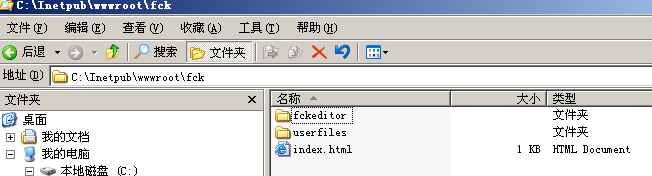
**Fckeditor编辑器漏洞**

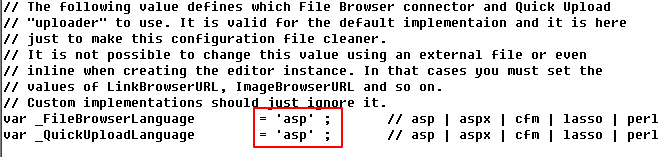
将Fckeditor2.6.6 编辑器上传到IIS6.0上，并且创建一个web服务来访问他



编辑配置文件： fckeditor/fckconfig.js 修改下面两个字段

var \_FileBrowserLanguage = 'asp' ; // asp | aspx | cfm | lasso | perl | php | py

var \_QuickUploadLanguage = 'asp' ; // asp | aspx | cfm | lasso | perl | php | py



编辑配置文件fckeditor\editor\filemanager\connectors\asp\config.asp把下面的功能开启

ConfigIsEnabled = True

然后使用浏览器访问编辑器



浏览器访问根目录下的（下同）fckeditor/\_whatsnew.html查看版本号



Fckeditor存在上传接口，如下：

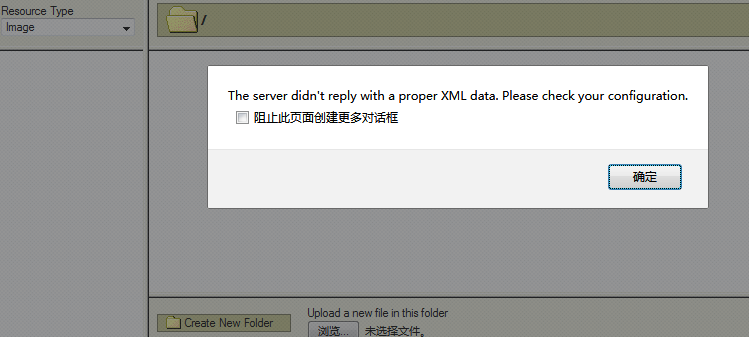
asp上传接口：

fckeditor/editor/filemanager/browser/default/browser.html?type=Image&connector=connectors/asp/connector.asp

php上传接口：

fckeditor/editor/filemanager/browser/default/browser.html?type=Image&connector=connectors/php/connector.php

访问但是由于这里配置原因，无法正常使用，不过没关系，下面有模板

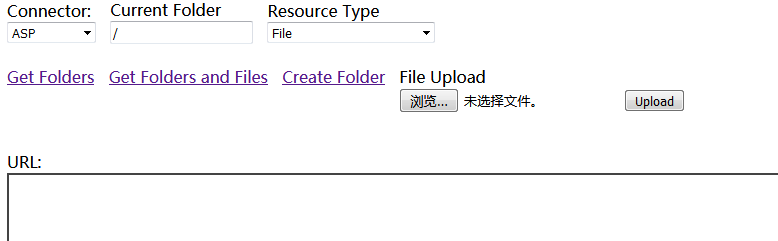


访问上传测试模板页面

fckeditor/editor/filemanager/connectors/test.html

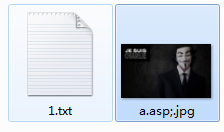
fckeditor/editor/filemanager/connectors/uploadtest.html

用浏览器访问上面的测试页面

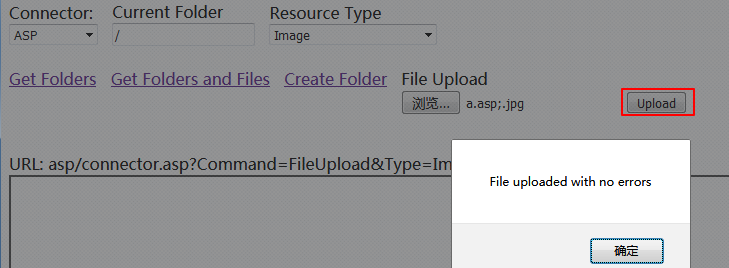


这里提供了几个功能：查看目录和文件，创建目录，上传文件，发送的参数会在URL：后面显示，这里准备好一个asp木马，将其名字改为

a.asp;.jpg



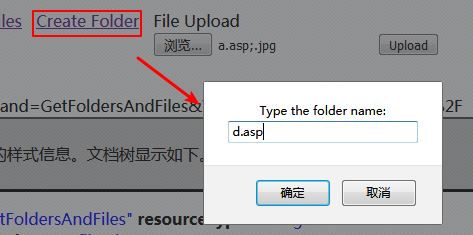
将木马上传上去Type选择image，上传好后点Get Folders and Files 按钮查看目录



