《软件安全》实验报告

姓名：冯思程 学号：2112213 班级： 计算机科学与技术二班

**实验名称：**

WEB开发实践

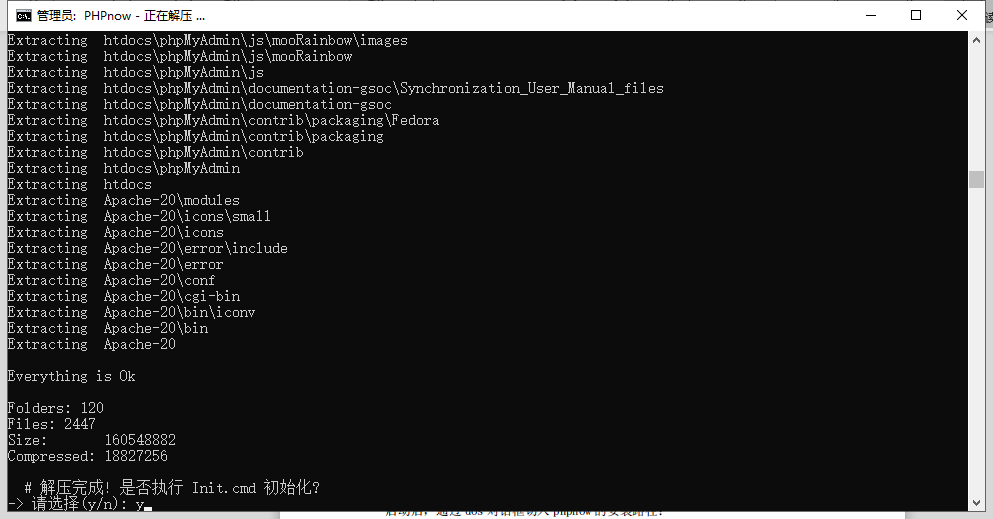
**实验要求：**

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. **首先进行PHPnow工具的安装：**

首先在网上找到PHPnow工具1.5.6版本的安装包下载，解压 phpnow 后（切近路径不能出现中文，有可能导致以后服务无法正常启动），右键点击setup.cmd 进行管理员身份运行即可进入安装界面，之后，选择 init.cmd：



