第一图书网, tushu007.com

<<Web前端黑客技术揭秘>>

图书基本信息

书名：<<Web前端黑客技术揭秘>>

13位ISBN编号：9787121192036

10位ISBN编号：7121192039

出版时间：2013-1

出版时间：电子工业出版社

作者：钟晨鸣,徐少培

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

<<Web前端黑客技术揭秘>>

内容概要

Web前端的黑客攻防技术是一门非常新颖且有趣的黑客技术，主要包含Web前端安全的跨站脚本（XSS）、跨站请求伪造（CSRF）、界面操作劫持这三大类，涉及的知识点涵盖信任与信任关系、Cookie安全、Flash安全、DOM渲染、字符集、跨域、原生态攻击、高级钓鱼、蠕虫思想等，这些都是研究前端安全的人必备的知识点。
本书作者深入剖析了许多经典的攻防技巧，并给出了许多独到的安全见解。

本书适合前端工程师阅读，同时也适合对Web前端各类安全问题或黑客攻防过程充满好奇的读者阅读，书中的内容可以让读者重新认识到Web的危险，并知道该如何去保护自己以免受黑客的攻击。

第一图书网, tushu007.com

作者简介

钟晨鸣，毕业于北京化工大学，网名：余弦。
国内著名Web安全团队xeye成员，除了爱好Web ；Hacking外，还对宇宙学、人类学等保持着浓厚兴趣。
2008年加入北京知道创宇信息技术有限公司，现任研究部总监，团队致力于Web安全与海量数据研究，并进行相关超酷平台的实现。
如果大家想和我交流，可以私信我微博：weibo.com/evilcos，同时本书的最新动态也会发布在我的微博上。
徐少培，毕业于河北工业大学。
网名：xisigr。
国内著名Web安全团队xeye成员。
2008年加入北京天融信公司，现任北京天融信资深安全专家，重点负责安全研究工作，主要研究领域包括：WEB安全、HTML5安全、浏览器安全、协议分析等。
同时也是国内信息安全大会常见的演讲者。
我的微博：weibo.com/xisigr，希望可以和大家交流。

