《漏洞利用及渗透测试基础》实验报告

姓名： 艾明旭 学号：2111033 班级：信息安全

**实验名称：**

Web开发实践

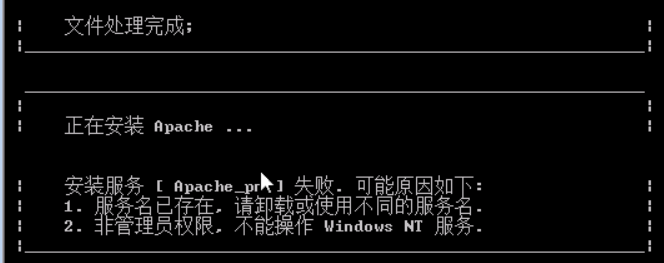
**实验要求：**

复现课本第十章实验三，利用PHP，编写简单的数据库插入、查询和删除操作示例。基于课本的完整的例子，进一步了解Web开发细节。

**实验过程：**

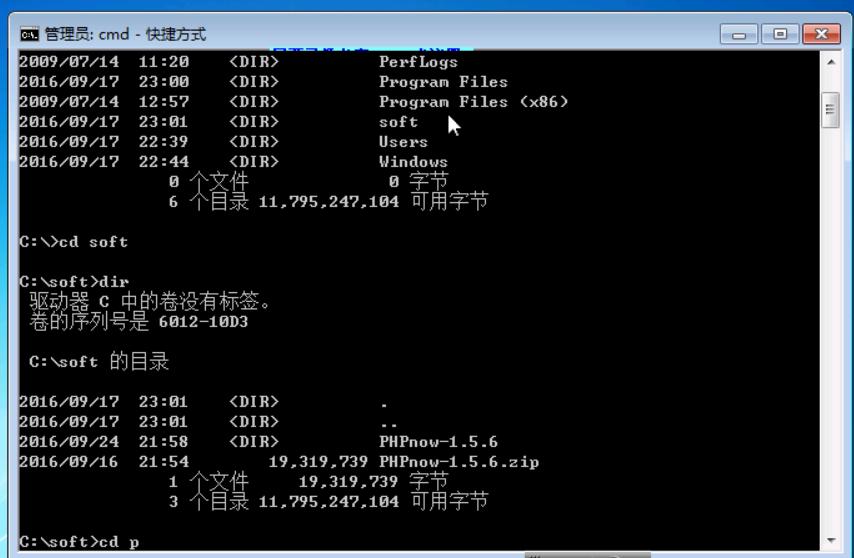
## 环境配置

由于xp系统之后，windows在不以管理员运行的情况下会禁止安装服务从而导致安装失败



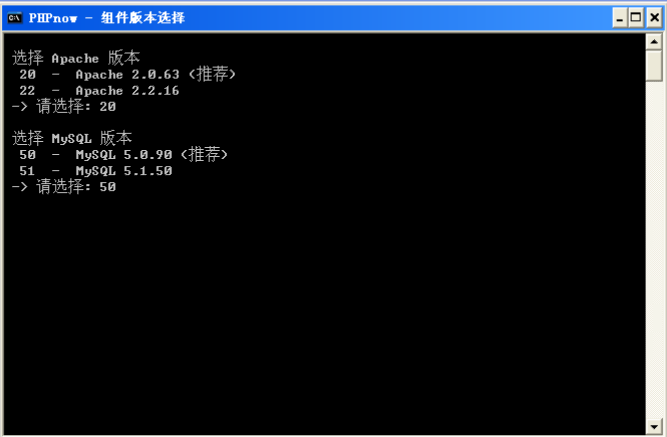
因此选择在虚拟机xp系统进行本次实验

（或者找到cmd.exe,以管理员身份运行，手动安装也可以）



安装过程:

选择版本

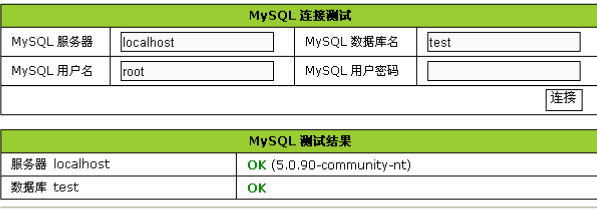


并设置MySQL的密码，完成安装

打开默认界面(实际上是http://127.0.0.1/index.php)



