

# 软件安全实验报告

学号: 2310764 姓名: 王亦辉 班次: 计科一班

## 1 实验名称 :

WEB开发实践

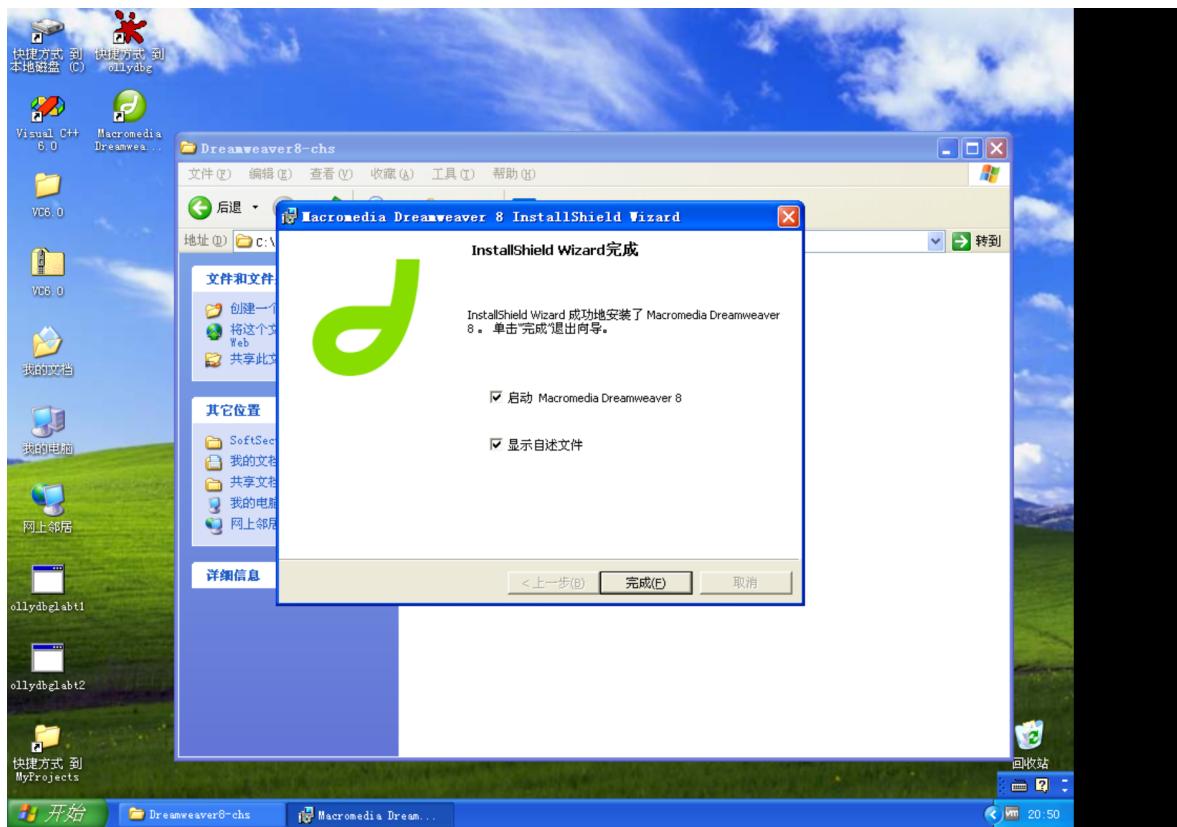
## 2 实验要求 :

