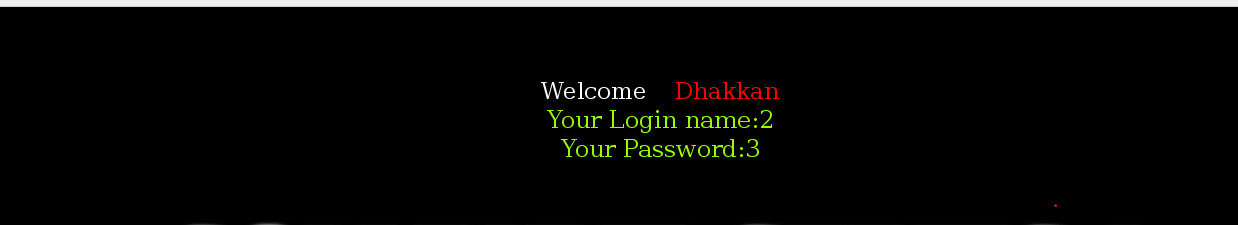
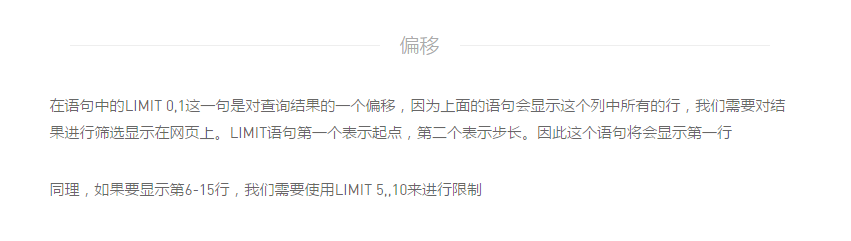
1. 为什么我的缺少黄色字段呀？是用什么显示出了那条查询代码啊？



