

软件安全实验10

姓名：何叶 学号：2313487 班级：范玲玲班

软件安全实验10

姓名：何叶 学号：2313487 班级：范玲玲班

实验名称：WEB开发

实验要求：

实验原理：

实验步骤：

一、安装Dreamweaver 8

- 1.解压缩后通过共享文件夹传入XP虚拟机
- 2.安装Dreamweaver 8
- 3.成功安装
- 4.打开Dreamweaver 8软件

二、安装PHPnow

- 1.setup.exe初始化
- 2.解压PHPnow
- 3.初始化失败
- 4.找到cmd.exe
- 5.在桌面创建快捷方式
- 6.cmd安装依然失败，选择在win11装
- 7.管理员进入初始化
- 8.设置root密码为123456
- 9.进入PHP默认界面
- 10.默认资源index.php
- 11.MYSQL连接正确
- 12.进入phpMyAdmin
- 13.输入用户名和密码
- 14.创建数据库 testDB 成功
- 15.新建userinfo，添加值username，pwd
- 16.得到表
- 17.插入admin

三、编写示例

- 1.打开Dreamweaver8新建html
- 2.编写login.html
- 3.进入127.0.0.1/login.html
- 4.新建loginok.php
- 5.打开loginok.php
- 6.写loginok.php
- 7.如果输入错误
- 8.输入正确
- 9.写sys.php
- 10.写数据库表news
- 11.写add.php用于增加新闻
- 12.新闻界面
- 13.写del.php用于删除新闻
- 14.写index.php用于查看新闻
- 15.写news.php点击

