白帽子讲 Web 安全

吴翰清 ⊙著

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

内 容 简 介

在互联网时代，数据安全与个人隐私受到了前所未有的挑战，各种新奇的攻击技术层出不穷。如何才能更好地保护我们的数据？本书将带你走进 Web 安全的世界，让你了解 Web 安全的方方面面。黑客不再变得神秘，攻击技术原来我也可以会，小网站主自己也能找到正确的安全道路。大公司是怎么做安全的，为什么要选择这样的方案呢？你能在本书中找到答案。详细的剖析，让你不仅能“知其然”，更能“知其所以然”。

本书是根据作者若干年实际工作中积累下来的丰富经验而写成的，在解决方案上具有极强的可操作性，深入分析了各种错误的解决方案与误区，对安全工作者有很好的参考价值。安全开发流程与运营的介绍，对同行业的工作具有指导意义。

图书在版编目（CIP）数据

白帽子讲 Web 安全 / 吴翰清著. —北京：电子工业出版社，2012.3
ISBN 978-7-121-16072-1

Ⅰ. ①白… Ⅱ. ①吴… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 025998 号

策划编辑：张春雨
责任编辑：葛 娜
印 刷：北京东光印刷厂
装 订：三河市皇庄路通装订厂
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：787×1092 1/16 印张：28 字数：716 千字
印 次：2012 年 3 月第 1 次印刷
印 数：4000 册 定价：69.00 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。

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。

服务热线：（010）88258888。

前言

在 2010 年年中的时候，博文视点的张春雨先生找到我，希望我可以写一本关于云计算安全的书。当时云计算的概念正如日中天，但市面上关于云计算安全应该怎么做却缺乏足够的资料。我由于工作的关系接触这方面比较多，但考虑到云计算的未来尚未清晰，以及其他的种种原因，婉拒了张春雨先生的要求，转而决定写一本关于 Web 安全的书。

我的安全之路

我对安全的兴趣起源于中学时期。当时在盗版市场买到了一本没有书号的黑客手册，其中 coolfire[1]的黑客教程令我印象深刻。此后在有限的能接触到互联网的机会里，我总会想方设法地寻找一些黑客教程，并以实践其中记载的方法为乐。

在 2000 年的时候，我进入了西安交通大学学习。在大学期间，最大的收获，是学校的计算机实验室平时会对学生开放。当时上网的资费仍然较贵，父母给我的生活费里，除了留下必要的生活所需费用之外，几乎全部投入在这里。也是在学校的计算机实验室里，让我迅速在这个领域中成长起来。

大学期间，在父母的资助下，我拥有了自己的第一台个人电脑，这加快了我成长的步伐。与此同时，我和一些互联网上志同道合的朋友，一起建立了一个技术型的安全组织，名字来源于我当时最喜爱的一部动漫：“幻影旅团”（ph4nt0m.org）。历经十余载，“幻影”由于种种原因未能得以延续，但它却曾以论坛的形式培养出了当今安全行业中非常多的顶尖人才。这也是我在这短短二十余载人生中的最大成就与自豪。

得益于互联网的开放性，以及我亲手缔造的良好技术交流氛围，我几乎见证了全部互联网安全技术的发展过程。在前 5 年，我投入了大量精力研究渗透测试技术、缓冲区溢出技术、网络攻击技术等；而在后 5 年，出于工作需要，我把主要精力放在了对 Web 安全的研究上。

加入阿里巴巴

发生这种专业方向的转变，是因为在 2005 年，我在一位挚友的推荐下，加入了阿里巴巴。加入的过程颇具传奇色彩，在面试的过程中主管要求我展示自己的能力，于是我远程关闭了阿

1 Coolfire，真名林正隆，台湾著名黑客，中国黑客文化的先驱者。

里巴巴内网上游运营商的一台路由设备，导致阿里巴巴内部网络中断。事后主管立即要求与运营商重新签订可用性协议。

大学时期的兴趣爱好，居然可以变成一份正经的职业（当时很多大学都尚未开设网络安全的课程与专业），这使得我的父母很震惊，同时也更坚定了我自己以此作为事业的想法。

在阿里巴巴我很快就崭露头角，曾经在内网中通过网络嗅探捕获到了开发总监的邮箱密码；也曾经在压力测试中一瞬间瘫痪了公司的网络；还有好几次，成功获取到了域控服务器的权限，从而可以以管理员的身份进入任何一位员工的电脑。

但这些工作成果，都远远比不上那厚厚的一摞网站安全评估报告让我更有成就感，因为我知道，网站上的每一个漏洞，都在影响着成千上万的用户。能够为百万、千万的互联网用户服务，让我倍感自豪。当时，Web 正在逐渐成为互联网的核心，Web 安全技术也正在兴起，于是我义无返顾地投入到对 Web 安全的研究中。

