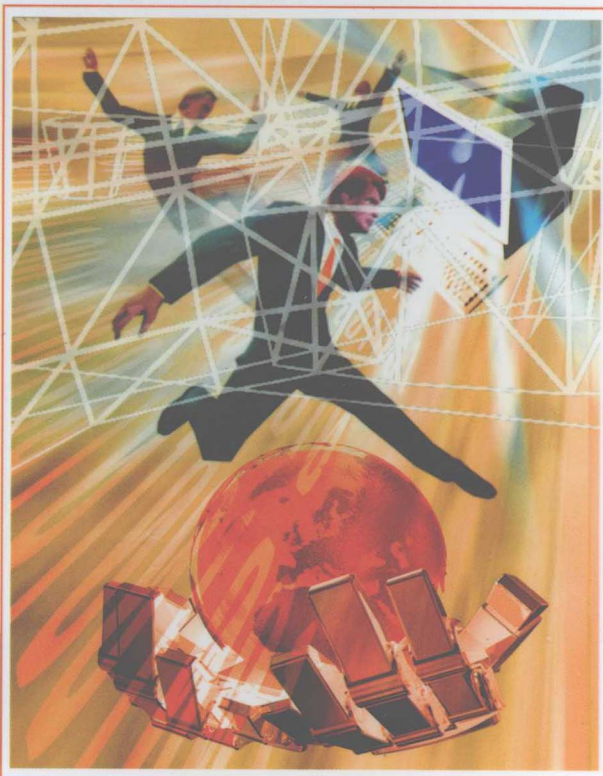


黑客入侵网页 攻防修炼

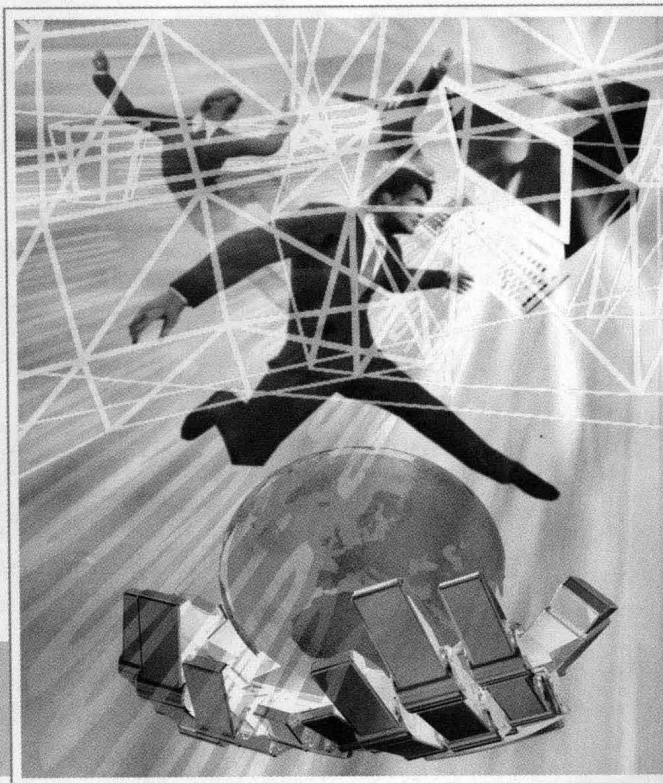
- 网页程序完全基于PHP
- 攻击手法 Vs 防范策略
 - 命令注入攻击
 - 客户端脚本植入攻击
 - 跨网站脚本攻击
 - SQL注入攻击
 - 跨网站请求伪造攻击
 - 会话劫持攻击
 - 响应拆分攻击
 - 文件上传攻击
 - 目录/文件攻击

