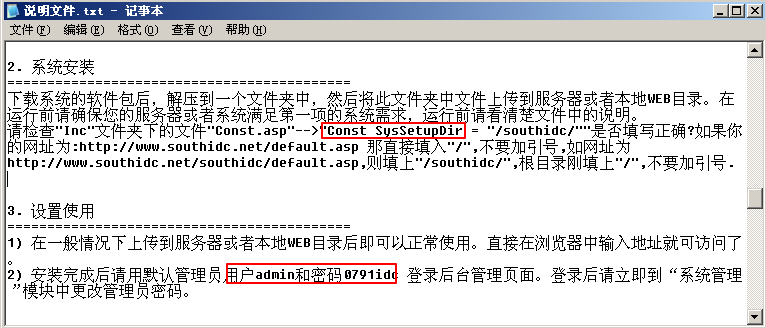
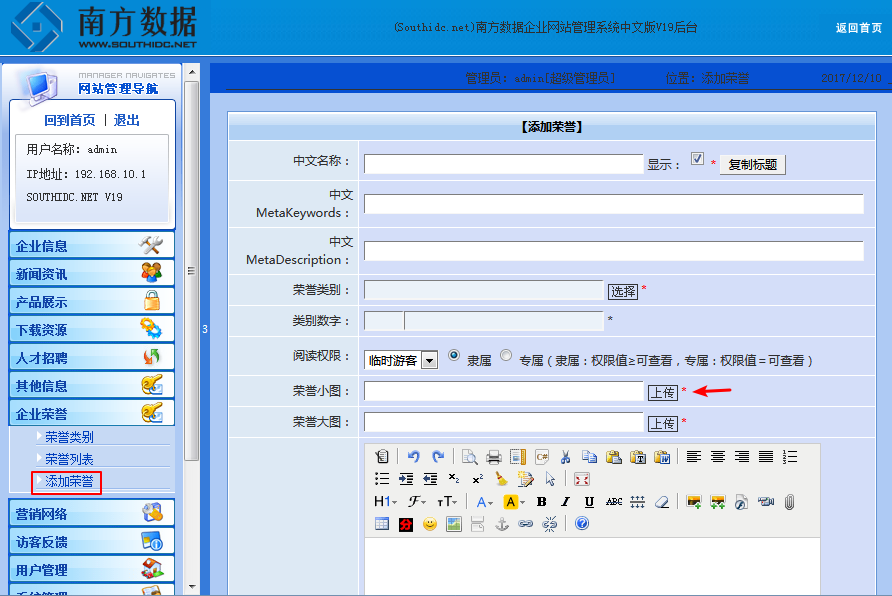
# 数据库备份拿webshell

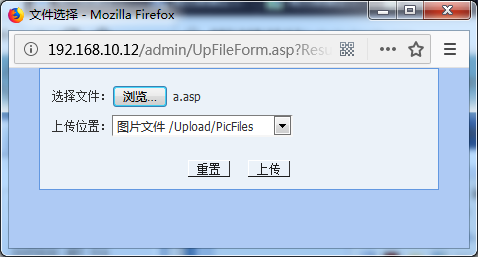
测试源码： 南方数据企业cms - v19版

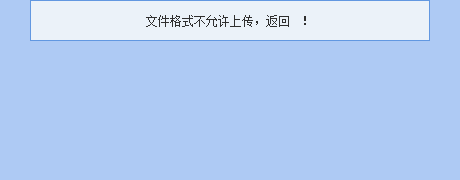




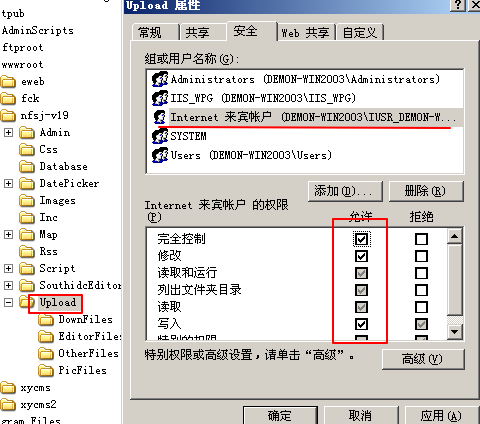
找到上传接口，尝试直接上传asp文件是会被过滤的



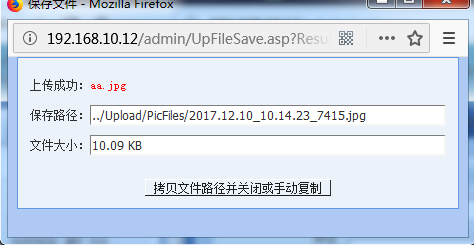




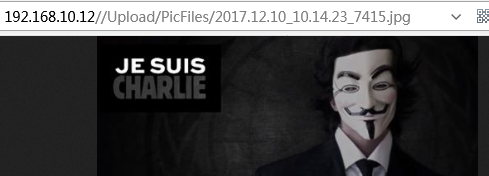
所以我们只能上传图片格式的木马，另外记得upload目录要给足权限，不然上传会报错



上传成功后，图片会被改名成特定的命名格式



如果直接用浏览器访问，是不会被当做asp脚本解析，也就无法让一句话木马生效





这时我们把Upload/PicFiles/2017.12.10\_10.14.23\_7415.jpg

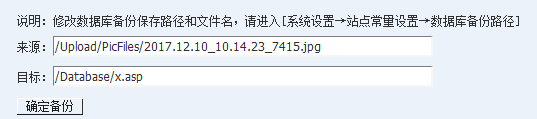
在该后台管理界面提供了一个数据库备份接口



把来源改成刚刚上传的木马文件，目标改成asp或者asa格式的文件，直接改是改不了，所以这里用调试工具来修改



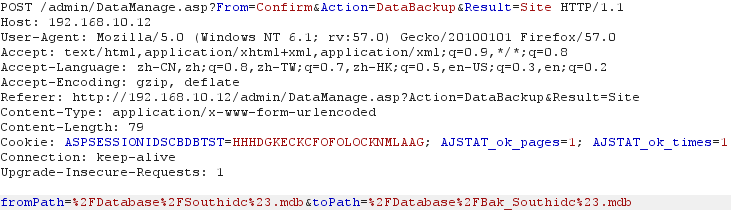
修改好后如下



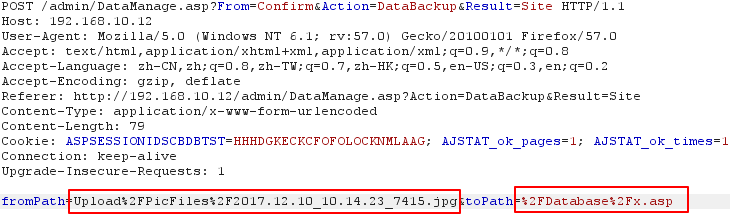
点击确认备份，然后访问对应的文件链接



尝试抓包修改



改成



然后发包，尝试访问 Database/x.asp文件，但结果还是不行，看来文件在后台给写死了