《软件安全》实验报告

姓名：曹瑜　　学号：2212794　　班级：密码科学与技术

实验名称：

WEB 开发实践

实验要求：

复现课本第十章的实验三(10.3.5 节):利用 php，编写简单的数据库插入、查询和删除操作的示例。

基于课本的完整的例子，进一步了解 WEB 开发的细节

实验过程：

1、配置环境

在虚拟机 xp 中完成 PHPnow 的安装以及数据库连接

127.0.0.1
Let's PHP now !

为何只能本地访问?
此服务器互联网 IP
60.29.153.11

Server Information	
SERVER_NAME	127.0.0.1
SERVER_ADDR:PORT	127.0.0.1:80
SERVER_SOFTWARE	Apache/2.0.63 (Win32) PHP/5.2.14
PHP_SAPI	apache2handler
php.ini	C:\PHPnow-1.5.6\php-5.2.14-Win32\php-apache2handler.ini
网站主目录	C:/PHPnow-1.5.6/htdocs
Server Date / Time	2023-05-12 08:41:00 (+08:00)
Other Links	phpinfo() | phpMyAdmin

PHP 组件支持	
Zend Optimizer	Yes / 3.3.3
MySQL 支持	Yes / client lib version 5.0.90
GD library	Yes / bundled (2.0.34 compatible)
eAccelerator	No

MySQL 连接测试			
MySQL 服务器	localhost	MySQL 数据库名	test
MySQL 用户名	root	MySQL 用户密码	
			连接

MySQL 测试结果	
服务器 localhost	OK (5.0.90-community-nt)
数据库 test	OK

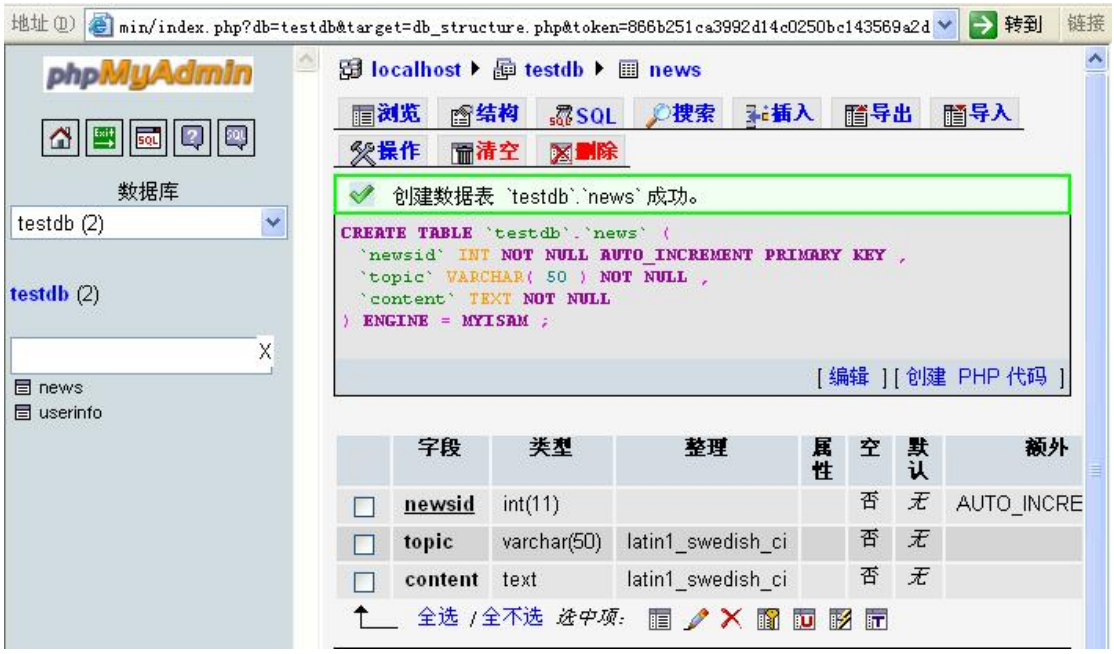
Valid XHTML 1.0 Strict / Copyleft ! 2007-? by PHPnow.org