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。

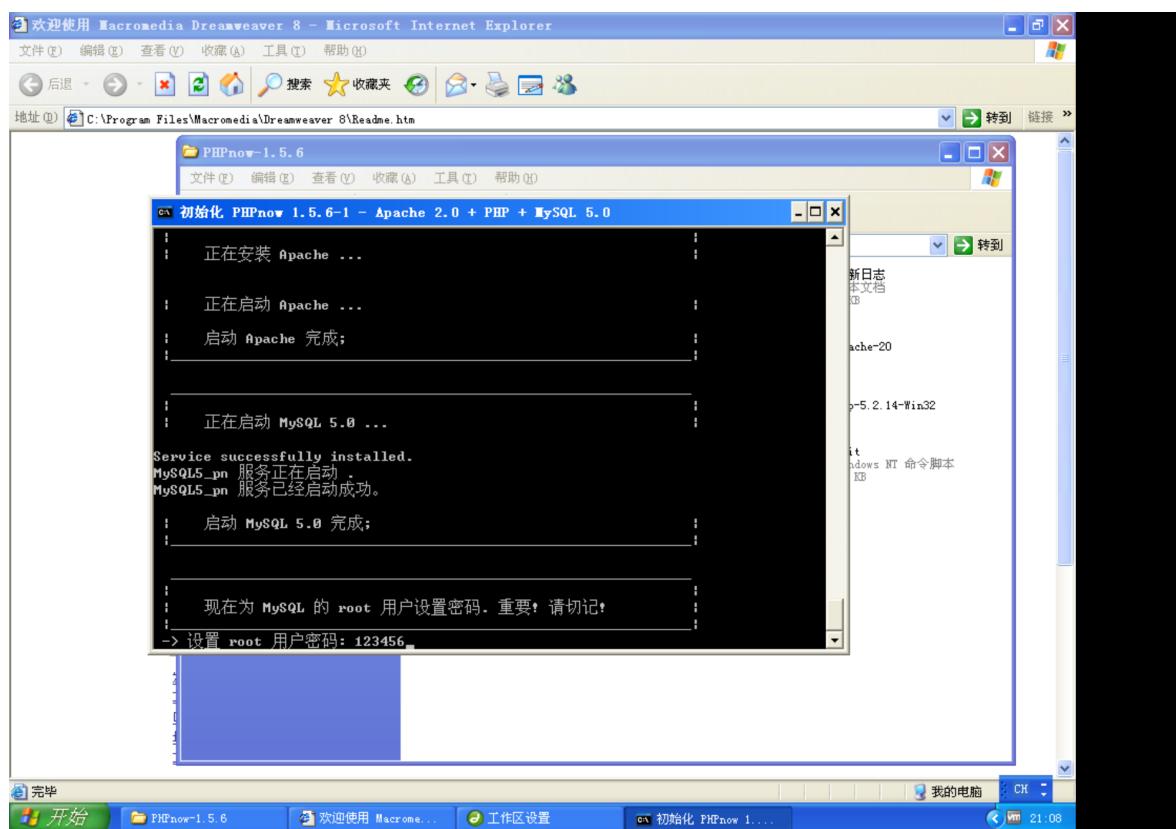
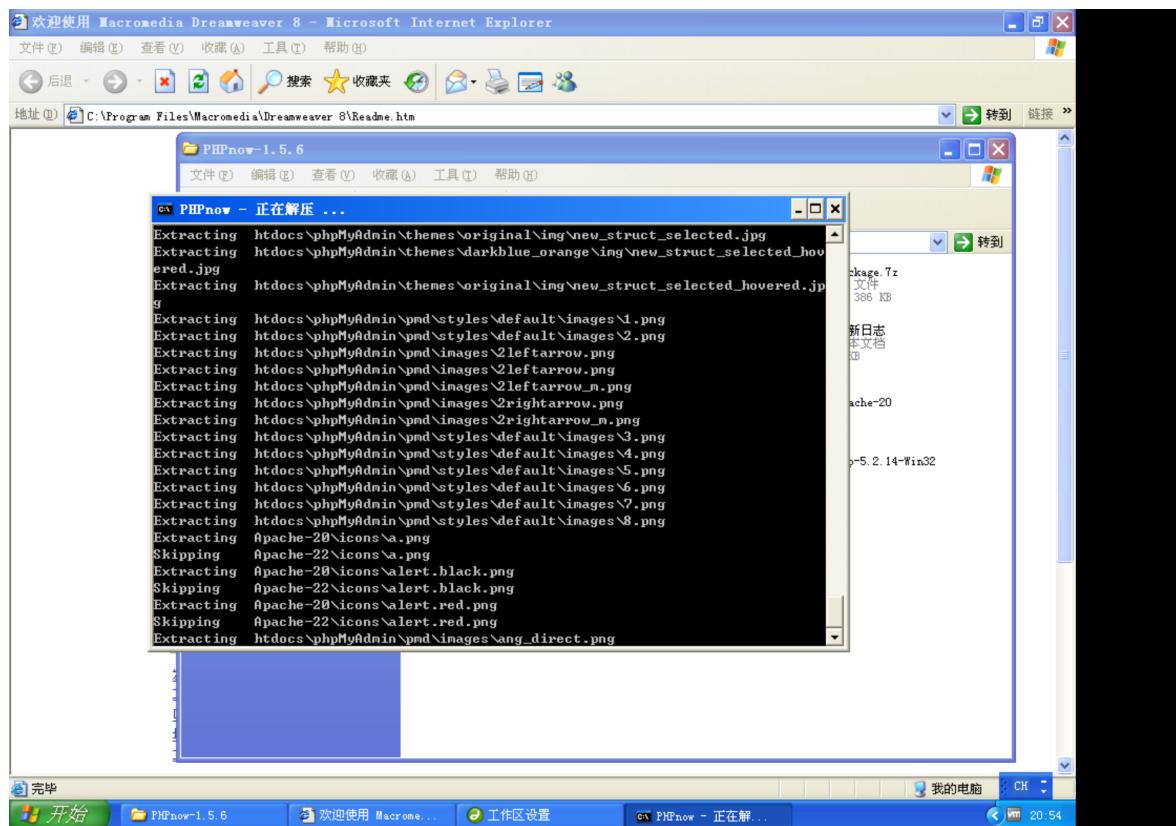
## 3 实验过程 :

### 3.1 环境配置

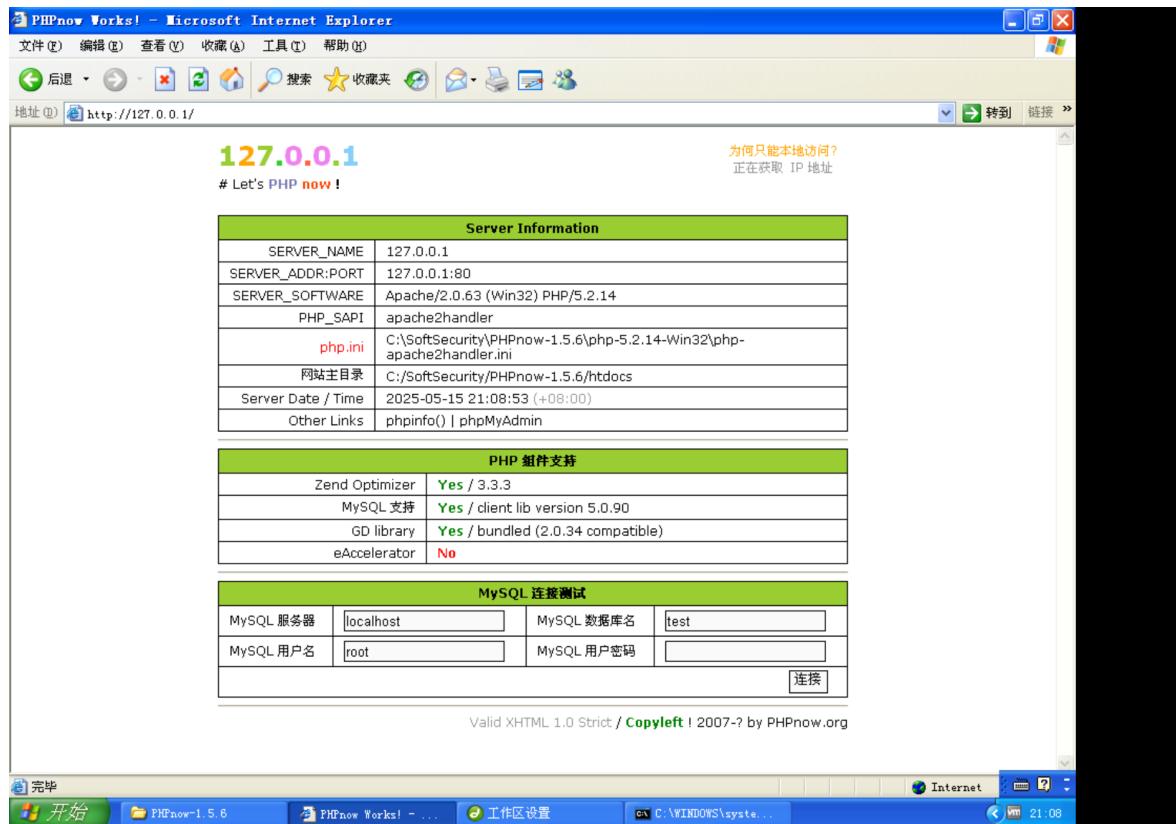
使用课程资源内的安装包, 复制进虚拟机的 xp 系统, 然后安装 [Dreamweaver](#)