你的blog

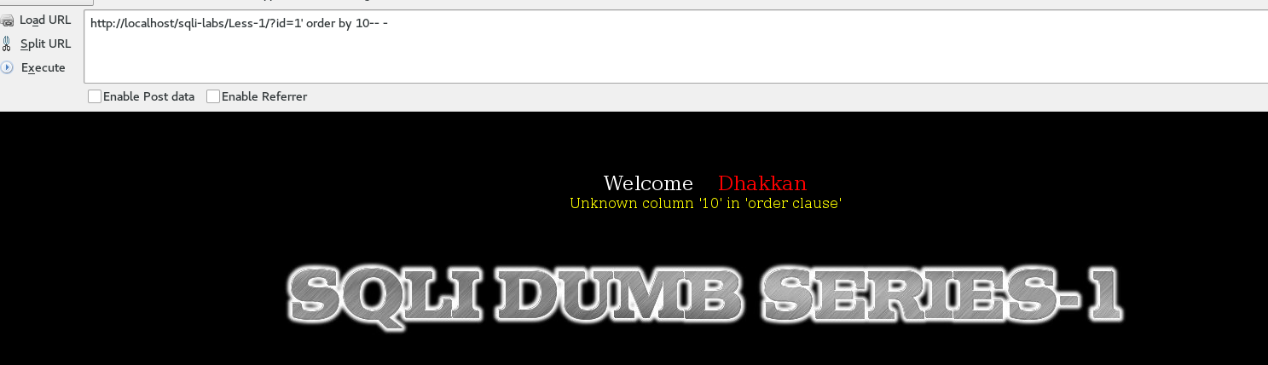


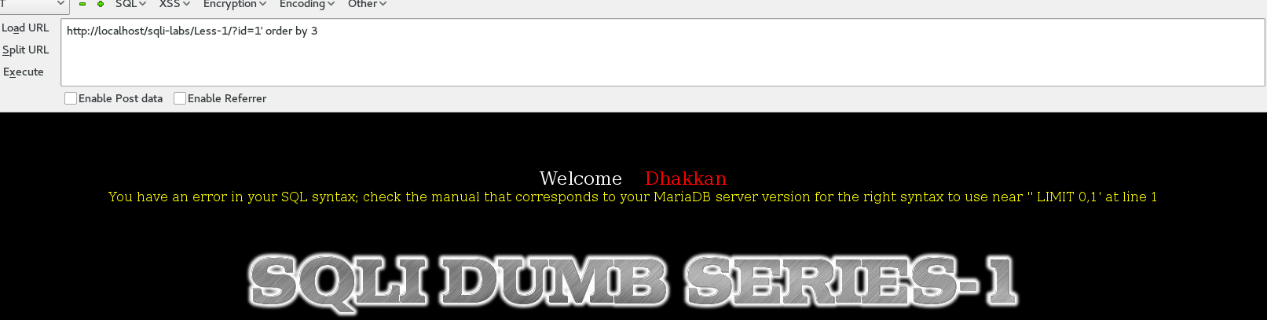
我的sql-labs

1. 没有看懂这个偏移，不能理解(。﹏。\*)，看到后面可以获取表名是为什么啊？
2. 引号未闭合导致单引号报错的原因是什么？
3. 留存留存，呆会查

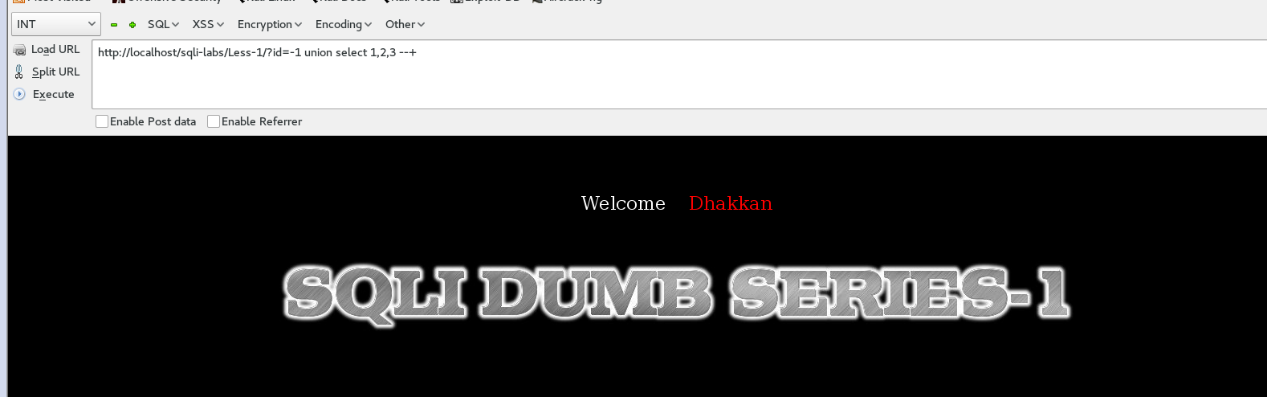


1. 为啥order by后面一定要有注释呢？-- -或者+--+，不用注释就会有偏移的那个错误

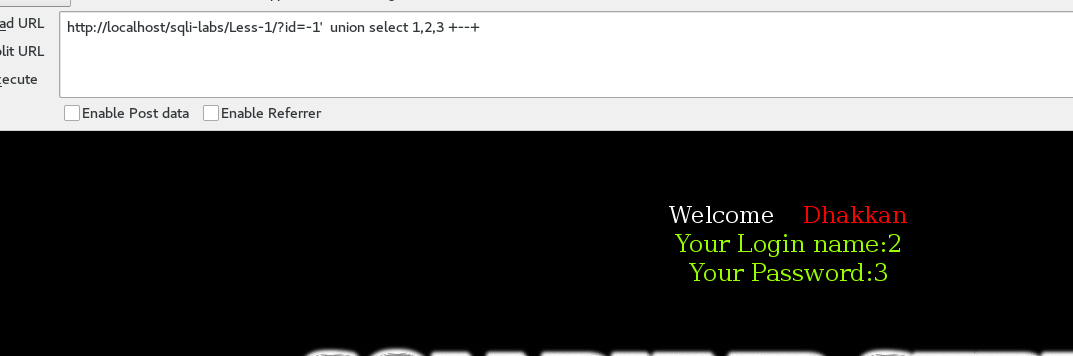




1. 为什么无论是使用order by还是union select都需要?id=-1’，主要是为什么要打单引号，-1是使结果为假，改成1和1’后就是报1的name和password，直接使用-1不爆，但是为什么一定要单引号呢？