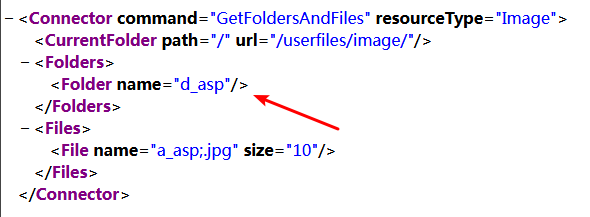
很可惜，这里的a.asp;.jpg 被改名成 a\_asp;.jpg 因此IIS文件名解析漏洞无法利用



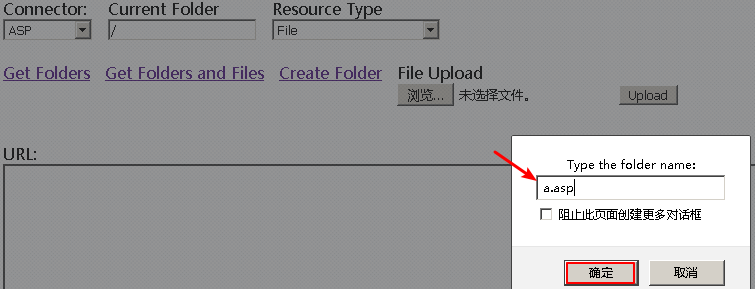
可以尝试IIS目录名解析漏洞，创建一个名为a.asp的文件夹，然后点击查看目录



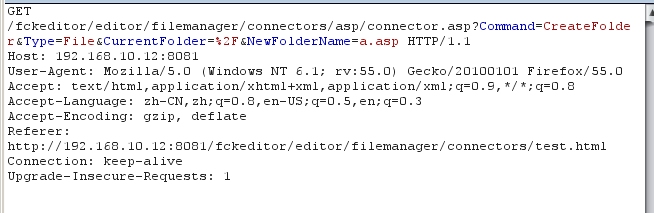
结果发现，d.asp目录也被改成d\_asp了，那么如何绕过呢？

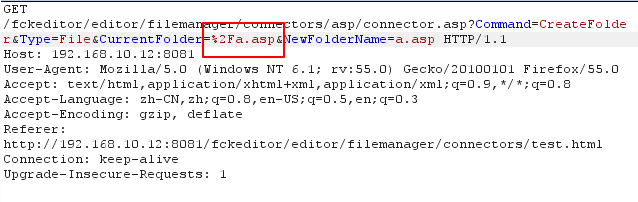


这里用到一个创建递归多目录的漏洞绕过，打开burp抓包，点击创建目录名字为a.asp

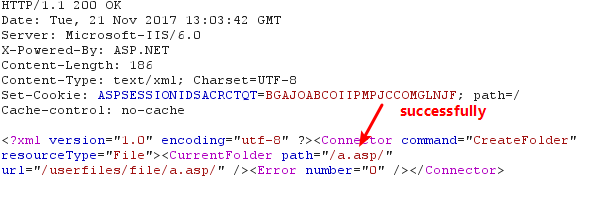


抓到包送到reapter重放模块，将currentFolder的值改成 %2Fa.asp 也就是 /a.asp

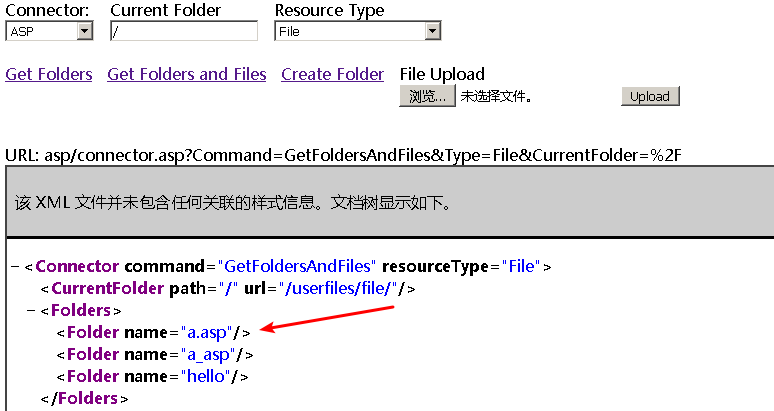




点击发送，在旁边的放回结果栏可以看到成功的创建了递归多目录了



返回浏览器，枚举/目录下的所有文件和目录



此时可以看到a.asp目录被创建了

这时候就可以结合IIS的目录名解析漏洞拿到webshell了，这个绕过的原理利用一个变量Current Folder当前目录来一次性创建了两个目录，两者为父子递归关系，虽然子目录没有逃过截杀被改名成a\_asp，但是父目录不会被改名，这样就成功创建了一个a.asp，至于后面怎么利用看操作。

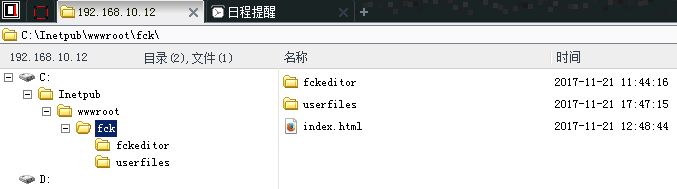
切换到a.asp下上传一句话木马图片



点击按钮查看结果，上传位置在输出框有



使用菜刀连接即可



因为时间关系，记录的很潦草，希望各位看到有什么需要改进的可以提点意见