接下来安装 [PHPnow](#)，设置 root 的密码为 123456。



之后来到 phpnw 的默认界面

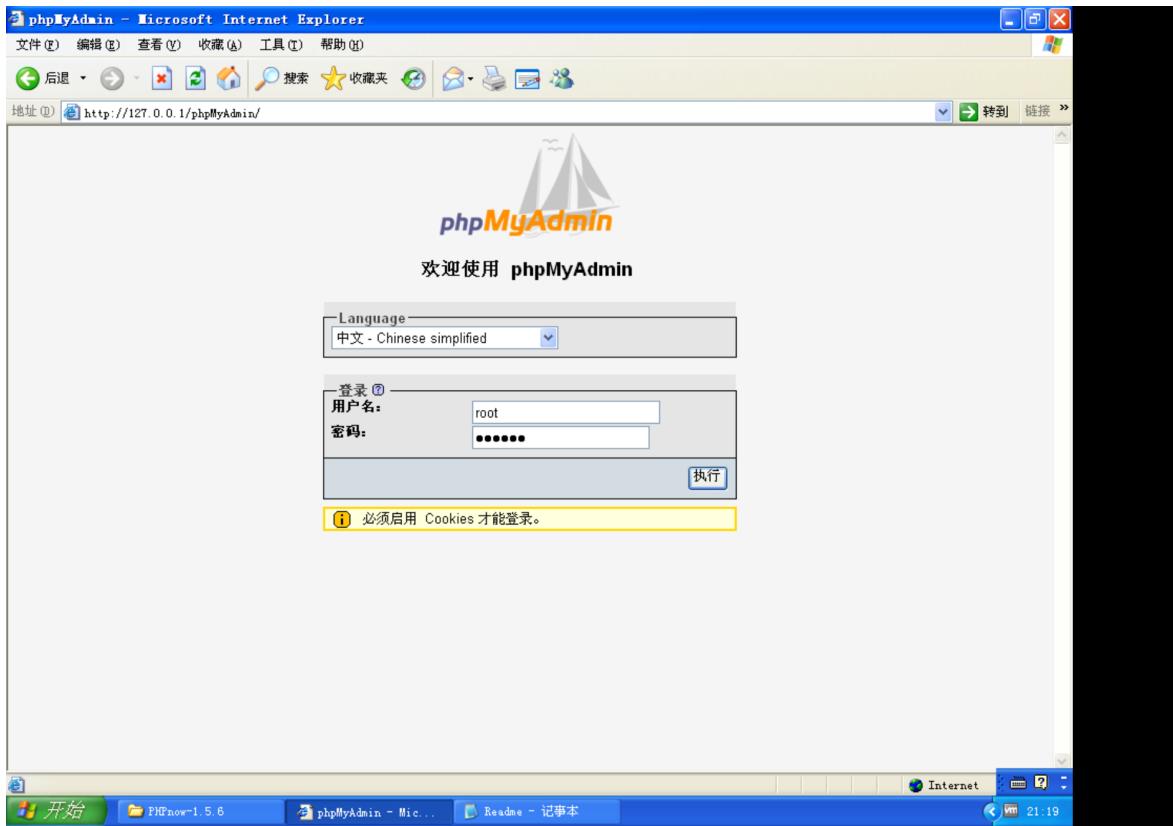


环境配置完成，接下来可以开始开发了。

## 3.2 进行 web 开发

### 3.2.1 创建数据库和表

进入 [phpadmin](#)



A screenshot of the phpMyAdmin dashboard in Microsoft Internet Explorer. The title bar says "127.0.0.1 / localhost | phpMyAdmin 3.3.7 - Microsoft Internet Explorer". The left sidebar lists databases: "information\_schema (17)", "mysql (17)", and "test". The main content area has tabs for "数据库", "SQL", "状态", "变量", "字符集", "引擎", "权限", "复制", "进程", "导出", and "导入". Under "操作", there are links for "修改密码" and "退出". The "MySQL localhost" section shows a "新建数据库" input field and a "MySQL 连接校对" dropdown set to "utf8\_general\_ci". The "界面" section includes "Language" (Chinese simplified), "主题 / 风格" (Original), "自定义颜色" (Rainbow), and "字号" (82%). The "网站服务器" section lists "Apache/2.0.63 (Win32) PHP/5.2.14", "MySQL 客户端版本: 5.0.90", and "PHP 扩展: mysql". The "phpMyAdmin" sidebar provides links for "版本信息: 3.3.7", "文档", "维基 (Wiki) (外链, 英文)", "官方主页 (外链, 英文)", "[ChangeLog] [Git] [Lists]", and the phpMyAdmin logo. A yellow warning box at the bottom says "链接表的附加功能尚未激活。要查出原因, 请点击此处" (Additional features for linked tables are not activated. Click here to find out why). The taskbar at the bottom shows icons for "开始", "PHPnow-1.5.8", "127.0.0.1 / loca...", and "Readme - 记事本".