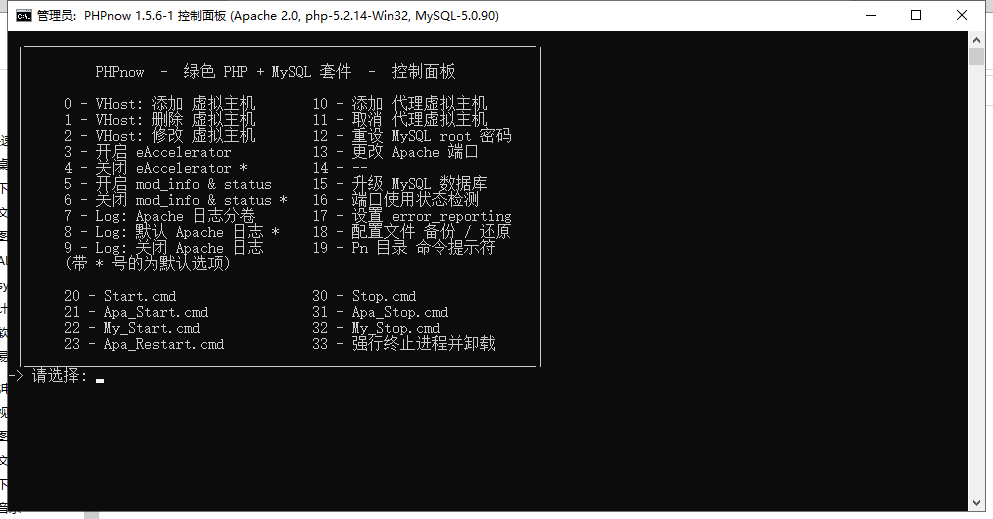
有了管理员的权限可以直接安装成功，然后设置MySQL的root用户密码设置：



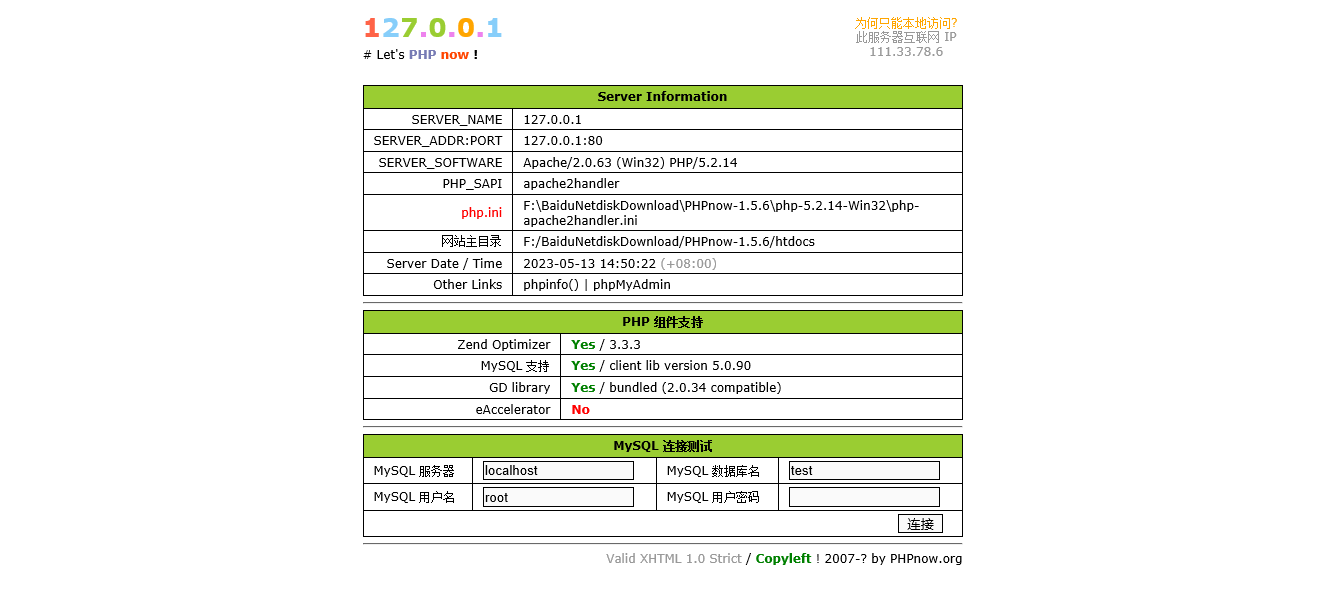