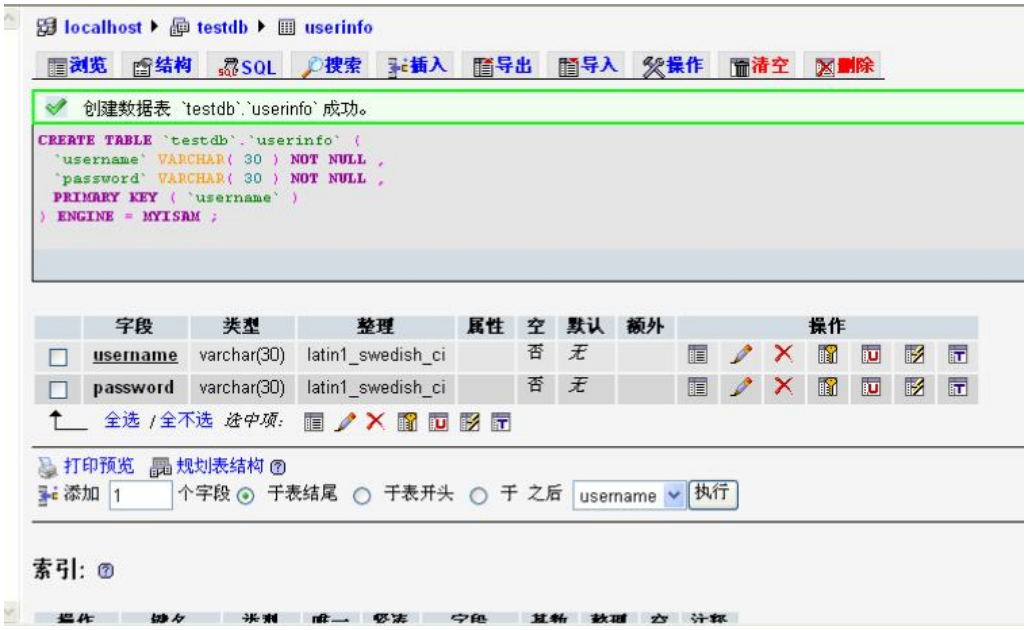
数据库管理系统：

2、复现实验三：

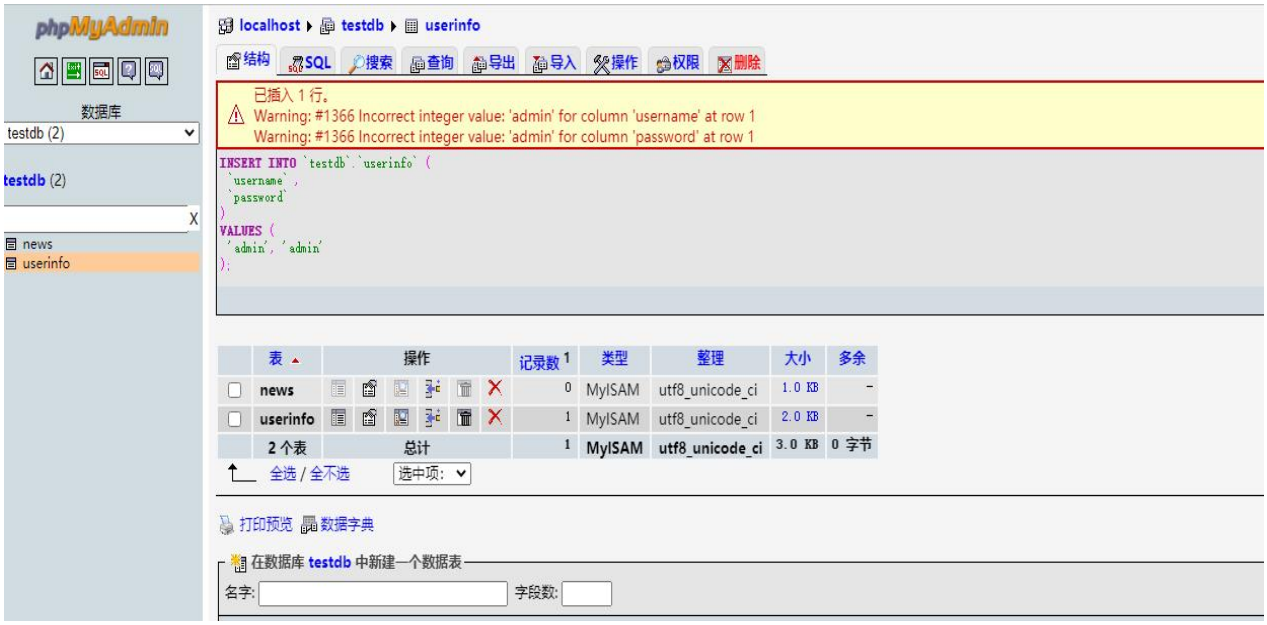
新建数据库：TestDB

表 1：News（newsid, topic, content） 表 2：userinfo（username, password）

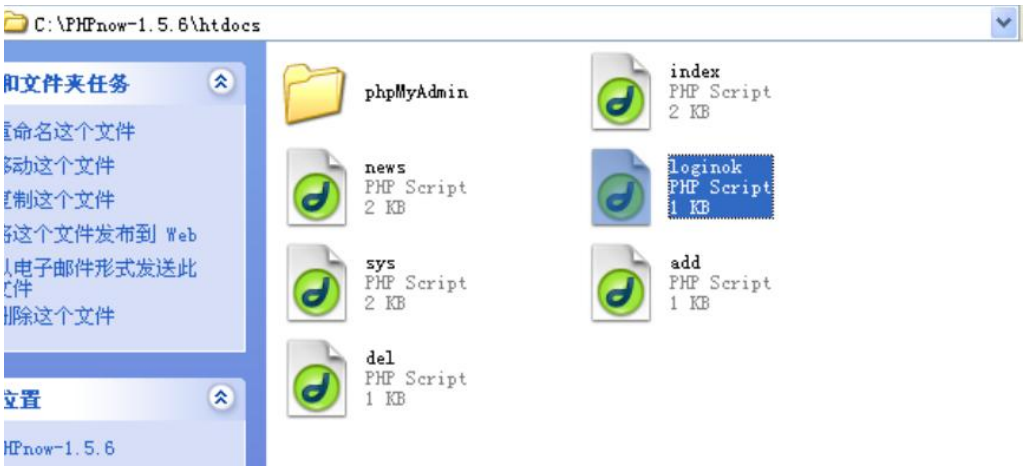




往表中插入数据：



使用 Dreamwaver 创建网页文件：



Web 程序编写：

所编辑的 login.htm 代码如下：

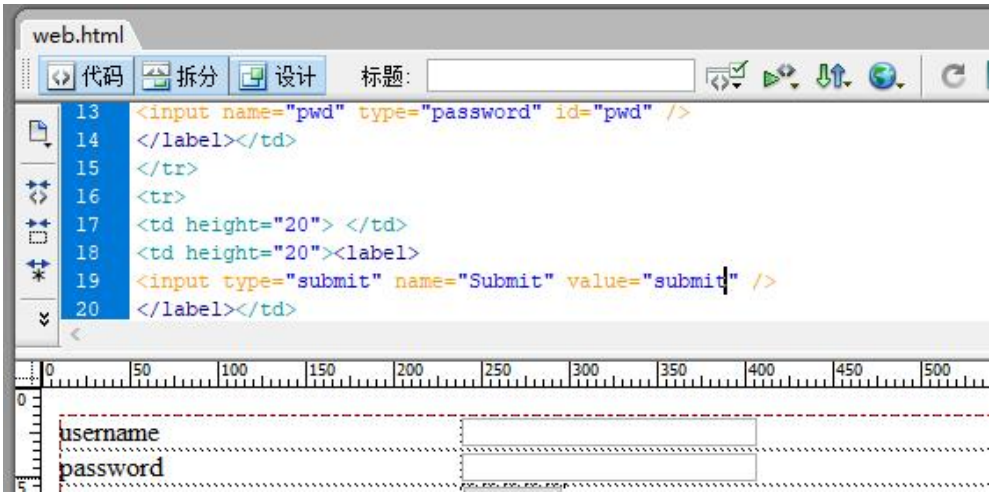
```
<html>
<body>
<form id="form1" name="form1" method="post" action="loginok.php">
<table width="900" border="0" cellspacing="0" cellpadding="0">
<tr>
<td height="20">姓名</td>
<td height="20"><label>
<input name="username" type="text" id="username" />
</label></td>
</tr>
<tr>
<td height="20">口令</td>
<td height="20"><label>
<input name="pwd" type="password" id="pwd" />
</label></td>
</tr>
<tr>
<td height="20"> </td>
<td height="20"><label>
<input type="submit" name="Submit" value="提交" />
</label></td>
```