## 建立数据库表

数据库: TestDB

表1: News (newsid, topic, content)

表2: userinfo (username, password)

The screenshot shows the phpMyAdmin interface for the testdb database. A green success message at the top states "创建数据表 'testdb'.'userinfo' 成功。" (Table 'userinfo' created successfully). Below it is the SQL code for creating the table:

```
CREATE TABLE `testdb`.`userinfo` (
  `username` VARCHAR(30) NOT NULL ,
  `password` VARCHAR(30) NOT NULL
) ENGINE = MYISAM ;
```

The table structure is displayed in a grid with columns: 字段 (Field), 类型 (Type), 整理 (Collation), 属性 (Attributes), 空 (Null), 默认 (Default), 额外 (Extra), and 操作 (Operations). The 'userinfo' table has two fields: 'username' (VARCHAR(30)) and 'password' (VARCHAR(30)).

The screenshot shows the phpMyAdmin interface for the testdb database. A green success message at the top states "创建数据表 'testdb'.'News' 成功。" (Table 'News' created successfully). Below it is the SQL code for creating the table:

```
CREATE TABLE `testdb`.`News` (
  `newsid` INT NOT NULL ,
  `topic` VARCHAR( 30 ) NOT NULL ,
  `content` TEXT NOT NULL
) ENGINE = MYISAM ;
```

The table structure is displayed in a grid with columns: 字段 (Field), 类型 (Type), 整理 (Collation), 属性 (Attributes), 空 (Null), 默认 (Default), 额外 (Extra), and 操作 (Operations). The 'News' table has three fields: 'newsid' (INT), 'topic' (VARCHAR(30)), and 'content' (TEXT).

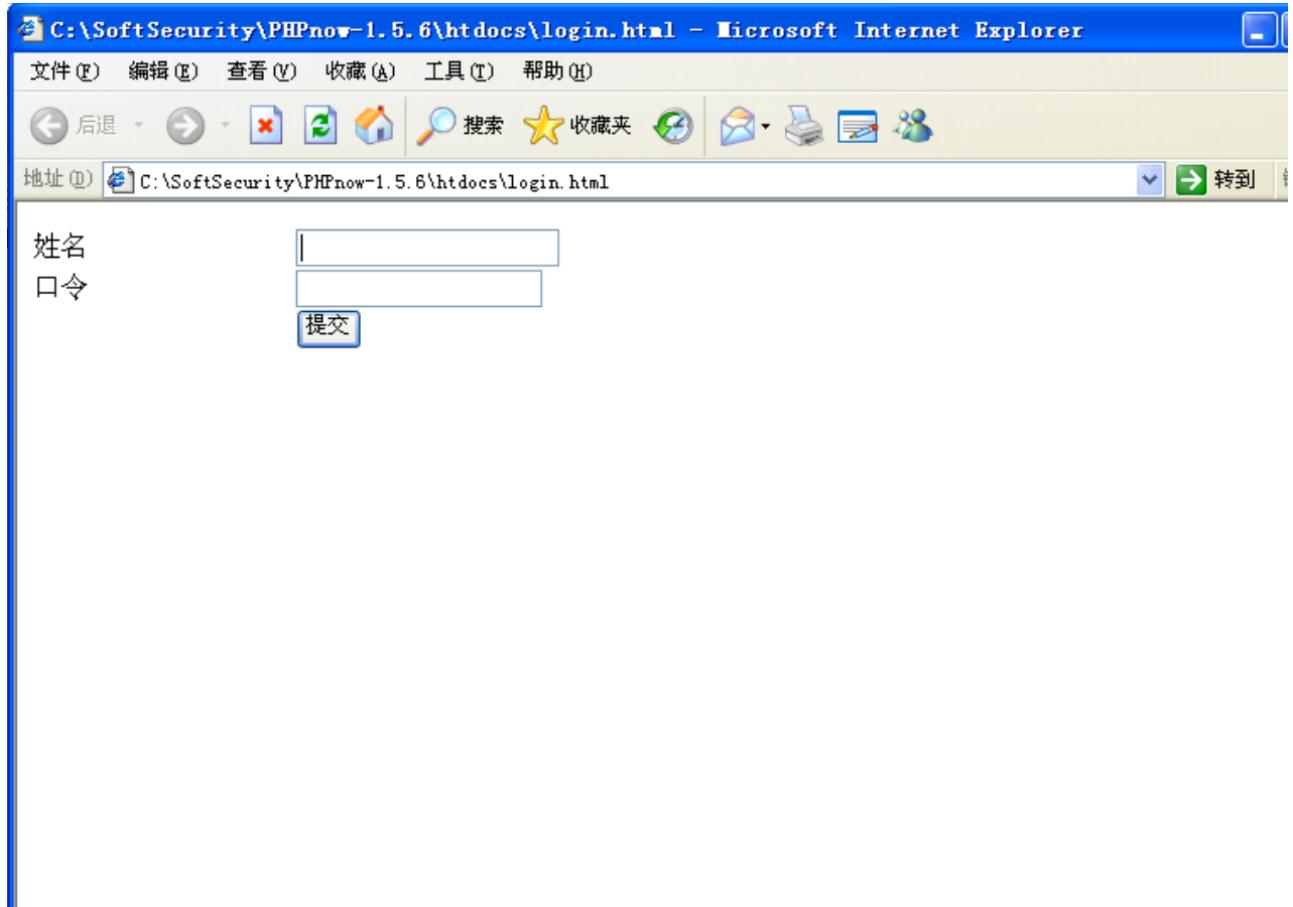
接下来我们就开始编写代码完成基本的插入、查询和删除操作。

### 3.2.2 [login.html](#)

登录界面代码

```
1 <html>
2 <body>
3 <form id="form1" name="form1" method="post" action="loginok.php">
4 <table width="900" border="0" cellspacing="0" cellpadding="0">
5 <tr>
6 <td height="20">姓名</td>
7 <td height="20"><label>
8 <input name="username" type="text" id="username" />
9 </label></td>
10 </tr>
11 <tr>
12 <td height="20">口令</td>
13 <td height="20"><label>
14 <input name="pwd" type="password" id="pwd" />
15 </label></td>
16 </tr>
17 <tr>
18 <td height="20"> </td>
19 <td height="20"><label>
20 <input type="submit" name="Submit" value="提交" />
21 </label></td>
22 </tr>
23 </table>
24 </form>
25 </body>
26 </html>
```

