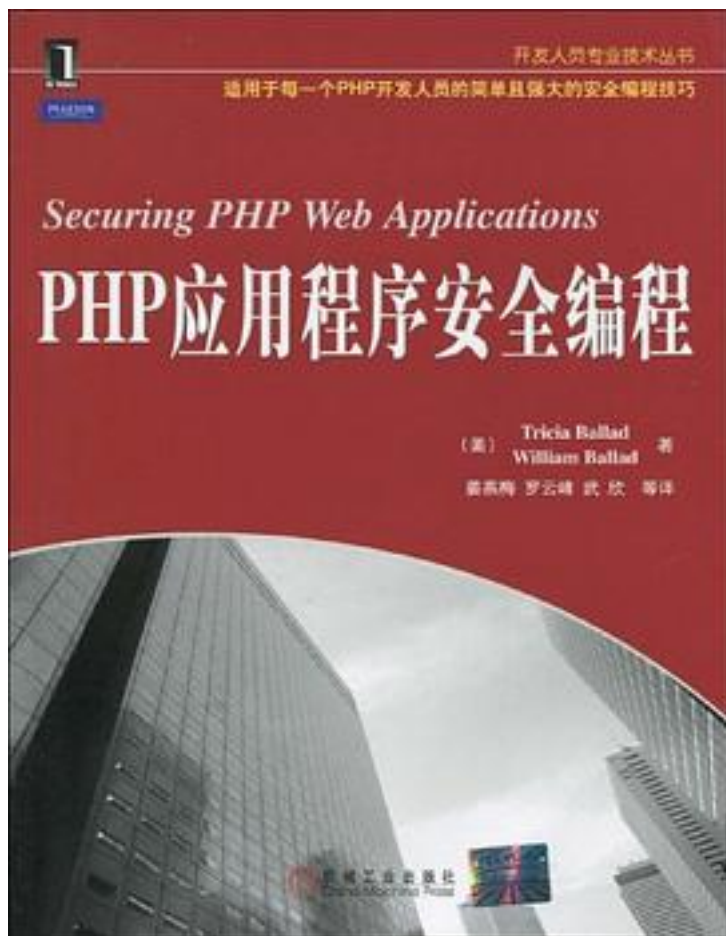


# PHP应用程序安全编程



[PHP应用程序安全编程\\_下载链接1\\_](#)

著者:[美] Tricia Ballard

出版者:机械工业出版社

出版时间:2010-1

装帧:

isbn:9787111291817

《PHP应用程序安全编程》通过实际情景、示例代码深入浅出地介绍了经常困扰PHPWeb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。

《PHP应用程序安全编程》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。《PHP应用程序安全编程》适用于各个阶段的Web应用程序开发人员。

作者介绍:

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。

William Ballad

曾经工作在信息技术领域的各个层面，从父母的ISP公司的硬件维护工程师到世界级大型公司的基于Windows和异构网络的架构师。他多年来一直活跃在IT安全领域，最近领导着一支专门抵御国际化黑客组织攻击OptionCart（一个广泛使用的电子商务系统）的团队。

