实验吧-简单的sql注入 Writeup

原创

baynk 于 2019-07-28 03:06:47 发布 212 收藏

分类专栏： # 实验吧 Writeup 文章标签： CTF 实验吧

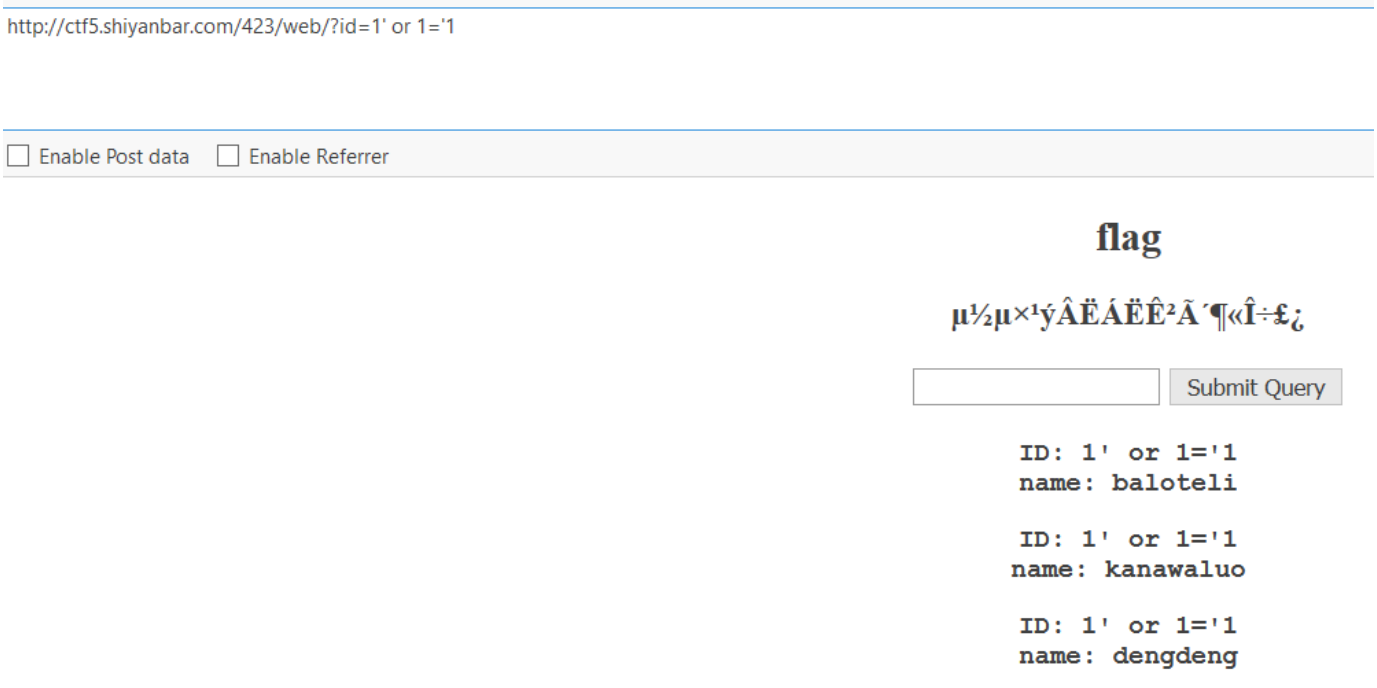
本文链接：https://blog.csdn.net/u014029795/article/details/97580883

