《Web应用安全威胁与防治》

图书基本信息

书名：《Web应用安全威胁与防治》

13位ISBN编号：9787121188572

10位ISBN编号：7121188570

出版时间：2013-1

出版社：电子工业出版社

作者：王文君,李建蒙

页数：466

《Web应用安全威胁与防治》

前言

序1　　随着社交网络、微博等一系列新型的互联网产品的诞生，尤其是Web 2.0技术的推广，基于Web环境的面向普通终端用户的互联网应用越来越广泛。在企业界，随着企业信息化的不断深入，各种服务于企业的应用都架设在Web平台上。Web业务的迅速发展把越来越多的个人和企业的敏感数据通过Web展现给用户。这引起黑客们的强烈关注，他们跃跃欲试，利用网站操作系统的漏洞和Web服务程序的SQL注入等漏洞得到Web服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据。更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。这些也使得越来越多的用户关注应用层的安全问题，业界对Web应用安全的关注度也逐渐升温。　　目前很多业务都依赖于互联网，如网上银行、网络购物、网游等，很多恶意攻击者会对Web服务器进行攻击，想方设法通过各种手段获取他人的个人账户信息以谋取利益。正是因为这样，Web业务平台非常容易遭受攻击。为了防止黑客的攻击，除了对Web服务器做相应的配置外，Web应用程序的设计和开发也需要杜绝黑客攻击的隐患。本书有针对性地面向广大Web应用程序员提供了系统的安全设计原则和编程技巧。　　作为应用程序员，你可能非常熟悉你所负责的业务逻辑，你也一定精通几种编程语言和数据库。但是，就我所接触的程序员来说，很少有懂得怎样在编程中避免留下安全漏洞的。对于产品架构师，很多产品在其设计之时没有考虑系统的安全问题，没有相应的安全标准。请仔细阅读本书，本书为你的Web产品提供了一个可行的安全标准，同时也为你提供了系统的针对各种安全漏洞的行之有效的编程技巧。

作者之一的王文君是我领导的惠普软件PPM产品研发团队的安全架构师。他将OWASP Top 10应用于PPM，使之成为该企业级产品的安全标准。事实证明，OWASP Top 10及相应的ESAPI有效地满足了用户对该产品安全方面的苛刻要求。不久前，我们的产品通过了我们的客户之一某国国防部的安全攻击测试。所以，我极力将本书推荐给你。你将会有针对性地在你的程序里满足安全性要求，对于潜在的安全隐患，你将有足够的智慧和手段去解决它。　　李维纲　　惠普软件部研发团队经理

《Web应用安全威胁与防治》

内容概要

容提要
本书是一本讲解Web应用中最常见的安全风险以及解决方案的实用教材。它以当今公认的安全权威机构OWASP（Open Web Application Security Project）制定的OWASP Top 10为蓝本，介绍了十项最严重的Web应用程序安全风险，并利用ESAPI（Enterprise Security API）提出了解决方案。本书共有五篇，第1篇通过几个故事引领读者进入安全的世界；第2篇是基础知识篇，读者可以了解基本的Web应用安全的技术和知识；第3篇介绍了常用的安全测试和扫描工具；第4篇介绍了各种威胁以及测试和解决方案；第5篇在前几篇的基础上，总结在设计和编码过程中的安全原则。
本书各章以一个生动的小故事或者实例开头，让读者快速了解其中的安全问题，然后分析其产生的原因和测试方法并提出有效的解决方案，最后列出处理相关问题的检查列表，帮助读者在以后的工作和学习中更好地理解和处理类似的问题。读完本书之后，相信读者可以将学过的内容应用到Web应用安全设计、开发、测试中，提高Web应用程序的安全，也可以很有信心地向客户熟练地讲解Web应用安全威胁和攻防，并在自己的事业发展中有更多的收获。
本书适用于Web开发人员、设计人员、测试人员、架构师、项目经理、安全咨询顾问等。本书也可以作为对Web应用安全有兴趣的高校学生的教材，是一本实用的讲解Web应用安全的教材和使用手册。