我于 2007 年以 23 岁之龄成为了阿里巴巴集团最年轻的技术专家。虽未有官方统计，但可能也是全集团里最年轻的高级技术专家，我于 2010 年获此殊荣。在阿里巴巴，我有幸见证了安全部门从无到有的建设过程。同时由于淘宝、支付宝草创，尚未建立自己的安全团队，因此我有幸参与了淘宝、支付宝的安全建设，为他们奠定了安全开发框架、安全开发流程的基础。

对互联网安全的思考

当时，我隐隐地感觉到了互联网公司安全，与传统的网络安全、信息安全技术的区别。就如同开发者会遇到的挑战一样，有很多问题，不放到一个海量用户的环境下，是难以暴露出来的。由于量变引起质变，所以管理 10 台服务器，和管理 1 万台服务器的方法肯定会有所区别；同样的，评估 10 名工程师的代码安全，和评估 1000 名工程师的代码安全，方法肯定也要有所不同。

互联网公司安全还有一些鲜明的特色，比如注重用户体验、注重性能、注重产品发布时间，因此传统的安全方案在这样的环境下可能完全行不通。这对安全工作提出了更高的要求和更大的挑战。

这些问题，使我感觉到，互联网公司安全可能会成为一门新的学科，或者说应该把安全技术变得更加工业化。可是我在书店中，却发现安全类目的书，要么是极为学术化的（一般人看不懂）教科书，要么就是极为娱乐化的（比如一些“黑客工具说明书”类型的书）说明书。极少数能够深入剖析安全技术原理的书，以我的经验看来，在工业化的环境中也会存在各种各样的问题。

这些问题，也就促使我萌发了一种写一本自己的书，分享多年来工作心得的想法。它将是一本阐述安全技术在企业级应用中实践的书，是一本大型互联网公司的工程师能够真正用得上的安全参考书。因此张春雨先生一提到邀请我写书的想法时，我没有做过多的思考，就答应了。

Web 是互联网的核心，是未来云计算和移动互联网的最佳载体，因此 Web 安全也是互联网公司安全业务中最重要的组成部分。我近年来的研究重心也在于此，因此将选题范围定在了 Web 安全。但其实本书的很多思路并不局限于 Web 安全，而是可以放宽到整个互联网安全的方方面面之中。

掌握了以正确的思路去看待安全问题，在解决它们时，都将无往而不利。我在 2007 年的时候，意识到了掌握这种正确思维方式的重要性，因此我告知好友：**安全工程师的核心竞争力不在于他能拥有多少个 0day，掌握多少种安全技术，而是在于他对安全理解的深度，以及由此引申的看待安全问题的角度和高度。**我是如此想的，也是如此做的。

因此在本书中，我认为最可贵的不是那一个个工业化的解决方案，而是在解决这些问题时，背后的思考过程。**我们不是要做一个能够解决问题的方案，而是要做一个能够“漂亮地”解决问题的方案。**这是每一名优秀的安全工程师所应有的追求。

安全启蒙运动

然而在当今的互联网行业中，对安全的重视程度普遍不高。有统计显示，互联网公司对安全的投入不足收入的百分之一。

在 2011 年岁末之际，中国互联网突然卷入了一场有史以来最大的安全危机。12 月 21 日，国内最大的开发者社区 CSDN 被黑客在互联网上公布了 600 万注册用户的数据。更糟糕的是，CSDN 在数据库中明文保存了用户的密码。接下来如同一场盛大的交响乐，黑客随后陆续公布了网易、人人、天涯、猫扑、多玩等多家大型网站的数据库，一时间风声鹤唳，草木皆兵。

这些数据其实在黑客的地下世界中已经辗转流传了多年，牵扯到了一条巨大的黑色产业链。这次的偶然事件使之浮出水面，公之于众，也让用户清醒地认识到中国互联网的安全现状有多么糟糕。

以往类似的事件我都会在博客上说点什么，但这次我保持了沉默。因为一来知道此种状况已经多年，网站只是在为以前的不作为而买单；二来要解决“拖库”的问题，其实是要解决整个互联网公司的安全问题，远非保证一个数据库的安全这么简单。这不是通过一段文字、一篇文章就能够讲清楚的。但我想最好的答案，可以在本书中找到。