又弄了一个，虽然说不难，但是这个有点蛋疼- -，有些地方坑了好久。。。

过程

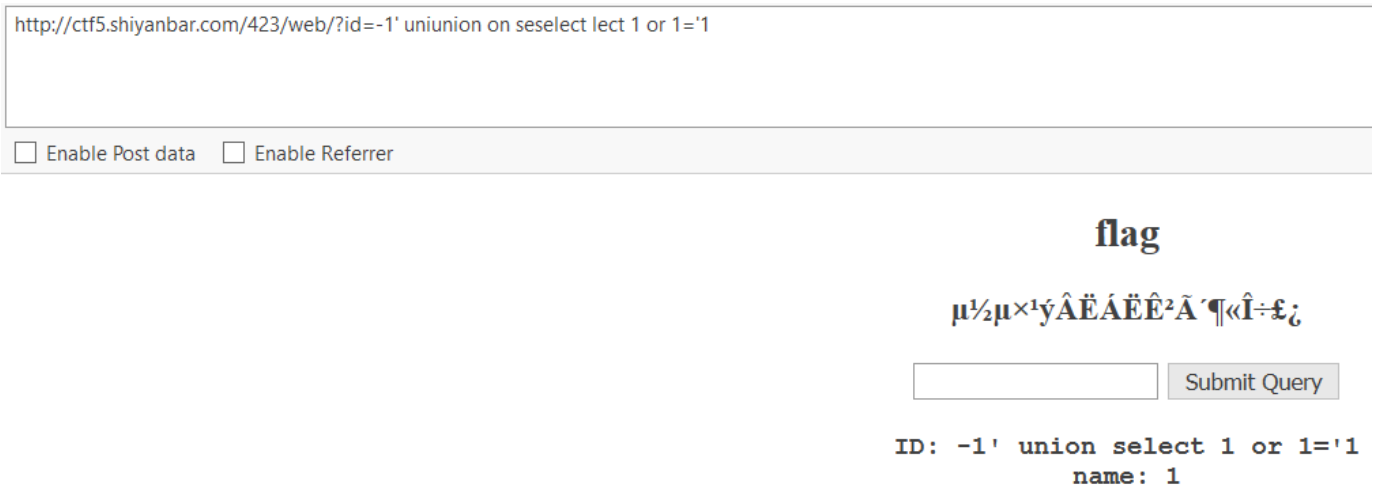
1. 一开始就是简单的输入数值进行查询，加引号后发现有报错。

2. 单引号闭合，试过了#和-- 都被过滤了，没法使用，所以试试自己闭合，这次是OK的。

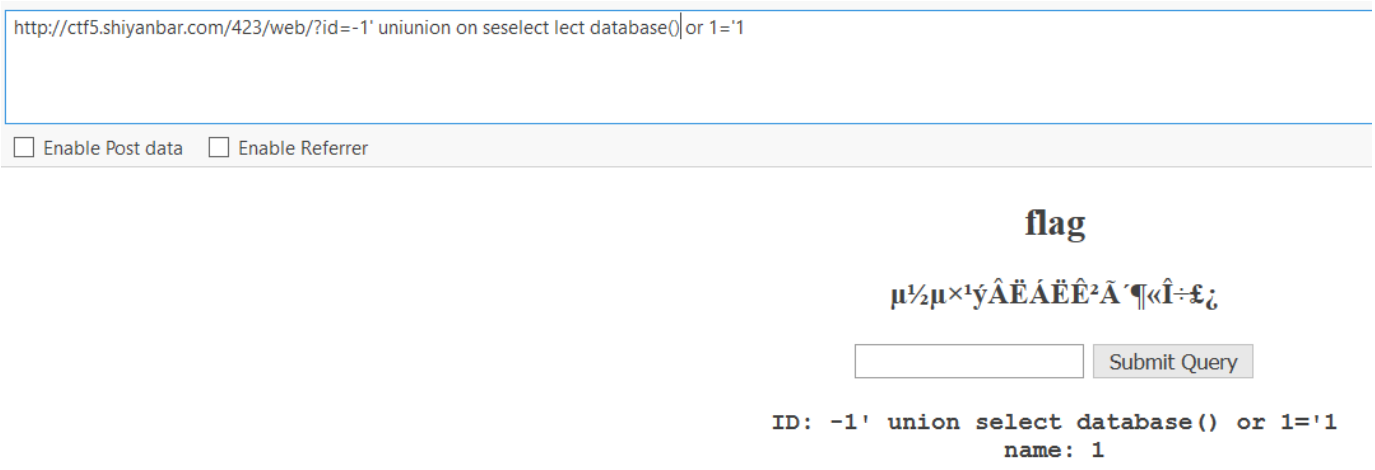


3. 回显点应该只有一个，就是name了，这里就不试order by了。直接union select，但是union select好像都被过滤了。试了下双写，发现过滤的时候如果最后不是空格就不会过滤，过滤的时候是连同关键字和关键字后的空格一起过滤的。。。

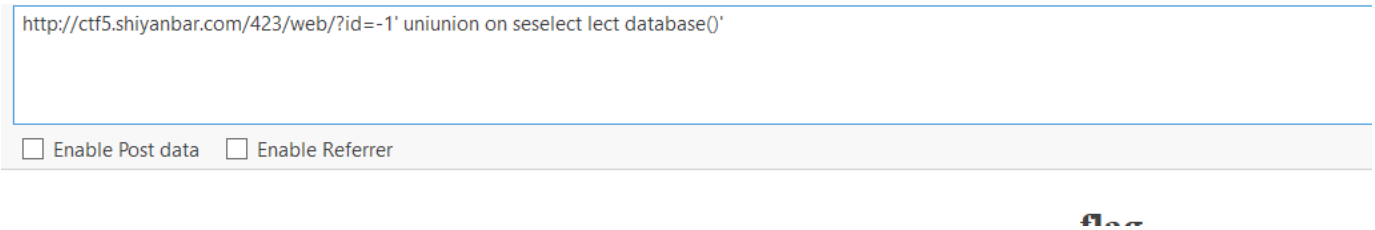
4. 于是我构造出了一种奇葩写法。。。后面查了下其它的writeup，确实发现挺奇葩，更好的方式是直接将空格用/**/代替掉，连双写都不需要使用，这里我还是写自己的方法吧。