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





黑客入侵网页 攻防修炼



德瑞工作室
杨立峰 陈彦平
飞思科技产品研发中心

著
改编
监制

电子工业出版社
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。

本书繁体字版名为《PHP 网页大作战: 如何防止骇客入侵您的网页》, 由统一元气资产管理股份有限公司出版, 版权属统一元气资产管理股份有限公司所有。本中文简体字版由统一元气资产管理股份有限公司授权电子工业出版社独家出版发行。未经本书原版出版者和本书出版者书面许可, 任何单位和个人均不得以任何方式或任何手段复制或传播本书的部分或全部。

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。

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、篡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

第 1 章	PHP 网页的安全性	1
1.1	什么是安全性	2
1.1.1	黑客攻击的方式	2
1.1.2	PHP 网页的安全性问题	3
1.2	Register Globals	4
1.3	安全模式	7
1.3.1	限制文件的存取	8
1.3.2	限制环境变量的存取	8
1.3.3	限制外部程序的执行	9
1.4	Magic Quotes	9
1.4.1	使用 Magic Quotes 的好处	10
1.4.2	使用 Magic Quotes 的坏处	10
1.4.3	取消 Magic Quotes 功能	11
1.5	修改 PHP 的设定值	11
1.5.1	在 php.ini 文件中修改设定值	12
1.5.2	在 httpd.conf 文件中修改设定值	13
1.5.3	在.htaccess 文件中修改设定值	13
1.5.4	在程序中修改设定值	13
第 2 章	Command Injection—命令注入攻击	15
2.1	PHP 的命令执行函数	16
2.1.1	System 函数	16
2.1.2	Exec 函数	17
2.1.3	passthru 函数	18
2.1.4	shell_exec 函数	18
2.1.5	运算符	19
2.2	命令注入攻击	19
2.2.1	攻击实例一	19
2.2.2	攻击实例二	20
2.2.3	攻击实例三	21
2.2.4	命令注入的方式	21
2.3	eval 注入攻击	22

2.3.1	攻击没有作用	23
2.3.2	可变变量	24
2.3.3	pre_replace 函数	24
2.3.4	ace 函数	26
2.3.5	动态函数	27
2.3.6	call_user_func 函数	29
2.4	防范的方法	30
2.4.1	使用 escapeshellarg 函数来处理命令的参数	30
2.4.2	使用 safe_mode_exec_dir 指定的可执行文件的路径	32
第 3 章	Script Insertion - 客户端脚本植入攻击	33
3.1	客户端脚本植入攻击	34
3.2	攻击实例: 在留言板中插入脚本	35
3.2.1	开始攻击: 显示简单的对话框	37
3.2.2	没有显示对话框	38
3.2.3	打开 Internet Explorer 的活动脚本功能	39
3.2.4	关闭 PHP 的 magic_quotes_gpc	40
3.2.5	利用数据库来攻击	41
3.2.6	本章的数据库	42
3.2.7	浏览植入脚本的留言	44
3.2.8	破坏性的攻击手法: 显示无穷尽的新窗口	45
3.2.9	引诱性的攻击手法: 跳转网址	46
3.3	防范的方法	48
3.3.1	HTML 输出过滤	48
3.3.2	使用 strip_tags 函数来进行 HTML 输出过滤	48
3.3.3	strip_tags 函数的缺点	50
3.3.4	使用 htmlspecialchars 函数来进行 HTML 输出过滤	52
第 4 章	XSS - 跨网站脚本攻击	53
4.1	什么是“跨网站脚本攻击”	56
4.2	跨网站脚本攻击	58
4.2.1	本章的数据库	60
4.2.2	登录首页	61
4.2.3	如何攻击	62
4.2.4	开始攻击	62

