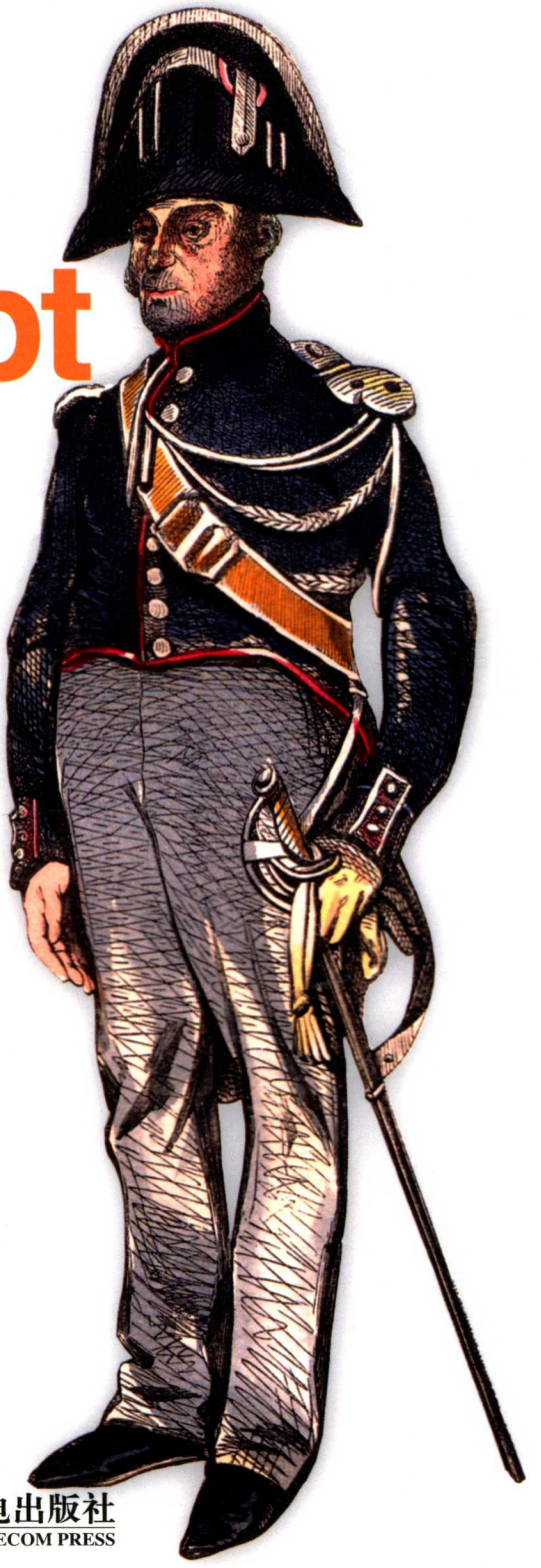
MANNING

第三方JavaScript编程

THIRD-PARTY JavaScript

〔美〕 Ben Vinegar
Anton Kovalyov 著
郭凯 译



中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

MANNING

第三方 JavaScript 编程

THIRD-PARTY JavaScript

〔美〕 Ben Vinegar
Anton Kovalyov 著
郭凯 译

人民邮电出版社
北京

图书在版编目（CIP）数据

第三方JavaScript编程 / (美) 维尼哲(Vinegar,B.), (美) 科瓦罗夫 (Kovalyov,A.) 著 ; 郭凯 译. -- 北京 : 人民邮电出版社, 2015.9
ISBN 978-7-115-39224-4

Ⅰ. ①第… Ⅱ. ①维… ②科… ③郭… Ⅲ. ①JAVA语言－程序设计 Ⅳ. ①TP312

中国版本图书馆CIP数据核字(2015)第162243号

◆ 著 [美] Ben Vinegar Anton Kovalyov
译 郭 凯
责任编辑 陈冀康
责任印制 张佳莹 焦志炜

◆ 人民邮电出版社出版发行 北京市丰台区成寿路 11 号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：16
字数：335 千字 2015 年 9 月第 1 版
印数：1－2 500 册 2015 年 9 月北京第 1 次印刷
著作权合同登记号 图字：01-2013-3652 号