《Web应用安全威胁与防治》

作者简介

王文君，2007年加入惠普软件从事软件开发、软件安全分析以及手机开发等工作。现为OWASP中国上海地区负责人之一，并于2011年被OWASP邀请参加OWASP亚洲峰会，作为演讲嘉宾和培训讲师，拥有CISSP、PMP、ITIL认证，2012年被评为HP Global Software Star。王文君于2002年毕业于上海交通大学，拥有电力工程硕士学位以及电力工程和涉外会计双学士学位。 李建蒙，2004年从日本回国之后。加入华为技术有限公司。开发移动通信平台。2006年加入思科，从事在线应用产品的后台开发和应用安全领域的工作，有丰富的多平台多语言开发、渗透测试和安全开发经验。曾于2011年被OWASP邀请作为OWASP亚洲峰会的演讲嘉宾和培训讲师。

《Web应用安全威胁与防治》

书籍目录

《Web应用安全威胁与防治》

章节摘录

版权页： 插图： 第一种，明文存储。这种方法是最不安全的一种，系统的管理员可以直接看到所有用户的密码明文，而且，一旦有SQL注入攻击，攻击者也可以直接拿到明文。前面说的CSDN遭受攻击之后，密码泄露，主要是有些用户的密码是明文存储的。第二种，密码经过对称转换后存储。这种方法是编写一个对称的转换算法，密码经过转换后，看起来和原来的密码完全不一样，但是，这种存储方法和第一种直接存储明文在本质上是相似的，只要知道转换方法，也就能知道如何将密文转换为明文。即使不知道转换方法，通过尝试和猜测，也可以逐步找到转换的规律，进而可以根据密文推导出明文，达到破解的目的。第三种，对称加密之后存储。对于对称加密存储，用户加密和解密来说，则需要加密的密钥，那么，对于密钥的保护，就和对密码的保护一样重要，一旦密钥泄露，则所有的密码也就都处于危险的境地。而且，密钥可能事先配置好或者直接写在代码里了，这样一旦负责维护的员工因为对公司不满而离开，很有可能导致密钥泄露，导致破解的可能性很大，Skype就曾经被揭露密钥写在代码里，导致产品的安全性大大降低。而且，系统管理员或者系统的维护人员很有可能获得这些密钥，也就能很容易地把密码的原文算出来。所以，对称加密之后存储密码，需要加强对密钥的管理，而且一旦密钥泄露，切换密钥也可能导致兼容问题。第四种，非对称加密后存储。虽然使用对称加密算法，但是由于密码经过公钥加密，需要私钥才能解密，那么，私钥的安全性就变得和密码的安全性一样重要，只有保证私钥的安全，才能够保证密码的安全。但是，使用非对称加密算法仍然需要管理密钥，而且非对称加密算法的效率也很低。以上四种方法，都有一个共同的特点，就是密码都可以从加密的存储形式还原到明文。像前面所说的，如果需要通过注册的邮箱找回原来的密码，那么肯定要用到以上四种方法中的一种。但是需要铭记的是：既然通过注册的邮箱可以找回密码，那么，网站的工作人员或者管理员也就有办法通过查看配置的密钥，然后解密得到明文。这对于一些对安全性要求很高的政府或者企业是不允许的。以上介绍的几种密码的存储方法的共同弱点就是密码是可逆的，系统有可能还原得到明文，所以，最好的保存密码的方法是以连系统都不可能还原明文的方式保存，也就是用哈希算法的单向性保证服务器端保存的是哈希之后的哈希值，从而系统就不可能知道密码的明文。使用哈希算法也有几种方式，如下所示。第一种，使用MD5和SHA－1哈希之后存储。MD5和SHA－1已经被破解，这意味着虽然不能通过逆运算还原密码原文，但很容易找到一个能生成相同哈希值的密码原文的碰撞，例如，密码是12345678，通过计算，可以得到abcdefgh的哈希值和12345678的哈希值一样，那么，输入密码时，输入12345678和abcdefgh都可以登录。还有一点，这两个算法相对速度比较快，这就意味着对暴力破解来说消耗的资源少，所消耗的时间也短。所以强烈建议不要使用这两个算法。第二种，使用更安全的SHA256算法。这在一定程度上降低或者杜绝了碰撞率，也增加了暴力破解的成本。但是，一般的密码输入的长度都是8个字符左右，有的用户为了容易记忆使用更短的密码，这样通过常用密码字典，就可以很快得到密码原文。所以，单纯地只是用SHA256这样的比较安全的哈希算法还是有一定风险的。第三种，使用加入盐（Salt）的SHA256算法。将密码原文和随机生成的盐字符串混淆，进行哈希，存储哈希之后的值以及盐。在密码验证的时候，只需要用同样的算法，把密码原文和盐再做一次同样的哈希，与存储的哈希值比较就可以验证密码了。建议使用的盐最少是8个字节，而且是随机的字符串，这样密码和盐的组合值就成为了一个不同寻常的字符串，密码字典很难构造这么巨大的字典，就可以增加密码字典破解的成本，甚至使之不可能。盐的长度越长，暴力破解的难度就越大，也限制了彩虹表的效力。随着机器硬件的更新以及性能的不断提高，暴力破解的速度也得到提高，为了应对日益提高的硬件速度，可以通过将具体的哈希进行若干次迭代，如SHA256（…SHA256（salt，SHA256（salt，password），这样，就可以增加暴力破解的难度。即使被暴力破解了，得到的也只是随机的盐和密码混淆之后的值，如果需要恢复密码原文，仍然需要进一步努力得到哪些是盐，然后才能得到密码，虽然这对一些资深的攻击者并不难，但这总是要花他们一些时间的。