4.2.5	没有显示对话框	64
4.2.6	如何取得目标用户的 cookie 内容	64
4.2.7	服务器的记录文件	67
4.3	防范的方法	67
4.4	隐藏在\$_SERVER["PHP_SELF"]变量内的脚本	70
4.4.1	实际范例	71
4.4.2	拆解<form>标签的内容	73
4.4.3	避免\$_SERVER["PHP_SELF"]被篡改	74
第 5 章	SQL Injection - SQL 注入攻击	77
5.1	SQL 注入攻击	78
5.2	攻击实例: 绕过账号、密码的检查	79
5.2.1	如何攻击	81
5.2.2	开始攻击	82
5.2.3	只填入账号	84
5.3	攻击实例: 删除数据库的所有记录	84
5.3.1	删除留言的记录	86
5.3.2	如何攻击	87
5.3.3	开始攻击	88
5.4	攻击实例: 盗取密码	89
5.4.1	如何攻击	91
5.4.2	开始攻击	91
5.5	防范的方法	93
5.5.1	数字型变量的过滤方式	93
5.5.2	字符串变量的过滤方式: 使用 addslashes 函数	94
第 6 章	CSRF - 跨网站请求伪造攻击	97
6.1	跨网站请求伪造攻击	98
6.2	攻击实例: 删除数据库的一条记录	99
6.2.1	删除留言的记录	101
6.2.2	如何攻击	102
6.2.3	开始攻击	103
6.3	攻击实例: 新增数据库的一条记录	104
6.3.1	如何攻击	105
6.3.2	开始攻击	106

6.4	防范的方法	107
6.4.1	检查网页的来源	108
6.4.2	检查内置的隐藏变量	111
6.4.3	使用 POST, 不要使用 GET	113
第 7 章	Session Hijacking—会话劫持攻击	115
7.1	什么是 Session	116
7.1.1	session id	116
7.1.2	Session 的名称	118
7.2	PHP 的 Session 机制	119
7.2.1	URL 参数	119
7.2.2	表单中隐藏属性的文本框	120
7.2.3	Cookie	121
7.3	会话劫持攻击	123
7.3.1	攻击的步骤	124
7.3.2	如何攻击	124
7.3.3	开始攻击	127
7.4	Session 固定攻击	129
7.4.1	攻击的步骤	130
7.4.2	攻击的方式	131
7.5	防范的方法	132
7.5.1	定期更改 session id	132
7.5.2	更改 Session 的名称	133
7.5.3	关闭透明化 session id 的功能	133
7.5.4	只从 cookie 检查 session id	134
7.5.5	检查浏览器是否改变	134
7.5.6	使用 URL 传递秘密参数	135
第 8 章	HTTP Response Splitting—HTTP 响应拆分攻击	137
8.1	HTTP 简介	138
8.1.1	HTTP 请求的格式	138
8.1.2	HTTP 请求的方法	139
8.1.3	HTTP 响应的格式	139
8.1.4	使用 header 函数发送 HTTP 表头	143
8.1.5	使用 PHP 的函数来替代 Telnet	143

8.2	HTTP 响应拆分攻击	144
8.3	攻击实例: 跳转地址	149
8.4	与 Session 固定结合攻击	150
8.5	防范的方法	150
8.5.1	将 session.use_only_cookies 设置为 1	152
8.5.2	使用最新版的 PHP	152
8.6	隐藏 HTTP 响应表头	152
第 9 章	File Upload Attack - 文件上传攻击	155
9.1	文件上传	156
9.1.1	上传文件的大小	157
9.1.2	\$_FILES 数组变量	158
9.1.3	存放上传文件的文件夹	159
9.1.4	上传文件时的错误信息	159
9.2	文件上传攻击	159
9.2.1	上传可执行文件	160
9.2.2	覆盖原有文件	162
9.2.3	瘫痪网站	162
9.2.4	存取上传的文件数据	162
9.3	防范的方法	162
9.3.1	关掉上传文件的功能	163
9.3.2	限制允许上传的文件大小	163
9.3.3	检查是否真的是上传的文件	164
9.3.4	更改临时文件夹的路径	166
9.3.5	读取上传文件的绝对路径与文件名称	167
9.3.6	隐藏文件的路径	168
第 10 章	目录/文件攻击	169
10.1	目录穿越攻击	170
10.1.1	如何攻击	170
10.1.2	开始攻击	171
10.1.3	Microsoft 的 IIS 服务器	173
10.2	远程文件引入攻击	173
10.2.1	如何攻击	174
10.2.2	开始攻击	174

