mysql_real_escape_string()这个函数是 PHP 过滤的常见函数,可以转义 SQL 语句中使用的字符串中的特殊字符。

- \x00
- \n
- \r
- \
- '
- "
- \x1a

如果成功，则该函数返回被转义的字符串。如果失败，则返回 false。

\x00相当于空，但和空是有区别的

```
>>> a='\x00'
>>> b=''
>>> print a

>>> print b

>>> a==b
False
>>> len(a)
1
>>> len(b)
0
>>> a[0]
'\x00'
>>> a[1]
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
IndexError: string index out of range
>>>
```

在《注入天书》中提到：

但是因 MySQL 我们并没有设置成 GBK，所以 `mysql_real_escape_string()`依旧能够被突破，方法和上述 `addslashes()`是一样的。

在使用mysql_real_escape_string()时，若想防范这种问题，需要将MySQL 设置为 GBK：

```
Mysql_set_charset('gbk','$conn')
```

绕过方法和Less32中的相同，用%bb%27和%bb%5c%5c%27均可绕过'过滤

Less36是get型，37是post型，其余都一样