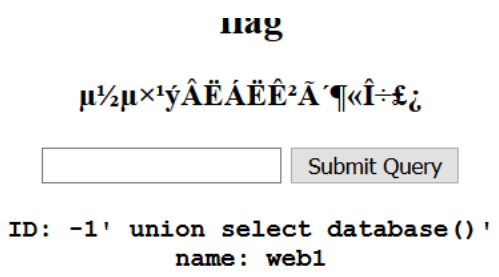


5. 将1换成database()，但是预想中的库名没到手。。。

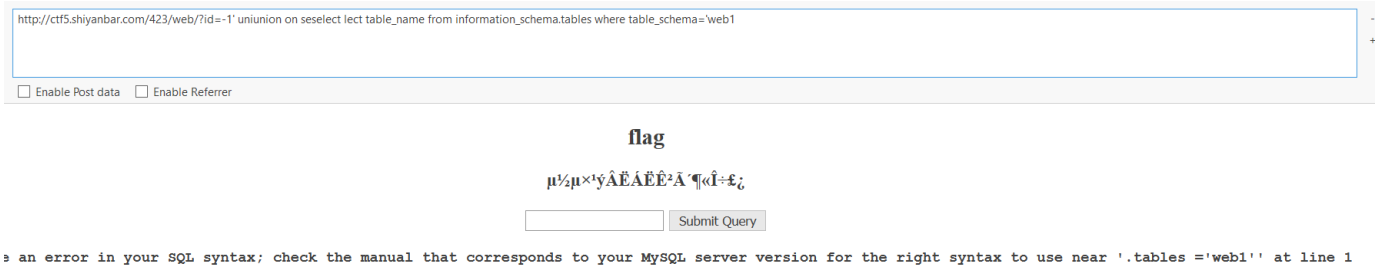


看了半天才发现，这里只有一个字段，后面的or 1=1和前面的字段一起恒等于1，所以不管查什么都是1，居然被只有一个字段的情况给坑了。。。最后试了半天，直接在database()后面加了个引号就成功了，库名为web1。。。

