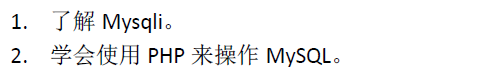
**2015-2016中山大学本科生实验报告**

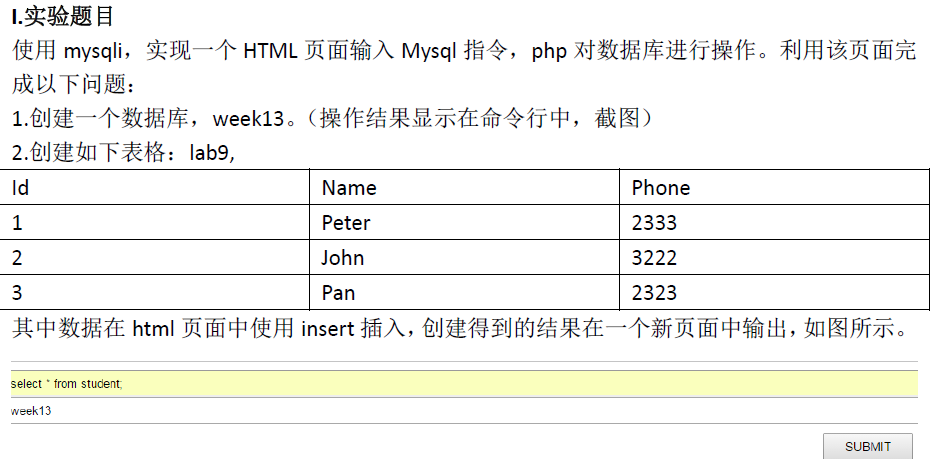
**科目**：数据库系统实验 **教师：**郑贵锋

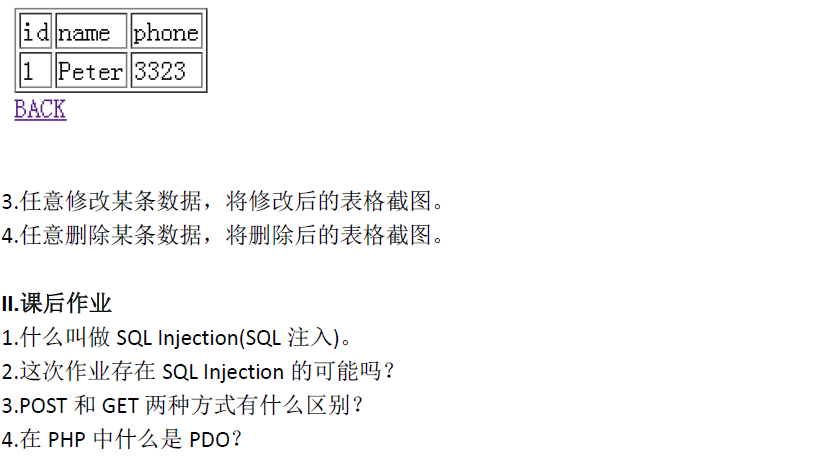
|  |  |  |  |
| --- | --- | --- | --- |
| 年级 | 13级 | 专业（方向） | 移动信息工程 |
| 学号 | 13354485 | 姓名 | 朱琳 |
| 电话 | 13726231932 | Email | [280273861@qq.com](mailto:280273861@qq.com) |