目录: 译者序

第一篇 Web开发是血腥运动——不打无准备仗

第1章 服务器安全问题以及其他高深问题 1

1.1 现实检查 1

1.2 服务器安全问题 2

1.2.1 黑客通过非安全应用程序获得控制权 3

1.2.2 编程人员可以提高应用程序的安全性 4

1.3 安全困惑 4

1.4 自身的会话管理提供安全性 6

1.5 “我的应用程序并不值得攻击” 6

1.6 “门卫”的典型表现 6

1.7 小结 7

第二篇 安全漏洞是否大到能开大卡车

第2章 处理错误 9

2.1 留言板应用程序 9

2.1.1 程序总结 9

2.1.2 主要代码清单 9

2.2 用户执行过度操作 10

2.2.1 这些代码会产生什么结果 10

2.2.2 期待非期望输入 13

2.3 构建错误处理机制 14

2.3.1 测试非期望输入 14

2.3.2 决定如何处理错误数据 17

2.3.3 简化系统的使用 18

2.4 小结 20

第3章 系统调用 21

3.1 了解exec()、system()以及backtick的风险 21

3.1.1 通过SUID位和sudo使用系统命令 22

3.1.2 使用系统资源 22

3.2 使用escapeshellcmd()和escapeshellarg()保护系统调用 23

3.2.1 escapeshellcmd() 23

3.2.2 escapeshellarg() 24

3.3 创建能够处理所有系统调用的API 24

- 3.3.1 为什么不转义参数呢 24
- 3.3.2 验证用户输入 25
- 3.4 修补留言板应用程序 25
  - 3.4.1 moveFile () 函数 25
  - 3.4.2 修补应用程序 26
- 3.5 小结 27
- 第三篇 名称里的内涵，远多于你所期望的
- 第4章 缓冲区溢出和变量整理 29
  - 4.1 什么是缓冲区，什么是缓冲区溢出以及为什么要关注它 29
    - 4.1.1 缓冲区、堆栈、堆和内存分配 30
    - 4.1.2 缓冲区溢出的后果 32
    - 4.1.3 内存分配和PHP 32
    - 4.1.4 关注最新的安全警告 34
  - 4.2 通过变量整理预防缓冲区溢出 37
    - 4.2.1 前提：数据在证实为安全之前，都可能是有问题的，尤其是来自应用程序之外的数据 37
    - 4.2.2 数据是从哪儿来的 37
    - 4.2.3 如何整理数据以防止缓冲区溢出 37
  - 4.3 为应用程序打补丁 38
    - 4.3.1 验证是否为最新的稳定版本… 38
    - 4.3.2 检查变量整理 39
  - 4.4 小结 40
- 第5章 验证输入 41
  - 5.1 新特性：允许用户对留言板留言签名 41
  - 5.2 问题：用户提供了过多的数据 42
    - 5.2.1 发送垃圾邮件 42
    - 5.2.2 注入攻击 42
  - 5.3 假设：你了解你的数据 42
    - 5.3.1 数据库限制 43
    - 5.3.2 逻辑限制 43
  - 5.4 解决方法：验证输入的正则表达式 44
    - 5.4.1 数据污损 44
    - 5.4.2 正则表达式简介 45
    - 5.4.3 正则表达式的贪婪模式和惰性模式 47
    - 5.4.4 常见验证输入模式 49
  - 5.5 小结 51
- 第6章 文件系统访问：访问文件系统的乐趣和益处 52
  - 6.1 打开文件 52
    - 6.1.1 本地文件系统访问 52
    - 6.1.2 远程文件系统访问 53
    - 6.1.3 防止远程文件系统漏洞 54
  - 6.2 创建并存储文件 55
    - 6.2.1 允许文件上传 55
    - 6.2.2 安全地存储文件 56
  - 6.3 安全地修改文件属性 57
    - 6.3.1 修改UNIX/Linux/Mac OS X的文件权限 57
    - 6.3.2 修改Windows文件权限 58
    - 6.3.3 在PHP中修改文件权限 63
  - 6.4 修补应用程序以便支持用户上传图像文件 64
    - 6.4.1 修改API 64
    - 6.4.2 创建上传表单 66
  - 6.5 小结 66
- 第四篇 “噢，你可以信任我”

第7章 身份验证	67
7.1 什么是用户身份验证	67
7.1.1 用户名和密码	68
7.1.2 图像识别	70
7.2 权限	71
7.3 验证用户的方法	71
7.3.1 基于字典的身份验证	71
7.3.2 用户数据库	79
7.4 保存用户名和密码	80
7.4.1 加密	80
7.4.2 密码强度	80
7.4.3 评估漏洞	81
7.5 修补应用程序以便增加用户身份验证	82
7.5.1 添加User数据库表和确认数据库的安全性	82
7.5.2 创建身份验证API	83
7.6 小结	84
第8章 加密	85
8.1 什么是加密	85
8.2 加密类型	86
8.2.1 算法能力	87
8.2.2 速度和安全性	87
8.2.3 数据的使用	88
8.3 密码的安全性	88
8.4 在应用程序中增加密码加密功能...	88
8.4.1 修改User表	89
8.4.2 创建加密和salt函数	89
8.4.3 修改密码验证系统	89
8.5 小结	90
第9章 会话安全性	91
9.1 什么是会话变量	91
9.2 会话攻击的主要类型	91
9.2.1 会话固化	91
9.2.2 会话劫持	93
9.2.3 会话毒化（注入）	94
9.3 修补应用程序代码以提高会话安全性	94
9.4 小结	96
第10章 跨站式脚本编程	97
10.1 什么是XSS	97
10.2 反射式XSS	97
10.3 存储式XSS	97
10.4 修补应用程序代码防范XSS攻击	98
10.5 小结	99
第五篇 夜晚得锁门	
第11章 保护Apache和MySQL	101
11.1 编程语言、Web服务器以及操作系统本身都是不安全的	101
11.2 提高UNIX、Linux或Mac OS X环境的安全性	102
11.3 保护Apache	103
11.3.1 升级或安装Apache最新的稳定版本	104
11.3.2 设置Apache专有的用户和组	106
11.3.3 隐藏版本号以及其他敏感信息	107
11.3.4 将Apache限制在自身的目录结构中	107
11.3.5 禁用任何不必要的选项	109
11.3.6 安装和启用ModSecurity	109
11.4 保护MySQL	113

