<<PHP应用程序安全编程>>

图书基本信息

书名：<<PHP应用程序安全编程>>

13位ISBN编号：9787111291817

10位ISBN编号：7111291816

出版时间：2010-1

出版时间：机械工业

作者：(美)巴雷德|译者:姜燕梅//罗云峰//武欣

页数：208

<<PHP应用程序安全编程>>

前言

PHP是一个非常适用于快速开发动态Web站点的编程语言。
它的很多特性对编程初学者来说非常友好，例如它不要求变量声明。
然而这些特性可能会导致用PHP开发的Web应用程序存在一些安全漏洞。
一旦你理解PHP应用程序漏洞的基本概念和类型，你就可以用PHP编写出与其他语言一样安全的代码。

对任何有志于编写更安全Web应用程序的PHP开发人员来说，本书都是非常不错的选择。
它涵盖了大量开发人员都应该熟悉的安全话题。
此外，本书还介绍一些测试PHP Web应用程序的方法和工具。

本书涵盖内容丰富，包括：

· Web应用程序安全的基础知识。
· 从开始阶段设计安全的应用程序——去除已有应用程序的安全漏洞。
· 缓冲区溢出、文件系统访问、身份验证、加密等。
· 防御PHP自身无法防御的会话劫持、固化以及毒化攻击。
· 提高运行PHP代码的服务器的安全性，包括针对Apache、MySQL、IIS／SQL服务器的具体指导。
· 实施严格的身份验证以及加密应用程序。
· 预防危险的跨站点脚本攻击。
· 系统化测试应用程序的安全性，包括探索式测试和PHP自动化测试。
· 解决第三方应用程序的已有漏洞。
· Web应用程序的自动化测试工具和框架。

综观全书，内容广泛，风格严谨，理论和实践紧密结合，既有详细的概念说明，又有复杂且完整的示例代码，还有浅显易懂的图表等。
读者能够轻松地将自己所需的理论知识付诸实践。
正是这个原因，本书适用的对象非常广泛。
对初学者来说，本书可以作为Web开发方面的安全教材和参考用书。
对经验丰富的PHP开发人员来说，本书也是很好的参考手册。
此外，本书还给出了关于自动化和手动测试Web应用程序的详细介绍。
因此，本书适用于PHP程序员和测试人员。

参加本书翻译工作的有：姜燕梅、罗云峰、武欣、余勇、贾顺林、于苗苗、王国勤、王萃、张春梅。
由武欣统一审校。

由于译者的水平有限，书中不妥和错误之处在所难免，敬请广大读者批评指正。

<<PHP应用程序安全编程>>

内容概要

本书通过实际情景、示例代码深入浅出地介绍了经常困挠PHP Web应用程序开发人员的常见安全问题。
主要内容包括：去除应用程序安全漏洞，防御PHP攻击，提高运行PHP代码的服务器安全，实施严格的身份验证以及加密应用程序，预防跨站点脚本攻击，系统化测试应用程序安全性，解决第三方应用程序已有漏洞等。
本书内容丰富，理论和实践紧密结合。
通过详细概念说明和完整实例代码，读者可以轻松将自己所学的理论知识付诸实践。
本书适用于各个阶段的Web应用程序开发人员。
本书将帮助你掌握编写可靠的PHP代码和提高你正在使用的PHP软件安全所需的技术、技巧以及最佳实践。
作者揭示经常困挠PHP程序开发人员的常见代码安全问题，同时给出实用且专业的解决方案——不管你拥有多少PHP编程经验，这些技术都非常容易理解和使用。
本书具体包括　　·从起步阶段设计安全的应用程序——去除已有应用程序安全漏洞。
·防御PHP自身无法防御的会话劫持、固化以及毒化攻击。
·提高运行PHP代码的服务器的安全性，包括针对Apache、MySQL、IIS/SQL服务器的具体指导。
·实施严格的身份验证以及加密应用。
·预防危险的跨站点脚本攻击。
·系统化测试应用程序的安全性，包括探索式测试和PHP自动化测试。
·解决第三方应用程序的已有漏洞。

作者简介

Tricia Ballad 在成为专职技术写作人员之前，她花费了几年时间从事LAMP（Linux、Apache、MySQL和PHP/Perl）平台上的Web应用程序开发工作。
目前她专门编写不同技术的在线课件。

<<PHP应用程序安全编程>>

书籍目录

章节摘录

1.2.2 编程人员可以提高应用程序的安全性　　作为世界信息技术最常见的话题，安全一直被认为是困难、复杂的，并且最好留给拥有大量证书的专家、计算机科学领域的博士以及具有20年行业经验的专家。
一旦理解安全的基础知识，你将发现最重要的安全概念其实并不像看上去那么困难。
有时候需要安全专家的帮助，但是你不一定要成为安全专家才能提高应用程序的安全。
本书提取了一些关于提高应用程序安全性的精华信息，它们可以帮助理解应用程序基础安全概念。
在开始了解特定安全技术之前，我们需要了解为什么需要理解安全。
只要你将应用程序发布给公众——尤其你的应用程序运行在唯一的服务器——你将成为黑客的靶子。
即使一个非常简单的应用程序都可能成为黑客的兴趣点。
其实，黑客并不需要非常聪明或受过高等教育，他们可以是普通的编程人员。
他们拥有大量的时间，希望测试自己能否应对系统管理员和应用程序编程人员。
只要你的代码在公共服务器运行，你就应该假设黑客可能会找到它并且尝试攻击它。
根据你的服务器吸引人的程度以及安全漏洞明显程度的不同，这可能需要几年的时间，也可能你几天后就能看到第一个攻击。
这是否意味着你应该放弃防御黑客？
当然不是。
安全漏洞不是不可避免的。
安全漏洞之所以常见，是因为大多数程序员都不理解提高应用程序安全的基本方法。
一旦阅读了本书，你就可以使用所有的工具来改善应用程序的安全性。
黑客将其精力集中在最容易攻击的目标，但是你可以采取一些步骤使得黑客放弃你的应用程序。
不用担心，本书介绍的所有技术都非常简单，但是却可以让应用程序的安全性有质的变化。
1.3 安全困惑　　有些程序员随机创建复杂的目录结构和文件，使用一些毫无意义的名称用来迷惑黑客。
遗憾的是，由于黑客攻击的方法，困惑的文件名称以及将其保存在复杂的目录结构并不能真正解决问题。
这种策略将使得你的代码难于维护、更新。
大多数黑客都不会通过查看你的应用程序代码来找到漏洞。
他们一般都比较懒惰（这是好事）。
与花费大量时间和精力直接查找应用程序漏洞不同，他们编写脚本来挖掘应用程序代码漏洞。
在花费足够的时间后，这些脚本最终将会找到有效的方法遍历最复杂的目录结构。
如图l-2所示。

<<PHP应用程序安全编程>>

版权说明