数据库成功连接



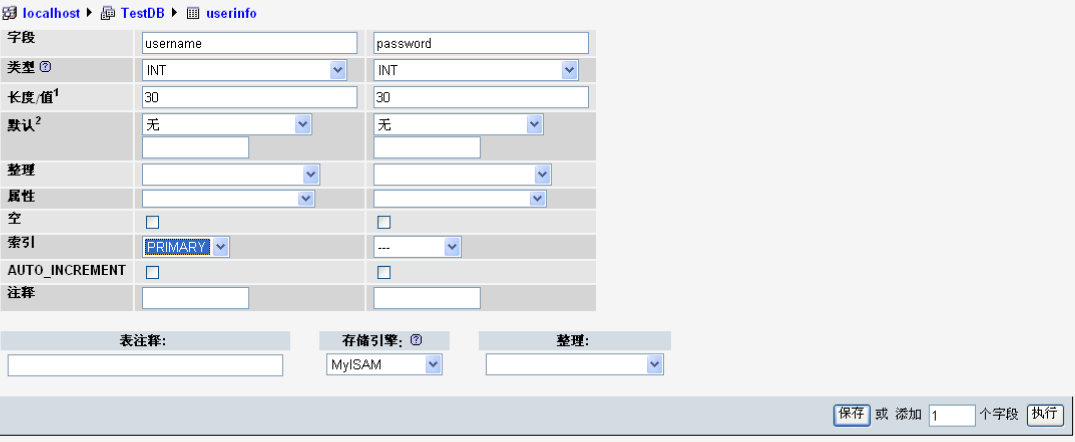
数据库管理系统



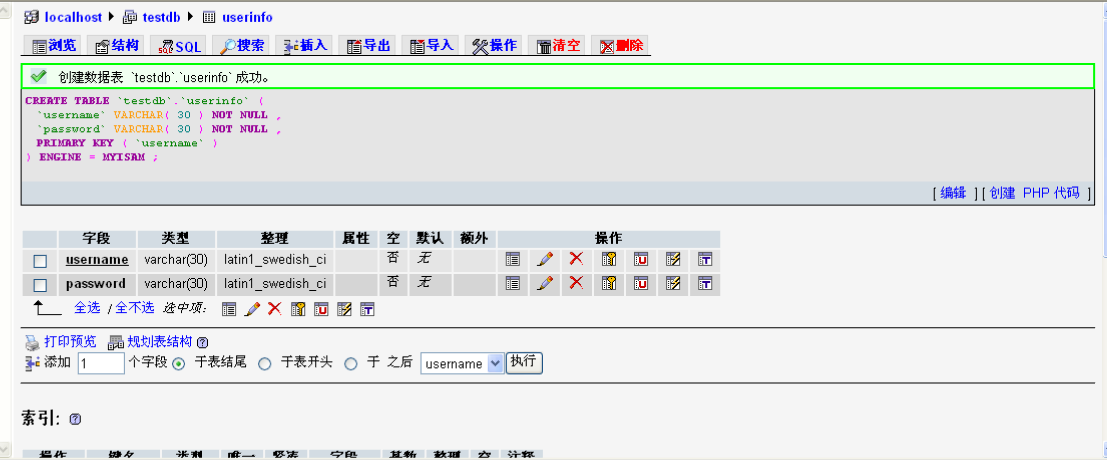
### 接下来开始实验三，利用php，编写简单的数据库插入、查询和删除操作的示例