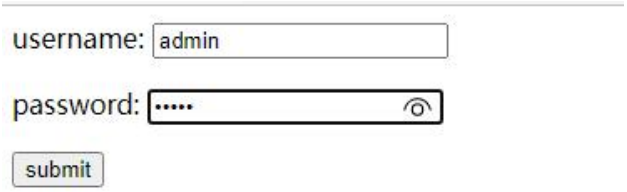
```
</tr>
</table>
</form>
</body>
</html>
```

在上面的页面中，定义了一个 form 表单。表单是一个包含表单元素的区域。表单区域里包含了两个文本框（<input>）、一个确认按钮(submit) 。确认按钮的作用是当用户单击确认 按钮时，表单的内容会被传送到另一个文件。而表单的动作属性(action)定义了目的文件的文件名。由动作属性定义的这个文件通常会对接收到的输入数据进行相关的处理。

在上面的表单中，定义了接受表单输入的处理文件为“loginok.php”，而 method 属性指定了与服务器进行信息交互的方法为 POST；

实际运行效果见下图：





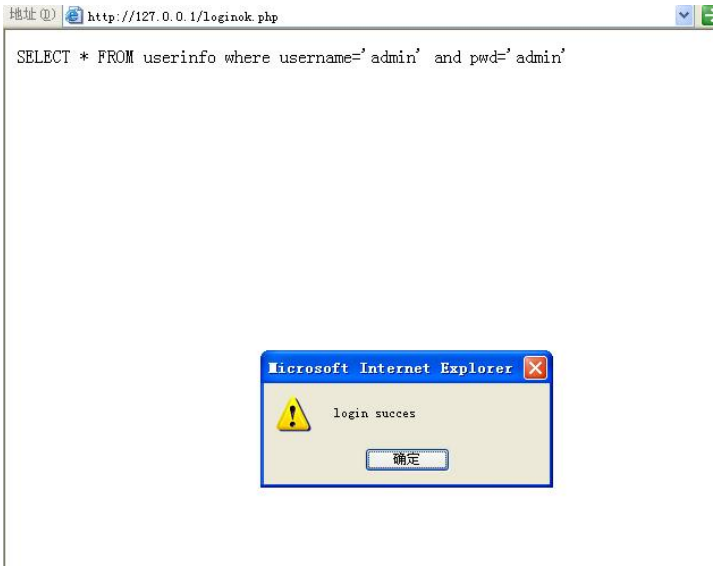
系统管理界面：

sys. php:

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>主页</title>
</head>
<?php
 $conn=mysql_connect("localhost", "root", "123456");
?>
```

