

sql 注入盲注时常常用函数

作者: [HuixiaZhang](#)

原文链接: <https://ld246.com/article/1538313535599>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

0x00 盲注

盲注是不能通过直接显示的途径来获取数据库数据的方法，在盲注中，攻击者根据其返回页面的不同判断信息。盲注一般可分为三类：Booleanbase、Timebase、Errorbase。

接下来介绍一些sql盲注中常用的函数。

0x01 limit()

limit()函数的作用是限制由SELECT语句返回的数据数量，用法是

```
SELECT column1, column2, columnN
```

```
FROM table_name
```

```
LIMIT [no of rows]
```

```
select * from user limit 2,1; //从第三行开始提取一行
```

其中各参数意义如下：

- column : 必要参数，要查询的字段名，可以同时查询多个。
- table_name : 必要参数，要查询的表名。
- no of rows : limit之后的第一个数字代表行数（从0开始算）后面数字代表从这行要返回的行数。

和offset同时用时用法如下

```
SELECT column1, column2, columnN
```

```
FROM table_name
```

```
LIMIT [no of rows] OFFSET [row num]。
```

```
select * from user limit 1 offset 2 //从第三行开始提取一行
```

其中各参数意义如下：

- no of rows : 取到的行数。
- row num : 起始位置（从0开始算）

0x02 mid()

mid()函数的作用是截取字符串的一部分，用法是

```
mid(column_name,start[,length])
```

其中各参数的意义如下：

- column_name : 必要参数，要提取字符的字段。
- start : 必要参数，规定提取的起始位置，从1开始。
- length : 可选参数，要返回的字符长度，如果省略会返回剩余的全部文本。

如：

```
mid(database(),1,1)
```

返回数据库名的第一位。

```
mid(database(),1,1)>'a'
```

返回数据库名的第一位并与a的ascii作比较。

```
mid((SELECT table_name FROM INFORMATION_SCHEMA.TABLES WHERE table_schema=0x7657374 LIMIT 0,1),1,1)
```

查找test数据库的第一个表名并提取表名的第一位。

0x03 substr()、substring()

substr()、substring()函数的作用也是截取字符串，用法同mid()

substring(string, start, length)

substr(string, start, length)

其中各参数意义如下：

string：必要参数，要提取字符的字段。

start：必要参数，规定提取的起始位置，从1开始。

length：可选参数，要返回的字符长度，如果省略会返回剩余的全部文本。

```
substr(DATABASE(),2,1)>'a'
```

返回数据库名的第二位并与a的ascii作比较。

```
substr((SELECT table_name FROM INFORMATION_SCHEMA.TABLES WHERE table_schema=0x6657374 LIMIT 0,1),1,1)>'a'
```

查找test数据库的第一个表名并提取表名的第一位,然后有a的ascii作比较。

0x04 left()

left()函数的作用是得到字符串左部开始指定个数的字符。

left(string,n)

其中各参数意义如下：

string：必要参数，要截取的字符串。

n：必要参数，规定截取的长度，从1开始。

```
left(database(),1)>'a'
```

查看数据库名的第一位并和a的ascii作比较。

0x05 ord()

ord()函数的作用是返回字符串中第一个字符的ASCII值。

ord(string)

其中各参数意义如下：

string：必要参数，要获取的字符串。

```
ord(mid(user(),1,1))=114
```

检测user()的第一个字符是否等于114，即是否等于r，一般用来判断是否是root权限。

0x06 sleep()

sleep()函数的作用是让代码执行延迟若干秒。

sleep(seconds)

其中各参数意义如下：

seconds：必要参数，延迟的秒数。

```
if(ascii(substr(database(),1,1))>'a',1,sleep(5))#
```

检测数据库的第一个字符的ascii和a比较，如果浏览器直接显示，说明比a大，如果浏览器五秒后才显示，说明比a小。

0x07 benchmark()

benchmark()函数的作用是重复执行指令。

benchmark(count,expr)

其中各参数意义如下：

count：必要参数，重复的次数。

expr：必要参数，执行的语句。

0x08 group_concat()

group_concat()函数的作用是连接字段字符串。

group_concat([DISTINCT] name [Order BY ASC/DESC 排序字段] [Separator '分隔符'])

其中各参数意义如下：

name：要连接的字段

```
substr((select group_concat(schema_name) from information_schema.schemata limit 0,1),1,1)
105
```

0x09 总结

盲注是sql注入中十分常用的手段，而且盲注很多时候需要写脚本来实现，熟悉这些函数，结合前面绕过方法，会让自己的脚本更加灵活。