心得体会：

实验名称：WEB开发

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

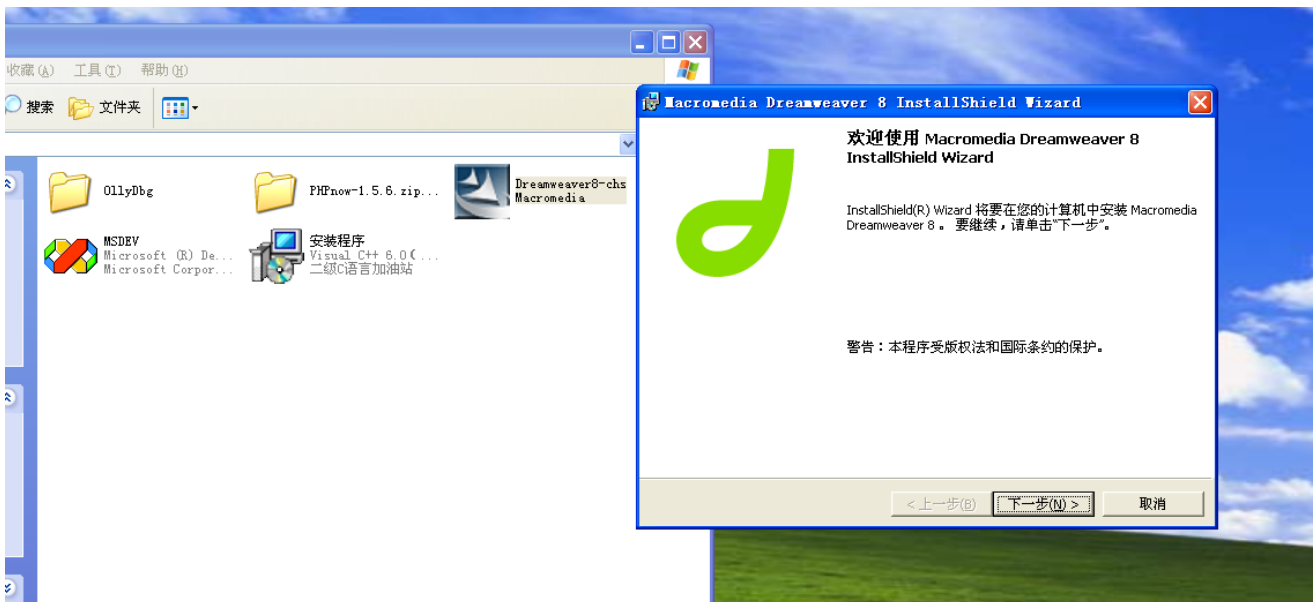
实验原理：

本实验主要通过使用PHP语言结合MySQL数据库，实现一个简单的Web应用程序，完成用户登录、新闻添加、查询和删除等功能。实验的核心在于PHP与MySQL的交互，通过PHP的 `mysql_connect` 、`mysql_db_query` 等函数，实现与MySQL数据库的连接、查询和操作。同时，利用HTML表单将用户输入的数据提交到PHP脚本进行处理，例如登录表单提交用户名和密码，新闻添加表单提交新闻标题和内容。根据用户输入和操作需求，构造相应的SQL语句（如 `SELECT` 、`INSERT` 、`DELETE` ），并通过PHP执行这些语句来完成数据库操作。此外，实验还涉及Web页面的动态生成，根据数据库查询结果动态生成HTML页面内容，例如显示新闻列表或新闻详情。