《Web应用安全威胁与防治》

媒体关注与评论

这是一本带点酷酷的工程师范儿和人文气质的“ 硬货 ”。作为一名资深IT文艺老人，特别喜欢这种带着思想气息却又有着丰富案例娓娓道来的实用信息安全书，过去却往往只在国外作者中读到。正如书中开头的引子说的那样：“ 家有IT，如有一宝 ”。那么在Web安全日益火爆的今天，你会不会在读完这本书后的未来也成为传说中让我们顶礼膜拜的大牛呢^-^ ——IDF威慑防御实验室益云（公益互联网）社会创新中心联合创始人万涛@黑客老鹰 伴随互联网的高速发展，基于B/S架构的业务系统对安全要求越来越高，安全从业人员面临空前的压力。如何让安全从业人员快速掌握Web应用安全？本书以诙谐、幽默的语言，精彩、丰富的实例，帮助安全从业人员从端到端理解Web应用安全。不失为近几年Web应用安全书籍的上佳之作。 ——OWASP中国区主席SecZone高级安全顾问 RIP 很乐意看到有人将自身的资深安全积累和OWASP的最佳实践出版成书，内容严谨细致却不乏生动。这本信息安全领域的实用手册将成为银基安全致力于互联网安全的参考指导书目之一，我们广泛的电信、银行、保险、证券和政府部门等客户都会从中受益。 ——上海银基信息安全技术有限公司首席技术官胡绍勇（Kurau） 随着安全访问控制策略ACL的普及应用，互联网企业目前面临的安全风险面主要集中在Web服务层。其中Web应用系统在架构设计、开发编码过程中是安全漏洞和风险引入的主要阶段，而普遍地我们的架构、开发、测试岗位在安全技能与意识上恰恰是相对比较欠缺的。本书详细介绍了Web安全基础知识、测试平台与方法，常见漏洞形式与原理，并结合OWASP最佳实践经验给出预防建议、设计和编码原则等。书中举例生动形象，图文代码并茂，步骤归纳清晰。特别推荐给广大Web开发、测试、安全岗位的朋友们。 ——中国金山软件集团信息安全负责人程冲 在网络攻击愈加复杂，手段日益翻新的今天，Web攻击依然是大多数攻击者首选的入侵手段。反思CSDN泄密及新浪微博蠕虫事件，Web应用的安全突显其重要性。OWASP作为全球领先的Web应用安全研究团队，透过本书将Web应用安全的威胁、防御以及相关的工具进行了详细的探讨和研究。详尽的操作步骤说明是本书的亮点之一，这些详实且图文并茂的内容为逐步深入学习Web应用安全提供了很好的帮助。我衷心希望这本书能够成为信息安全专业的在校生以及应用安全相关从业人员的学习指导书。 —— 上海交通大学信息安全工程学院施勇（CISSP CISA）

