MySQL 处理重复数据 MySQL 导出数据

MySQL 及 SQL 注入

如果您通过网页获取用户输入的数据并将其插入一个MySQL数据库，那么就有可能发生SQL注入安全的问题。

本章节将为大家介绍如何防止SQL注入，并通过脚本来过滤SQL中注入的字符。

所谓SQL注入，就是通过把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。

我们永远不要信任用户的输入，我们必须认定用户输入的数据都是不安全的，我们都需要对用户输入的数据进行过滤处理。

以下实例中，输入的用户名必须为字母、数字及下划线的组合，且用户名长度为 8 到 20 个字符之间：

```
if (preg_match("/^\w{8,20}$/", $_GET['username'], $matches))
{
   $result = mysqli_query($conn, "SELECT * FROM users
                           WHERE username=$matches[0]");
}
 else
{
   echo "username 输入异常";
}
```

让我们看下在没有过滤特殊字符时，出现的SQL情况：

```
// 设定$name 中插入了我们不需要的SQL语句
$name = "Qadir'; DELETE FROM users;";
 mysqli_query($conn, "SELECT * FROM users WHERE name='{$name}'");
```

以上的注入语句中，我们没有对 $name 的变量进行过滤，$name 中插入了我们不需要的SQL语句，将删除 users 表中的所有数据。

在PHP中的 mysqli_query() 是不允许执行多个 SQL 语句的，但是在 SQLite 和 PostgreSQL 是可以同时执行多条SQL语句的，所以我们对这些用户的数据需要进行严格的验证。

防止SQL注入，我们需要注意以下几个要点：

- 1.永远不要信任用户的输入。对用户的输入进行校验，可以通过正则表达式，或限制长度；对单引号和 双"-"进行转换等。
- 2.永远不要使用动态拼装sql，可以使用参数化的sql或者直接使用存储过程进行数据查询存取。
- 3.永远不要使用管理员权限的数据库连接，为每个应用使用单独的权限有限的数据库连接。
- 4.不要把机密信息直接存放，加密或者hash掉密码和敏感的信息。
- 5.应用的异常信息应该给出尽可能少的提示，最好使用自定义的错误信息对原始错误信息进行包装

- 6.sql注入的检测方法一般采取辅助软件或网站平台来检测，软件一般采用sql注入检测工具jsky，网站平台就有亿思网站安全平台检测工具。MDCSOFT SCAN等。采用MDCSOFT-IPS可以有效的防御SQL注入，XSS攻击等。

防止SQL注入

在脚本语言，如Perl和PHP你可以对用户输入的数据进行转义从而来防止SQL注入。

PHP的MySQL扩展提供了mysqli_real_escape_string()函数来转义特殊的输入字符。

```
if (get_magic_quotes_gpc())
{
  $name = stripslashes($name);
}
$name = mysqli_real_escape_string($conn, $name);
 mysqli_query($conn, "SELECT * FROM users WHERE name='{$name}'");
```

Like语句中的注入

like查询时，如果用户输入的值有"_"和"%"，则会出现这种情况：用户本来只是想查询"abcd_"，查询结果中却有"abcd_"、"abcde"、"abcdf"等等；用户要查询"30%"（注：百分之三十）时也会出现问题。

在PHP脚本中我们可以使用addcslashes()函数来处理以上情况，如下实例：

```
$sub = addcslashes(mysqli_real_escape_string($conn, "%something_"), "%_");
// $sub == \%something\_
 mysqli_query($conn, "SELECT * FROM messages WHERE subject LIKE '{$sub}%'");
```

addcslashes() 函数在指定的字符前添加反斜杠。

语法格式:

```
addcslashes(string,characters)
```

参数	描述
string	必需。规定要检查的字符串。
characters	可选。规定受 addcslashes() 影响的字符或字符范围。

具体应用可以查看：PHP addcslashes() 函数

← MySQL 处理重复数据 MySQL 导出数据 →

点我分享笔记