经历这场危机之后，希望整个中国互联网，在安全问题的认识上，能够有一个新的高度。那这场危机也就物有所值，或许还能借此契机成就中国互联网的一场安全启蒙运动。

这是我的第一本书，也是我坚持自己一个人写完的书，因此可以在书中尽情地阐述自己的安全世界观，且对书中的任何错漏之处以及不成熟的观点都没有可以推卸责任的借口。

由于工作繁忙，写此书只能利用业余时间，交稿时间多次推迟，深感写书的不易。但最终能成书，则有赖于各位亲朋的支持，以及编辑的鼓励，在此深表感谢。本书中很多地方未能写

得更为深入细致，实乃精力有限所致，尚请多多包涵。

关于白帽子

在安全圈子里，素有“白帽”、“黑帽”一说。

黑帽子是指那些造成破坏的黑客，而白帽子则是研究安全，但不造成破坏的黑客。**白帽子均以建设更安全的互联网为己任**。

我于 2008 年开始在国内互联网行业中倡导白帽子的理念，并联合了一些主要互联网公司的安全工程师，建立了白帽子社区，旨在交流工作中遇到的各种问题，以及经验心得。

本书名为《白帽子讲 Web 安全》，即是站在白帽子的视角，讲述 Web 安全的方方面面。虽然也剖析攻击原理，但更重要的是如何防范这些问题。同时也希望“白帽子”这一理念，能够更加的广为人知，为中国互联网所接受。

本书结构

全书分为 4 大篇共 18 章，读者可以通过浏览目录以进一步了解各篇章的内容。在有的章节末尾，还附上了笔者曾经写过的一些博客文章，可以作为延伸阅读以及本书正文的补充。

第一篇　我的安全世界观是全书的纲领。在此篇中先回顾了安全的历史，然后阐述了笔者对安全的看法与态度，并提出了一些思考问题的方式以及做事的方法。理解了本篇，就能明白全书中所涉及的解决方案在抉择时的取舍。

第二篇　客户端脚本安全就当前比较流行的客户端脚本攻击进行了深入阐述。当网站的安全做到一定程度后，黑客可能难以再找到类似注入攻击、脚本执行等高风险的漏洞，从而可能将注意力转移到客户端脚本攻击上。

客户端脚本安全与浏览器的特性息息相关，因此对浏览器的深入理解将有助于做好客户端脚本安全的解决方案。

如果读者所要解决的问题比较严峻，比如网站的安全是从零开始，则建议跳过此篇，先阅读下一篇“服务器端应用安全”，解决优先级更高的安全问题。

第三篇　服务器端应用安全就常见的服务器端应用安全问题进行了阐述。这些问题往往能引起非常严重的后果，在网站的安全建设之初需要优先解决这些问题，避免留下任何隐患。

第四篇　互联网公司安全运营提出了一个大安全运营的思想。安全是一个持续的过程，最终仍然要由安全工程师来保证结果。

在本篇中，首先就互联网业务安全问题进行了一些讨论，这些问题对于互联网公司来说有时候会比漏洞更为重要。

在接下来的两章中，首先阐述了安全开发流程的实施过程，以及笔者积累的一些经验。然后谈到了公司安全团队的职责，以及如何建立一个健康完善的安全体系。

本书也可以当做一本安全参考书，读者在遇到问题时，可以挑选任何所需要的章节进行阅读。

致谢

感谢我的妻子，她的支持是对我最大的鼓励。本书最后的成书时日，是陪伴在她的病床边完成的，我将铭记一生。

感谢我的父母，是他们养育了我，并一直在背后默默地支持我的事业，使我最终能有机会在这里写下这些话。

感谢我的公司阿里巴巴集团，它营造了良好的技术与实践氛围，使我能够有今天的积累。同时也感谢在工作中一直给予我帮助和鼓励的同事、上司，他们包括但不限于：魏兴国、汤城、刘志生、侯欣杰、林松英、聂万全、谢雄钦、徐敏、刘坤、李泽洋、肖力、叶怡恺。

感谢季昕华先生为本书作序，他一直是所有安全工作者的楷模与学习的对象。

也感谢博文视点的张春雨先生以及他的团队，是他们的努力使本书最终能与广大读者见面。他们的专业意见给了我很多的帮助。

最后特别感谢我的同事周拓，他对本书提出了很多有建设性的意见。

联系方式：

邮箱：opensystem@gmail.com

博客：http://hi.baidu.com/aullik5

微博：http://t.qq.com/aullik5

http://weibo.com/n/aullik5

吴翰清

2012 年 1 月于杭州

序言

2012 年农历春节，我回到了浙西的老家，外面白雪皑皑。在这与网络隔离的小乡村里，在这可以夜不闭户的小乡村里，过着与网络无关、与安全无关的生活，而我终于可以有时间安安静静拜读吴翰清先生的这本大作了。

