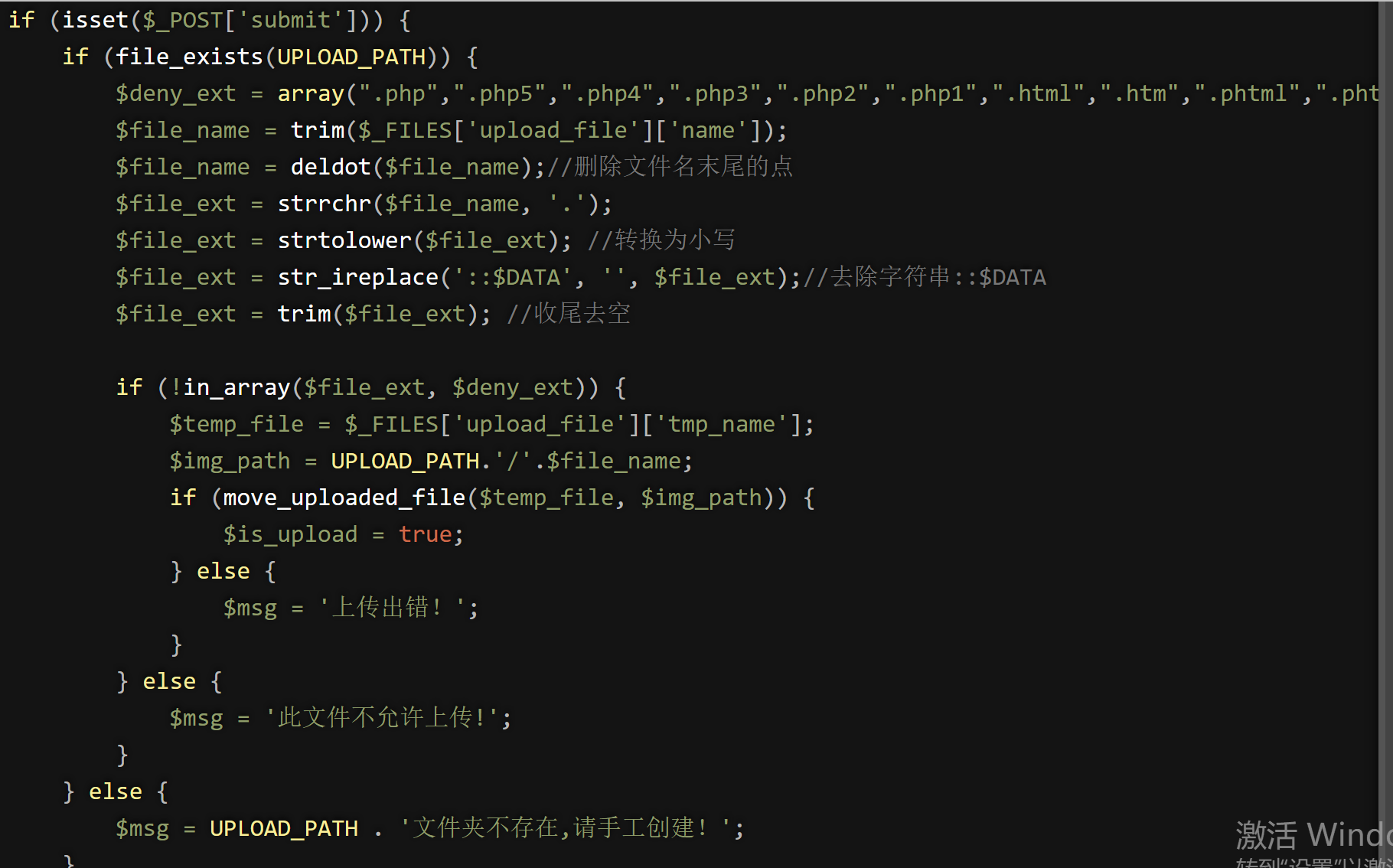
此处黑名单没有过滤.htaccess后缀，故此处也可上传.htaccess文件进行绕过。  
*注: .htaccess文件生效前提条件为1.mod\_rewrite模块开启。2.AllowOverride All*

.htaccess文件是Apache服务器中的一个配置文件，它负责相关目录下的网页配置。通过htaccess文件，可以实现：网页301重定向、自定义404错误页面、改变文件扩展名、允许/阻止特定的用户或者目录的访问、禁止目录列表、配置默认文档等功能IIS平台上不存在该文件，该文件默认开启，启用和关闭在httpd.conf文件中配置。

构造.htaccess文件，内容如下:AddType application/x-httpd-php .jpg  
这里代码的意思可以让 .jpg后缀名文件格式的文件名以php格式解析，因此达到了可执行的效果。所以我们可以把要上传的php文件的后缀名改为.jpg格式从而绕过

查看源代码：

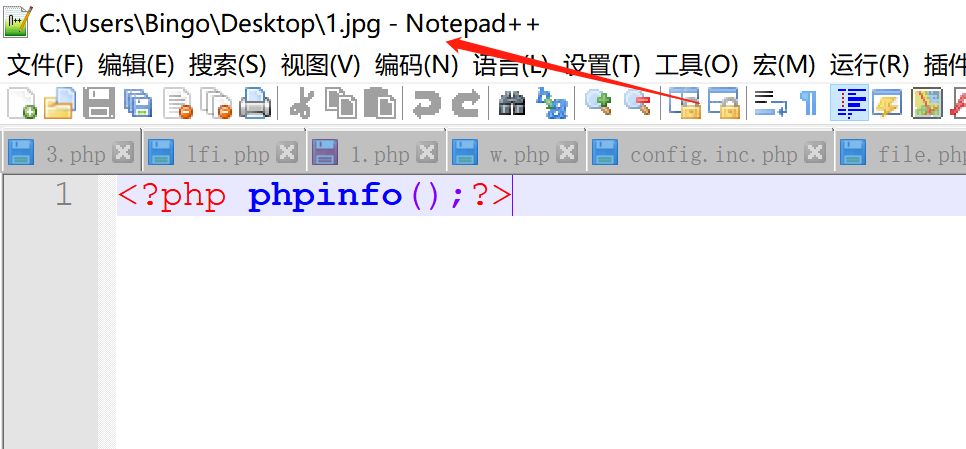


虽然还是黑名单，但几乎过滤了所有有问题的后缀名，除了.htaccess，于是首先上传一个.htaccess内容如下的文件:

SetHandler application/x-httpd-php



这样所有文件都会解析为php，然后再上传图片马，就可以解析：



访问：