第一图书网, tushu007.com

<<Web前端黑客技术揭秘>>

书籍目录

第1章Web安全的关键点1 1.1数据与指令1 1.2浏览器的同源策略4 1.3信任与信任关系7 1.4社会工程学的作用9 1.5攻防不单一9 1.6场景很重要10 1.7小结11 第2章前端基础12 2.1W3C的世界法则12 2.2URL14 2.3HTTP协议15 2.4松散的HTML世界19 2.4.1DOM树20 2.4.2iframe内嵌出一个开放的世界21 2.4.3HTML内嵌脚本执行22 2.5跨站之魂——JavaScript23 2.5.1DOM树操作23 2.5.2AJAX风险25 2.5.3模拟用户发起浏览器请求30 2.5.4Cookie安全33 2.5.5本地存储风险43 2.5.6E4X带来的混乱世界48 2.5.7JavaScript函数劫持49 2.6一个伪装出来的世界——CSS51 2.6.1CSS容错性51 2.6.2样式伪装52 2.6.3CSS伪类52 2.6.4CSS3的属性选择符53 2.7另一个幽灵——ActionScript55 2.7.1Flash安全沙箱55 2.7.2HTML嵌入Flash的安全相关配置59 2.7.3跨站Flash61 2.7.4参数传递64 2.7.5Flash里的内嵌HTML65 2.7.6与JavaScript通信67 2.7.7网络通信71 2.7.8其他安全问题71 第3章前端黑客之XSS72 3.1XSS概述73 3.1.1“跨站脚本”重要的是脚本73 3.1.2一个小例子74 3.2XSS类型76 3.2.1反射型XSS76 3.2.2存储型XSS77 3.2.3DOMXSS78 3.3哪里可以出现XSS攻击80 3.4有何危害81 第4章前端黑客之CSRF83 4.1CSRF概述84 4.1.1跨站点的请求84 4.1.2请求是伪造的84 4.1.3一个场景84 4.2CSRF类型89 4.2.1HTMLCSRF攻击89 4.2.2JSONHiJacking攻击90 4.2.3FlashCSRF攻击94 4.3有何危害96 第5章前端黑客之界面操作劫持97 5.1界面操作劫持概述97 5.1.1点击劫持（Clickjacking）98 5.1.2拖放劫持（Drag＆Dropjacking）98 5.1.3触屏劫持（Tapjacking）99 5.2界面操作劫持技术原理分析99 5.2.1透明层+iframe99 5.2.2点击劫持技术实现100 5.2.3拖放劫持技术实现101 5.2.4触屏劫持技术实现103 5.3界面操作劫持实例106 5.3.1点击劫持实例106 5.3.2拖放劫持实例111 5.3.3触屏劫持实例119 5.4有何危害121 第6章漏洞挖掘123 6.1普通XSS漏洞自动化挖掘思路124 6.1.1URL上的玄机125 6.1.2HTML中的玄机127 6.1.3请求中的玄机134 6.1.4关于存储型XSS挖掘135 6.2神奇的DOM渲染135 6.2.1HTML与JavaScript自解码机制136 6.2.2具备HtmlEncode功能的标签140 6.2.3URL编码差异142 6.2.4DOM修正式渲染145 6.2.5一种DOMfuzzing技巧146 6.3DOMXSS挖掘150 6.3.1静态方法150 6.3.2动态方法151 6.4FlashXSS挖掘153 6.4.1XSF挖掘思路153 6.4.2GoogleFlashXSS挖掘156 6.5字符集缺陷导致的XSS159 6.5.1宽字节编码带来的安全问题160 6.5.2UTF—7问题161 6.5.3浏览器处理字符集编码BUG带来的安全问题165 6.6绕过浏览器XSSFilter165 6.6.1响应头CRLF注入绕过165 6.6.2针对同域的白名单166 6.6.3场景依赖性高的绕过167 6.7混淆的代码169 6.7.1浏览器的进制常识169 6.7.2浏览器的编码常识175 6.7.3HTML中的代码注入技巧177 6.7.4CSS中的代码注入技巧190 6.7.5JavaScript中的代码注入技巧196 6.7.6突破URL过滤201 6.7.7更多经典的混淆CheckList202 6.8其他案例分享——GmailCookieXSS204 第7章漏洞利用206 7.1渗透前的准备206 7.2偷取隐私数据208 7.2.1XSS探针：xssprobe208 7.2.2Referer惹的祸214 7.2.3浏览器记住的明文密码216 7.2.4键盘记录器219 7.2.5偷取黑客隐私的一个小技巧222 7.3内网渗透技术223 7.3.1获取内网IP223 7.3.2获取内网IP端口224 7.3.3获取内网主机存活状态225 7.3.4开启路由器的远程访问能力226 7.3.5内网脆弱的Web应用控制227 7.4基于CSRF的攻击技术228 7.4.1基于CSRF的XSS攻击229 7.5浏览器劫持技术230 7.6一些跨域操作技术232 7.6.1IEres：协议跨域232 7.6.2CSSStringInjection跨域233 7.6.3浏览器特权区域风险235 7.6.4浏览器扩展风险237 7.6.5跨子域：document.domain技巧240 7.6.6更多经典的跨域索引245 7.7XSSProxy技术246 7.7.1浏览器＜script＞请求247 7.7.2浏览器跨域AJAX请求248 7.7.3服务端WebSocket推送指令249 7.7.4postMessage方式推送指令251 7.8真实案例剖析254 7.8.1高级钓鱼攻击之百度空间登录DIV层钓鱼254 7.8.2高级钓鱼攻击之Gmail正常服务钓鱼261 7.8.3人人网跨子域盗取MSN号265 7.8.4跨站获取更高权限267 7.8.5大规模XSS攻击思想275 7.9关于XSS利用框架276 第8章HTML5安全277 8.1新标签和新属性绕过黑名单策略278 8.1.1跨站中的黑名单策略278 8.1.2新元素突破黑名单策略280 8.2HistoryAPI中的新方法282 8.2.1pushState（）和replaceState（）282 8.2.2短地址+History新方法=完美隐藏URL恶意代码283 8.2.3伪造历史记录284 8.3HTML5下的僵尸网络285 8.3.1WebWorker的使用286 8.3.2CORS向任意网站发送跨域请求287 8.3.3一个HTML5僵尸网络实例287 8.4地理定位暴露你的位置290 8.4.1隐私保护机制290 8.4.2通过XSS盗取地理位置292 第9章Web蠕虫293 9.1Web蠕虫思想294 9.2XSS蠕虫295 9.2.1原理+一个故事295 9.2.2危害性297 9.2.3SNS社区XSS蠕虫300 9.2.4简约且原生态的蠕虫304 9.2.5蠕虫需要追求原生态305 9.3CSRF蠕虫307 9.3.1关于原理和危害性307 9.3.2译言CSRF蠕虫308 9.3.3饭否CSRF蠕虫——邪恶的Flash游戏314 9.3.4CSRF蠕虫存在的可能性分析320 9.4ClickJacking蠕虫324 9.4.1ClickJacking蠕虫的由来325 9.4.2ClickJacking蠕虫技术原理分析325 9.4.3Facebook的LikeJacking蠕虫327 9.4.4GoogleReader