```
<body>
<div align="center">
  <table width="900" border="0" cellspacing="0" cellpadding="0">
    <tr>
      <td height="40"><form id="form1" name="form1" method="post" action="add.php">
        <div align="right">新闻标题：
          <input name="topic" type="text" id="topic" size="50" />
          <BR>
          新闻内容：
          <textarea name="content" cols="60" rows="8" id="content"></textarea><BR>
          <input type="submit" name="Submit" value="添加" />
        </div>
      </form>
      </td>
    </tr>
    <tr>
      <td><hr /></td>
    </tr>
    <tr>
      <td height="300" align="center" valign="top"><table width="600" border="0" cellspacing="0" cellpadding="0">
        <tr>
          <td width="100" height="30"><div align="center">新闻序号</div></td>
          <td><div align="center">新闻标题</div></td>
          <td><div align="center">删除</div></td>
        </tr>
<?php
      $SQLStr = "select * from news";
      $result=mysql_db_query("testDB", $SQLStr, $conn);
      if ($row=mysql_fetch_array($result))//通过循环读取数据内容
      {
        // 定位到第一条记录
        mysql_data_seek($result, 0);
        // 循环取出记录
        while ($row=mysql_fetch_row($result))
        {
?>
 <tr>
```

```
            <td height="30"><div align="center"> <?php echo $row[0] ?> </div></td>
            <td width="400"> <div align="center"> <?php echo $row[1] ?>     </div></td>
            <td><div  align="center"><a  href="del.php?newsid=<?php  echo  $row[0]  ?>  " >    删除   </a>
</div></td>
          </tr>
<?php
            }
          }
?>
        </table></td>
      </tr>
    </table>
</div>
</body>
</html>

<?php
    // 释放资源
    mysql_free_result($result);
    // 关闭连接
    mysql_close($conn);
?>
```



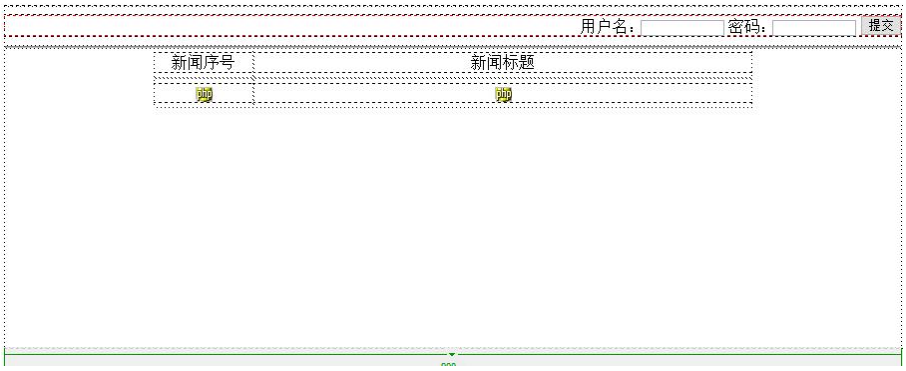
允许用户查看新闻和进行登录：

Index. php:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>主页</title>
</head>
<?php
 $conn=mysql_connect("localhost", "root", "123456");
?>
<body>
<div align="center">
  <table width="900" border="0" cellspacing="0" cellpadding="0">
    <tr>
      <td height="40"><form id="form1" name="form1" method="post" action="loginok.php">
        <div align="right">用户名：
          <input name="username" type="text" id="username" size="12" />
          密码：
          <input name="password" type="password" id="password" size="12" />
          <input type="submit" name="Submit" value="提交" />
        </div>
      </form>
      </td>
    </tr>
    <tr>
      <td><hr /></td>
    </tr>
    <tr>
      <td height="300" align="center" valign="top"><table width="600" border="0" cellspacing="0" cellpadding="0">
        <tr>
          <td width="100" height="30"><div align="center">新闻序号</div></td>
          <td><div align="center">新闻标题</div></td>
        </tr>
<?php
       $SQLStr = "select * from news";
       $result=mysql_db_query("testDB", $SQLStr, $conn);
       if ($row=mysql_fetch_array($result))//通过循环读取数据内容
       {
          // 定位到第一条记录
          mysql_data_seek($result, 0);
          // 循环取出记录
          while ($row=mysql_fetch_row($result))
          {
?>
 <tr>
          <td height="30"><div align="center"> <?php echo $row[0] ?> </div></td>
          <td> <div align="center"> <a href="news.php?newsid=<?php echo $row[0] ?> " > <?php echo $row[1] ?>  </a> </div></td>
        </tr>
<?php
          }
       }
?>
      </table></td>
    </tr>
```

```
  </table>
</div>
</body>
</html>

<?php
    // 释放资源
    mysql_free_result($result);
    // 关闭连接
    mysql_close($conn);
?>
```

