Atitit 防止sql注入 函数过滤函数过滤法

虽然可以用mysql\_real\_escape\_string()函数过滤用户提交的值，但是也有缺陷。而使用PHP的PDO扩展的 prepare 方法，就可以避免 sql injection 风险。

mysql\_real\_escape\_string() 函数转义 SQL 语句中使用的字符串中的特殊字符。

下列字符受影响：

* \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。

防数据库攻击的正确做法：

<?php

function check\_input($value)

{// 去除斜杠

if (get\_magic\_quotes\_gpc())

{

$value = stripslashes($value);

}// 如果不是数字则加引号

if (!is\_numeric($value))

{

$value = "'" . mysql\_real\_escape\_string($value) . "'";

}

return $value;

}