《Web应用安全威胁与防治》

编辑推荐

《Web应用安全威胁与防治》

名人推荐

这是一本带点酷酷的工程师范儿和人文气质的“硬货”。作为一名资深IT文艺老人，特别喜欢这种带着思想气息却又有着丰富案例娓娓道来的实用信息安全书，过去却往往只在国外作者中读到。正如书中开头的引子说的那样：“家有IT，如有一宝”。那么在Web安全日益火爆的今天，你会不会在读完这本书后的未来也成为传说中让我们顶礼膜拜的大牛呢。 ——IDF威慑防御实验室益云（公益互联网）社会创新中心联合创始人 万涛@黑客老鹰 伴随互联网的高速发展，基于B／S架构的业务系统对安全要求越来越高，安全从业人员面临空前的压力。如何让安全从业人员快速掌握Web应用安全？本书以诙谐、幽默的语言，精彩、丰富的实例，帮助安全从业人员从端到端理解Web应用安全。不失为近几年Web应用安全书籍的上佳之作。 ——OWASP中国区主席SecZone高级安全顾问 RIP 很乐意看到有人将自身的资深安全积累和OWASP的最佳实践出版成书，内容严谨细致却不乏生动。这本信息安全领域的实用手册将成为银基安全致力于互联网安全的参考指导书目之一，我们广泛的电信、银行、保险、证券和政府部门等客户都会从中受益。 ——上海银基信息安全技术有限公司首席技术官 胡绍勇（Kurau） 随着安全访问控制策略ACL的普及应用，互联网企业目前面临的安全风险面主要集中在Web服务层。其中Web应用系统在架构设计、开发编码过程中是安全漏洞和风险引入的主要阶段，而普遍地我们的架构、开发、测试岗位在安全技能与意识上恰恰是相对比较欠缺的。本书详细介绍了Web安全基础知识、测试平台与方法，常见漏洞形式与原理，并结合OWASP最佳实践经验给出预防建议、设计和编码原则等。书中举例生动形象，图文代码并茂，步骤归纳清晰。特别推荐给广大Web开发、测试、安全岗位的朋友们。 ——中国金山软件集团信息安全负责人 程冲 在网络攻击愈加复杂，手段日益翻新的今天，Web攻击依然是大多数攻击者首选的入侵手段。反思CSDN泄密及新浪微博蠕虫事件，Web应用的安全突显其重要性。OWASP作为全球领先的Web应用安全研究团队，透过本书将Web应用安全的威胁、防御以及相关的工具进行了详细的探讨和研究。详尽的操作步骤说明是本书的亮点之一，这些详实且图文并茂的内容为逐步深入学习Web应用安全提供了很好的帮助。我衷心希望这本书能够成为信息安全专业的在校生以及应用安全相关从业人员的学习指导书。 ——上海交通大学信息安全工程学院 施勇（CISSP CISA）

《Web应用安全威胁与防治》

精彩短评

1、做毕设时候看的书 理论帮助比较大 涵盖的东西也比较全面
2、不错，正在看。总体不敢说好坏
3、很好，一直想买，终于到手了！
4、中国话的OWASP
5、关于TOP 10 介绍的很详细！值得一看！
6、这本书写的尚可，入门后不久的朋友可以买来看看。本书更类似于学习笔记倾向的读物，因为写的略微有点散，且不深入，。买这本书的时候最希望看到的是作者以淘宝安全专家的身份写一些目前常见的攻击手法在时间中出现的比率以及危害等、淘宝、csdn这些商业网站常遇到的攻击问题等等，还有一个是目前中小网站在经济能力有限的情况下如何做好安全工作等。结果都没有，虽然本书有深度但是不深入，有宽度但是不够宽。中规中矩的一本书，对照着做做试验，热身下看看也就还好。给四星，建议在书店看下再考虑购买。还有就是OWASP是个好站点，里面有针对语言方面编程需要注意的事项，都是与网站安全有关的。最重要的是该站点其中将Python语言单独列出作为一项，这对于Python编程人员来说是个福音。其他语言或者演示的也可以看看，与语言自身有关的安全问题只是一小部分，大多数是来自于语言之外的软硬件环境有关的安全注意事项。
7、以前在学校图书馆就看这个，现在收藏一本
8、书里面的ESAPI方法貌似有错误，我使用的是2.0版本。建议小心使用。
9、没怎么看 品质不错
10、挺好的书，赶紧买，超值！
11、作为入门级书不错，这个你懂得
12、很好哦，晒晒
13、专业图书，很有用，正品！
14、与《白帽子》搭配看，实践加理论，实在！
15、虽然 黑客攻防技术宝典:Web实战篇 讲得更加全面，但入门知识及注入原理没有这本书细致，入门非常好的选择。
16、确实不错~~~，还没全部看完
17、尚可，至少owasp的介绍帮我扛过了面试-v-
18、基于OWASP Top 10与ESAPI
19、覆盖面很全
20、好书，不用多说了，实用。

《Web应用安全威胁与防治》

版权说明