相应 html 文件被浏览器渲染如下。接下来我们用 [loginok.php](#) 来处理提交的表单(登录)。



### 3.2.3 [loginok.php](#)

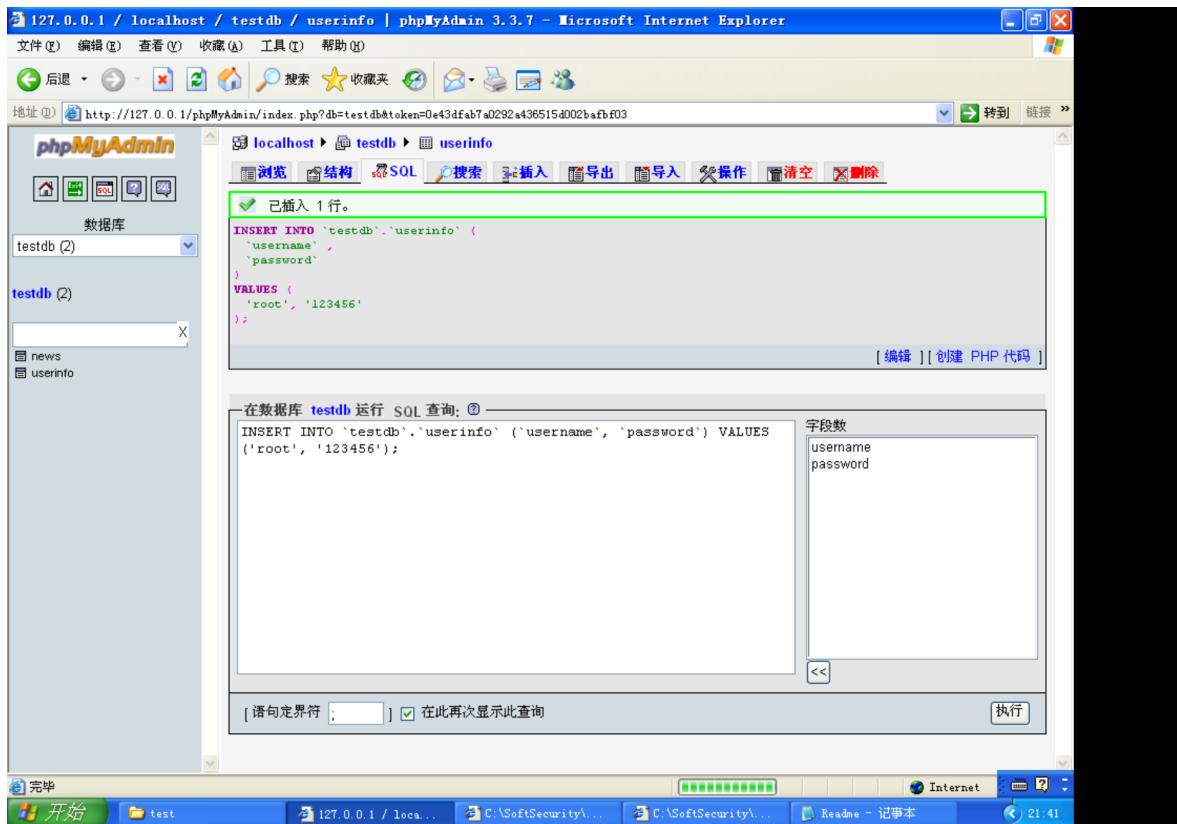
登录验证部分代码:

```
1 <?php
2 $loginok=0;
3 $conn=mysql_connect("localhost", "root", "123456");
4 $username = $_POST['username'];
5 $pwd = $_POST['pwd'];
6 $SQLStr = "SELECT * FROM userinfo where username='".$username' and
password='".$pwd."'";
7 echo $SQLStr;
8 $result=mysql_db_query("testDB", $SQLStr, $conn);
9 if ($row=mysql_fetch_array($result)) //通过循环读取数据内容
{
11 $loginok=1;
12 }
13 // 释放资源
```

```
14 mysql_free_result($result);
15 // 关闭连接
16 mysql_close($conn);
17 if ($loginok==1)
18 {
19 ?>
20 <script>
21 alert("login succes");
22 window.location.href="sys.php";
23 </script>
24 <?php
25 }
26 else{
27 ?>
28 <script>
29 alert("login failed");
30 history.back();
31 </script>
32 <?php
33 }
34
35 ?>
```

这个主要实现的是，读取数据库的 userinfo 表，检查表单提交的用户名和密码是否在其中，如果在就提示成功登录并跳转到 [sys.php](#)；错误则提示登录失败并后退。

因此我们可以插入一个用户，然后进行验证。



当输入正确密码时

```
SELECT * FROM userinfo where username='root' and password='123456'
```



输入错误密码时

```
SELECT * FROM userinfo where username='root' and password='3232'
```