第一图书网, tushu007.com

的ShareJacking蠕虫327 9.4.5ClickJacking蠕虫爆发的可能性335 第10章关于防御336 10.1浏览器厂商的防御336 10.1.1HTTP响应的X—头部337 10.1.2迟到的CSP策略338 10.2Web厂商的防御341 10.2.1域分离341 10.2.2安全传输342 10.2.3安全的Cookie343 10.2.4优秀的验证码343 10.2.5谨慎第三方内容344 10.2.6XSS防御方案345 10.2.7CSRF防御方案348 10.2.8界面操作劫持防御353 10.3用户的防御357 10.4邪恶的SNS社区359

第一图书网, tushu007.com

章节摘录

版权页： 插图：

第一图书网, tushu007.com

媒体关注与评论

《Web前端黑客技术揭秘》是每名Web前端工程师都必备的安全参考书。
钟晨鸣先生与徐少培先生是我多年的好友，他们在Web安全领域有着很深的造诣。
这本书是他们多年经验的总结，深入剖析了Web前端安全的方方面面，很多独特的见解发人深省。
对于安全从业者和对互联网安全关心的读者，这本书是不容错过的上上之选。
——吴翰清《白帽子讲Web安全》作者，安全宝联合产品副总裁，前阿里巴巴集团高级安全专家通过Web前端应用对Web用户个人敏感信息进行攻击已经成为当前主流的攻击手段之一。
本书作者是国内Web前端安全研究的资深专家，本书也是国内迄今为止在这一领域内最为全面和深刻的专著。
作者用生动诙谐的语言为我们全面刨析了当前Web前端黑客的各种技术，对专业的安全工作者、浏览器开发人员、Web开发人员具有很好的参考价值，对提升广大Web用户自身的安全防范意识和知识也有很好的借鉴意义，推荐大家阅读。
——姚崎北京天融信公司副总裁《Web前端黑客技术揭秘》是每名Web前端工程师都必备的安全参考书。
钟晨鸣先生与徐少培先生是我多年的好友，他们在Web安全领域有着很深的造诣。
这本书是他们多年经验的总结，深入剖析了Web前端安全的方方面面，很多独特的见解发人深省。
对于安全从业者和对互联网安全关心的读者，这本书是不容错过的上上之选。
——吴翰清《白帽子讲Web安全》作者，安全宝联合产品副总裁，前阿里巴巴集团高级安全专家通过Web前端应用对Web用户个人敏感信息进行攻击已经成为当前主流的攻击手段之一。
本书作者是国内Web前端安全研究的资深专家，本书也是国内迄今为止在这一领域内最为全面和深刻的专著。
作者用生动诙谐的语言为我们全面刨析了当前Web前端黑客的各种技术，对专业的安全工作者、浏览器开发人员、Web开发人员具有很好的参考价值，对提升广大Web用户自身的安全防范意识和知识也有很好的借鉴意义，推荐大家阅读。
——姚崎北京天融信公司副总裁时至今日，我已经拥有过万的信息安全学员，但每逢学员让我推荐实战技术参考书时，都为推荐好书发愁，而这本书的诞生带来了攻防实战技术耀眼的光芒。
本书既讲解了先进的XSS精粹，又展示了“借刀杀人、杀人不见血”的CSRF威力，通过研读该书，渗透测试与应急响应工程师将能收获详尽的理论知识和最新实践指南；风险评估与安全审计工程师阅读后将能透彻了解到Web2.0的新威胁，他们将不得不扩展评估和审计的技术标准；IT运维安全工程师们阅读后，将会意识到新的噩梦已经到来，为避免更多网站成为攻击目标，唯一做的就是积极学习、与时俱进！
——张胜生CISSP/CISP/CISA/攻防技术资深讲师，网络犯罪重现与侦查云端平台总设计师随着Web2.0的发展，Web前端攻击已逐渐成为主流攻击方式之一，但目前业界对Web前端安全方面的研究成果并没有系统的输出。
今日有幸能优先拜读《Web前端黑客技术揭秘》一书，才发现原来已经有人在进行这方面的工作了。通读下来发现该书是两位作者对Web安全技术多年的系统研究和技术沉淀，涵盖了Web前端安全的方方面面，是一本能提升业界整体Web安全水平的得力之作。
力荐！
此外，两位作者钟晨鸣先生与徐少培先生都凭借深厚的Web安全技术功底多次帮助腾讯提升产品的安全质量，在此一并表示感谢。
——lake2腾讯安全应急响应中心经理钟晨鸣先生和徐少培先生是我多年来的挚友，很高兴终于看到这本书的面世，在我所熟悉的Web领域里，本书绝对是国内Web安全书籍中的首选，书中许多经典的case和思路，都是二位多年宝贵经验的总结，对于喜爱Web安全的同学和相关从业人员来说，细细研读该书一定能使读者对Web安全领域达到一个更深层的认识。
——罗诗尧《黑客攻防实战》系列图书作者，新浪微博应用安全技术专家、微博安全中心负责人，前百度高级工程师