还有这个union select查出来的是什么呢？2和3是之后显示信息在表单中的位置？怎么理解，2行3列？



1. 都查出来的是什么鬼啊啊啊啊啊啊啊！！！！！！！！！看不懂啊！！！！！！！

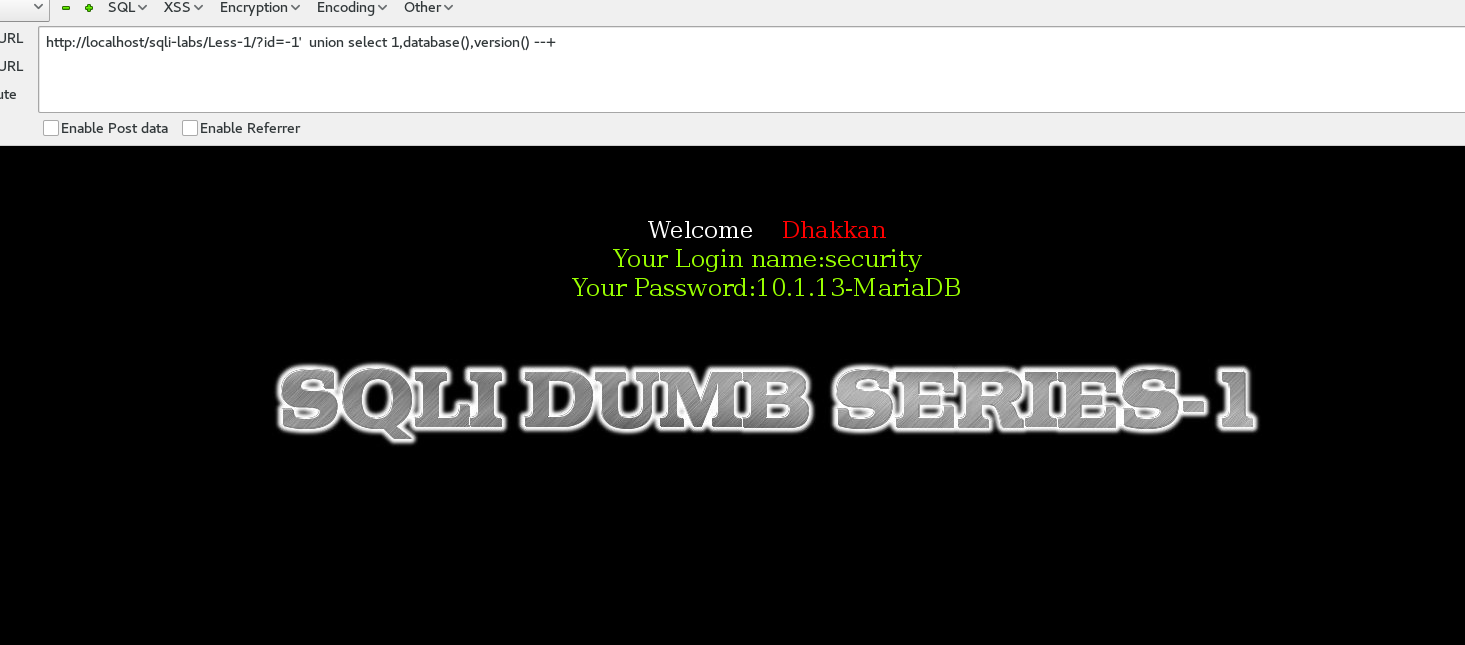
冷静冷静。

（这个没懂）union select 1是选择第一列么？因为只能显示两行数据么？