说明我们的登录验证逻辑正常运行。

### 3.2.4 sys.php

实现系统管理员界面，这是我们管理员管理新闻的界面。代码如下

```
1 <html xmlns="http://www.w3.org/1999/xhtml">
2 <head>
3 <meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
4 <title>主页</title>
5 </head>
6 <?php
7 $conn=mysql_connect("localhost", "root", "123456");
8 ?>
9 <body>
10 <div align="center">
11 <table width="900" border="0" cellspacing="0" cellpadding="0">
12 <tr>
13 <td height="40"><form id="form1" name="form1" method="post"
action="add.php">
14 <div align="right">新闻标题:
15 <input name="topic" type="text" id="topic" size="50" />
16 <BR>
17 新闻内容:
18 <textarea name="content" cols="60" rows="8" id="content"></textarea>
19 <BR>
20 <input type="submit" name="Submit" value="添加" />
21 </div>
22 </form>
23 </td>
</tr>
```

```
24 <tr>
25 <td><hr /></td>
26 </tr>
27 <tr>
28 <td height="300" align="center" valign="top"><table width="600"
border="0" cellspacing="0"
cellpadding="0">
29 <tr>
30 <td width="100" height="30"><div align="center">新闻序号</div></td>
31 <td><div align="center">新闻标题</div></td>
32 <td><div align="center">删除</div></td>
33 </tr>
34 <?php
35 $SQLStr = "select * from news";
36 $result=mysql_db_query("testDB", $SQLStr, $conn);
37 if ($row=mysql_fetch_array($result))//通过循环读取数据内容
38 {
39 // 定位到第一条记录
40 mysql_data_seek($result, 0);
41 // 循环取出记录
42 while ($row=mysql_fetch_row($result))
43 {
44 ?
45 ?>
46 <tr>
47 <td height="30"><div align="center"> <?php echo $row[0] ?> </div></td>
48 <td width="400"> <div align="center"> <?php echo $row[1] ?> </div>
</td>
49 <td><div align="center"><a href="del.php?newsid=<?php echo $row[0] ?> "
> 删除 </a>
50 </div></td>
51 </tr>
52 <?php
53 }
54 }
55 ?>
56 </table></td>
57 </tr>
58 </table>
59 </div>
60 </body>
61 </html>
62 <?php
63 // 释放资源
64 mysql_free_result($result);
```

```
65 // 关闭连接  
66 mysql_close($conn);  
67 ?>
```

当我们成功登录后，来到这个界面。可以通过填写表单来添加新闻到数据库。

新闻序号	新闻标题	删除

### 3.2.5 add.php

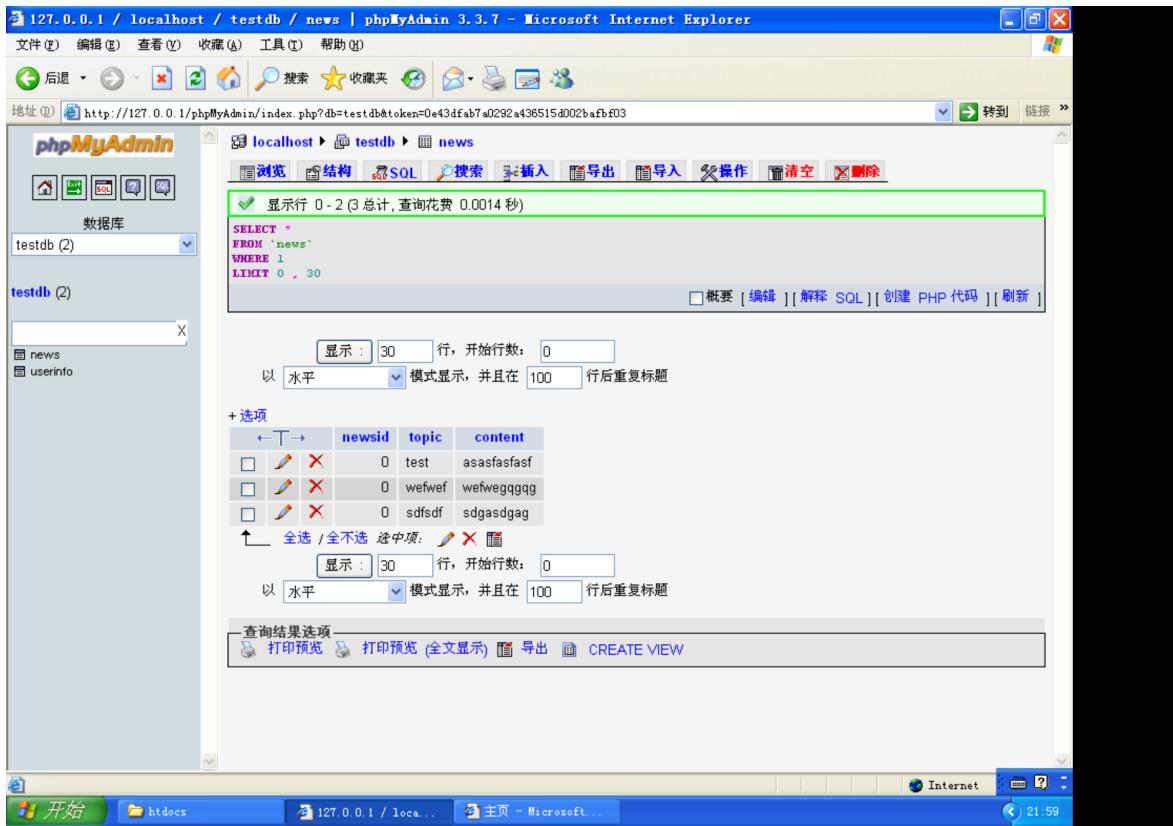
在前一个界面我们按下添加按钮，会来到这个界面并执行代码。我们把这个添加新闻的代码写上，即可添加新闻。

```
1 <?php  
2 $conn=mysql_connect("localhost", "root", "123456");  
3 mysql_select_db("TestDB");  
4 $topic = $_POST['topic'];  
5 $content = $_POST['content'];  
6 $SQLStr = "insert into news(topic, content) values('$topic',  
7 '$content')";  
echo $SQLStr;  
8 $result=mysql_query($SQLStr);  
9  
10 // 关闭连接  
11 mysql_close($conn);  
12 if ($result)  
13 {  
14 ?>  
15 <script>  
16 alert("insert succes");  
17 window.location.href="sys.php";  
18 </script>  
19 <?php  
20 }
```

```
21 else{
22 ?>
23 <script>
24 alert("insert failed");
25 history.back();
26 </script>
27 <?php
28 }
29
30 ?>
```