首先新建TestDB数据库，以及News（newsid, topic, content）、userinfo（username, password）两张表

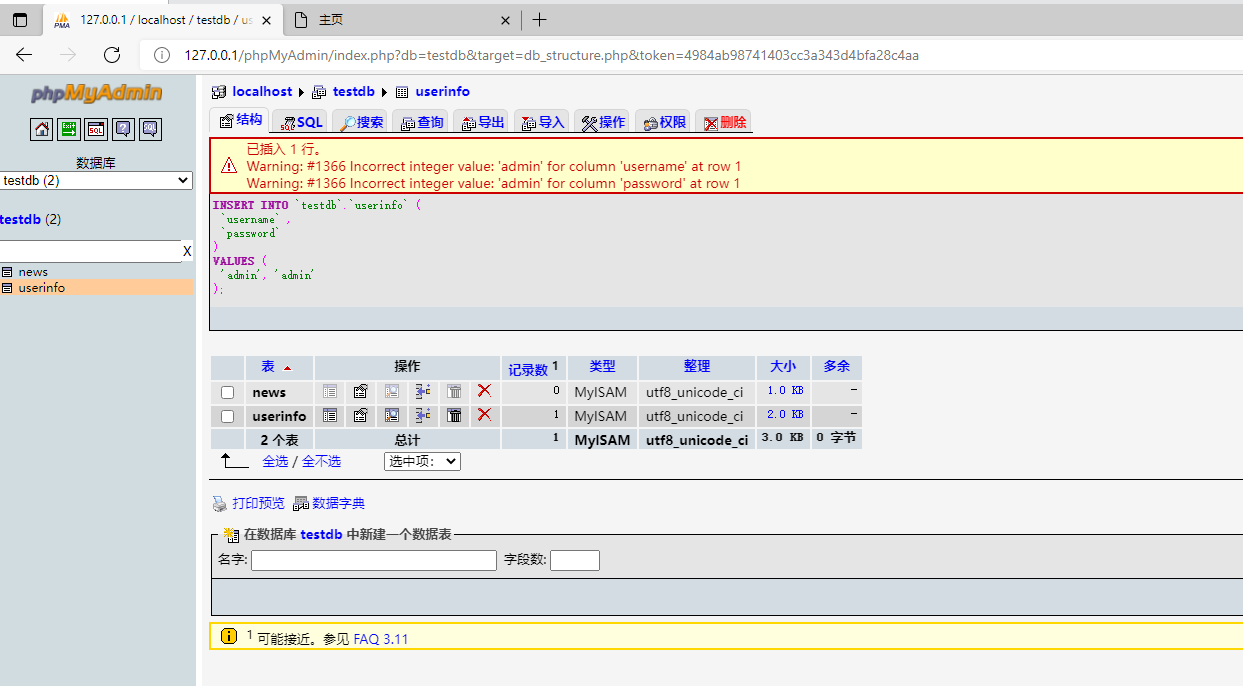




创建成功

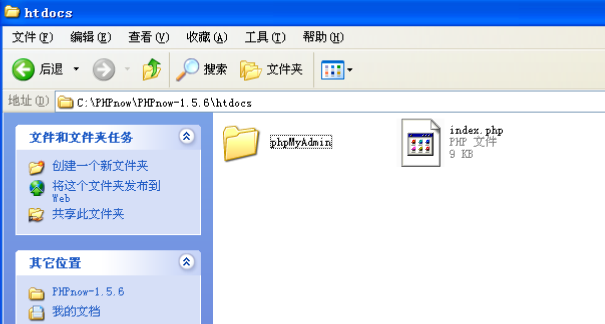


向表中插入数据：



接着建网页文件（用Dreamwaver）

工作目录，html文件应保存在此处



新建HTML文件



## 3、进行第一个Web程序的编写

Web.html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">username</td>

<td height="20"><label>

<input name="username" type="text" id="username" />

</label></td>

</tr>

<tr>

<td height="20">password</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>

此段代码定义了一个 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

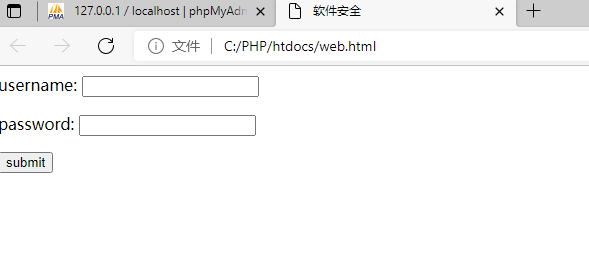
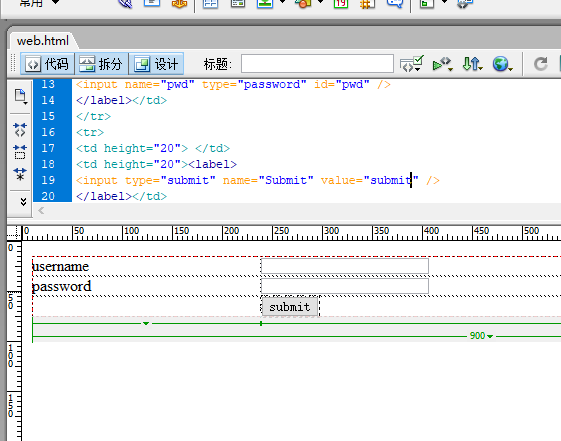
文件名。由动作属性定义的这个文件通常会对接收到的输入数据进行相关的处理

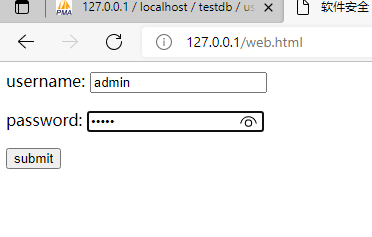
表单中，定义了接受表单输入的处理文件为“loginok.php”，所以点击确认会跳转到loginok.php