运行效果：

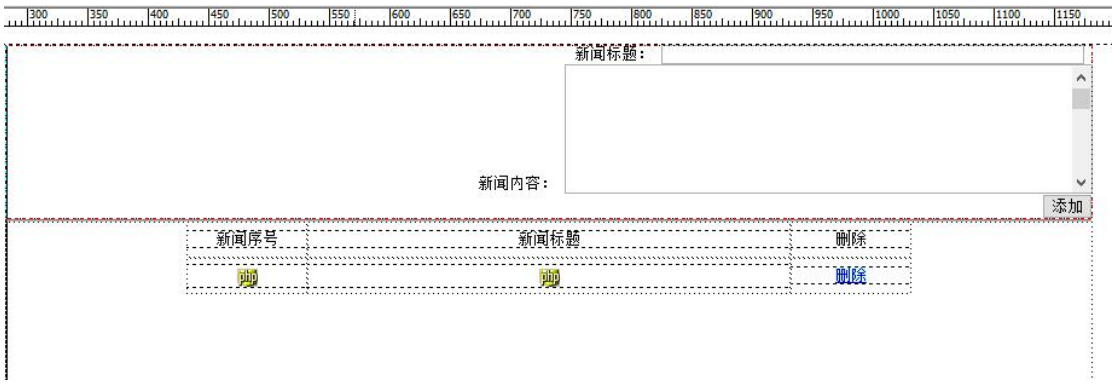


添加操作：

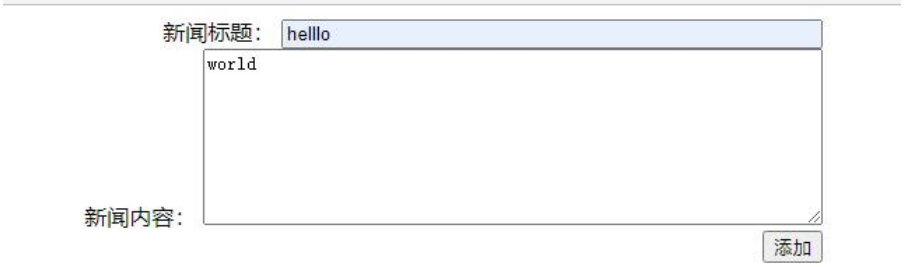
add.php:

```
<?php
$conn=mysql_connect("localhost", "root", "123456");
mysql_select_db("testDB");
$topic = $_POST['topic'];
$content = $_POST['content'];
$SQLStr = "insert into news(topic, content) values('$topic', '$content')";
echo $SQLStr;
$result=mysql_query($SQLStr);

// 关闭连接
mysql_close($conn);
if ($result)
{
    ?>
```

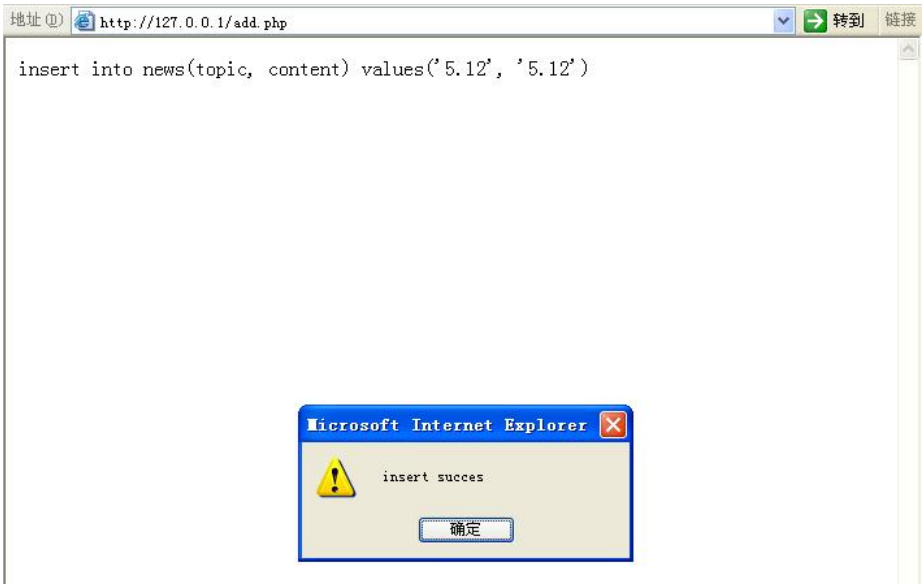
```
        <script>
            alert("insert succes");
            window.location.href="sys.php";
        </script>
         <?php
    }
    else{
        ?>
        <script>
            alert("insert failed");
            history.back();
        </script>
         <?php
    }

?>
```