（这里搞定）database()不是数据库信息么？可是返回根本看不出一点点数据库信息啊，version()也看不出版本信息啊！！！！！！悲伤地捂脸

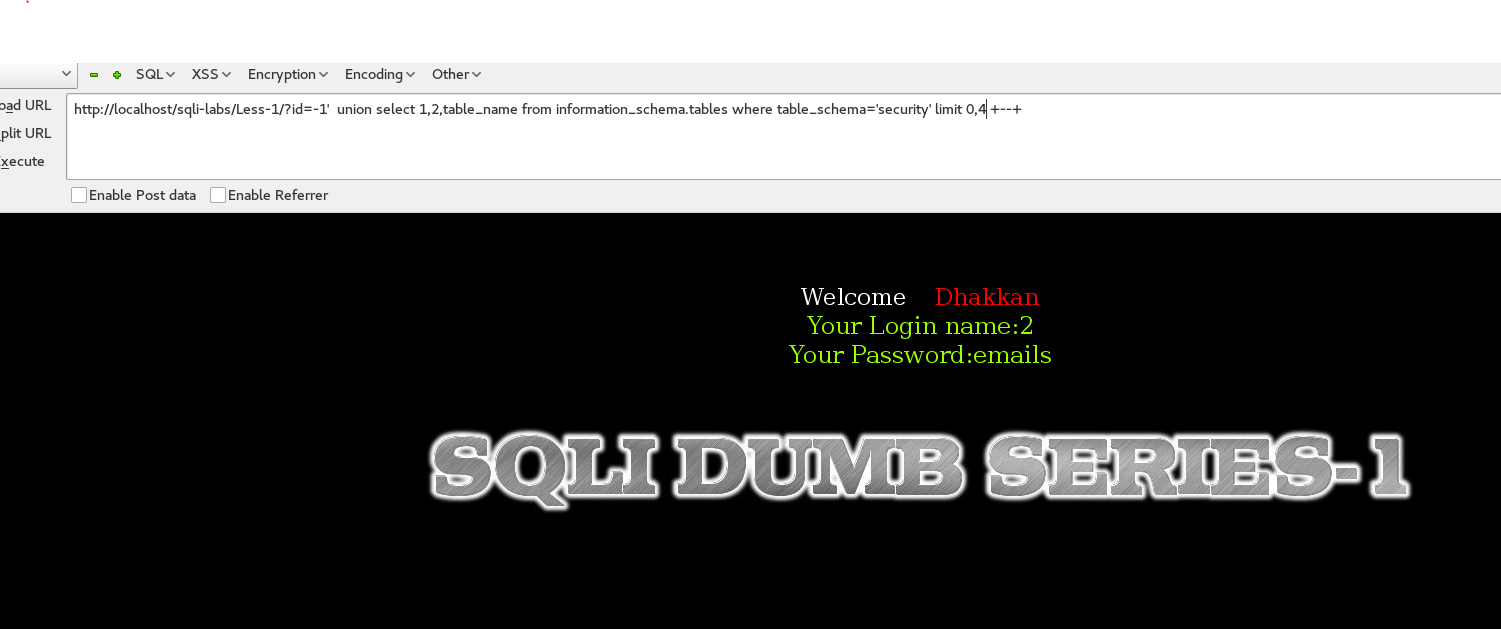
另外是必须把database()函数和其他函数连用么？不连用就会报错

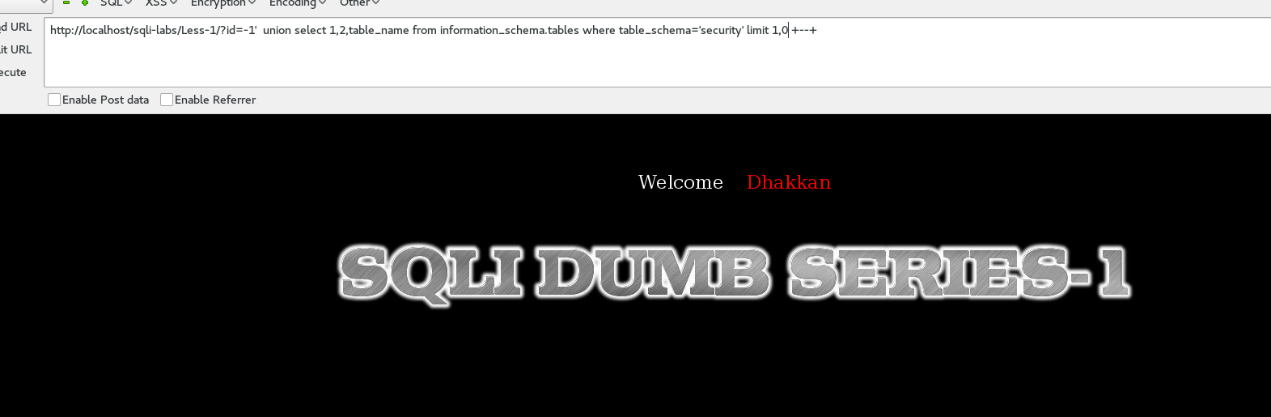
Password就是答案，那name那里表示的就是数据库名，security表示数据库名。