定价：55.00 元

读者服务热线：(010)81055410 印装质量热线：(010)81055316
反盗版热线：(010)81055315

内容提要

第三方 JavaScript 应用程序是自包含的应用组件，通常都是小脚本或插件，能够为 Web 站点增加功能。它们往往是由独立的组织或个人提供的，代码和文件都是来自远程的 Web 地址。

本书由两位第三方应用程序开发领域的专家编写完成，通过丰富的示例和讲解让读者掌握第三方 Web 开发的相关技术及如何开发运行在第三方环境的 JavaScript 代码。全书共 10 章，分别介绍了第三方 JavaScript 的定义、如何加载和执行代码、DOM 渲染、第三方脚本和数据服务器之间的通信、跨窗口的消息传递方法、身份验证和 Cookie、第三方应用程序的安全性、JavaScript SDK 的发展、性能、测试和调试。

本书并非 JavaScript 语言的初级读本，适用于有一定第三方代码开发经验的开发者以及致力于研究其如何在外部环境运行的开发者们阅读。

前言

第三方 JavaScript 是从一个远程 Web 服务的地址获得服务，并在发布者页面上独立运行的客户端代码。第三方 JavaScript 用于创造高度分布式的 Web 应用程序，例如从社交微件到数据跟踪分析，到功能齐全的嵌入式应用程序。

本书介绍了第三方 JavaScript 应用程序的开发，不仅告诉读者如何开发运行在第三方环境的 JavaScript 代码，也介绍了第三方 Web 开发的相关技术，包括 HTML、CSS 和 HTTP 等。本书适用于有第三方代码开发经验的开发者（例如在自己的网站上运行），也适用于希望致力于研究这些问题如何在外部环境运行的开发者们（在其他人的网站上运行）。

本书不是 JavaScript 编程语言的初级读本，也不介绍 HTML 和 CSS 的基本原理。本书介绍的要点包括动态脚本加载、Cookies、HTTPS 以及其他中间件和高级 Web 开发技术。

线路图

本书包含如下章节。

第 1 章介绍了第三方 JavaScript 的定义。本章告诉读者什么是第三方 JavaScript，并介绍了一些现实案例。本章以一个快速的第三方应用程序示例结束，并指出了第三方 Web 开发的难点。

第 2 章指导读者如何在一个内容提供者的网站上实际加载和执行他们的代码。描述了如何设置本地开发环境来模拟第三方开发，然后进入脚本加载最佳实践，如何从一个内容提供者的网站中提取配置变量。

第 3 章重点介绍 DOM 渲染。指导读者在开发过程中，在不能控制的内容提供商的 DOM 中呈现最佳实践。本章还包括使用 CSS 样式和 iframe 元素避免冲突的策略。

第 4 章介绍在第三方脚本和数据服务器之间的通信。首先讨论了同源策略，以及由于同源策略限制带来的跨域通信的困难。其次，重点关注在两个工作区进行跨域请求：JSONP 和子域名代理。最后，介绍了跨源资源共享（Cross Origin Resource Sharing，

CORS），一个新的 HTML5 浏览器特性，使得在现代浏览器中跨域请求成为可能。

第 5 章继续介绍跨窗口的消息传递方法，包括在 iframe 直接的数据传递方法。方法包括 window.postMessage——一种 HTML5 提供的支持在多窗口之间传递消息的特性。其次，介绍了一系列不支持 window.postMessage 的浏览器。同时，介绍了 easyXDM（一个开源 JavaScript 库），该库提供了与 postMessage 类似的特性，同时支持现代浏览器和老版本浏览器。

第 6 章是关于身份验证和 Cookies。本章介绍了 Cookies 在第三方 JavaScript 中的行为，并提供了当第三方 Cookies 失效时的解决方案。同时，简要介绍了使用 Cookies 时需要注意的安全问题。

第 7 章讨论了第三方应用程序的安全性，涵盖了传统漏洞，包括基于 JavaScript 的应用程序的跨站点脚本攻击（XSS）、跨站点请求伪造（XSRF）的攻击，也包括特定于第三方应用程序的漏洞。