10.2.3	与目录穿越结合攻击	175
10.2.4	与 HTTP 响应分割结合攻击	177
10.3	防范的方法	179
10.3.1	使用者输入的文件名	179
10.3.2	设置 open_basedir	181
10.3.3	设置 allow_url_fopen 为 Off	182
10.3.4	使用 realpath 与 basename 函数来处理文件名	182
第 11 章	其他的攻击	183
11.1	变量指定攻击	184
11.2	URL 攻击	187
11.2.1	开始攻击	187
11.2.2	防范的方法	188
11.3	表单欺骗攻击	189
11.4	HTTP 请求欺骗攻击	191
11.5	拒绝服务攻击	193
11.5.1	SYN Flood 攻击	194
11.5.2	LAND 攻击	195
11.5.3	Ping of Death 攻击	195
11.5.4	Ping Flood 攻击	195
11.5.5	Teardrop 攻击	195
11.5.6	Pear-to-pear 攻击	196
11.5.7	分布式拒绝服务攻击	196
11.5.8	防范的方法	196
11.5.9	SYN Cookies	197
11.5.10	防火墙	197
11.5.11	分享器与路由器	197
11.5.12	应用程序前端硬件	197
11.6	网页劫持攻击	198
11.7	缓冲区溢位攻击	198
11.7.1	基本范例	199
11.7.2	堆栈溢出	199
第 12 章	攻击手法汇总	201
12.1	命令注入攻击	202

12.1.1	程序代码漏洞 1	202
12.1.2	攻击手法 1	202
12.1.3	程序代码漏洞 2	203
12.1.4	攻击手法 2	203
12.1.5	命令注入的方式	203
12.1.6	防范的方法	204
12.2	eval 注入攻击	204
12.2.1	程序代码漏洞 1	204
12.2.2	攻击手法	205
12.2.3	程序代码漏洞 2	205
12.2.4	攻击手法	205
12.2.5	程序代码漏洞 3	206
12.2.6	攻击手法	206
12.2.7	程序代码漏洞 4	206
12.2.8	攻击手法	206
12.2.9	防范的方法	207
12.3	客户端脚本注入攻击	207
12.3.1	程序代码漏洞 1	207
12.3.2	攻击手法	207
12.3.3	程序代码漏洞 2	207
12.3.4	攻击手法	208
12.3.5	防范的方法	208
12.4	跨网站脚本攻击	208
12.4.1	程序代码漏洞 1	209
12.4.2	攻击手法	209
12.4.3	程序代码漏洞 2	209
12.4.4	攻击手法	209
12.4.5	防范的方法	209
12.5	SQL 注入攻击	210
12.5.1	程序代码漏洞 1	210
12.5.2	攻击手法	211
12.5.3	程序代码漏洞 2	211
12.5.4	攻击手法	211

12.5.5	程序代码漏洞 3	211
12.5.6	攻击手法	212
12.5.7	防范的方法	212
12.6	跨网站请求伪造攻击	213
12.6.1	程序代码漏洞 1	213
12.6.2	攻击手法	214
12.6.3	程序代码漏洞 2	214
12.6.4	攻击手法	214
12.6.5	防范的方法	215
12.7	Session 劫持攻击	216
12.7.1	程序代码漏洞	216
12.7.2	攻击手法	217
12.7.3	防范的方法	217
12.8	Session 固定攻击	218
12.8.1	程序代码漏洞	218
12.8.2	攻击手法	218
12.8.3	防范的方法	219
12.9	HTTP 响应拆分攻击	221
12.9.1	程序代码漏洞 1	221
12.9.2	攻击手法	221
12.9.3	程序代码漏洞 2	222
12.9.4	攻击手法	222
12.9.5	防范的方法	222
12.10	文件上传攻击	223
12.10.1	程序代码漏洞	223
12.10.2	攻击手法	224
12.10.3	防范的方法	224
12.11	目录穿越攻击	225
12.11.1	程序代码漏洞	225
12.11.2	攻击手法	226
12.11.3	防范的方法	226
12.12	远程文件引入攻击	226
12.12.1	程序代码漏洞	227