**一 实验目的**



**二 实验内容**

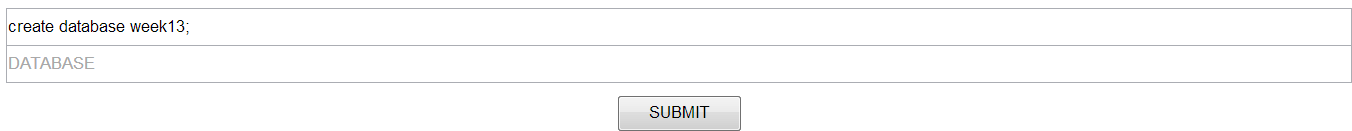


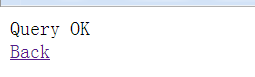


**三 实验结果**

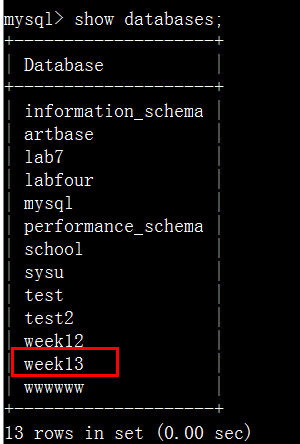
**1.创建一个数据库，week13。（操作结果显示在命令行中，截图）**

**(1)html中操作结果**



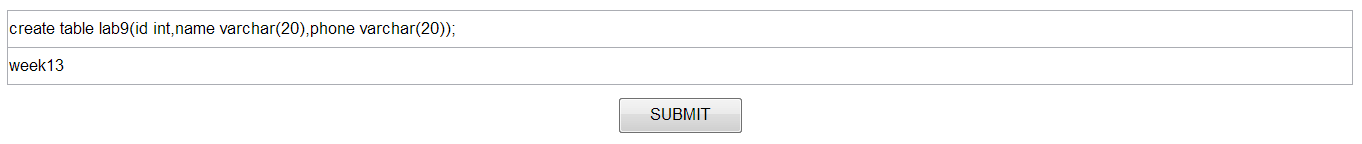


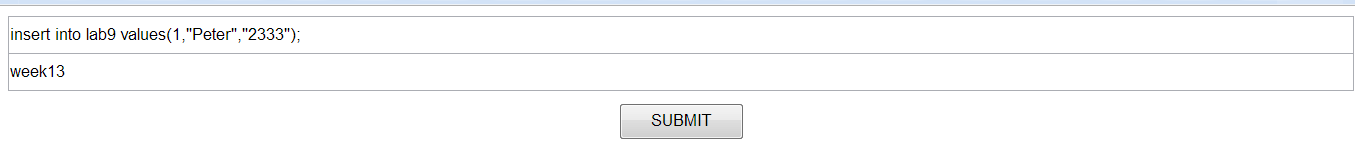
1. **命令行结果：**

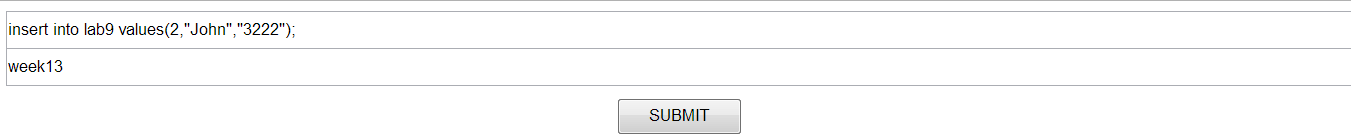


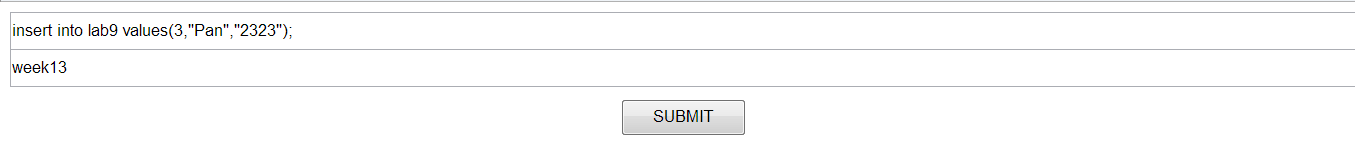
1. **创建如下表格：lab9**

**(1)操作：**





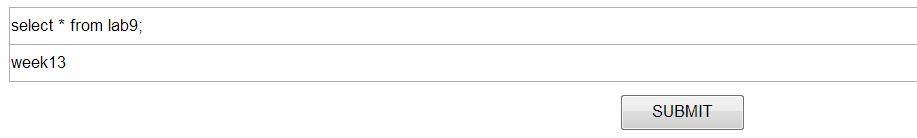




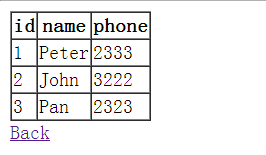
**结果均为：**



**(2)现在查看插入情况：**



**(3)点击submit之后：**



**3.任意修改某条数据，将修改后的表格截图。**

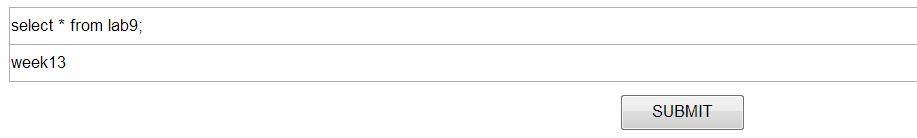
**(1)html运行：**

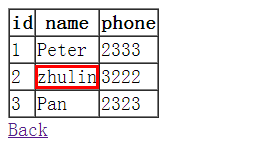


**(2)执行结果：**



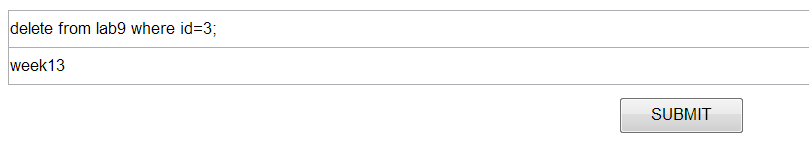
1. **查看执行结果**





**4.任意删除某条数据，将删除后的表格截图。**

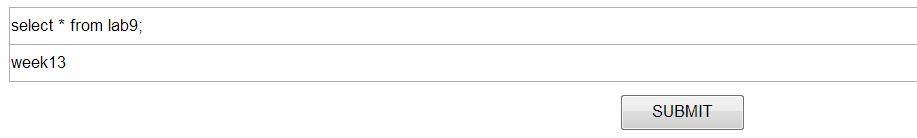
**(1)html执行：**

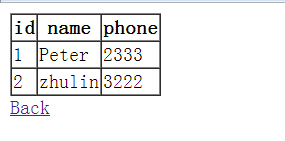


**(2)执行结果：**



1. **查看执行结果：**





**四 课后作业解答**

1. **什么叫做SQL Injection(SQL注入)。**

SQL注入攻击是黑客对数据库进行攻击的常用手段之一。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的SQL Injection。SQL注入是从正常的WWW端口访问，而且表面看起来跟一般的Web页面访问没什么区别，所以目前市面的防火墙都不会对SQL注入发出警报，如果管理员没查看IIS日志的习惯，可能被入侵很长时间都不会发觉。但是，SQL注入的手法相当灵活，在注入的时候会碰到很多意外的情况，需要构造巧妙的SQL语句，从而成功获取想要的数据。

1. **这次作业存在SQL Injection的可能吗？**

存在。很明显，我们并没有对html中输入的字符串做任何的处理，并且我们使用安全性较低的GET方法，安全性大大下降。

1. **POST和GET两种方式有什么区别？**

|  |  |  |
| --- | --- | --- |