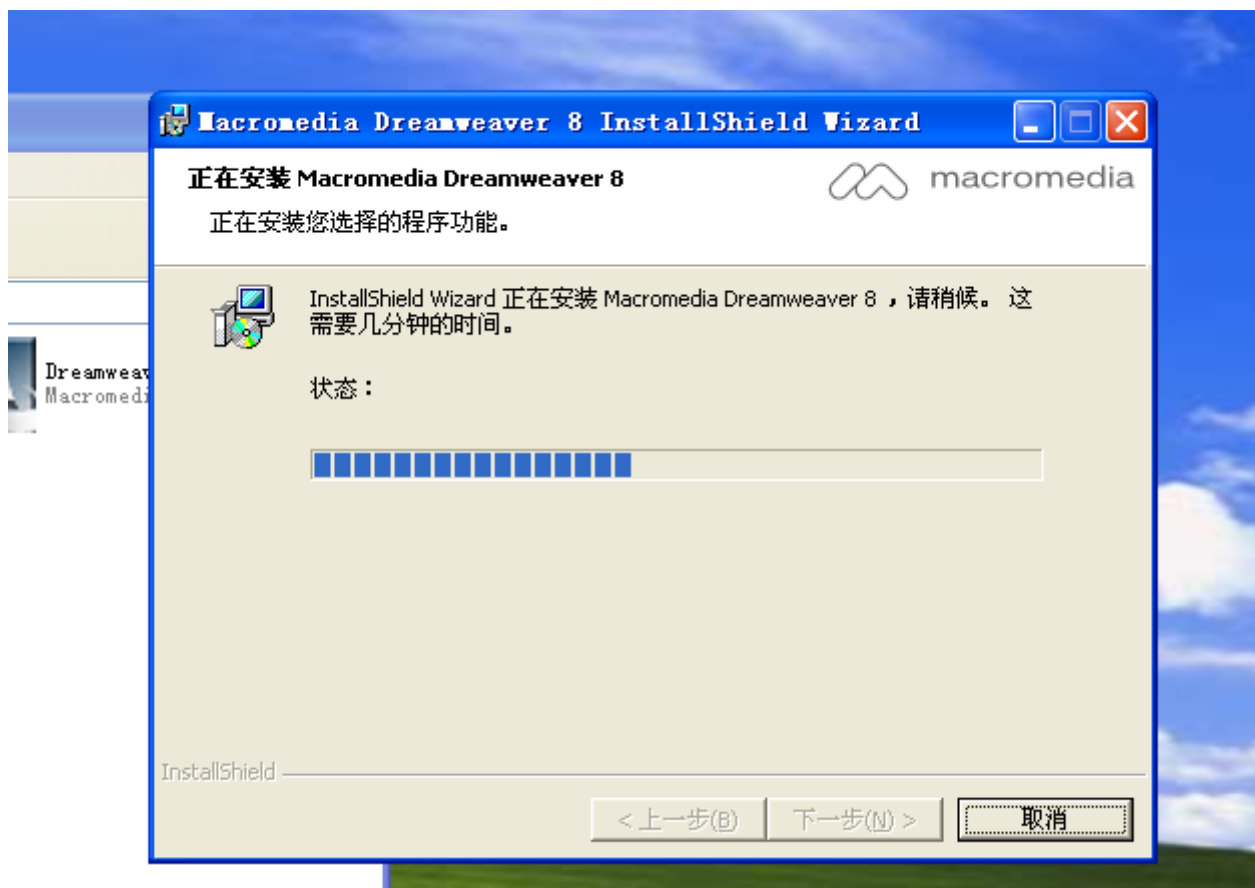
实验步骤：

一、安装Dreamweaver 8

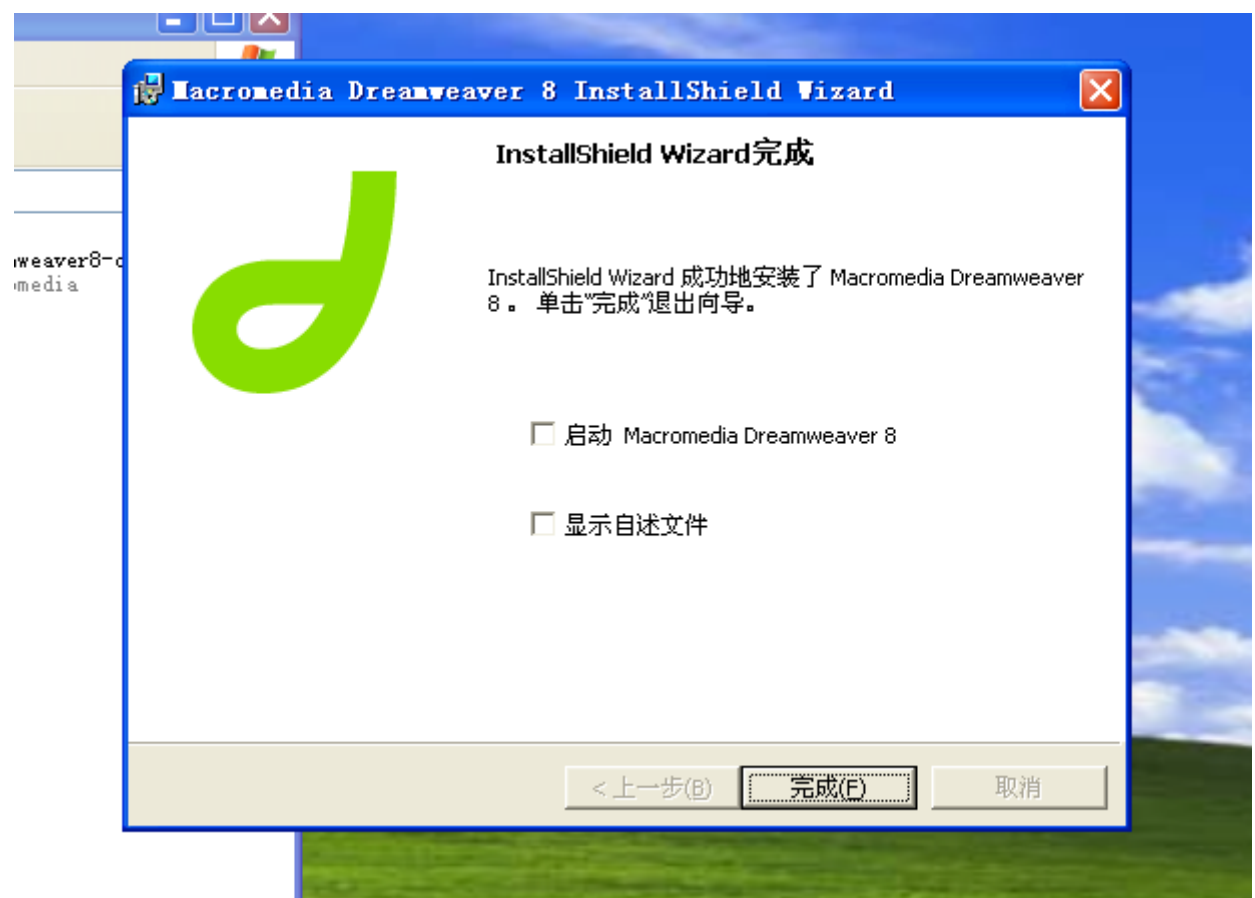
1.解压缩后通过共享文件夹传入XP虚拟机



2.安装Dreamweaver 8



3.成功安装



4.打开Dreamweaver 8软件

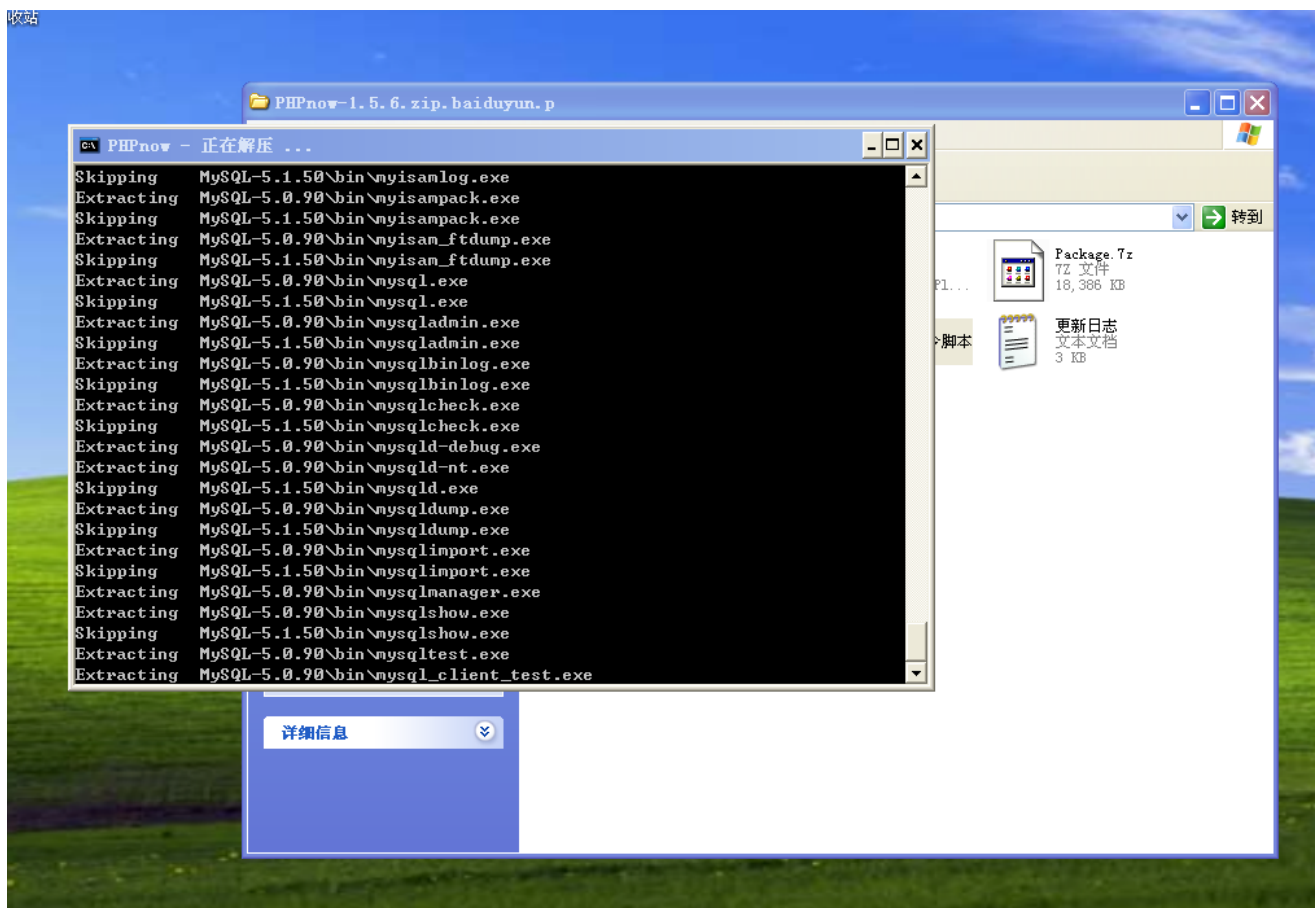