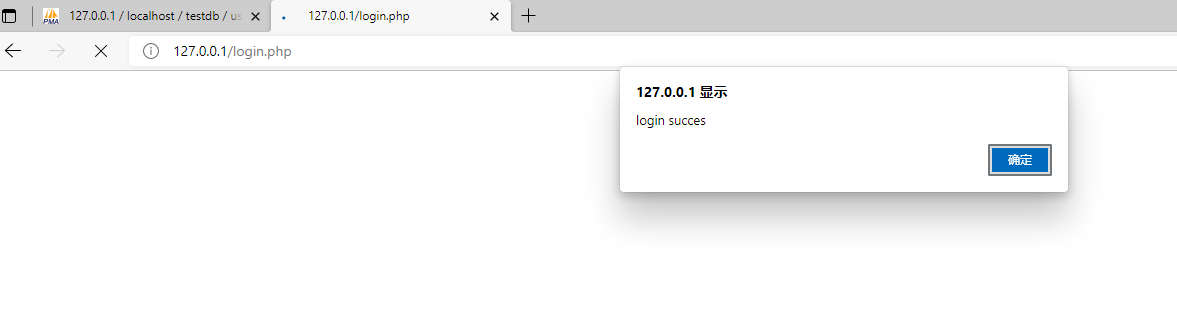
Login.html:

|  |
| --- |
| <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> |

运行效果如下:





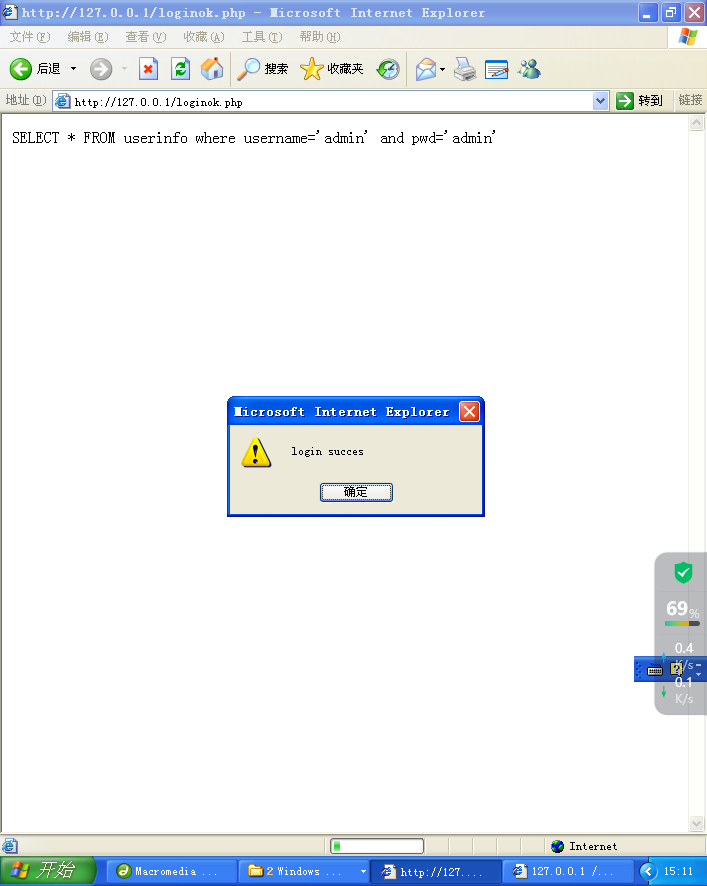


## 用 php编写简单的数据库插入、查询和删除操作的示例

首先是系统管理界面：

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);  ?> |



然后是实现新闻添加

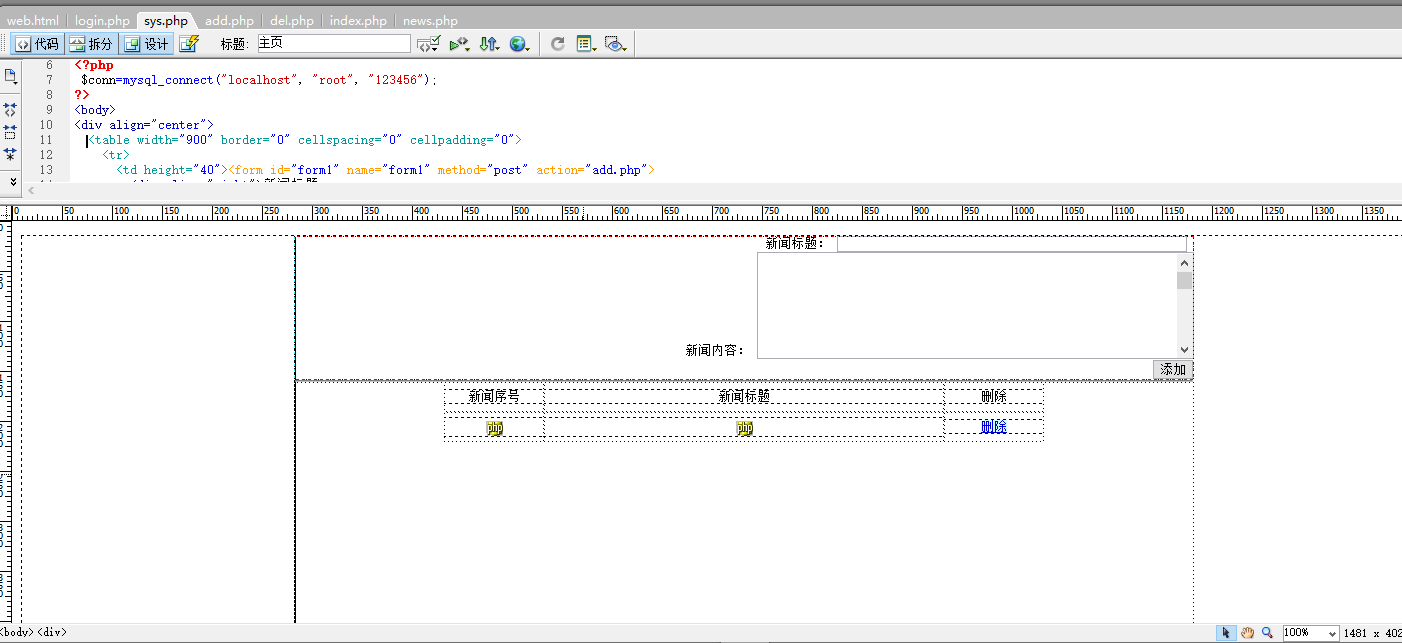
注：在 add.php 中数据库访问操作是通过 mysql\_select\_db("testDB")连接数据库之后，使用