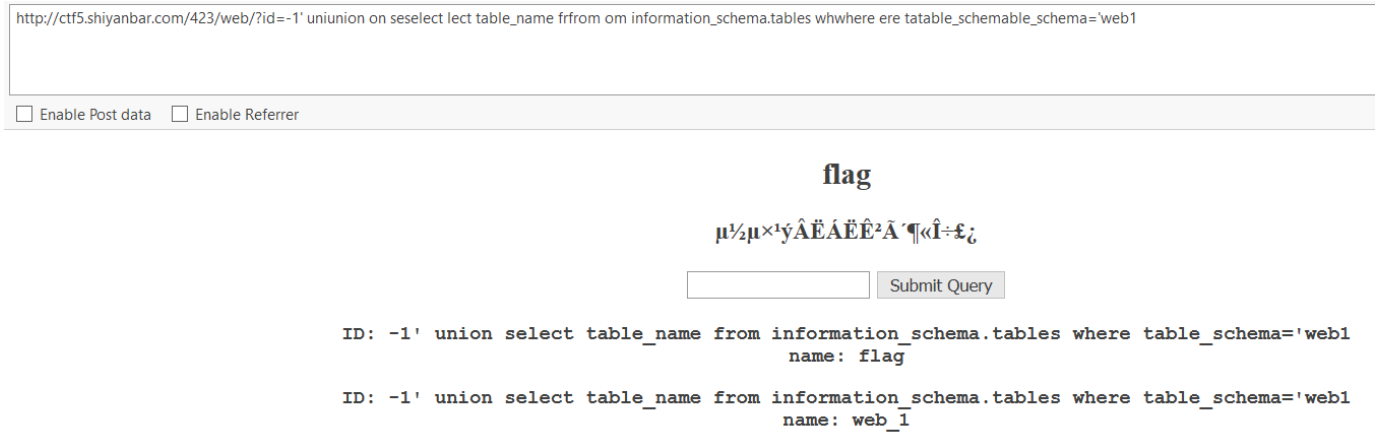




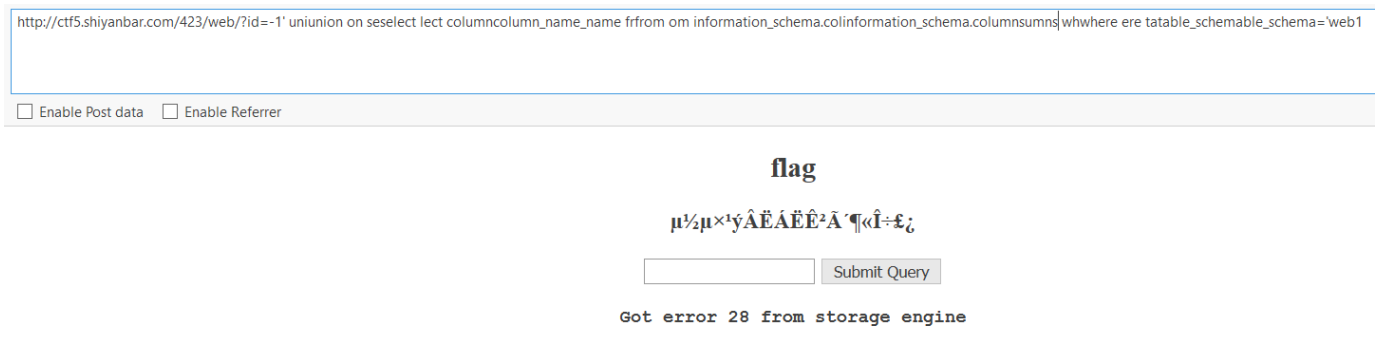
6. 继续来拿表，语句写好了后发现又被过滤了不少，从下图至少能看出来where，table_schema都被过滤了，前面的information_schema可能也过滤了，估计from也少不了。



7. 经过大量测试后(真的是超级大，其中from,where都是和之前一样过滤带上空格，information_schema是没有过滤的，table_schema是有过滤的)，发现过滤table_schema关键字时和之前不太一样，是不算上最后的空格的，得出以下payload。。。

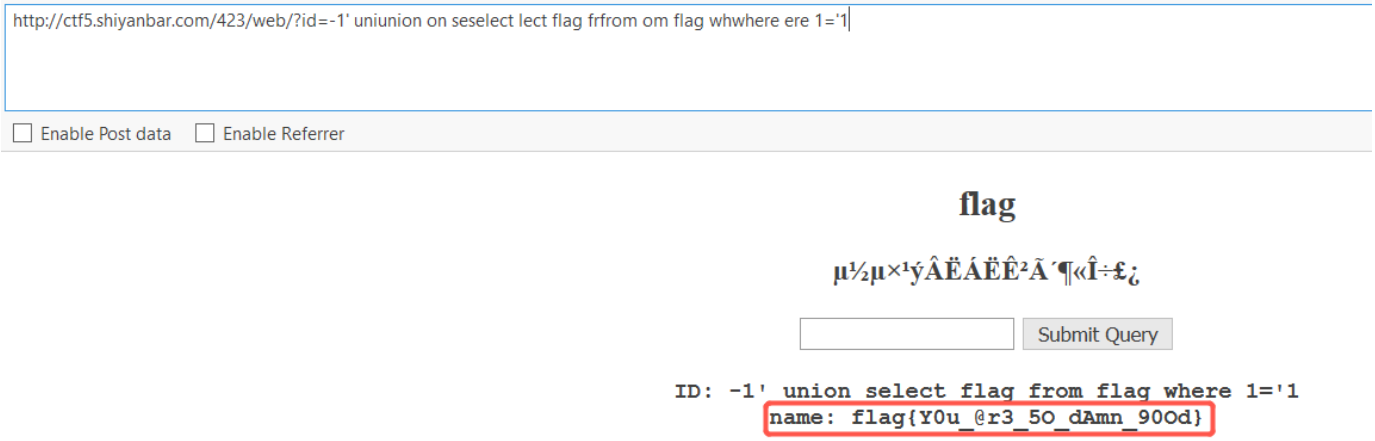


8. 终于是拿到了表名flag。。接下来拿字段，其实再继续猜就好了，有点恶心的是，过滤的字段又不一样了，column_name，information_schema.columns成了过滤的关键字，好不容易搞好了，结果题目出Bug了，查了下，有不少人出了这个情况，我这里确信我的语句没有问题，并且也拿其它成功的payload试过了，会有同样的报错发生，所以这里只能“借”其他人的字段来使用了，这里的字段也。。。



9. 知道了表名和字段名都是flag，所以直接拿值就好。

这里还是蛮奇怪的，之前拿database()的时候最后直接加单引号可以闭合，到这就闭合不了，不晓得是为啥。。。当然，换个方法就行了。



总结

感觉还是蛮顺利的，就是有些地方挺怪，也从其它WriteUp那里学到了一些方法，虽然我这个方法写有点丑，但是还是挺好用的，目前还没看到有人和我这样的写法。。。