安装完毕，目录如下：



点击 PnCp.cmd，如下图：



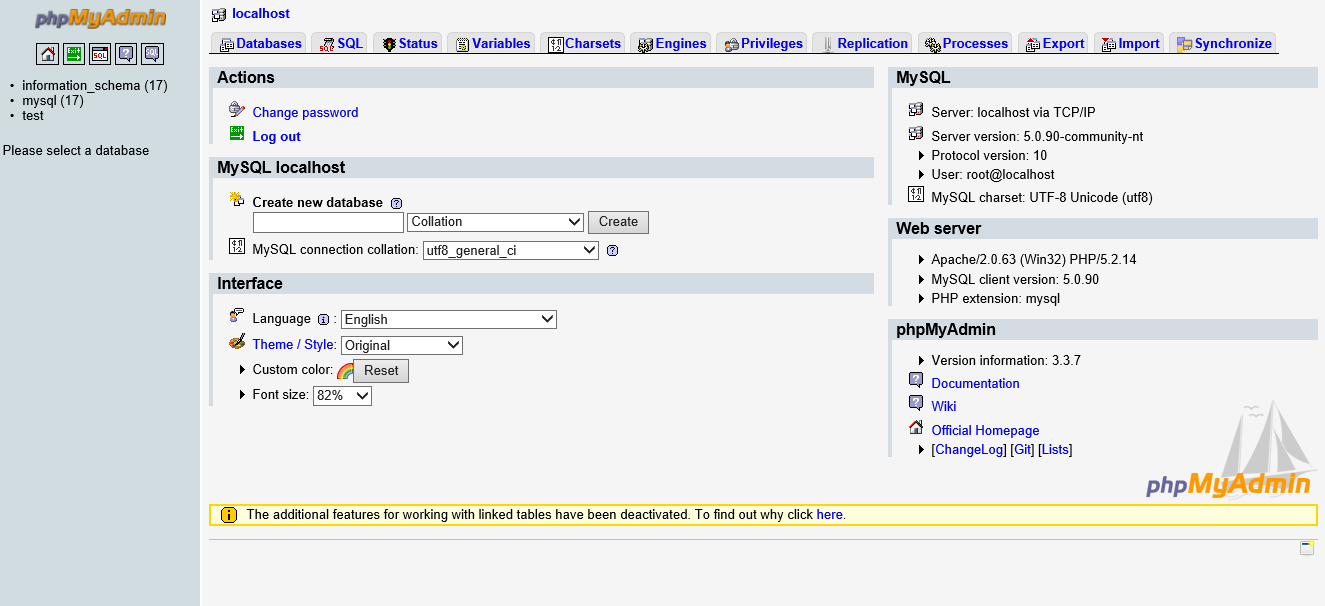
选择序号 20，即可启动 PHPnow。打开网页，访问 http://127.0.0.1 如下图：



