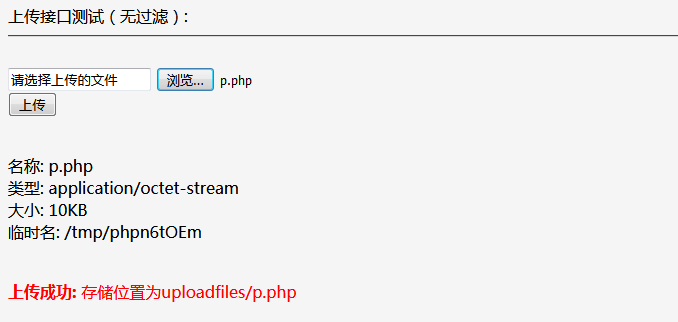
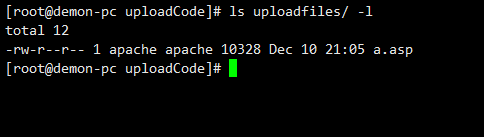
# 突破上传过滤拿webshell

测试靶机：createByDemon-v1.0.tar.gz/lzx/uploadCode

## 无过滤

如果对上传接口没有过滤，任何类型的文件都可以上传，那么我们就可以直接上传一句话木马使用，菜刀连接即可。

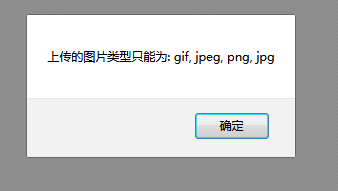




## JS过滤

如果有前端的js来过滤上传格式，我们可以直接修改代码或者转包改格式

直接上传php木马会弹出警告



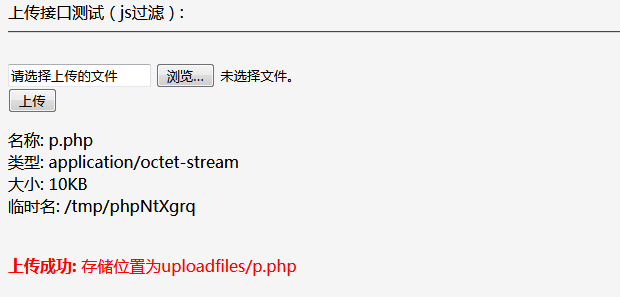
对前端代码审计一下，可以看到有个过滤函数

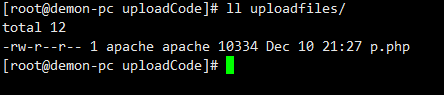


直接把return CheckFile 改成 return true 即可



然后重新上传php一句话木马

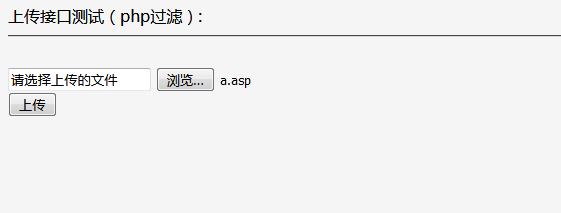


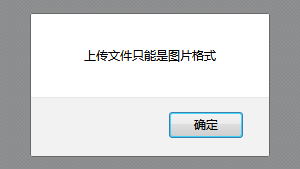


如果懒得代码审计，也可以直接用brup抓包修改

## php过滤

如果是后端php代码进行过滤，并且服务器是apache，我们可以利用apache解析漏洞来上传一句话木马。



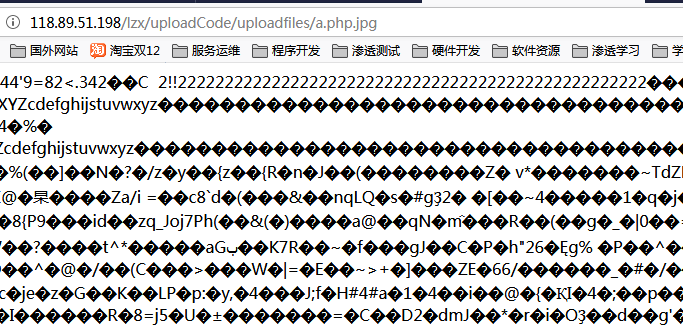


对其代码审计，发现过滤代码并没有在前端



利用apache解析漏洞上传 a.php.jpg格式的木马图片

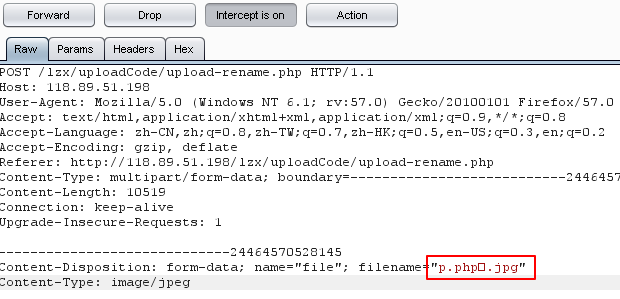


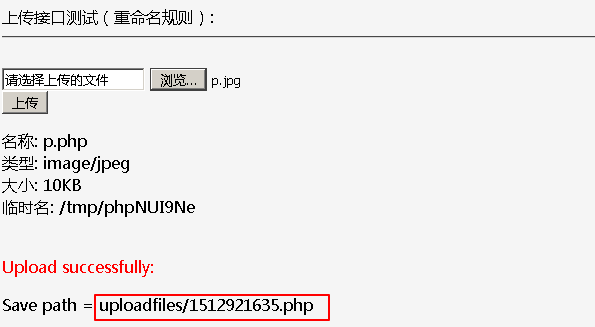


## 上传重命名



使用00截断 绕过过滤





因为会对上传的文件重命名，所以绝大多数使用了正则，正则遇到00会被截断，所以php格式就能保留下来了