二、安装PHPnow

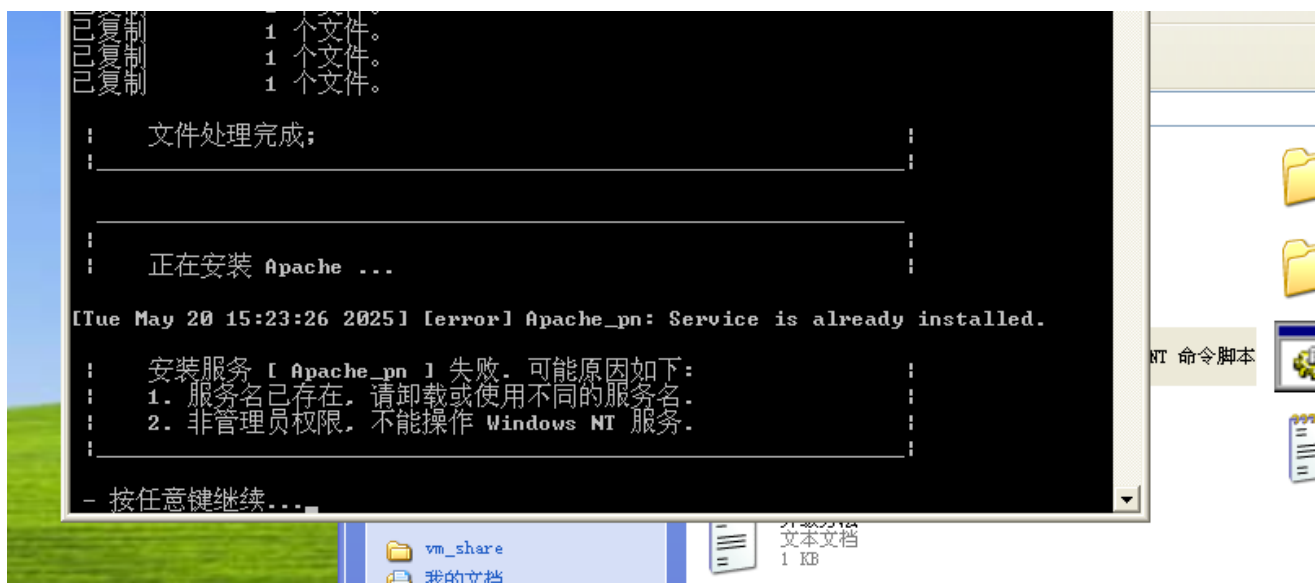
1.setup.exe初始化



2.解压PHPnow



3.初始化失败



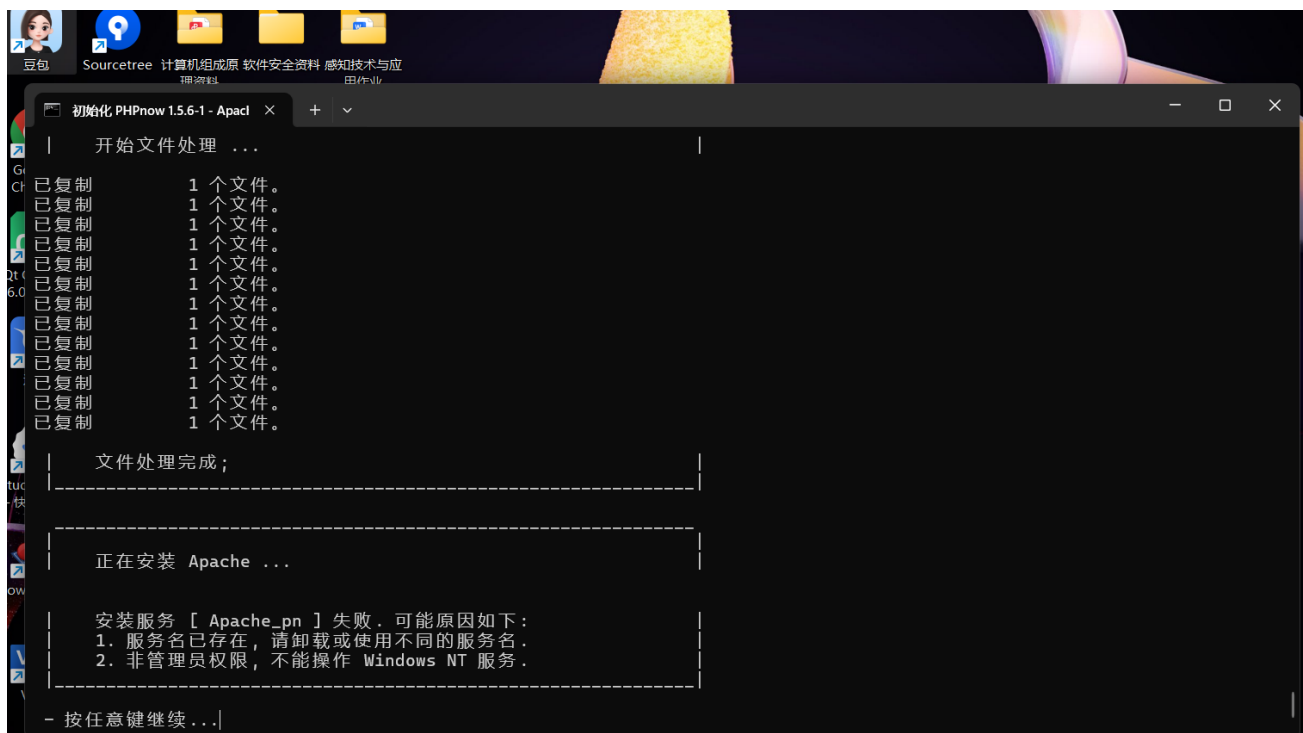
4.找到cmd.exe



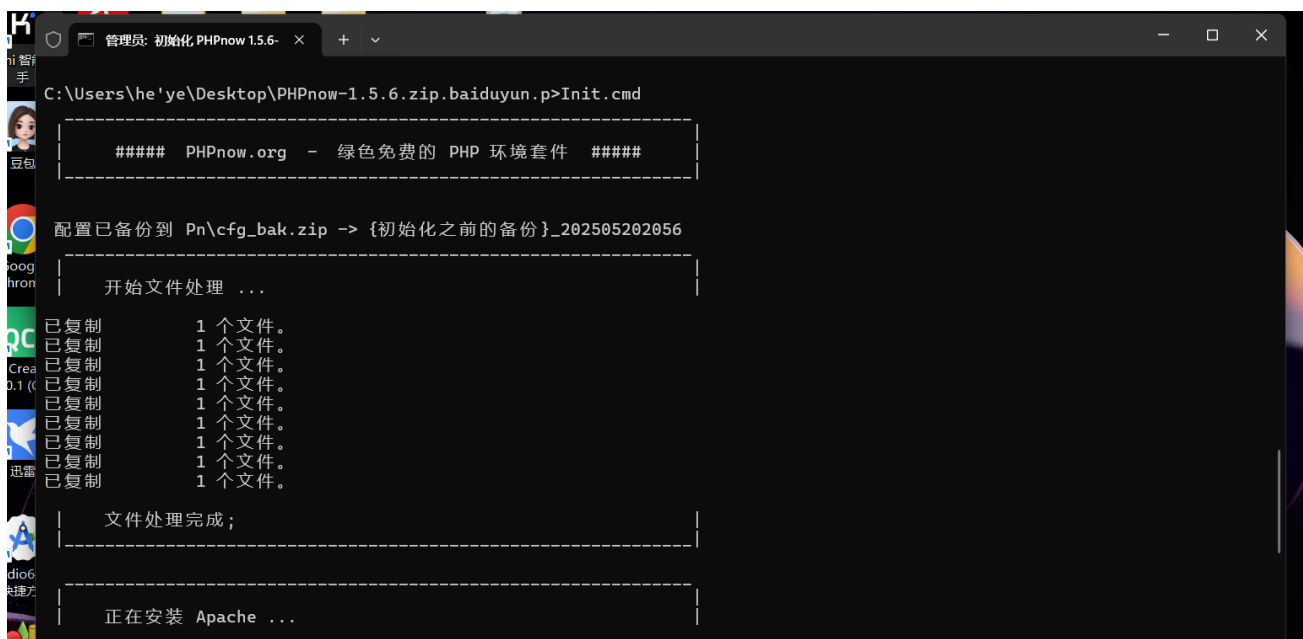