添加“hello：world”的新闻内容：



插入成功


地址(D) http://127.0.0.1/add.php
转到
链接
insert into news(topic, content) values('5.12', '5.12')
Microsoft Internet Explorer
insert succes
确定

检查数据库中：


localhost ▸ testdb ▸ news
浏览
结构
SQL
搜索
插入
导出
导入
操作
清空
删除
显示行 0 - 1 (2 总计, 查询花费 0.0008 秒)
SELECT *
FROM `news`
LIMIT 0 , 30
显示 : 30 行，开始行数: 0
以 水平 模式显示，并且在 100 行后重复标题
主键排序: 无
+ 选项
newsid
topic
content
1
helllo
world

查询操作：

news.php：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>主页</title>
</head>
<body>
<div align="center">
  <table width="900" border="0" cellspacing="0" cellpadding="0">
    <tr>
      <td height="40"><form id="form1" name="form1" method="post" action="loginok.php">
        <div align="right">用户名：
          <input name="username" type="text" id="username" size="12" />
          密码：
          <input name="password" type="password" id="password" size="12" />
          <input type="submit" name="Submit" value="提交" />
        </div>
      </form>
      </td>
    </tr>
    <tr>
      <td><hr /></td>
    </tr>
    <tr>
      <td height="300" align="center" valign="top"><p> </p>
      <?php
```

```
        $conn=mysql_connect("localhost", "root", "123456");
        $newsid = $_GET['newsid'];

        $SQLStr = "select * from news where newsid=$newsid";
        $result=mysql_db_query("testDB", $SQLStr, $conn);
        if ($row=mysql_fetch_array($result))//通过循环读取数据内容
        {
            // 定位到第一条记录
            mysql_data_seek($result, 0);
            // 循环取出记录
            while ($row=mysql_fetch_row($result))
            {
                echo "$row[1]<br>";
                echo "$row[2]<br>";
            }
         }
        // 释放资源
        mysql_free_result($result);
        // 关闭连接
        mysql_close($conn);

?>
 </td>
    </tr>
  </table>
</div>
</body>
</html>
```

可根据 id 来查询对应的新闻内容：

删除操作：

del.php:

```
<?php
$conn=mysql_connect("localhost", "root", "123456");
mysql_select_db("testDB");
$newsid =$_GET['newsid'];
$SQLStr = "delete from news where newsid=$newsid";
echo $SQLStr;
$result=mysql_query($SQLStr);
// 关闭连接
mysql_close($conn);
if ($result)
{
    ?>
    <script>
        alert("delete succes");
        window.location.href="sys.php";
    </script>
     <?php
```

```
    }
    else{
        ?>
        <script>
            alert("delete failed");
            history.back();
        </script>
         <?php
    }
?>
```

例如此处删除第二条新闻：

完成删除，仅剩一条内容

心得体会：

通过本次实验，成功在 windows xp 上安装了 php，并成功复现了利用 php 来编写简单的数据库插入、查询和删除操作，同时也基于课本的完整例子，进一步了解了 WEB 开发的细节，也认识到了 php 代码在 WEB 应用中的重要性，以及数据库在数据存储和检索方面的关键作用。