第 8 章介绍了 JavaScript SDK（Software Development Kit）的发展。开发 JavaScript SDK 采用了前几章介绍到的技术，并封装成公共的方法。本章还演示了如何为一个基于 HTTP 的 Web 服务提供一个客户端 JavaScript 包装器的 API。

第 9 章关于性能。涵盖的技术包括如何减少文件大小、如何减少应用程序发出的 HTTP 请求的数量。同时，也介绍了不阻塞浏览器或其他脚本的 JavaScript 代码的最佳实践。

第 10 章介绍测试和调试。本章演示了如何使用工具重写代理、如何从生产环境切换到调试应用程序代码的调试环境，并展示了如何为第三方代码编写单元测试。

编码规范和下载

所有的源代码清单使用等宽字体显示，以便与其他普通文字区分开来。代码注释中强调了许多重要的信息和概念。在某些情况下，通过项目符号标识特定的代码清单。

本书的配套源代码是在 MIT 许可下发布的。在出版社网站 www.manning.com/Third-PartyJavaScript 中提供免费下载。你也可以在 GitHub 查看源码，地址是 http://github.com/thirdpartyjs。

在线帮助

购买本书的读者可以免费访问 Manning 出版社运营的私有 Web 论坛，在该论坛中你可以发表关于本书的评论，发布技术问题，并能够获得作者以及其他读者的帮助。在该论坛上注册后，用浏览器打开 www.manning.com/Third-PartyJavaScript 页面。这个页面上有关于如何进入论坛、注册、能够获取哪些帮助以及论坛的规则等内容。

Manning 论坛为读者提供了一个有意义的场所，是读者和读者、读者和作者之间对话的桥梁。任何作者的参与、读者的讨论都是自愿的。我们建议你试着问作者一些挑战性的问题以吸引他们的兴趣!

作者在线论坛以及讨论的档案可以从书中提到的出版商网站中获取。

封面简介

本书的封面图标题是“联合指挥官”。插图来自法国 19 世纪版 *Sylvain Maréchal* 的第四卷——地区服饰习俗和军事制服。每个插图的刻画都很细致，并且手工着色。丰富多样的 Maréchal 集合生动地向我们揭示了 200 年前世界上不同城镇和地区的文化。彼此独立，人们讲不同的方言和语言。在街上或在乡下，仅仅根据一个人的穿着就能够很容易识别出他们生活的地方以及所从事的行业。

着装习俗自此改变了，当时地区的多样性着装风俗也逐渐消失了。现在很难分辨不同洲的居民，更不用说不同的城镇或地区了。或许我们已经由文化的多样性演变到了个人生活的多样性，当然还有更多样，快节奏的科技生活。

在很难区分不同计算机书籍的时代，Manning 释放创造力并倡导用两个世纪前丰富多样的地区生活作为计算机图书封面，将人们带回图片中的生活时代。

作者简介

Ben Vinegar 是 Disqus 的一名软件工程师，Disqus 是一个第三方评论平台，为超过 30 万的博客、在线出版物以及其他 Web 网站提供服务，其中包括 CNN、连线杂志、每日电讯报和 IGN。Ben 在加入 Disqus 之前，在一个非常热门的 Web 记账应用公司（FreshBooks）担任软件开发团队的主管。

Anton Kovalyov 是 Mozilla 的一名软件工程师，帮助 Firefox 浏览器编写开发者工具。他还负责 JSHint——一个开源的 JavaScript 代码质量检查工具的开发和维护。在加入 Mozilla 之前，Anton 曾经是 Disqus 的一名软件工程师，负责内嵌式评论应用的 JavaScript 开发工作。

序一

作为一个第三方 JavaScript 的开发者，你会有很多的担忧：需要跨多个站点和平台管理并部署代码。像本书中这样深入地介绍如何编写坚实的第三方 JavaScript 的细节和最佳实践以前也从未有过。这可能是一个复杂的业务，因此请允许我向你介绍关于 Douglas Crockford 的一个故事来说明潜在的意想不到的后果，Douglas Crockford 创造了一个流行很广泛的第三方脚本，以及一个名为 OnlineBootyCall 的站点。