第一图书网, tushu007.com

第一图书网, tushu007.com

编辑推荐

《安全技术大系:Web前端黑客技术揭秘》共10章，每章的关联性不强，大家可以根据自己的喜好跳跃性地阅读，不过我们建议从头到尾地阅读，因为每章的信息量都比较大，我们没法完全照顾初学者，很多更基础的知识点需要自己去弥补。
第1章介绍wleb安全的几个关键点。
这些关键点是我们研究前端安全的意识点，缺乏这些关键意识，就很难真正弄懂前端安全，本章的内容值得细细阅读。
第2章介绍前端基础。
实际上，其中的很多内容并非真正的基础，《安全技术大系:Web前端黑客技术揭秘》不会像传统的教材那样回顾那些语言的语法、用法等以此来理解做前端安全都需要具备哪些基本技能，我们觉得基础是关键，所以本章内容会比较多。

第一图书网, tushu007.com

名人推荐

《安全技术大系:Web前端黑客技术揭秘》是每名Web前端工程师都必备的安全参考书。
钟展鸣先生与徐少培先生是我多年的好友，他们在Web安全领域有着很深的造诣。
这本书是他们多年经验的总结，深入剖析7Web前端安全的方方面面，很多独特的见解发人深省。
对于安全从业者和关心互联网安全的读者来说，这本书是不容错过的上上之选。
——吴翰清 《自帽子讲Web安全》作者，安全宝联合产品副总裁，前阿里巴巴集团高级安全专家 通过Web前端应用对Web用户个人敏感信息进行攻击已经成为当前主流的攻击手段之一。
本书作者是国内Web前端安全研究的资深专家，本书也是该领域内容介绍较全面和详细的专著。
作者用生动诙谐的语言全面剖析了当前Web前端黑客的各种技术，对专业的安全工作者、浏览器开发人员、Web开发人员具有很好的参考价值；对提升广大Web用户自身的安全防范意识也有很好的借鉴意义，推荐大家阅读。
——姚崎 北京天融信公司副总裁 时至今日，我已经拥有过万名的信息安全学员，但每逢学员让我推荐实战技术的参考书时，都为推荐好书而发愁，而这本书的诞生带来了攻防实战技术耀眼的光芒。
本书既讲解了先进的XSS精粹，又展示了“ 借刀杀人、杀人不见血 ”的CSRF威力。
通过研读该书，渗透测试与应急响应工程师将能收获详尽的理论知识和最新的实践指南；风险评估与安全审计工程师将能透彻了解Web 2.0的新威胁，这样他们将不得不扩展评估和审计的技术标准；IT运维安全工程师将会意识到新的噩梦已经到来，为避免更多的网站成为攻击目标，他们唯一要做的就是积极学习、与时俱进！
——张胜生 CISSP／CISP／CISA／攻防技术资深讲师，网络犯罪重现与侦查云端平台总设计师 随着Web 2.0的发展，Web前端攻击已逐渐成为主流的攻击方式之一，但目前业界对Web前端安全方面的研究成果并没有系统地输出。
今日有幸能优先拜读《安全技术大系:Web前端黑客技术揭秘》一书，才发现原来已经有人在进行这方面的工作了。
通读下来，发现该书是两位作者对Web安全技术多年的系统研究和技术沉淀，该书内容涵盖了Web前端安全的方方面面，是一本能提升业界整体Web安全水平的得力之作。
在此力荐！
此外，两位作者都凭借深厚的Web安全技术功底多次帮助过腾讯提升产品的安全质量，在此对他们表示感谢。
——lake2 腾讯安全应急响应中心经理 钟展鸣先生和徐少培先生是我多年来的挚友，很高兴终于看到这本书的面世。
在我所熟悉的Web领域里，本书可以算是国内Web安全书籍中的首选，书中许多经典的案例和思路都是二位多年宝贵经验的总结。
对于喜爱Web安全的朋友和相关从业人员来说，细细研读该书后，对Web安全领域将会有一个更深的认识。
——罗诗尧 《黑客攻防实战》系列图书作者，新浪微博应用安全技术专家、微博安全中心负责人，前百度高级工程师

第一图书网, tushu007.com

<<Web前端黑客技术揭秘>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com