|  | **GET** | **POST** |
| **方式** | 从服务器上获取数据 | 向服务器传送数据。 |
| **过程** | get是把参数数据队列加到提交表单的ACTION属性所指的URL中，值和表单内各个字段一一对应，**在URL中可以看到** | post是通过HTTP post机制，将表单内各个字段与其内容放置在HTML HEADER内一起传送到ACTION属性所指的URL地址。**用户看不到这个过程。** |
| **服务器处理方式** | 服务器端用Request.QueryString获取变量的值 | 服务器端用Request.Form获取提交的数据。 |
| **数据传送量** | get传送的数据量较小，不能大于2KB | post传送的数据量较大，一般被默认为不受限制。 |
| **安全性** | get安全性非常低,但是执行效率却比Post方法好 | post安全性较高 |
| **数据集** | 限制Form表单的数据集的值必须为ASCII字符 | 支持整个ISO10646字符集。 |
| **备注** | 1、get方式的安全性较Post方式要差些，包含机密信息的话，建议用Post数据提交方式；  2、在做数据查询时，建议用Get方式；而在做数据添加、修改或删除时，建议用Post方式；  3.GET是Form默认方式 | |

**4.在PHP中什么是PDO？**

PHP Data Object,PHP数据对象，PDO扩展为PHP访问数据库定义了一个轻量级的、一致性的接口，它提供了一个数据访问抽象层，这样无论使用什么数据库，都可以通过一致的函数执行查询和获取数据，提高了数据库的安全性。

相比于Mysql和mysqli，其更具有安全性，简便性。

①PDO 连接数据库时通过 Connection String 来决定连接何种数据库。

②PDO 可以通过 PDO::setAttribute 来决定连接时的设定，比如 Persistent Connection，回传错误的方式（Exception，E\_WARNING，NULL）。甚至是回传参数名称的大小写等等。

③PDO 支持 Bind Column 的功能，除了基本的 Prepare，Execute 以外，也可以 Bind 单一参数，并且指定参数类型。

④PDO 是 Abstraction Layer，所以就算更换储存媒介，需要花的功夫比起来是最少的。

**五 实验感想**

1. 本次实验，主要是使用mysqli，在网页中输出想要的结果，其中操作数据库的操作需要表单来完成。不过之前对于表单接触比较少，因此用起来也没有那么得心应手，不过好在TA已经把html文件给出，我也就没有这个烦恼了。
2. 不过最开始我想通过JavaScript来控制数据的运输什么的（上周我是这样做的），后来发现麻烦，才知道TA已经给了一个html。
3. 一说到正则表达式，我就想起了java的正则表达式，然而运行之后发现并不行，我才知道php的正则跟java很不一样呀。需要用preg\_match(“/select.+/”,$sql)这种形式。而java中值需要$sql=”select%”什么的就行了。
4. 然后在网页上输出一个table什么的，因为jsp实验刚做了，也就没什么难度了。