- 11.4.1 升级或安装最新版本 113
- 11.4.2 禁用远程访问 116
- 11.4.3 修改管理员用户名和密码… 116
- 11.4.4 删除默认的数据库用户并为每个应用程序创建新账户… 117
- 11.4.5 删除示例数据库 118
- 11.5 小结 118
- 第12章 IIS和SQL Server的安全性… 119
- 12.1 Windows服务器环境的安全性… 119
- 12.2 IIS的安全性 125
- 12.2.1 减少服务器的开放点 125
- 12.2.2 Web Root的安全性 126
- 12.3 SQL Server的安全性 131
- 12.3.1 安装或升级到最新版本 131
- 12.3.2 Microsoft SQL Server的安全性 138
- 12.4 小结 143
- 第13章 服务器端PHP的安全性 144
- 13.1 使用最新版本的PHP 144
- 13.1.1 Zend框架和Zend优化器 144
- 13.1.2 找到最新版本的PHP 148
- 13.1.3 使用Suhosin补丁和扩展 149
- 13.2 使用PHP和Apache内置的安全特性 149
- 13.2.1 safe\_mode 149
- 13.2.2 SuEXEC 150
- 13.3 使用ModSecurity 150
- 13.4 php.ini的安全性 151
- 13.5 小结 153
- 第14章 自动化测试介绍 154
- 14.1 为什么在关于安全的书籍中介绍测试 154
- 14.2 测试框架 155
- 14.3 测试类型 156
- 14.3.1 单元测试 156
- 14.3.2 系统测试 157
- 14.4 选择合适的测试数据 157
- 14.5 小结 158
- 第15章 探索性测试介绍 159
- 15.1 什么是探索性测试 159
- 15.2 Fuzz测试 160
- 15.2.1 安装和配置PowerFuzzer 160
- 15.2.2 使用PowerFuzzer 162
- 15.3 测试工具集 165
- 15.3.1 下载CAL 9000166
- 15.3.2 使用CAL 9000167
- 15.4 专有测试套件 176
- 15.4.1 专有测试套件的优点和特性 176
- 15.4.2 使用专有测试套件扫描你的应用程序 176
- 15.5 小结 181
- 第六篇 “不被攻击”并不是一个可行的安全策略
- 第16章 计划A：从开始阶段设计安全的应用程序 183
- 16.1 在开始编写代码之前 183
- 16.1.1 概念总结 183
- 16.1.2 工作流和角色图 185
- 16.1.3 数据设计 186
- 16.1.4 框架函数 189
- 16.2 标识故障点 190

16.2.1 登录和登出	190
16.2.2 文件上传	191
16.2.3 用户输入	192
16.2.4 文件系统访问	192
16.3 小结	192
第17章 计划B：去除已有应用程序的安全漏洞	193
17.1 设置环境	193
17.1.1 使用三阶段部署	193
17.1.2 使用版本控制	194
17.2 提高应用程序安全的检查列表...	195
17.2.1 检查服务器安全性	195
17.2.2 找到代码漏洞	195
17.2.3 修复最明显的问题	196
17.2.4 同事间的代码评审	197
17.3 小结	197
第18章 安全是生活方式的选择：成为一个优秀的编程人员	198
18.1 避免过多特性	198
18.2 编写自文档化代码	199
18.3 使用适合工作的工具	200
18.4 执行同事间的代码评审	201
18.5 小结	201
附录 额外资源	202
术语表	206
• • • • •	( <a href="#">收起</a> )

[PHP应用程序安全编程\\_下载链接1](#)

## 标签

PHP

安全

编程

web开发

计算机

服务器

运维

基础理论

## 评论

能帮助建立一些概念，深度很不够。

-----  
翻译得有点差了，并且没多少内容

-----  
大杂烩，浅尝辄止，啥也没讲清楚。

-----  
一般的书，虽然是老外写的，比较水

-----  
适合PHP开发员借鉴.安全是个big problem.

-----  
入门级的，讲了很多原则性的东西，对我这样的业余php程序员很有用。专家就不用看了，赫赫。

-----  
蜻蜓点水的介绍了一些基础知识，适合入门级的，先了解下php web开发应该具备哪些最基本的安全意识~

-----  
[PHP应用程序安全编程\\_下载链接1\\_](#)

## 书评

-----

[PHP应用程序安全编程 下载链接1](#)