容策略师、开发运营人员、产品经理、搜索引擎优化专家、数据科学家、软件工程师或者计算机科学家。大家都有一个共同的需求，即创建安全的 Web 应用程序，让用户能以有意义的方式与之交互。这些人员都是之前开发过 Web 应用程序的专业人士，可能真正需要的是重新了解新形势下的安全技能。这种新形势指的是大部分应用程序是被非传统的方式攻破的，比如通过污染第三方的 API 和库。

本书会给出系统性的安全方案，但不会过多地进行手把手的指导。本书假设你想要了解最新的关于如何在不同级别阻止安全威胁的信息，其中包括对这些威胁的精确解读，以及黑客如何使用它们破坏你的安全措施。

本书包含一些安全编程的示例。要想使用这些例子，你需要具备良好的 CSS3、HTML5 和 JavaScript 编程技术方面的基础。但如果你不具备相关的技能，则可以跳过编程示例，但仍然能够从本书中获得大量有用的信息。编程示例提供只有程序员才会关注的细节。

除了编程技巧，更重要的是你接受过一定程度的安全培训。举个例子，如果你根本不知道什么是中间人攻击，那么确实需要先阅读较为基础的图书。本书当然不会假设你是了解中间人攻击各种细节的专家，但确实会认为你之前接触过它。

开发环境

运行本书中的编程示例，只需要文本编辑器和浏览器。文本编辑器必须输出纯文本，不要有任何形式的格式化。它还要能够用正确的文件扩展名（.html、.css 和 .js）来保存这些示例文件。我和多位图书编辑、试读者使用 Linux、Mac 和 Windows 平台上最流行的浏览器测试过书中的例子。事实上，我们甚至在 Windows 10 系统的 Edge 浏览器上测试过这些例子。

本书使用的图标

不同的图标用于传达不同种类的重点信息。本书使用的图标很少，但你需要知道其中每一个图标的含义。

此图标强调一些重要内容，这些内容略微偏离主题或者可能会破坏文字的连贯性。你需要阅读这些说明，因为它们通常会提供有助于你更好执行安全任务的信息。它们还会方便你找到所记得的重要内容，否则你可能很难找到。

此图标表示你必须知道的信息；如果不知道这些信息，你可能会遭受可怕的后果。与说明图标一样，这个图标强调了特殊的内容，这些内容会告诉你可能导致更严重问题的潜在问题。如果你读过某章后没有任何收获，那么一定要将这些警告内容学好并记牢，这能让你在今后避免代价高昂的错误。

补充信息

这一部分包含一些有用的信息，但你在开发 Web 应用程序时不一定需要了解它们。你应该找个时间将这些内容都看一遍，因为它们非常有趣，但没必要立即阅读。这部分内容是对当前话题的补充，不一定是关于该话题的内容。

排版约定

本书使用了下列排版约定。

- 楷体
  表示新术语或重点强调的内容。
- 等宽字体（`constant width`）
  表示程序片段，以及正文中出现的变量、函数名、数据库、数据类型、环境变量、语句和关键字等。
- 加粗等宽字体（**`constant width bold`**）
  表示应该由用户输入的命令或其他文本。

- 等宽斜体（*Constant width italic*）
  表示应该由用户输入的值或根据上下文确定的值替换的文本。

获取更多信息

我想要尽量确保你能够获得最好的阅读体验。如果有任何关于本书的问题，请一定发邮件到 John@JohnMuellerBooks.com。你也可以关注本书的博客 http://blog.johnmuellerbooks.com/category/technical/security-for-web-developers/。这个博客会提供更多的内容，并回答读者常问的问题。如果本书有勘误之处，你也能在博客上找到相关的修正。

使用代码示例

补充材料（代码示例、练习等）可以从 https://github.com/oreillymedia/Security_for_Web_Developers 下载。

本书是要帮你完成工作的。一般来说，如果本书提供了示例代码，你可以把它用在你的程序或文档中。除非你使用了很大一部分代码，否则无需联系我们获得许可。比如，用本书的几个代码片段写一个程序就无需获得许可，销售或分发 O'Reilly 图书的示例光盘则需要获得许可；引用本书中的示例代码回答问题无需获得许可，将书中大量的代码放到你的产品文档中则需要获得许可。

我们很希望但并不强制要求你在引用本书内容时加上引用说明。引用说明一般包括书名、作者、出版社和 ISBN。比如："*Security for Web Developers* by John Paul Mueller (O'Reilly). Copyright 2016 John Paul Mueller, 978-1-49192-864-6."

如果你觉得自己对示例代码的用法超出了上述许可的范围，欢迎你通过 permissions@oreilly.com 与我们联系。

Safari® Books Online

Safari Books Online（http://www.safaribooksonline.com）是应运而生的数字图书馆。它同时以图书和视频的形式出版世界顶级技术和商务作家的专业作品。技术专家、软件开发人员、Web 设计师、商务人士和创意专家等，在开展调研、解决问题、学习和认证培训时，都将 Safari Books Online 视作获取资料的首选渠道。

对于组织团体、政府机构和个人，Safari Books Online 提供各种产品组合和灵活的定价策略。用户可通过一个功能完备的数据库检索系统访问 O'Reilly Media、Prentice Hall Professional、Addison-Wesley Professional、Microsoft Press、Sams、Que、Peachpit Press、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 以及其他几十家出版社的上千种图书、培训视频和正式出版之前的书稿。要了解 Safari Books Online 的更多信息，我们网上见。

联系我们

请把对本书的评价和问题发给出版社。

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

O'Reilly 的每一本书都有专属网页，你可以在那儿找到本书的相关信息，包括勘误表、示例代码以及其他信息。本书的网站地址是：

http://shop.oreilly.com/product/0636920041429.do

对于本书的评论和技术性问题，请发送电子邮件到：

bookquestions@oreilly.com

要了解更多 O'Reilly 图书、培训课程、会议和新闻的信息，请访问以下网站：

http://www.oreilly.com

我们在 Facebook 的地址如下：

http://facebook.com/oreilly

请关注我们的 Twitter 动态：

http://twitter.com/oreillymedia

我们的 YouTube 视频地址如下：

http://www.youtube.com/oreillymedia

致谢

感谢我的妻子 Rebecca。虽然她已离世，但她的精神存在于我写的每一本书以及每一个词里。当没有人相信我的时候，她一直相信我。

感谢 Russ Mullen、Billy Rios 和 Wade Woolwine 对本书进行的技术编辑。这三位技术编辑极大地提升了书中内容的准确性和深度。很多时候，我都能与他们就书中核心话题的研究进行交流，并寻求他们的帮助。

感谢我的经纪人 Matt Wagner 帮我取得了这份合同，并帮忙打理大多数作者都不会关注的各种细枝末节。我一直感激他的帮助。知道有人愿意帮忙真的是一件非常棒的事情。

许多人阅读了全书或者部分内容，帮助我改进了方法，测试脚本，并提供了所有读者都希望包含的大量输入数据。这些不收酬劳的志愿者以各种各样的方式提供帮助，这里就不一一罗列了。我特别感谢 Eva Beattie、Glenn A. Russell 和 Luca Massaron 的帮助，他们提

供了大量输入数据并读完整本书，忘我地参与到这个项目中来。

最后，我要感谢 Meg Foley、Nicole Shelby、Jasmine Kwityn 以及参与编辑和印制工作的所有其他人员。

电子书

扫描如下二维码，即可购买本书电子版。

目录

第二部分　运用成功的编码实践