Atitit 安全pdo执行sql法

### 范例[¶](https://www.php.net/manual/zh/pdo.prepare.php" \l "refsect1-pdo.prepare-examples)

**Example #1 用命名参数形式准备 SQL 语句参数**

<?php  
/\* 传入数组的值，并执行准备好的语句 \*/  
$sql = 'SELECT name, colour, calories  
    FROM fruit  
    WHERE calories < :calories AND colour = :colour';  
$sth = $dbh->prepare($sql, array(PDO::ATTR\_CURSOR => PDO::CURSOR\_FWDONLY));  
$sth->execute(array(':calories' => 150, ':colour' => 'red'));  
$red = $sth->fetchAll();  
$sth->execute(array(':calories' => 175, ':colour' => 'yellow'));  
$yellow = $sth->fetchAll();  
?>

**Example #2 用问号形式准备 SQL 语句参数**

<?php  
/\* 传入数组的值，并执行准备好的语句 \*/  
$sth = $dbh->prepare('SELECT name, colour, calories  
    FROM fruit  
    WHERE calories < ? AND colour = ?');  
$sth->execute(array(150, 'red'));  
$red = $sth->fetchAll();  
$sth->execute(array(175, 'yellow'));  
$yellow = $sth->fetchAll();  
?>

<?php  
/\* 通过绑定的 PHP 变量执行一条预处理语句  \*/  
$calories = 150;  
$colour = 'red';  
$sth = $dbh->prepare('SELECT name, colour, calories  
    FROM fruit  
    WHERE calories < :calories AND colour = :colour');  
$sth->bindParam(':calories', $calories, PDO::PARAM\_INT);  
$sth->bindParam(':colour', $colour, PDO::PARAM\_STR, 12);  
$sth->execute();  
?>

**Example #2 执行一条使用问号占位符的预处理语句**

<?php  
/\*  通过绑定的 PHP 变量执行一条预处理语句 \*/  
$calories = 150;  
$colour = 'red';  
$sth = $dbh->prepare('SELECT name, colour, calories  
    FROM fruit  
    WHERE calories < ? AND colour = ?');  
$sth->bindParam(1, $calories, PDO::PARAM\_INT);  
$sth->bindParam(2, $colour, PDO::PARAM\_STR, 12);  
$sth->execute();  
?>

PHP\_ PDO\_\_prepare - Manual.html