在界面下方，输入刚才设置的MySQL密码，进行连接测试，验证是否成功配置好，如下图：



点击 phpMyAdmin，输入密码后成功登录，进入数据库管理界面，可以自行创建数据库、表以及录入数据，方便进行接下来的实验部分：



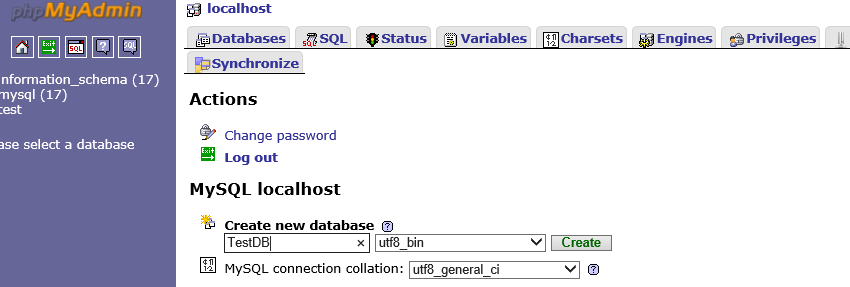
1. **创建数据库TestDB，并建表News，userinfo：**

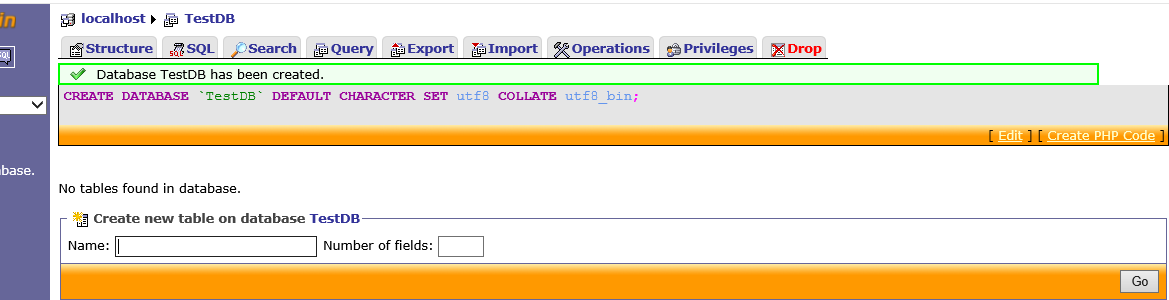
两个表的关系模式如下：

表1：News（newsid, topic, content）

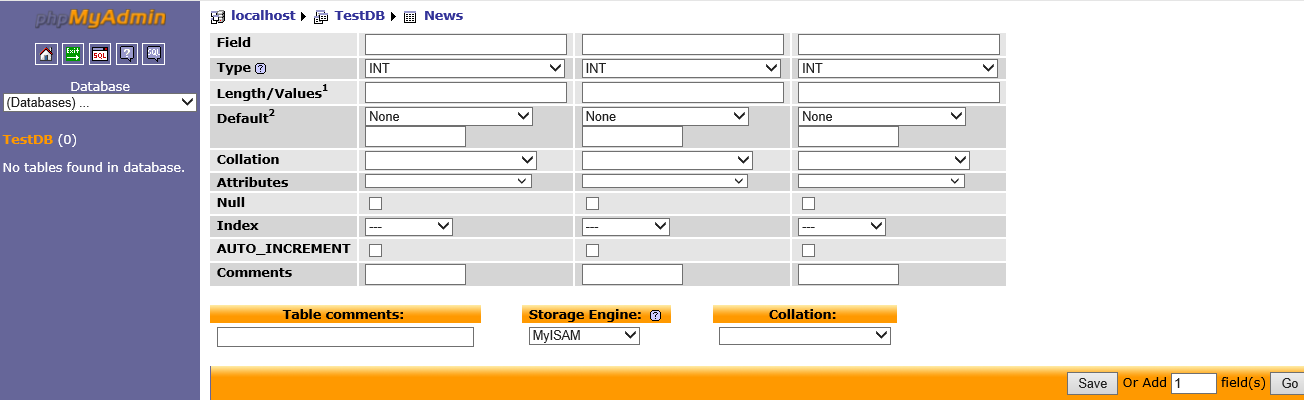
表 2：userinfo（username, password）

首先在首页创建数据库TestDB，确定字符集为utf8，排序规则默认即可，如下：

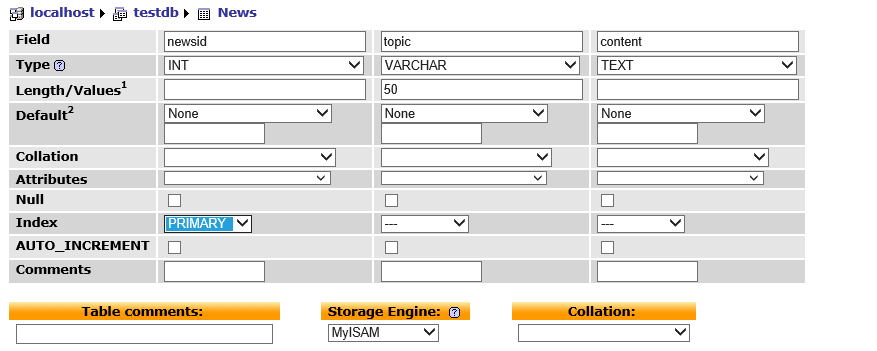




然后创建表News，输入这个表要声明的属性列个数，这里News表一共有三个属性列，点击go进行创建，如下：

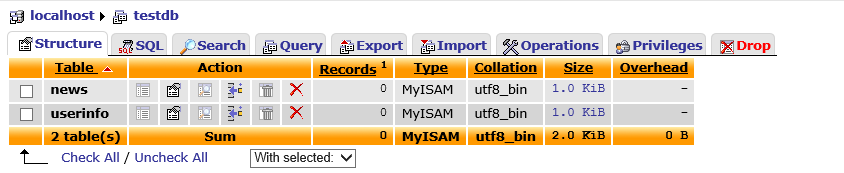


然后进行属性列的声明，其中包括属性列的名字和数据类型，其中newsid的数据类型是int型，topic的数据类型是varchar，它的长度限制成50，content的数据库是text，其中我将newsid设置成主键（primary），这里注意newsid是定义成自增排序，然后点击save进行表的创建，如下：



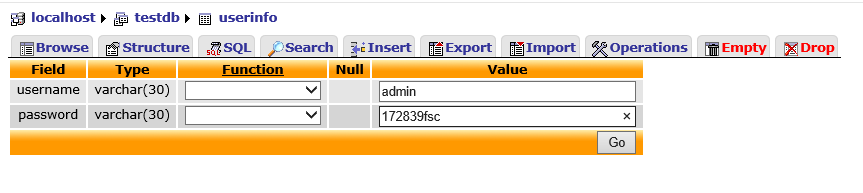
然后同理建立userinfo表，其中username属性列的数据类型是varchar，长度限制为30，password属性列的数据类型是varchar，长度限制为30，其中我将username属性设置成主键（primary），然后点击save进行表的创建，如下：

