# Apache重写URL利用拿webshell

实验靶机： createByDemon-v1.0.tar.gz/lzx/uploadCode/upload-htaccess.php

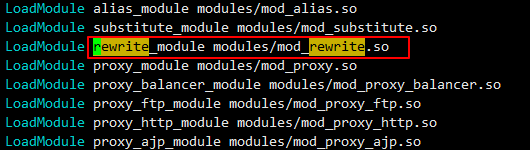
利用.htaccess的功能，使得我们的图片格式被当做php脚本解析

但是此利用需要满足以下条件：

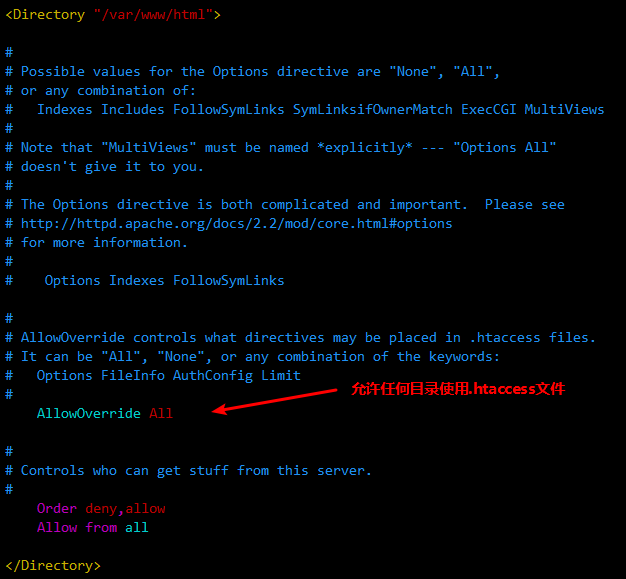
* apache 要开启重写模块 和 重写功能
* apache 要允许所有目录都可以重写
* 该服务器可以上传 .htaccess 文件

下面模拟如何利用apache重写功能来把图片格式解析成php文件

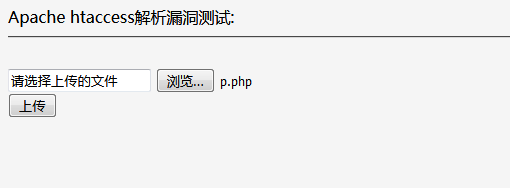
在apache配置文件，开启重写功能和模块

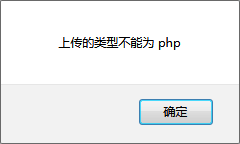






配置完后，开始实验，在上传接口如果直接上传php文件就会被后台过滤





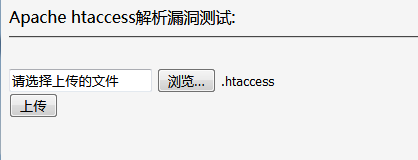
如果后台没有过滤 .htaccess结尾的文件，我们就可以把重写配置功能上传上去

.htaccess内容如下

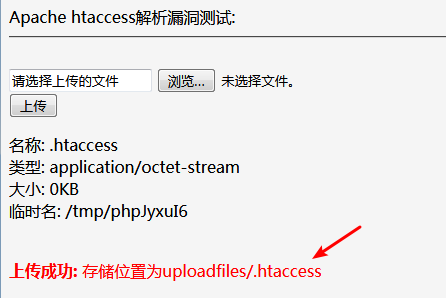
<FilesMatch "shell.jpg">

SetHandler application/x-httpd-php

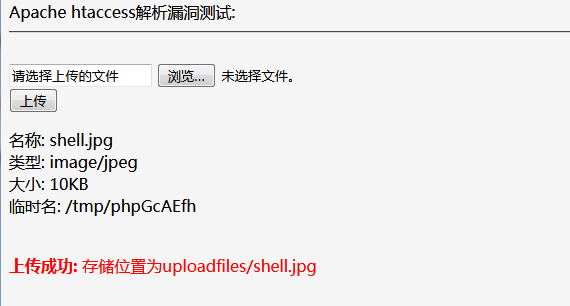
</FilesMatch>



点击上传



这时候，我们再上传shell.jpg图片木马



然后访问这个图片URL