效果如下，且可以在后端数据库查到这条添加的新闻





### 3.2.6 del.php

在 `sys.php` 界面，我们可以通过点击删除按钮来删掉已有的新闻，这是通过如下代码实现的：

```

1 <?php
2 $conn=mysql_connect("localhost", "root", "123456");
3 mysql_select_db("TestDB");
4 $newsid = $_GET['newsid'];
5 $SQLStr = "delete from news where newsid=$newsid";
6 echo $SQLStr;
7 $result=mysql_query($SQLStr);
8 // 关闭连接
9 mysql_close($conn);
10 if ($result)
11 {
12 ?>
13 <script>
14 alert("delete succes");
15 window.location.href="sys.php";
16 </script>
17 <?php
18 }
19 else{
20 ?>
```

```
21 <script>
22 alert("delete failed");
23 history.back();
24 </script>
25 <?php
26 }
27 ?>
```

删除的时候，先连接数据库，然后查找相应的条目进行删除。尝试删除一条数据，结果如下。

```
delete from news where newsid=0
```



### 3.2.7 index.php

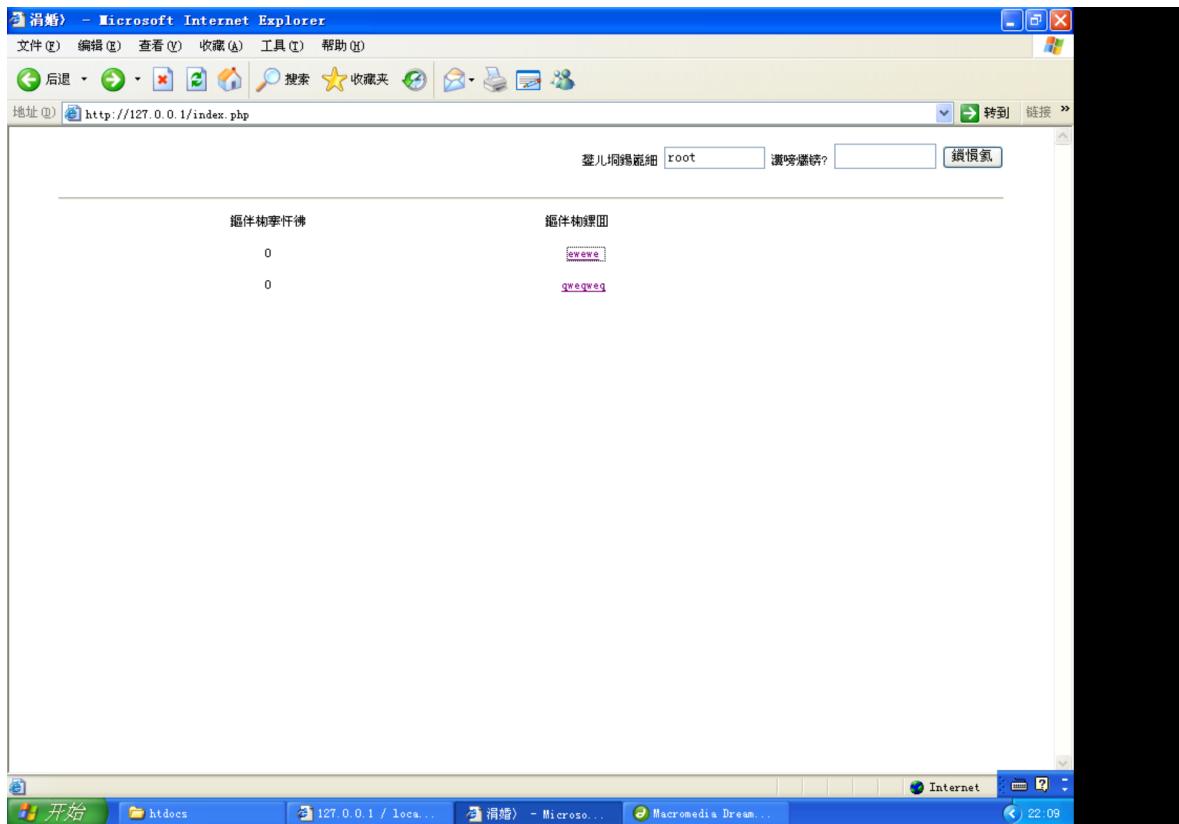
新闻主页，供用户进行新闻查看，代码如下：

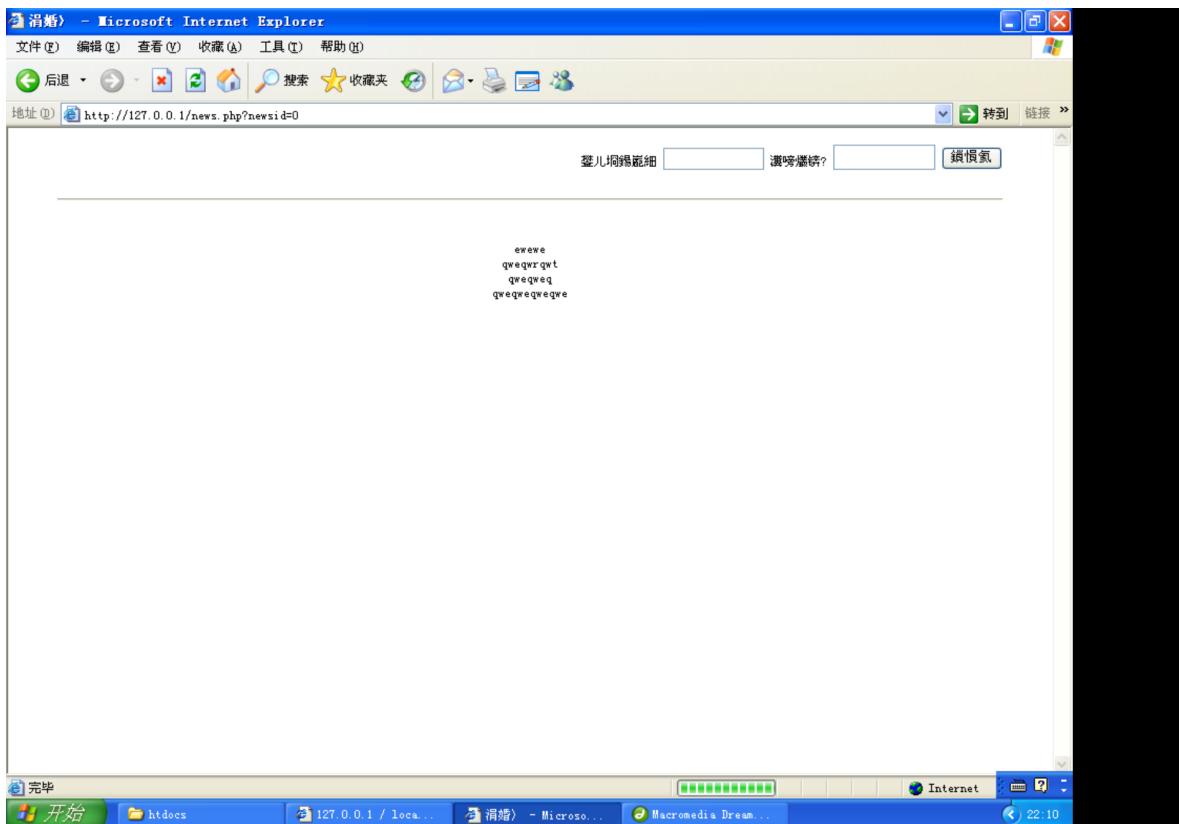
```
1 <html>
2 <head>
3 <meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
4 <title>主页</title>
5 </head>
6 <?php
7 $conn=mysql_connect("localhost", "root", "123456");
8 ?>
9 <body>
10 <div align="center">
11 <table width="900" border="0" cellspacing="0" cellpadding="0">
12 <tr>
13 <td height="40"><form id="form1" name="form1" method="post"
action="loginok.php">
14 <div align="right">用户名:
15 <input name="username" type="text" id="username" size="12" /> 密码:
```

```
16 <input name="pwd" type="password" id="pwd" size="12" />
17 <input type="submit" name="Submit" value="提交" />
18 </div>
19 </form>
20 </td>
21 </tr>
22 <tr>
23 <td><hr /></td>
24 </tr>
25 <tr>
26 <td height="300" align="center" valign="top"><table width="600"
border="0" cellspacing="0" cellpadding="0">
27 <tr>
28 <td width="100" height="30"><div align="center">新闻序号</div></td>
29 <td><div align="center">新闻标题</div></td>
30 </tr>
31 <?php
32 $SQLStr = "select * from news";
33 $result=mysql_db_query("testDB", $SQLStr, $conn);
34 if ($row=mysql_fetch_array($result))//通过循环读取数据内容
35 {
36 // 定位到第一条记录
37 mysql_data_seek($result, 0);
38 // 循环取出记录
39 while ($row=mysql_fetch_row($result))
40 {
41 ?>
42 <tr>