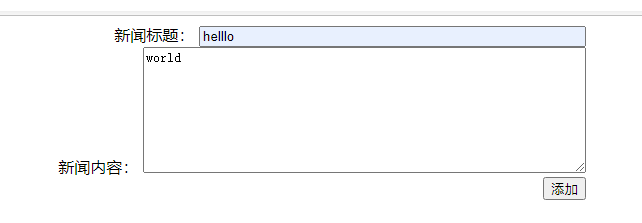
$result=mysql\_query($SQLStr)进行更新和删除语句的执行，可见 mysql\_query 比较适合更新和删除语句，

其返回值是 boolean，可以校验执行成功与失败

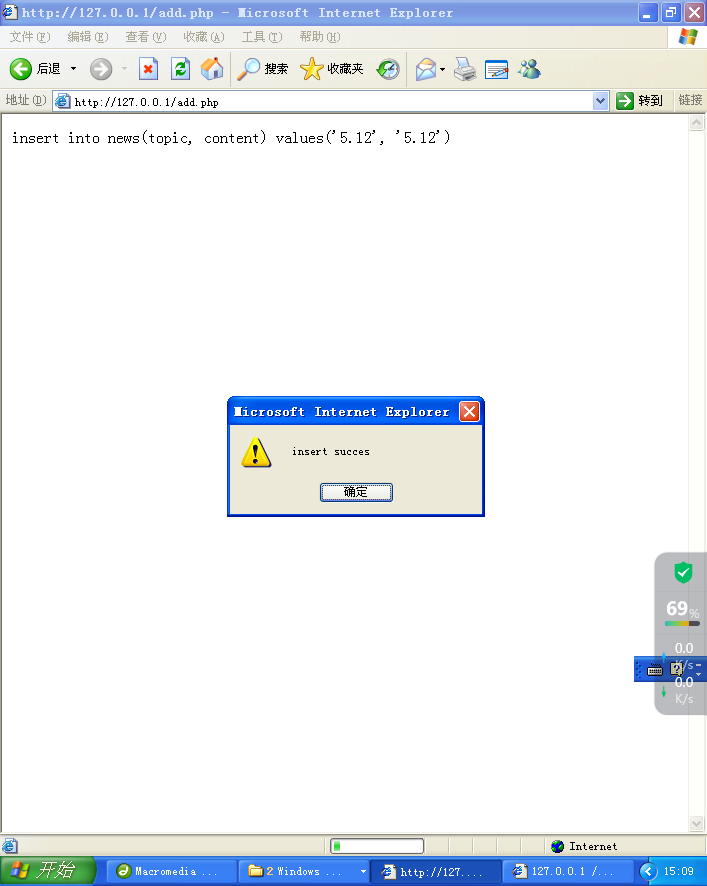
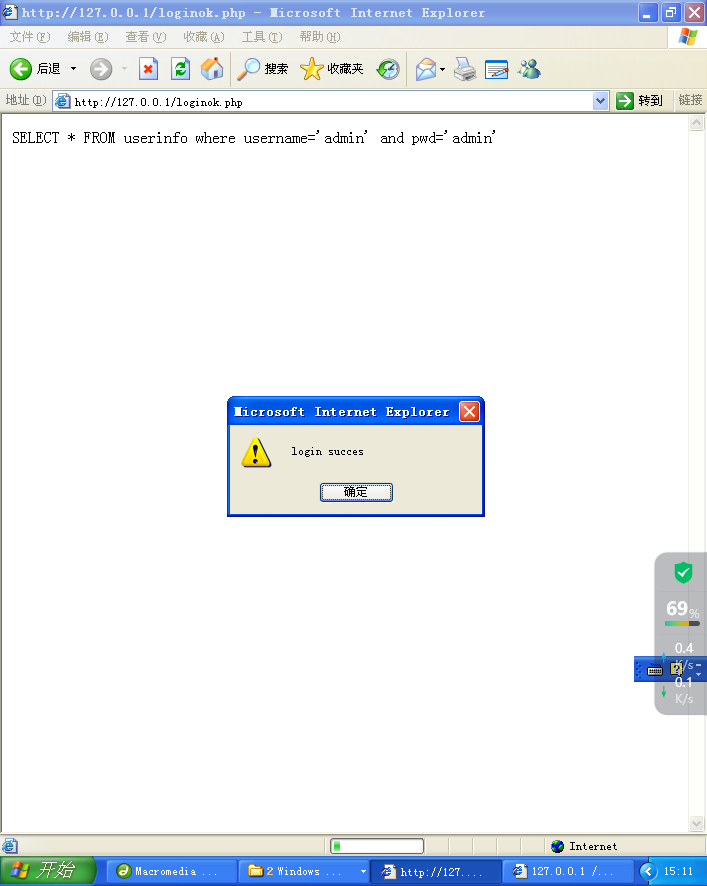
add.php:

|  |
| --- |
| <?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  }    ?> |

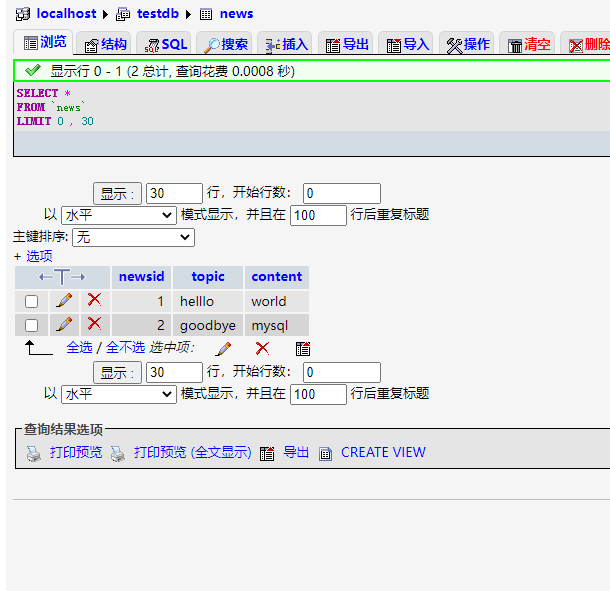




显示添加成功：



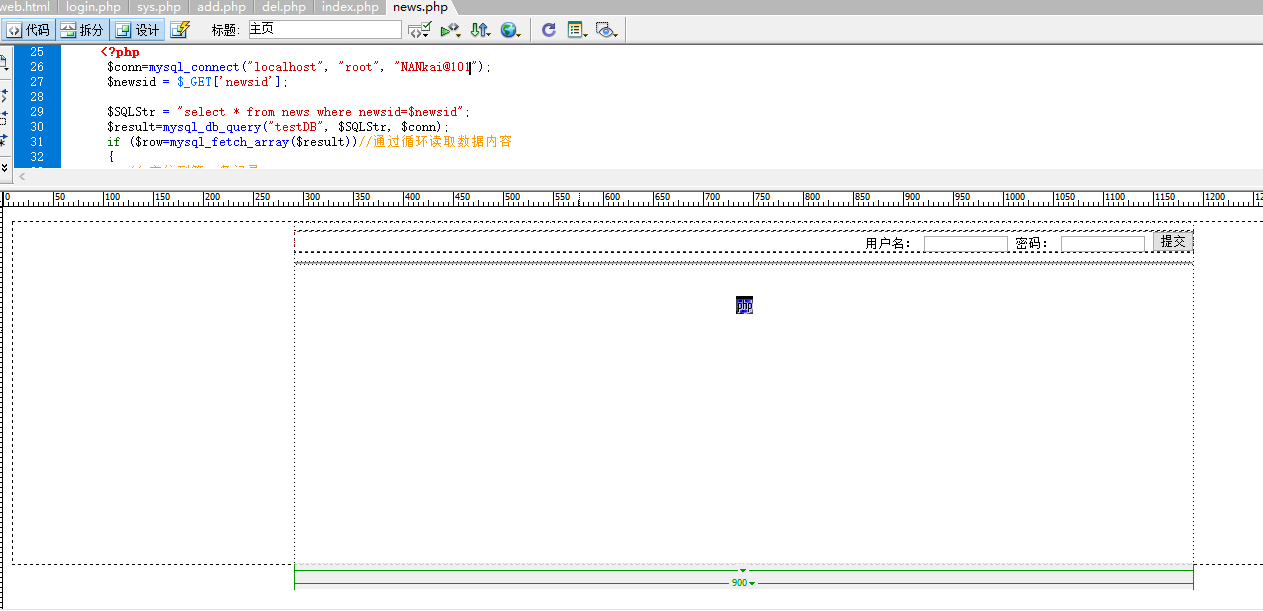
表里也有了我添加的内容：



然后是根据传入的 id 查看新闻内容

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>&nbsp;</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> |