12.12.2	攻击手法 1	227
12.12.3	攻击手法 2	227
12.12.4	防范的方法	227
12.13	变量指定攻击	228
12.13.1	程序代码漏洞	228
12.13.2	攻击手法	228
12.13.3	防范的方法	229
第 13 章	漏洞扫描器	231
13.1	什么是“漏洞扫描器”	232
13.2	Nessus 漏洞扫描器	232
13.2.1	Nessus 的特点	233
13.2.2	下载与安装	233
13.2.3	执行 Nessus	234
13.2.4	Nessus 检查漏洞的方式	237
13.3	MaxPatrol 漏洞扫描器	238
13.4	Paros 漏洞扫描器	240
13.4.1	Paros 的特点	240
13.4.2	下载与安装	241
13.4.3	设置浏览器的 Proxy	241
13.4.4	执行 Paros	243
13.4.5	扫描漏洞	244
13.4.6	检视 HTTP 请求与响应的内容	245
13.4.7	Paros 的 Trap 功能	245
13.4.8	URL 编码与解码	246
第 14 章	开发安全的 Web 程序	247
14.1	什么是“安全的 Web 应用程序”	248
14.2	过滤输入的数据	248
14.2.1	为什么要过滤数据	249
14.2.2	基本的数据过滤程序	251
14.2.3	数字数据的过滤	252
14.2.4	字符串数据的过滤	253
14.2.5	HTML 与 PHP 标签的过滤	254
14.2.6	文件路径的过滤	255

14.2.7	序列化字符串的过滤	256
14.3	转义输出的数据	257
14.3.1	基本的转义程序	257
14.3.2	转义 SQL 表达式的字符串	258
14.3.3	使用 addslashes 函数	258
14.4	Register Globals	259
14.4.1	隐藏 Register Globals 所发生的问题	260
14.4.2	\$_REQUEST 变量	261
14.4.3	\$_SERVER 变量	261
14.5	magic_quotes_gpc	261
14.6	错误信息的报告	262
14.7	文件的安全	263
14.8	Session 的安全	264
14.8.1	Session 固定攻击	264
14.8.2	Session 的保存	265
14.9	虚拟主机	266
14.9.1	可预测的临时文件名称	266
14.9.2	隐藏表头的信息	267
14.9.3	系统异常的监测	267
附录 A	Telnet 使用说明	269
A.1	Telnet 简介	270
A.2	打开 Windows 的 Telnet 服务	270
A.3	Telnet 使用说明	272
A.4	使用 Telnet 连接到本地主机	273
A.5	在 HTTP 表头内加上要执行的文件	275
附录 B	查看 HTTP 请求与响应的实际内容	277
B.1	如何查看 HTTP 请求与响应的实际内容	280
B.2	修改 HTTP 请求/响应的内容	281
B.3	显示 HTTP 请求/响应的参数	282
B.4	显示上传文件的 HTTP 请求	283
附录 C	URL 编码与解码	285
附录 D	构建 PHP 的测试环境	285
D.1	AppServ 整合包	288

D.2	安装 AppServ 整合包	289
D.3	测试 AppServ 是否正确安装	293
D.4	服务器的文件夹位置	293
附录 E	找出网站的 IP 地址	285
E.1	使用 Ping 命令	296
E.2	使用 NetInfo	296
E.3	无法找出 IP 地址	297

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

黑客入侵网页攻防修炼

