

<<黑客入侵网页攻防修炼>>

图书基本信息

书名：<<黑客入侵网页攻防修炼>>

13位ISBN编号：9787121067648

10位ISBN编号：7121067641

出版时间：2008-6

出版时间：电子工业出版社

作者：德瑞工作室 著，杨立峰，陈彦平 改编

页数：298

字数：442400

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>

<<黑客入侵网页攻防修炼>>

内容概要

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。

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。

<<黑客入侵网页攻防修炼>>

书籍目录

第1章 PHP网页的安全性

1.1 什么是安全性

1.1.1 黑客攻击的方式

1.1.2 PHP网页的安全性问题

1.2 Register Globals

1.3 安全模式

1.3.1 限制文件的存取

1.3.2 限制环境变量的存取

1.3.3 限制外部程序的执行

1.4 Magic Quotes

1.4.1 使用Magic Quotes的好处

1.4.2 使用Magic Quotes的坏处

1.4.3 取消Magic Quotes功能

1.5 修改PHP的设定值

1.5.1 在php.ini文件中修改设定值

1.5.2 在httpd.conf文件中修改设定值

1.5.3 在.htaccess文件中修改设定值

1.5.4 在程序中修改设定值

第2章 Command Injection -命令注入攻击

2.1 PHP的命令执行函数

2.1.1 System函数

2.1.2 Exec函数

2.1.3 passthru函数

2.1.4 shell_exec 函数

2.1.5 运算符

2.2 命令注入攻击

2.2.1 攻击实例一

2.2.2 攻击实例二

2.2.3 攻击实例三

2.2.4 命令注入的方式

2.3 eval注入攻击

2.3.1 攻击没有作用

2.3.2 可变变量

2.3.3 pre_replace函数

2.3.4 ace函数

2.3.5 动态函数

2.3.6 call_user_func函数

2.4 防范的方法

2.4.1 使用escapeshellarg函数来处理命令的参数

2.4.2 使用safe_mode_exec_dir指定的可执行文件的路径

第3章 Script Insertion -客户端脚本植入攻击

3.1 客户端脚本植入攻击

3.2 攻击实例：在留言板中插入脚本

3.2.1 开始攻击：显示简单的对话框

3.2.2 没有显示对话框

<<黑客入侵网页攻防修炼>>

3.2.3 打开Internet Explorer的活动脚本功能

3.2.4 关闭PHP的magic_quotes_gpc

3.2.5 利用数据库来攻击

3.2.6 本章的数据库

3.2.7 浏览植入脚本的留言

3.2.8 破坏性的攻击手法：显示无穷尽的新窗口

3.2.9 引诱性的攻击手法：跳转网址

3.3 防范的方法

3.3.1 HTML输出过滤

3.3.2 使用strip_tags函数来进行HTML输出过滤

3.3.3 strip_tags函数的缺点

3.3.4 使用htmlspecialchars函数来进行HTML输出过滤

第4章 XSS -跨网站脚本攻击

4.1 什么是“跨网站脚本攻击”

4.2 跨网站脚本攻击

4.2.1 本章的数据库

4.2.2 登录首页

4.2.3 如何攻击

4.2.4 开始攻击

4.2.5 没有显示对话框

4.2.6 如何取得目标用户的cookie内容

4.2.7 服务器的记录文件

4.3 防范的方法

4.4 隐藏在\$_SERVER["PHP_SELF"]变量内的脚本

4.4.1 实际范例

4.4.2 拆解标签的内容

4.4.3 避免\$_SERVER["PHP_SELF"]被篡改

第5章 SQL Injection -SQL注入攻击

第6章 CSRF -跨网站请求伪造攻击

第7章 Session Hijacking -会话劫持攻击

第8章 HTTP Response Splitting -HTTP响应拆分攻击

第9章 File Upload Attack -文件上传攻击

第10章 目录/文件攻击

第11章 其他的攻击

第12章 攻击手法汇总

第13章 漏洞扫描器

第14章 开发安全的Web程序

附录A Telnet使用说明

附录B 查看HTTP请求与响应的实际内容

附录C URL编码与解码

附录D 构建PHP的测试环境

附录E 找出网站的IP地址

<<黑客入侵网页攻防修炼>>

章节摘录

第1章 PHP网页的安全性 1.1 什么是安全性 所谓安全性 (security) 就是要保护Web应用程序与网页不会受到黑客的攻击。

有些黑客纯粹是为了好玩而入侵他人的电脑, 但有更多的黑客费尽心思要窃取他人电脑中的机密文件, 甚至使整台电脑瘫痪来达到他的目的。

电脑中放置的资料, 其重要性视电脑的使用种类而定。

如果是个人电脑的主机, 那么安全性的问题就要视个人的观念而定。

有的人根本不在乎电脑的安全, 反正遇到问题时重新安装就好了。

有的人确实会担心自己的电脑被黑客入侵, 却又不知道如何去防范。

如果您管理的是公司内部或者对外开放的网站, 如购物或者拍卖网站, 安全性的议题就非常重要了。

如果黑客入侵了您的网站, 不但有可能使公司或者客户的隐私信息被盗取, 甚至黑客还可以在您的网站内植入木马程序, 或者当做僵尸电脑来攻击他人。

黑客也可以消耗网站的带宽或软件资源, 使电脑瘫痪而让别人无法使用您的网站。

现在网上有很多可以让黑客使用的软件, 这些软件多半是免费的而且简单好用。

所以一般人要攻击您的电脑, 并不是一件非常困难的事情。

关键是您对电脑进行了什么样的保护?

如果只是安装了查毒软件或是防火墙就以为平安无事了, 那么您对安全性的真正意义可以说是完全不了解。

1.1.1 黑客攻击的方式 黑客要攻击您的电脑有很多种方式, 比较简单的就是使用磁盘共享。

磁盘共享是在文件管理系统或是网络邻居内, 通过网络连接进入其他的电脑或主机。

由于黑客猜到了密码, 或者因为您的疏忽而开启了磁盘共享功能, 以致黑客可以使用Port139来简单地入侵您的电脑。

另外, 暴力破解 (Brute Force) 也是黑客常用的方式, 黑客使用尝试错误的方式来破解网站的账户和密码。

有了账户和密码, 黑客就可以堂而皇之地登录您的网站。

如果黑客使用的是具有最高权限的账户和密码, 他就能够任意删除、修改或查看您电脑内的所有文件资料。

上述这些攻击方式虽然讲起来容易, 但只要您细心地对您的系统进行设置, 黑客根本无法使用这些方式来攻击您的电脑。

现在要谈的是与本书有关的攻击方式, 使用网页或者电子邮件来攻击。

<<黑客入侵网页攻防修炼>>

编辑推荐

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/中文攻击。

本书详尽解说黑客攻击PHP应用程序的各种技术，当然更有破解与防范方法的说明。

要想建立安全的Web应用程序与网页，光精通PHP程序编码是不能做到的。

了解黑客实际的攻击手法，才能知道如何来防范问题的发生。

本书精选各种黑客的攻击技术，总共有18种之多，大致能够概括目前PHP网页所遇到的攻击手段

。要想建立能够让客户与上司信任的网页，您一定要阅读本书。

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。

<<黑客入侵网页攻防修炼>>

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>