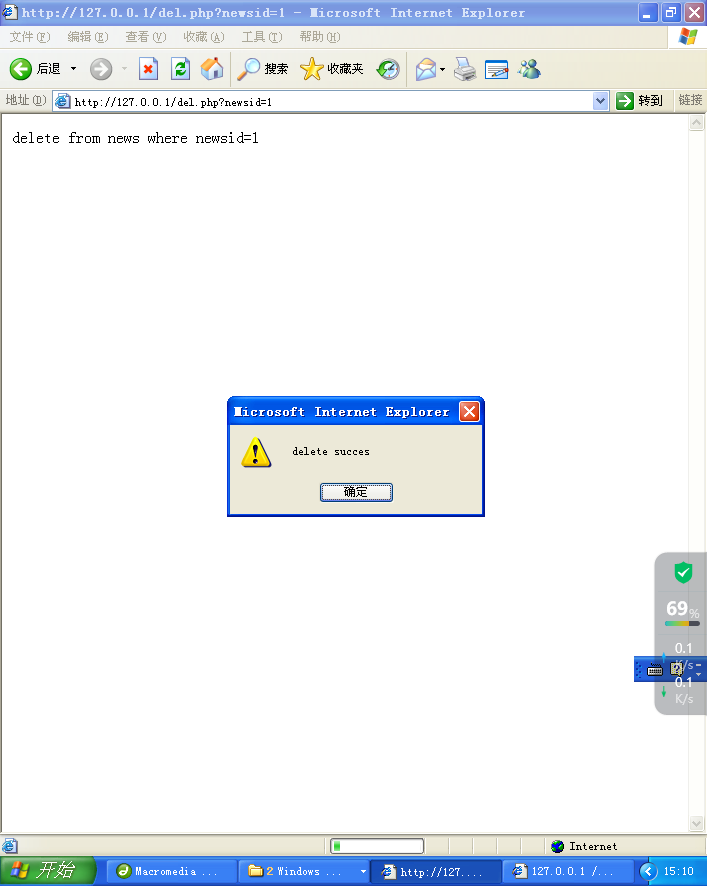
删除新闻

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  }  ?> |

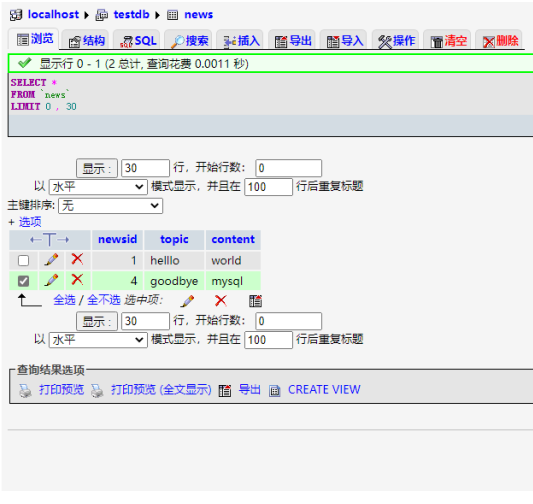
运行效果：

显示新闻序号和新闻标题，以及可以对某条新闻进行删除操作

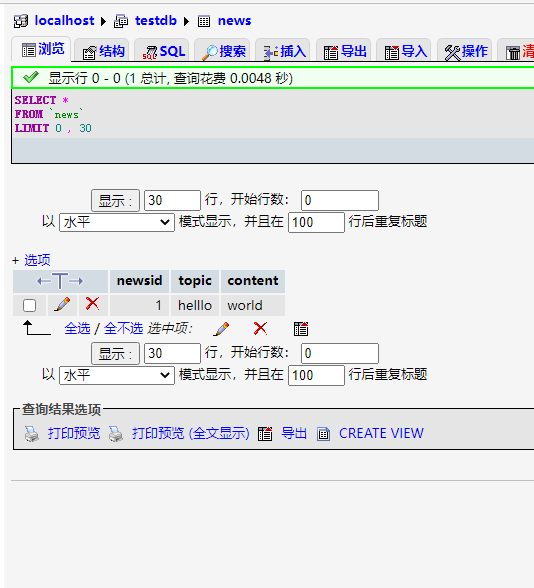
****

这里删除第二条新闻，删除前后数据库表内容对比：

（此处为删除后再添加截图，由于newsid自增，故序号为4）



删除后，说明删除成功



最后编写允许用户查看新闻和进行登录界面

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />

<title>主页</title>

</head>

<?php

$conn=mysql\_connect("localhost", "root", "NANkai@101");

?>

<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);

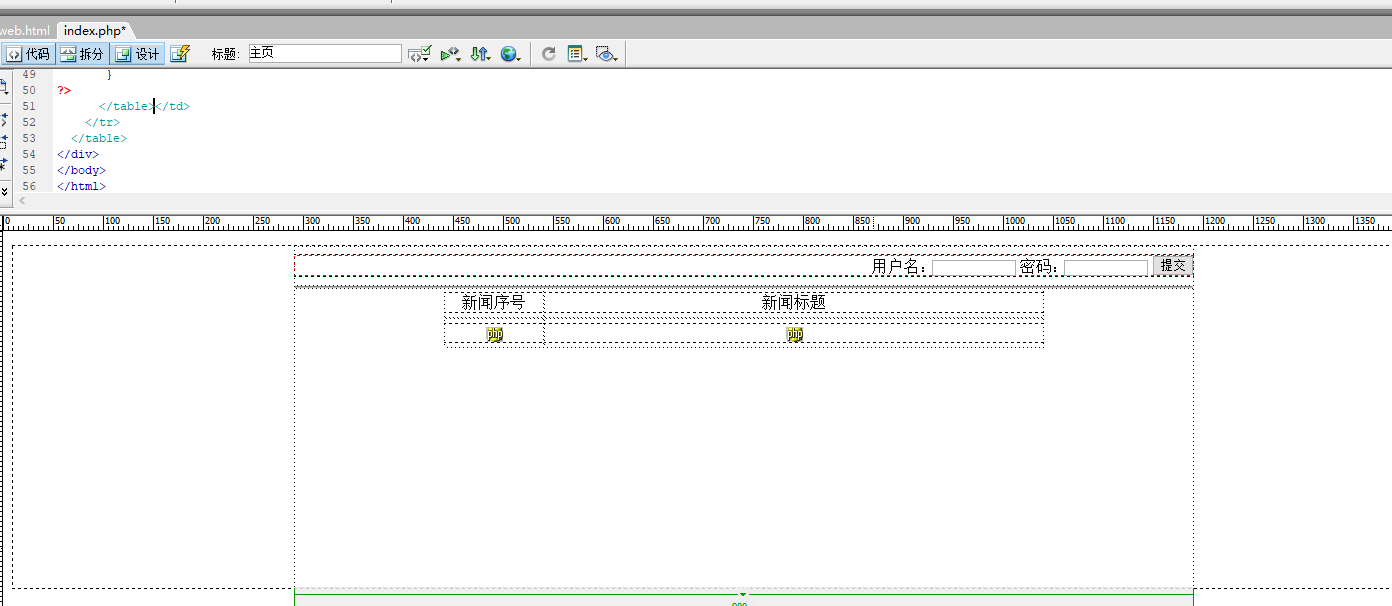
// 关闭连接

mysql\_close($conn);

?>

Index.php代码如下

运行效果：





**心得体会：**

通过这次实验，我熟悉了php开发，实现了编写简单的数据库插入、查询和删除操作。进一步了解了WEB开发的细节。

我学习了PHP的基础知识，包括语法、变量、函数、流程控制等，了解PHP的基本概念有利于更好地理解和编写代码。

我使用了合适的开发工具：我选择了Dreamweaver这个开发工具进行php代码的开发，这个工具提供自动补全和调试等功能，可以提高开发效率。

同时，我还学习了一定的php框架，他们能够提供一系列强大的功能和组件，可以加快开发速度并提高代码的可维护性。学习和使用这些框架能够使开发更加高效和专业。

同时，我在调试运行PHP代码的过程中

PHP是一门不断发展的语言，不断学习和实践是保持技术更新的关键。关注PHP的最新发展，学习新的特性和工具，不断改进自己的编码技能。