43 <td height="30"><div align="center"> <?php echo $row[0] ?> </div></td>
44 <td> <div align="center"> <a href="news.php?newsid=<?php echo $row[0] ?>
" > <?php echo
45 $row[1] ?> </a> </div></td>
46 </tr>
47 <?php
48 }
49 }
50 ?>
51 </table></td>
52 </tr>
53 </table>
54 </div>
55 </body>
56 </html>
57 <?php
```

```
58 // 释放资源  
59 mysql_free_result($result);  
60 // 关闭连接  
61 mysql_close($conn);  
62 ?>
```

效果如下，点击链接可以就会通过 php 动态生成页面展示该新闻（这是通过 `news.php` 实现的）。





### 3.2.8 news.php

当我们在 `index.php` 点击链接时，会通过下面代码动态生成新闻内容的页面，效果见上。

```
1 <html>
2 <head>
3 <meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
4 <title>主页</title>
5 </head>
6 <body>
7 <div align="center">
8 <table width="900" border="0" cellspacing="0" cellpadding="0">
9 <tr>
10 <td height="40"><form id="form1" name="form1" method="post"
action="loginok.php">
11 <div align="right">用户名:
12 <input name="username" type="text" id="username" size="12" /> 密码:
13 <input name="password" type="password" id="password" size="12" />
14 <input type="submit" name="Submit" value="提交" />
15 </div>
16 </form>
17 </td>
18 </tr>
19 <tr>
```

```
20 <td><hr /></td>
21 </tr>
22 <tr>
23 <td height="300" align="center" valign="top"><p>&ampnbsp</p>
24 <?php
25 $conn=mysql_connect("localhost", "root", "123456");
26 $newsid = $_GET['newsid'];
27 $SQLStr = "select * from news where newsid=$newsid";
28 $result=mysql_db_query("testDB", $SQLStr, $conn);
29 if ($row=mysql_fetch_array($result))//通过循环读取数据内容
30 {
31 // 定位到第一条记录
32 mysql_data_seek($result, 0);
33 // 循环取出记录
34 while ($row=mysql_fetch_row($result))
35 {
36 echo "$row[1]<br>"; echo "$row[2]<br>";
37 }
38 }
39 // 释放资源
40 mysql_free_result($result);
41 // 关闭连接
42 mysql_close($conn);
43 ?>
44 </td>
45 </tr>
46 </table>
47 </div>
48 </body>
49 </html>
```

至此，我们完成了一个简单的 web 应用，可以用来查看新闻，并供管理员用户添加、删除新闻。完成了基本的增改删查功能的实现。

## 4 心得体会：

第一回使用 php 来创建网站。了解了 web 应用的围绕数据进行增删改查的特性。php 由于是直接基于 html 进行动态生成的，逻辑简单直观，可以用来做 web 的激素入门，让我们简单地体会一下 web 应用的运作方式。从 php 开始入门 web 大概比表达丰富但稍显复杂的 javascript 稍微容易一些。