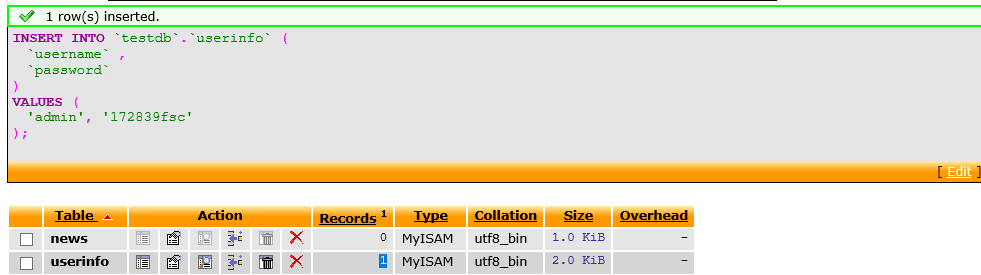


然后查看TestDB数据库，发现两张表都已经成功建好，如下：  


1. **向表userinfo插入一条数据，方便一会进行操作：**

其中username属性是admin，password属性是172839fsc，设置一个管理员的身份和密码，点击go即可执行插入，如下：

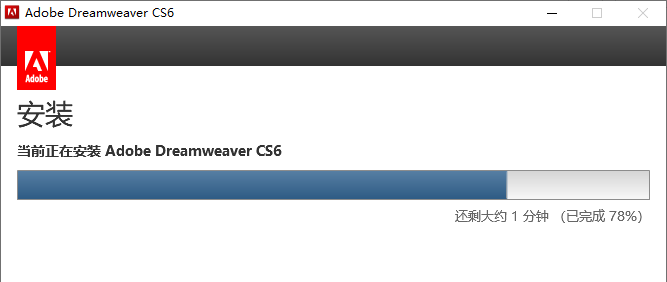




1. **进行Dreamweaver CS6的安装配置：**

这里我是找到了一共网上的安装包和安装教程：<http://www.downza.cn/soft/27432.html>

其中具体步骤这里不一一介绍，只需安装教程的过程即可实现软件的安装和破解，如下：

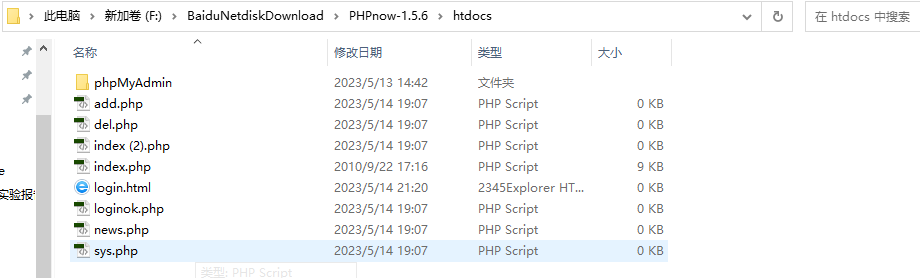




1. **根据教材给出的代码分别创建需要的php文件和html文件：**

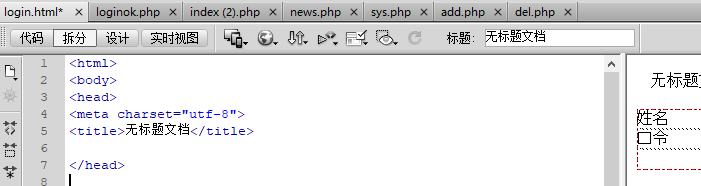
首先，在F:\BaiduNetdiskDownload\PHPnow-1.5.6\htdocs路径下创建出7个txt文件，然后分别将这7个文件重命名为如下：

index(2).php,news.php,loginok.php,sys.php,add.php,del.php,login.html。其中的index(2).php是因为原来的路径下已经存在一个index.php文件了所以只能命名成index(2).php，如下图：

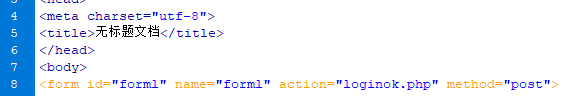


对他们的功能进行一个小的简介：index.php（允许用户查看新闻和进行登录）、news.php（根据传入的 id 查看新闻内容）、loginok.php（判断用户登录是否成功）、sys.php（系统管理界面）、add.php（新闻添加）、del.php（删除新闻），login.html（登录网页）。