认识吴翰清先生源于网络、源于安全，并从网络走向生活，成为朋友。他对于安全技术孜孜不倦的研究，使得他年纪轻轻便成为系统、网络、Web 等多方面安全的专家；他对于安全技术的分享，创建了“幻影旅团”（ph4nt0m.org）组织，培养了一批安全方面的技术人才，并带动了整个行业的交流氛围；他和同事在大型互联网公司对安全方面的不断实践，全面保护着阿里巴巴集团的安全；他对于安全的反思和总结并发布在他的博客上，使得我们能够更为深入地理解安全的意义，处理安全问题的方法论。而今天，很幸运，我们能系统的地看到吴翰清先生多年在大型互联网公司工作实践、总结反思所积累的安全观和 Web 安全技术。

中国人自己编写的安全专著不多，而在这为数不多的书中，绝大部分也都是“黑客攻击”速成手册。这些书除了在技术上仅立足于零碎的技术点、工具使用手册、攻击过程演示，不系统之外，更为关键的是，它们不是以建设者的角度去解决安全问题。吴翰清先生是我非常佩服的“白帽子”，他和一群志同道合的朋友，一直以建设更安全的互联网为己任，系统地研究安全，积极分享知识，为中国的互联网安全添砖加瓦。而这本书也正是站在白帽子的视角，讲述 Web 安全的方方面面，它剖析攻击原理，目的是让互联网开发者、技术人员了解原理，并通过自身的实践，告诉大家分析这些问题的方法论、思想以及对应的防范方案。

最让我共鸣的是“安全运营”的思路，我相信这也是吴翰清先生这么多年在互联网公司工作的最大收获之一，因为运营是互联网公司的最大特色和法宝。安全是一个动态的过程，因为敌方攻击手段在变，攻击方法在变，漏洞不断出现；我方业务在变，软件在变，人员在变，妄图通过一个系统、一个方案解决所有的问题是不现实的，也是不可能的，安全需要不断地运营、持续地优化。

瑞雪兆丰年，一直在下的雪预示着今年的丰收。我想在经历了 2011 年中国互联网最大安全危机之后，如白雪一样纯洁的《白帽子讲 Web 安全》应该会给广大的从事互联网技术人员带来更多的帮助，保障中国互联网的安全，迎来互联网的又一个春天。

季昕华 Benjurry

目录

第一篇　世界观安全

第二篇　客户端脚本安全

第三篇 服务器端应用安全

第四篇 互联网公司安全运营

第一篇

世界观安全

- 第 1 章　我的安全世界观

第 1 章

我的安全世界观

互联网本来是安全的，自从有了研究安全的人之后，互联网就变得不安全了。

1.1 Web 安全简史

起初，研究计算机系统和网络的人，被称为“Hacker”，他们对计算机系统有着深入的理解，因此往往能够发现其中的问题。“Hacker”在中国按照音译，被称为“黑客”。在计算机安全领域，黑客是一群破坏规则、不喜欢被拘束的人，因此总想着能够找到系统的漏洞，以获得一些规则之外的权力。

对于现代计算机系统来说，在用户态的最高权限是 root（administrator），也是黑客们最渴望能够获取的系统最高权限。“root”对黑客的吸引，就像大米对老鼠的吸引，美女对色狼的吸引。

不想拿到“root”的黑客，不是好黑客。漏洞利用代码能够帮助黑客们达成这一目标。黑客们使用的漏洞利用代码，被称为“exploit”。在黑客的世界里，有的黑客，精通计算机技术，能自己挖掘漏洞，并编写 exploit；而有的黑客，则只对攻击本身感兴趣，对计算机原理和各种编程技术的了解比较粗浅，因此只懂得编译别人的代码，自己并没有动手能力，这种黑客被称为“Script Kids”，即“脚本小子”。在现实世界里，真正造成破坏的，往往并非那些挖掘并研究漏洞的“黑客”们，而是这些脚本小子。而在今天已经形成产业的计算机犯罪、网络犯罪中，造成主要破坏的，也是这些“脚本小子”。

1.1.1 中国黑客简史

中国黑客的发展分为几个阶段，到今天已经形成了一条黑色产业链。

笔者把中国黑客的发展分为了：启蒙时代、黄金时代、黑暗时代。

首先是启蒙时代，这个时期大概处在 20 世纪 90 年代，此时中国的互联网也刚刚处于起步阶段，一些热爱新兴技术的青年受到国外黑客技术的影响，开始研究安全漏洞。启蒙时代的黑客们大多是由于个人爱好而走上这条道路，好奇心与求知欲是驱使他们前进的动力，没有任何利益的瓜葛。这个时期的中国黑客们通过互联网，看到了世界，因此与西方发达国家同期诞生