JSON（JavaScript 对象表示法）作为 JavaScript 的子集，是由 Douglas 设计的轻量级的数据交换语言，以文字为基础，且易于阅读。早在 2005 年，他编写了 json.js——一个可以将 JSON 解析为 JavaScript 对象，反之也可以将 JavaScript 对象序列化为 JSON 的小型库。它深受喜爱并立即被大规模采用，但它添加了 Object.prototype.toJSONString 和 String.prototype.parseJSON 方法让很多人感到不解。

2007 年 10 月，Douglas 推出了 json2.js。这并非开发者现在使用的 JavaScript 版本，而是 Douglas 自己分享出来的副本。很快，它的托管公司发邮件询问有关 OnlineBootyCall.com 流量很高的异常情况。Douglas 在 json2.js 代码中包含了一段警告信息："使用你自己的副本。从一个你不可控的服务器加载代码是很不明智的。"他添加了一个会阻塞浏览器，同步的 JavaScript 模态 alert()提示。结果就使所有从 OnlineBootyCall 加载资源的页面都会弹出这则消息。

这种情况下，Douglas 作为一个第三方脚本的开发者是在保护自己。但更多是因为其他原因导致的。例如，json2.js 的出现部分原因是由于 Douglas 的 Object.prototype 扩展并不友好。

本书由两名在第三方 JavaScript 开发领域最专业的开发者编写，书中列出了当下所有的技术来帮你编写第一个初出茅庐的脚本并完成首次部署。我希望本书能够真正帮到你，并且像我一样对下一代网络感到兴奋。

PAUL IRISH
DEVELOPER RELATIONS:
GOOGLE CHROME, JQUERY
LEAD DEVELOPER:
MODERNIZR AND HTML5 BOILERPLATE

序二

2010 年 2 月，我接到 Jason Yan 的电话面试，Jason Yan 是初创公司 Disqus 的 CTO 兼共同创始人。当时，Disqus 虽然还是一家小公司，但是具有快速增长的评论应用程序，作为一个第三方脚本分发，并受到众多的博客作者和少数大型媒体公司的欢迎。Jason Yan 计划专门聘请一位从事快速增长的客户端代码库的 JavaScript 工程师。

通用 JavaScript 面试题常常涉及一系列类、主要类型、作用域等。但是，Jason Yan 采取了不同的策略。他问我以下（转述）的问题："假设我使用了内置函数 prototype，方法如 Array.prototype.indexOf 并将其指定为一个新值，你将如何获得其原值呢？"

我被吓懵了。这是我以前从未见过的一个问题，我也不知道答案。杰森跟我解释说他们无法控制 Disqus 应用程序的执行环境。在这些环境中，Disqus 应用程序依靠的内置属性有时会被覆盖或被改写得支离破碎。

我不打算放弃这个问题。所以在中面时，我打开了浏览器的 JavaScript 控制台，并开始调试函数原型。在短短几分钟，我有了惊人的发现，发现可以使用 JavaScript 的 delete 操作符删除被修改的内置属性，浏览器将恢复原始值。

事实上 Jason 不知道这个解决方案。他亲自采用该方法进行调试，果然有效。我们对于这个新发现都非常兴奋。我们开始讨论 Disqus 当前解决这一问题的方法，而面试也从严肃的"审讯"变成兴奋讨论，我们讨论了 iframes、浏览器 hacks 和其他脚本性能等。

当时我并不知道，但那是我第一次感受到第三方 JavaScript，感受到解决只有运行在别人的 Web 环境时客户端应用程序才遇到的问题，感受到一些 Web 开发人员可能永远不会意识到的技术和实践，我完全被迷住了。

随后又经过几轮面试。两个月后，我加入了 Disqus 团队，当时是在旧金山，只有 7 名员工。就是在那儿，我认识了 Anton Koval-yov，我的 JavaScript 新同事和未来的合作者。在接下来两年多的时间里，我和 Anton Koval-yov 负责维护和开发 Disqus 的客户端代码。Disqus 继续快速增长。到 2012 年，成千上万的网页安装 Disqus，每月页面浏览量超过 50 亿。其客户包括 CNN、MLB、IGN、Time.com、滚石，以及几十个其他的主

