<<白帽子讲Web安全>>

图书基本信息

书名:<<白帽子讲Web安全>>

13位ISBN编号:9787121160721

10位ISBN编号:7121160722

出版时间:2012-3

出版时间:电子工业出版社

作者:吴翰清

页数:432

字数:716000

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

<<白帽子讲Web安全>>

内容概要

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"。

《白帽子讲web安全》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。

<<白帽子讲Web安全>>

作者简介

吴翰清,毕业于西安交通大学少年班,从2000年开始研究网络攻防技术。

在大学期间创立了在中国安全圈内极具影响力的组织"幻影"。

2005年加入阿里巴巴,负责网络安全。

工作期间,对阿里巴巴的安全开发流程、应用安全建设做出了杰出的贡献,并多次获得公司的表彰。 曾先后帮助淘宝、支付宝建立了应用安全体系,保障公司业务得以快速而安全地发展。

2009年起,加入阿里巴巴支计算有限公司,负责云计算安全、反网络欺诈等工作,是阿里巴巴集团最具价值的安全专家。

长期专注于安全技术的创新与实践,多有建树。

同时还是OWASP在中国的区域负责人之一,在互联网安全领域有着极其丰富的经验。

平时乐于分享,个人博客的访问量迄今超过200万。

多年来活跃在安全社区中,有着巨大的影响力。

多次受邀在国内、国际安全会议上演讲,是中国安全行业的领军人物之一。

<<白帽子讲Web安全>>

书籍目录

第一篇 世界观安全

- 第1章 我的安全世界观
 - 1.1 web安全简史
 - 1.1.1 中国黑客简史
 - 1.1.2 黑客技术的发展历程
 - 1.1.3 web安全的兴起
 - 1.2 黑帽子,白帽子
 - 1.3 返璞归真,揭秘安全的本质
 - 1.4 破除迷信,没有银弹
 - 1.5 安全三要素
 - 1.6 如何实施安全评估
 - 1.6.1 资产等级划分
 - 1.6.2 威胁分析
 - 1.6.3 风险分析
 - 1.6.4 设计安全方案
 - 1.7 白帽子兵法
 - 1.7.1 secure by default原则
 - 1.7.2 纵深防御原则
 - 1.7.3 数据与代码分离原则
 - .1.7.4 不可预测性原则
 - 1.8 小结
 - (附)谁来为漏洞买单?

第二篇 客户端脚本安全

第2章 浏览器安全

- 2.1 同源策略
- 2.2 浏览器沙箱
- 2.3 恶意网址拦截
- 2.4 高速发展的浏览器安全
- 2.5 小结

第3章 跨站脚本攻击(xss)

- 3.1 xss简介
- 3.2 xss攻击进阶
- 3.2.1 初探xss payload
- 3.2.2 强大的xss payload
- 3.2.3 xss 攻击平台
- 3.2.4 终极武器: xss worm
- 3.2.5 调试javascript
- 3.2.6 xss构造技巧
- 3.2.7 变废为宝: mission impossible
- 3.2.8 容易被忽视的角落:flash xss
- 3.2.9 真的高枕无忧吗: javascript开发框架
- 3.3 xss的防御
- 3.3.1 四两拨千斤: httponly
- 3.3.2 输入检查

<<白帽子讲Web安全>>

- 3.3.3 输出检查
- 3.3.4 正确地防御xss
- 3.3.5 处理富文本
- 3.3.6 防御dom based xss
- 3.3.7 换个角度看xss的风险
- 3.4 小结

第4章 跨站点请求伪造(csrf)

- 4.1 csrf简介
- 4.2 csrf进阶
- 4.2.1 浏览器的cookie策略
- 4.2.2 p3p头的副作用
- 4.2.3 get? post?
- 4.2.4 flash csrf
- 4.2.5 csrf worm
- 4.3 csrf的防御
- 4.3.1 验证码
- 4.3.2 referer check
- 4.3.3 anti csrf token
- 4.4 小结

第5章 点击劫持 (clickjacking)

- 5.1 什么是点击劫持
- 5.2 flash点击劫持
- 5.3 图片覆盖攻击
- 5.4 拖拽劫持与数据窃取
- 5.5 clickjacking 3.0:触屏劫持
- 5.6 防御clickjacking
- 5.6.1 frame busting
- 5.6.2 x-frame-options
- 5.7 小结

第6章 html 5 安全

- 6.1 html 5新标签
- 6.1.1 新标签的xss
- 6.1.2 iframe的sandbox
- 6.1.3 link types: noreferrer
- 6.1.4 canvas的妙用
- 6.2 其他安全问题
- 6.2.1 cross-origin resource sharing
- 6.2.2 postmessage——跨窗口传递消息
- 6.2.3 web storage
- 6.3 小结

第三篇 服务器端应用安全

第7章 注入攻击

- 7.1 sql注入
- 7.1.1 盲注 (blind injection)
- 7.1.2 timing attack
- 7.2 数据库攻击技巧
- 7.2.1 常见的攻击技巧

<<白帽子讲Web安全>>

- 7.2.2 命令执行
- 7.2.3 攻击存储过程
- 7.2.4 编码问题
- 7.2.5 sql column truncation
- 7.3 正确地防御sql注入
- 7.3.1 使用预编译语句
- 7.3.2 使用存储过程
- 7.3.3 检查数据类型
- 7.3.4 使用安全函数
- 7.4 其他注入攻击
- 7.4.1 xml注入
- 7.4.2 代码注入
- 7.4.3 crlf注入
- 7.5 小结

