

【网络安全实验】解决 ERROR 1064 (42000): You have an error in your SQL syntax ... near ...

原创

[一百个Chocolate](#) 于 2020-06-11 15:50:17 发布 8178 收藏 1

分类专栏: [「秋招清单」前端的心路历程](#) 文章标签: [mysql](#) [数据库](#) [java](#) [sql](#) [oracle](#)

原则上允许部分内容转载, 转载请注明原文章地址!

本文链接: https://blog.csdn.net/weixin_42429718/article/details/106690378

版权



[「秋招清单」前端的心路历程](#) 专栏收录该内容

19 篇文章 2 订阅

订阅专栏

背景

今天做网络安全的时候, 遇到了这个错误, 这个问题之前遇到过几次, 但是总是会因为疏忽又相遇, 今天把这个问题写出来, 加深印象吧。

任务

操作4: 联合查询猜字段数

```
联合查询字段数量不同: select user,password from users union select
user,password from mysql.user;
猜前面的查询字段数
select user,first_name,password from users union select 1;
select user,first_name,password from users union select 1,2;
....
```

报错如下:

```
select user,password from users union select user,password from mysql.user;
ERROR 1064 (42000): 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 'select user,first_name,password from users union select user,passwo
rd from ' at line 1
```

解决

其实这个问题就是语法上的错误, 在MySQL中, 为了区分MySQL的关键字与普通字符, MySQL引入了一个反引号。

详情见: [传送门](#)

反引号不知道在哪？（快看下面这张图吧...）



```
select `user`,`password` from users union select `user`,`password` from mysql.user;
```

再次运行就不会报错了

```
mysql> select `user`,`password` from users union select `user`,`password` from mysql.user;
```

user	password
admin	21232f297a57a5a743894a0e4a801fc3
gordonb	e99a18c428cb38d5f260853678922e03
1337	8d3533d75ae2c3966d7e0d4fcc69216b
pablo	0d107d09f5bbe40cade3de5c71e9e9b7
smithy	5f4dcc3b5aa765d61d8327deb882cf99
user	ee11cbb19052e40b07aac0ca060c23ee
root	*73316569DAC7839C2A784FF263F5C0ABBC7086E2
root	*D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F
debian-sys-maint	*75F15FF5C9F06A7221FEB017724554294E40A327
phpmyadmin	*D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F
vicnum	*C7847100CDBE29050A338F78EA71F066D196ED98
wordpress	*C260A4F79FA905AF65142FFE0B9A14FE0E1519CC
phpbb	*CA1F8B0798B2857835107EA008871B4691769547
dvwa	*D67B38CDD1A55623ED5F55856A29B9654FF823D
mutillidae	*E82A07F59B0D83BEF29F79E41FA0F8A042CE3DE4
yazd	*3758F91540524F48F92FE932883C54F6E802A13A
personalblog	*3D118FD3FFC74F534A493C30ADC1F23A48510D9D
yazd10	*30B462BE16C04867D06113304F664BB9A5B57308
peruggia	*5297BE816CC703E8CB686D205071E9CD9E8F08A4

https://blog.csdn.net/weixin_42429718

学如逆水行舟，不进则退