要网络和媒体公司。

安东和我在这段时间，学会了许多有用的第三方脚本编写的技巧、贴士和 hack，其中大部分我们已经吸取了教训，其中有一些我们采取保密策略，因为这是我们的技术优势。

在这本书中，凝聚了我们集体的第三方 JavaScript 知识。我们认为本书不但能帮助无处不在的第三方脚本开发者，而且也认为我们讨论的做法可能让互联网变得更美好。我们希望通过阅读本书，你会同意我们的观点。

BEN VINEGAR

致谢

我们发现写这本书是一个艰巨、有挑战性的经历，我们也意识到别无他法，只能靠自己。我们想花一点时间感谢那些曾经直接或间接帮助过我们的人。

首先，感谢 Daniel Ha、Jason Yan 和 Disqus 团队，不仅雇佣了我们，还制作和维护了一个非常棒的平台，本书中大部分的重要内容均来自于此。其次，感谢 Manning 给予我们一个讨论的机会，其中许多话题都是小环境的。没有他们，本书将不存在。特别要感谢我们的编辑 Renae Gregoire，在整个写作的过程中从头到尾提供帮助。也非常感谢 Manning 的编辑和制作团队，帮助我们调整文本、改善许多数据和图表等。

我们特别感谢我们的技术评论家 Alex Sexton，分享了他在第三方 JavaScript 方面的宝贵经历；感谢 John Ryan III 临近出版前还在审查终稿；感谢 Paul Irish 贡献的前言，并同意我们这些微不足道的业余爱好者使用他的名号。

最后，感谢在不同的阶段阅读我们的手稿的许多评论家和顾问们，慷慨地分享他们的反馈、指出错误、反复确认我们的观点，他们有：Øyvind Sean Kinsey、Kyle Simpson、Henri d'Orgeval、Mike Pennisi、Peter DeHaan、Brian Arnold、Brian Chiasson、Brian Dillard、Brian Forester、David Vedder、Jake McCrary、Jeffrey Yustman、Jonas Bandi、Justin Pope、Margriet Bruggeman、Nikander Bruggeman、Sopan Shewale。

最后，感谢在 manning.com 论坛评论的每一位读者，在 Twitter 上@我们的人，以及私下评论本书的人，对于你们提供的每一点帮助，我们都非常感谢。

BEN VINEGAR

我想把这本书献给我的父母，David 和 Wendy。从我小时候起，他们就开始培养我对计算机的兴趣，如果没有他们，我完成不了这些。特别感谢我的搭档 Esther，在这么富有挑战的项目里给我的鼓励和耐心。

ANTON KOVALYOV

我想把这本书献给我的父母（甚至是 Ben 写的那一部分），是你们在我把大部分的时间都奉献在电脑前时仍不断地支持我。感谢 Pamela Fox 鼓励我暂停我这边的项目全力致力于本书的编写中去，而不是袖手旁观。

目录

第 1 章　第三方 JavaScript 介绍

本章包括

- 第三方 JavaScript 的定义
- 几个第三方应用实例
- 实现一个简单的嵌入式微件
- 了解第三方开发的挑战

第三方 JavaScript 是一种 JavaScript 编程模式，可以用来创建高度分布式的 Web 应用程序。常规的 Web 应用需要通过一个特定的 Web 地址访问，而第三方 JavaScript 创建的应用，只需要引入一些简单的 JavaScript 脚本就可以加载到任意页面上。

你之前也许就曾遇到过第三方 JavaScript。例如广告脚本，它可以在发布者网站上生成、定向投放广告。用户也许并不喜欢广告脚本，但是它却能帮助网站发布者获得收入并维持网站的运转。成千上万的网站上都能看到广告的身影。事实上，几乎所有的广告都是从单独的广告服务器加载的第三方脚本。

开发者通过第三方 JavaScript 可以解决许多问题，广告脚本仅是其中的一个使用场景。一些开发者用它们来创建独立的产品以满足网站发布者的需要。例如，位于旧金山的一个初创公司（Disqus）所开发的第三方评论应用，为 Web 发布者提供即时评论系统。本书的作者也是该公司的员工。还有一些开发者通过开发第三方 JavaScript 来扩展传统 Web 应用，从而获得其他网站的用户。例如，Facebook 和 Twitter 开发了数十个社交微件展示在发布者的网站上。这些微件能够帮助社交网站在它们应用的正常系统之外扩展