第8章 文件上传漏洞

- 8.1 文件上传漏洞概述
- 8.1.1 从fckeditor文件上传漏洞谈起
- 8.1.2 绕过文件上传检查功能
- 8.2 功能还是漏洞
- 8.2.1 apache文件解析问题
- 8.2.2 iis文件解析问题
- 8.2.3 php cqi路径解析问题
- 8.2.4 利用上传文件钓鱼
- 8.3 设计安全的文件上传功能
- 8.4 小结

第9章 认证与会话管理

- 9.1 who am i?
- 9.2 密码的那些事儿
- 9.3 多因素认证
- 9.4 session与认证
- 9.5 session fixation攻击
- 9.6 session保持攻击
- 9.7 单点登录 (sso)
- 9.8 小结

第10章 访问控制

- 10.1 what can i do?
- 10.2 垂直权限管理
- 10.3 水平权限管理
- 10.4 oauth简介
- 10.5 小结

第11章 加密算法与随机数

- 11.1 概述
- 11.2 stream cipher attack
- 11.2.1 reused key attack
- 11.2.2 bit-flipping attack
- 11.2.3 弱随机iv问题
- 11.3 wep破解

<<白帽子讲Web安全>>

- 11.4 ecb模式的缺陷
- 11.5 padding oracle attack
- 11.6 密钥管理
- 11.7 伪随机数问题
- 11.7.1 弱伪随机数的麻烦
- 11.7.2 时间真的随机吗
- 11.7.3 破解伪随机数算法的种子
- 11.7.4 使用安全的随机数
- 11.8 小结
- (附) understanding md5 length extension attack

第12章 web框架安全

- 12.1 mvc框架安全
- 12.2 模板引擎与xss防御
- 12.3 web框架与csrf防御
- 12.4 http headers管理
- 12.5 数据持久层与sql注入
- 12.6 还能想到什么
- 12.7 web框架自身安全
- 12.7.1 struts 2命令执行漏洞
- 12.7.2 struts 2的问题补丁
- 12.7.3 spring mvc命令执行漏洞
- 12.7.4 django命令执行漏洞
- 12.8 小结

第13章 应用层拒绝服务攻击

- 13.1 ddos简介
- 13.2 应用层ddos
- 13.2.1 cc攻击
- 13.2.2 限制请求频率
- 13.2.3 道高一尺,魔高一丈
- 13.3 验证码的那些事儿
- 13.4 防御应用层ddos
- 13.5 资源耗尽攻击
- 13.5.1 slowloris攻击
- 13.5.2 http post dos
- 13.5.3 server limit dos
- 13.6 一个正则引发的血案: redos
- 13.7 小结

第14章 php安全

- 14.1 文件包含漏洞
- 14.1.1 本地文件包含
- 14.1.2 远程文件包含
- 14.1.3 本地文件包含的利用技巧
- 14.2 变量覆盖漏洞
- 14.2.1 全局变量覆盖
- 14.2.2 extract()变量覆盖
- 14.2.3 遍历初始化变量
- 14.2.4 import_request_variables变量覆盖

<<白帽子讲Web安全>>

14.2.5 parse st	r()变量覆盖
-----------------	---------

- 14.3 代码执行漏洞
- 14.3.1 "危险函数"执行代码
- 14.3.2 "文件写入"执行代码
- 14.3.3 其他执行代码方式
- 14.4 定制安全的php环境
- 14.5 小结

第15章 web server配置安全

- 15.1 apache安全
- 15.2 nginx安全
- 15.3 jboss远程命令执行
- 15.4 tomcat远程命令执行
- 15.5 http parameter pollution
- 15.6 小结

第四篇 互联网公司安全运营

第16章 互联网业务安全

- 16.1 产品需要什么样的安全
- 16.1.1 互联网产品对安全的需求
- 16.1.2 什么是好的安全方案
- 16.2 业务逻辑安全
- 16.2.1 永远改不掉的密码
- 16.2.2 谁是大赢家
- 16.2.3 瞒天过海
- 16.2.4 关于密码取回流程
- 16.3 账户是如何被盗的
- 16.3.1 账户被盗的途径
- 16.3.2 分析账户被盗的原因
- 16.4 互联网的垃圾
- 16.4.1 垃圾的危害
- 16.4.2 垃圾处理
- 16.5 关于网络钓鱼
- 16.5.1 钓鱼网站简介
- 16.5.2 邮件钓鱼
- 16.5.3 钓鱼网站的防控
- 16.5.4 网购流程钓鱼
- 16.6 用户隐私保护
- 16.6.1 互联网的用户隐私挑战
- 16.6.2 如何保护用户隐私
- 16.6.3 do-not-track
- 16.7 小结
- (附)麻烦的终结者

第17章 安全开发流程(sdl)

- 17.1 sdl简介
- 17.2 敏捷sdl
- 17.3 sdl实战经验
- 17.4 需求分析与设计阶段
- 17.5 开发阶段

<<白帽子讲Web安全>>

- 17.5.1 提供安全的函数
- 17.5.2 代码安全审计工具
- 17.6 测试阶段
- 17.7 小结
- 第18章 安全运营
 - 18.1 把安全运营起来
 - 18.2 漏洞修补流程
 - 18.3 安全监控
 - 18.4 入侵检测
 - 18.5 紧急响应流程
 - 18.6 小结
 - (附)谈迈联网企业安全的发展方向

<<白帽子讲Web安全>>

章节摘录

版权页: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. IWeb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"sctiPtKids",即"脚本小子"。

<<白帽子讲Web安全>>

编辑推荐

《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。 《白帽子讲Web安全》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《白帽子讲Web安全》正文的补充。

<<白帽子讲Web安全>>

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