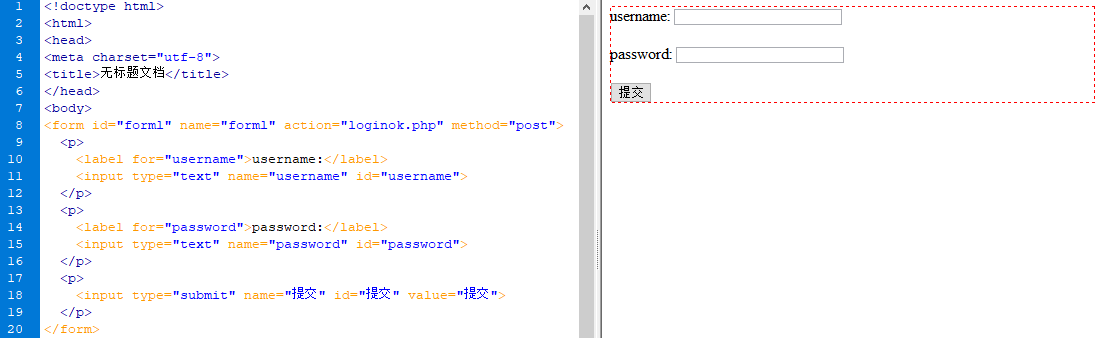
**然后先编写login.html文件**，用dreamweaver工具打开上面创建的html文件，如下：



然后根据实验视频的内容和编写目标进行代码的编写，这个文件编写想要实现的主要功能就是实现一共登录界面login，输入内容是username和password，然后有一共登录按钮，点击按钮则会去获取到输入的username和password的值从而进行后面的判断和操作，首先为了可以从web输入动态获得输入信息，需要插入一个表单，并将表单的action设置为loginok.php，如下：



然后对表单进行插入，首先插入两个文本框分别写上username和password，然后插入必要的按钮，这里将按钮命名为提交，如下：



**接着需要编写刚才已经声明的loginok.php脚本文件**，该脚本首先需要获取到刚输入的两个数据username和password，获取的方式我采用了POST方法，然后这里需要链接上数据库进行数据查询判断，如果输入的数据在userinfo表中则输出login success，否则输出login failed，这里我还利用了一个loginok的字符用他的0/1判断是否成功登录，这里我对当登录失败的时候做了一个小功能，history.back()可以让界面返回到上一层界面（登录界面），又利用script进行了一个小窗口的弹出提示是否成功登录，这里注意当登录成功之后会跳转执行一个名字是sys.php的脚本，最终代码如下：

<?php

$loginok=0;

$conn=mysql\_connect("localhost", "root", "172839fsc");

$username = $\_POST['username'];

$pwd = $\_POST['password'];

$SQLStr = "SELECT \* FROM userinfo where username='$username' and password='$pwd'";

echo $SQLStr;

$result=mysql\_db\_query("TestDB", $SQLStr, $conn);

if ($row=mysql\_fetch\_array($result))//通过循环读取数据内容

{

$loginok=1;

}

// 释放资源

mysql\_free\_result($result);

// 关闭连接

mysql\_close($conn);

if ($loginok==1)

{

?>

<script>

alert("login success");

window.location.href="sys.php";

</script>

<?php

}

else{

?>

<script>

alert("login failed");

history.back();

