# 绕过过滤注释符的 sql 注入

## 1、mysql 的注释符

注释符的作用:用于标记某段代码的作用，起到对代码功能的说明作用。但是注释掉的内容不会被执行。
Mysql 中的注释符:
1、单行注释:
--+或--空格或#
2、多行注释: /*多行注释内容*/
对于正常的 SQL 语句中，注释符起到说明作用的功能。但是对于在利用 SQL 注入漏洞过程中，注释符起到闭合单引号、多单引号、双引号、单括号、多括号的功能。

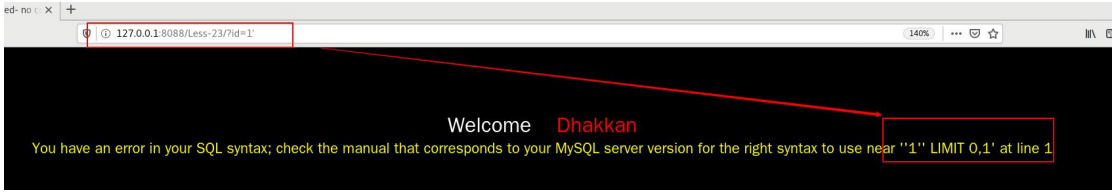
## 2、过滤注释符的代码分析

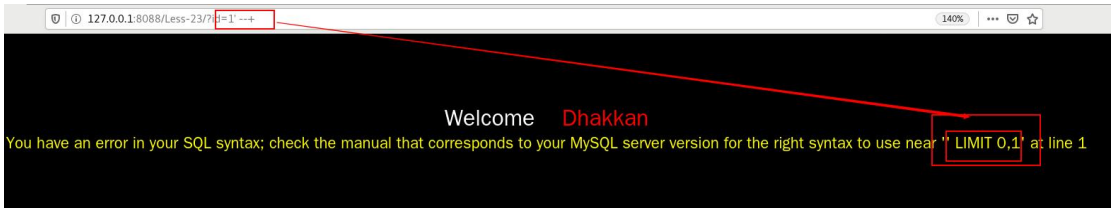
preg_ replace(mixed $pattern, mixed $replacement, mixed $subject):执行一个正则表达式的搜索和替换。
$pattern:要搜索的模式，可以是字符串或一个字符串数组
$replacement:用于替换的字符串或字符串数组。
$subject:要搜索替换的目标字符串或字符串数组。

```
// take the variables
if(isset($_GET['id']))
{
$id=$_GET['id'];

//filter the comments out so as to comments should not work
$reg = "/#/";
$reg1 = "/--/";
$replace = "";                                    替换掉注释
$id = preg_replace($reg, $replace, $id);
$id = preg_replace($reg1, $replace, $id);
//logging the connection parameters to a file for analysis.
$fp=fopen('result.txt','a');
fwrite($fp,'ID:'.$id."\n");
fclose($fp);
```

输入如下，报错，多一个单引号






## 3、绕过过滤注释符的 sql 注入

利用注释符别过滤不能成功闭合单引号等，换一种思路利用 or ’1’=’1 闭合单引号等。

http://127 .0.0.1/sqli/Less-23/?id=-1%27%20union%20select%201 ,database(),%273


或者


这里配合联合查询，然后用 3 之前的单引号闭合语句中的单引号。