1. 4个表名，emials , referrers, uagents, users,

更改limit x,y的y值为正整数没有变化的，0的话无显示，这个代表什么？



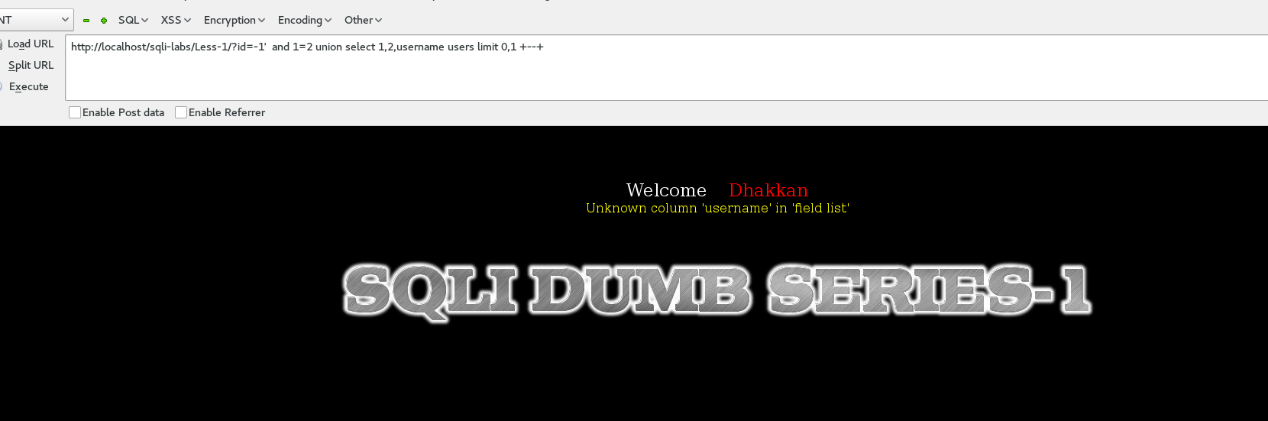


table\_name是表，column\_name 是列名？所以我上面问的没变化是因为table\_name只能查询表名么？

1. <http://www.111cn.net/database/mysql/47633.htm>

CONCAT\_WS与CONCAT()用法

1. 这个语句什么都怼不出。。。。



1.黄色字段（噫…）是后来改的源码，为了方便查看，在PHP文件里加了一个echo

2.如果查询的结果有10条，但你只能显示一条，你就要用偏移去控制你要显示哪一条

3.在后面加了一个引号的话他就有三个单引号了，就有一个没闭合，这是语法错误呀，SQL语法错了所以会报错

4.那个是你语法输错了，语句构造的不对

5.因为原来的语句里面会加上偏移，但你用order by的话就没有查询，因此不能和偏移语句一起使用，所以需要注释掉

6.加引号是为了闭合前面的，如果不闭合的话就会让后面的内容和前面的1合在一起，构成字符串的一个部分，就不会被SQL理解为命令去执行，union select后面的123是随便的几个数，你可以改一下，只是为了看在页面上哪些元素会被显示出来

7.…………………………你不要再用上面写的name和password混淆自己了，他本来是name和password，但你要查出他不让你查的东西啊，只是借了个位置去显示而已，和它有啥关系

查询资料：

<https://shawnleon.github.io/2016/08/02/sql-1-GET-Error-based-single-quotes-String/>

<http://mt.sohu.com/20160823/n465519340.shtml>

<http://www.lai18.com/content/2141745.html>

<http://m.blog.csdn.net/article/details?id=52334264>