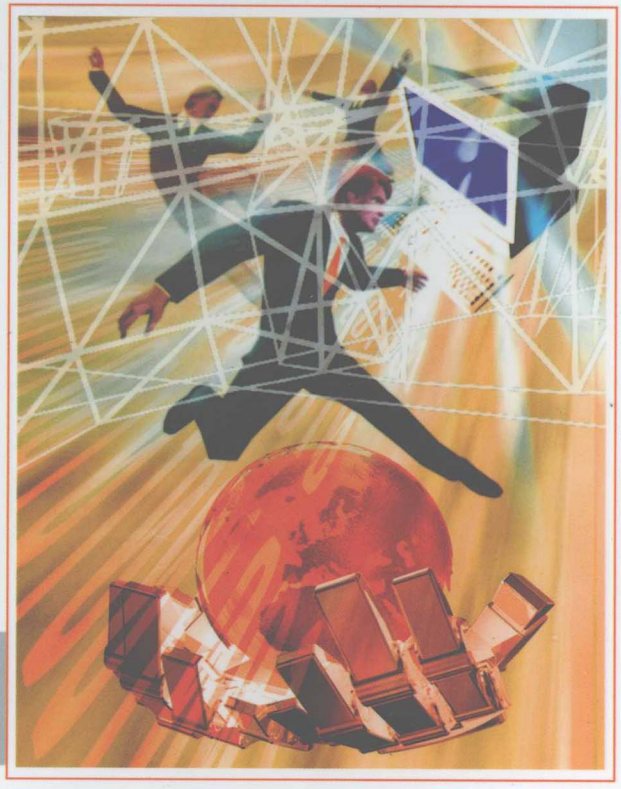
文魁資訊
Kings Information Co., Ltd.
http://www.kingsinfo.com.tw

网络安全专家

# 黑客入侵网页攻防修炼

- 网页程序完全基于PHP
- 攻击手法 Vs 防范策略
  - 命令注入攻击
  - 客户端脚本植入攻击
  - 跨网站脚本攻击
  - SQL注入攻击
  - 跨网站请求伪造攻击
  - 会话劫持攻击
  - 响应拆分攻击
  - 文件上传攻击
  - 目录/文件攻击



德瑞工作室 著
杨立峰 陈彦平 改编
飞思科技产品研发中心 监制

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

书中源文件、实例设计代码、数据库数据请到www.fecit.com.cn的“下载专区”中下载

网络安全专家

# 黑客入侵网页攻防修炼

德瑞工作室 著
杨立峰 陈彦平 改编
飞思科技产品研发中心 监制

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

# 内容简介

本书将 PHP 的技术技巧与 Web 应用相结合，分别对黑客的入侵和页面设计时的防范措施进行了深入浅出的分析，通过实例演示了包括 Command Injection、Script Insertion、XSS 、SQL Injection 、CSRF、Session Hijacking 和 HTTP Response Splitting 等在内的 18 种技术，这其中包含了作者对网页安全的独到见解。本书以一种清晰而简练的风格介绍了黑客惯用的技术要点，通过大量的示例演示了这种入侵是如何发生的，并指导读者如何防止类似问题的发生。在透彻地介绍基础知识的同时，还加入了作者自己的应用经验，可以大大提高读者的编程能力和应用水平。

书中源文件、实例设计代码、数据库数据请到 www.fecit.com.cn 的“下载专区”中下载。

本书适合的读者包括 PHP 中级、高级技术人员和网络安全从业人员等。



**版权贸易合同登记号 图字：01-2007-6078**

**图书在版编目（CIP）数据**

黑客入侵网页攻防修炼 / 德瑞工作室著；杨立峰，陈彦平改编. —北京：

电子工业出版社，2008.6

（网络安全专家）

ISBN 978-7-121-06764-8

I. 黑… II.①德… ②杨… ③陈… III.计算机网络－安全技术 IV.TP393.08

中国版本图书馆 CIP 数据核字（2008）第 073957 号

责任编辑：王树伟 李新承

印 刷：北京机工印刷厂

装 订：三河市鹏成印业有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编：100036

开 本：720×1000 1/16 印张：19.75 字数：442.4 千字

印 次：2008 年 6 月第 1 次印刷

印 数：5 000 册 定价：38.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

# 前　言

经过几个月的辛苦写作,终于将这本书完成，看到书名就应该会联想到是一本教您防御黑客攻击的书籍。没错，而且是专门针对使用 PHP 来开发 Web 应用程序的人员写的。PHP 是相当热门的程序语言，只要到书店走一趟就能感受到 PHP 受欢迎的程度。

虽然黑客入侵各大网站的事您略知一二，但是您可能对病毒、木马程序、破解密码、窜改分数等新闻名词仅仅是知道而已。如果您是使用 PHP 来开发 Web 应用程序的技术人员，您是否考虑过黑客能够通过您编写的网页来攻击您的网站呢？

在单机环境下开发 PHP 应用程序的人，可能没有考虑过黑客入侵网页的事，但如果您是替公司或客户编写网页，而且您写的网页是要放在因特网上让人浏览的话，您就不能不慎重仔细地考虑黑客入侵的问题了。如果因为您的网页出错而导致公司或客户受到损失，相信您的日子一定不会好过吧!

这本书精选了各种黑客攻击 PHP 网页的手法，虽然不能说是全部的入侵手段，但大致上已经能够概括绝大部分的攻击方式。本书详细解说每个攻击手法的原理与实际操作，当然，如何防范这些入侵才是本书的重点。想要开发安全的 PHP 应用程序，就赶快拿起这本书仔细地阅读吧！

德瑞工作室　谨识

**网上下载资料使用说明**

- 书中源文件、实例设计代码、数据库数据请到 www.fecit.com.cn 的“下载专区”中下载。
- 源文件中 Chx 文件夹对应第 x 章。
- 每章的实例设计代码都保存在该章对应文件夹下。
- Chx 文件夹中包括该章节使用到的数据库数据，通常命名为 Chx.sql。
- 本书所有实例及系统均基于 apache2+mysql5+php5 环境下开发设计，低版本的 A.M.P.环境运行文件时可能出现错误。
- 在使用该代码之前需要先建立和连接数据库，具体使用详见各章节说明。

# 关 于 飞 思

我们经常感谢生活的慷慨，让我们这些原本并不同源的人得以同本，为了同一个梦想走到一起。

因为身处科技教育前沿，我们深感任重道远；因为伴随知识更新节奏，我们一刻不敢停歇。虽然我们年轻，但我们拥有：

“严谨、高效、协作”的团队精神

全方位、立体化的服务意识

实力雄厚的作者群和开发队伍

当然，最重要的是我们拥有：

恒久不变的理想和永不枯竭的激情和灵感

正因如此，我们敢于宣称：

**飞思科技＝丰富的内容+完美的形式**

这也是我们共同精心培育的品牌 

的承诺。

“问渠哪得清如许，为有源头活水来”。路再远，终需用脚去量；风景再美，终需自然抚育。

年轻的飞思人愿为清风细雨、阳光晨露，滋润您发芽、成长；更甘当坚实的铺路石，为您铺就成功之路。

飞思科技产品研发中心


联系方式

咨询电话：（010）68134545　　88254161-67

电子邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn　　http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

# 目　录

# 01 PHP 网页的安全性

学习重点：

- 了解安全性的概念
- 了解 Register Globals 和 Magic Quotes 的使用
- 理解安全模式的概念
- 掌握修改 PHP 设置值的方法