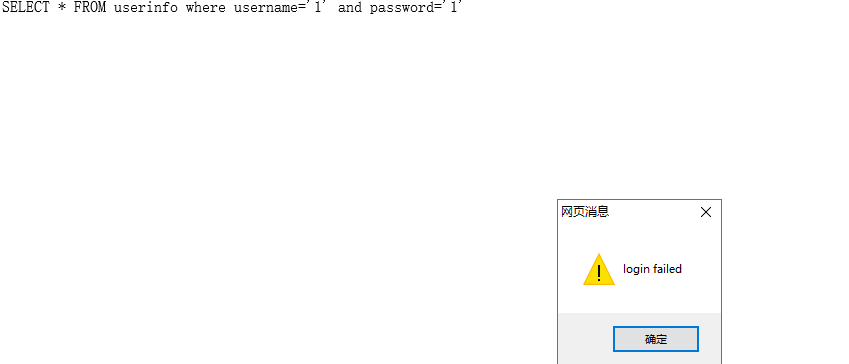
</script>

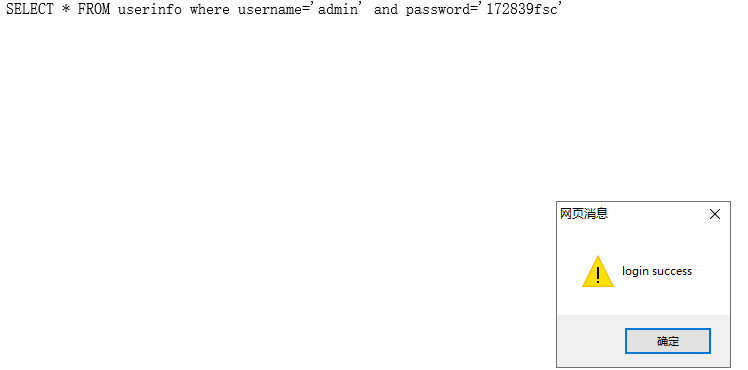
<?php

}

?>

然后登陆上网页进行简单验证，结果如下：（这里就利用到了上文我插入的admin/172839fsc用户）





可以成功的实现目标功能。

**接着是进行sys.php文件的编写**：这个脚本是进行新闻主页的界面，那么新闻包括news、topic、content，根据界面设计按照上文的方法先进行界面展示的代码编辑，其中功能包括添加一个新闻（topic和content），然后数据库中的所有新闻都会被显示在下面的列表框中（这个地方的功能实现方法就是通过链接数据库然后执行select \*的sql语句进行查询，然后将结果进行展示。），还可以选择一个新闻进行删除，主要的代码如下：

<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", "172839fsc");

?>

<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

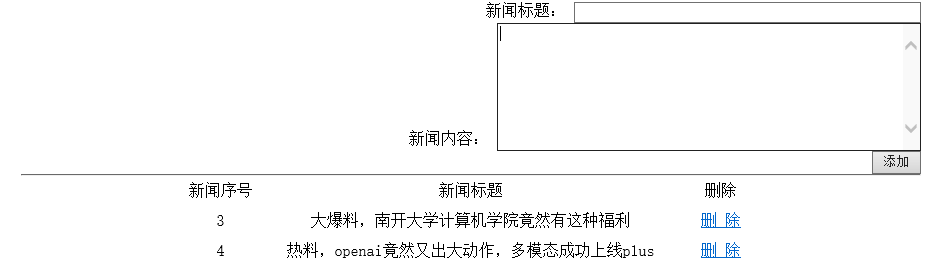
// 释放资源

mysql\_free\_result($result);

// 关闭连接

mysql\_close($conn);

?>

主页界面如下：  


其中添加功能和删除功能和查询到新闻序号并可视化新闻标题都是由接下来编写的php脚本文件进行实现的。

**接下来进行添加功能add.php文件的编写**：这里的编写逻辑与框架类似与loginok.php文件的编写方法，获取到用户输入的topic和content两个数据，然后链接上数据库进行插入操作，然后会对插入操作的成功与否进行验证，如果成功则弹出insert success，否则弹出insert failed，而且无论成功与否都会跳转到原来的sys主页，代码如下：

<?php

$conn=mysql\_connect("localhost", "root", "172839fsc");

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 success");

window.location.href="sys.php";

</script>

<?php

}

else{

?>

<script>

alert("insert failed");

history.back();

</script>

<?php

}

?>

然后登录上网页进行简单测试，如下：



**接下来进行del.php文件的编写**：这里的编写逻辑和方法和add十分类似，只是这次要实现的功能是删除记录元组，这里所用的删除方法是通过newsid这个主键进行删除，代码框架与add.php文件十分类似，同样也有一个对操作成功与否的判断，并输出信息进行可视化，代码如下：

<?php

$conn=mysql\_connect("localhost", "root", "172839fsc");

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

}

?>

登录网页进行简单的验证：



**然后进行index(2).php文件的编写：**这里是想实现一个通过点击新闻的标题来实现对新闻的内容的访问，这里我们需要利用上面用过sys的一部分代码，这部分就是可视化出所有的新闻的newsid、topic然后通过点击标题即可实现对内容的访问，具体对内容的访问会在news.php文件中进行实现，代码逻辑到这里已经很清晰了，如下：

<html>

<head>

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

<title>主页</title>

</head>

<?php

$conn=mysql\_connect("localhost", "root", "172839fsc");

?>

<body>

<div align="center">

<table width="900" border="0" cellspacing="0" cellpadding="0">

<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

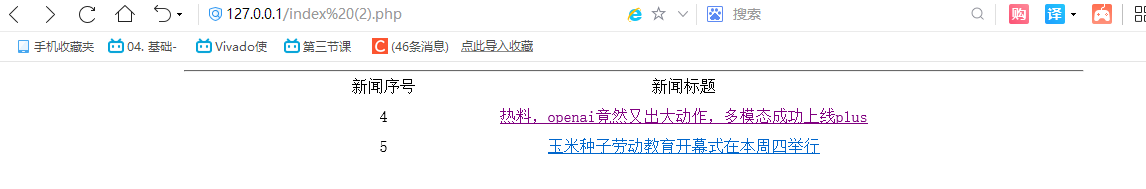
// 释放资源

mysql\_free\_result($result);

// 关闭连接

mysql\_close($conn);

?>

登录到127.0.0.1/index(2).php进行简单验证，如下：  


**最后就是进行news.php文件的编写**：这里我们是通过与上文相似的过程继续书写，主要实现的功能就是查询到每个新闻标题对应的新闻内容，这里代码可以通过直接复制index(2).php文件然后通过对展示部分进行更改即可，为了节省篇幅我这里只对更改部分的代码进行展示，如下：（红色部分是我更改的部分）

while ($row=mysql\_fetch\_row($result))

{

?>

<tr>

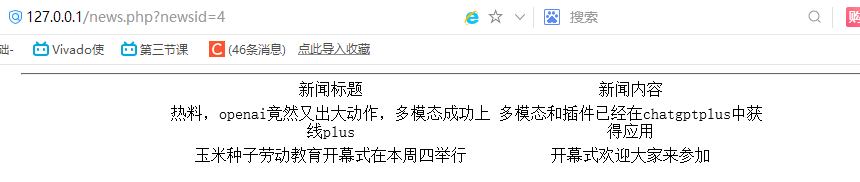
<td height="30"><div align="center"> <?php echo $row[1] ?> </div></td>

<td height="30"><div align="center"> <?php echo $row[2] ?> </div></td>

</tr>

<?php

}

然后登录进行验证，结果如下：  


综上所有的目标功能均开发完毕，且均开发成功，实现了对数据库的增删查操作。

1. **然后是对整个流程的总结与思考**：

我深刻详细地了解了整个教材展示的网页的开发环节：

1. 首先是index.php

在URL中地址127.0.0.1后可以直接添加本地文件夹想要运行的php文件，和我上文中直接在目标路径下新建txt文件的做法吻合。

1. 在输入我们的用户名和密码后，点击“提交”会跳转到“loginok.php”

其中使用的是post连接方式，防止把信息写在url中泄露，如果用get方式获取的话，用户的信息会被直接的展示在url上很容易造成信息泄露。

1. 在loginok.php中，与我们的数据库相连接，并且使用mysql查询指令来确认登录信息是否正确。
2. 登入后对不同的按钮链接不同的php文件以执行相应的插入删除操作，具体操作上文中有着十分详细的步骤和解释。

**心得体会：**

在这次实验中，我使用了phpnow工具进行web开发，并利用PHP编写了一些数据库操作的示例，包括插入、查询和删除操作。这个实验让我进一步了解了WEB开发的细节，并且我基于课本上提供的完整例子进行了探索。

首先，我创建了一个简单的新闻管理系统，数据库中有一个新闻表和一个用户表，其中实现的操作包括对新闻的增删查操作。通过这个实验，我学会了如何使用PHP连接到数据库，并且利用SQL语句执行数据库操作。我使用phpnow工具提供的函数和类，编写了与数据库的交互代码。

在新闻管理系统中，我实现了新闻的插入功能。通过表单输入新闻的标题、内容和发布日期，我可以将这些数据插入到数据库的新闻表中。这个过程让我熟悉了如何处理表单数据，并将其传递给PHP脚本进行处理。

另外，我还实现了新闻的查询功能。系统可以在数据库中找到目标新闻内容，并将结果显示在网页上。这个功能的实现让我了解了如何编写SQL查询语句，并将查询结果展示给用户。

除了新闻的增删查功能，我还实现了登录验证过程。用户需要输入用户名和密码才能登录系统。通过与数据库中的用户表进行比对，我可以验证用户输入的凭据是否正确。这个过程让我学会了如何处理用户输入的敏感信息，并进行安全验证。

通过这次实验，我对WEB开发的流程有了更深入的了解。我明白了连接数据库、执行数据库操作以及与用户交互的重要性。我也认识到了安全性在WEB开发中的重要性，特别是在处理用户输入和验证过程中，这里对post和get不同获取信息的方式进行对比发现了post是更加安全的方式。

总的来说，这次实验是一次有收获的经历。这次实验不仅加深了我对WEB开发的理解，也提升了我的实践能力。