5.在桌面创建快捷方式



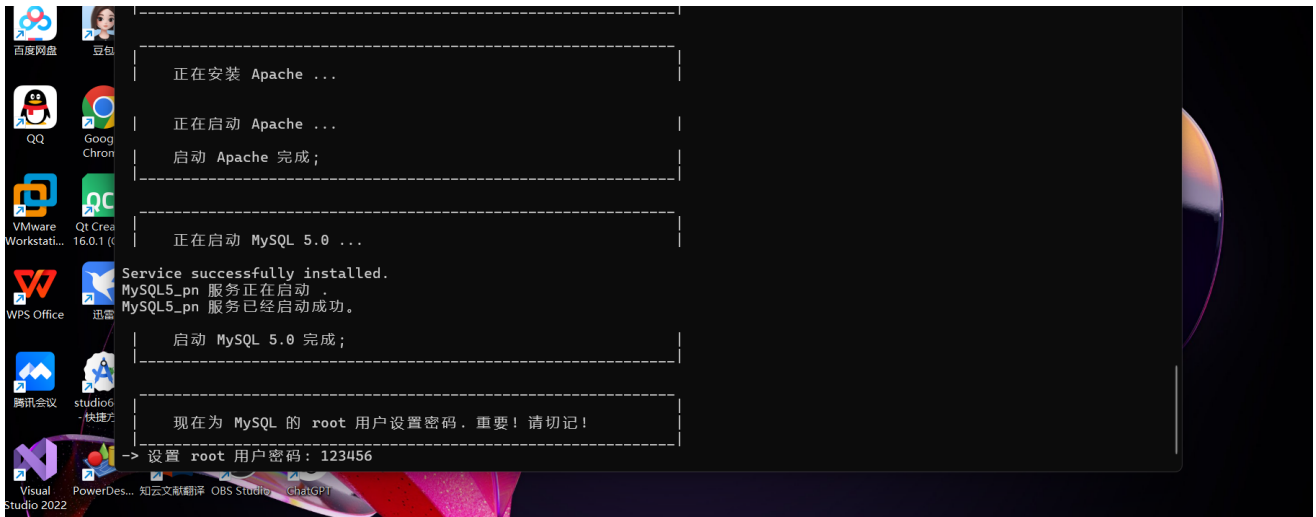
6.cmd安装依然失败，选择在win11装



7.管理员进入初始化



8.设置root密码为123456



9.进入PHP默认界面



127.0.0.1
Let's PHP now !

为何只能本地访问?
此服务器互联网 IP
117.131.219.63

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:\Users\he'ye\Desktop\PHPnow-1.5.6.zip.baiduyun.p\php-5.2.14-Win32\php-apache2handler.ini
网站主目录	C:/Users/he'ye/Desktop/PHPnow-1.5.6.zip.baiduyun.p/htdocs
Server Date / Time	2025-05-20 20:59:49 (+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	<input type="text" value="localhost"/>	MySQL 数据库名	<input type="text" value="test"/>
MySQL 用户名	<input type="text" value="root"/>	MySQL 用户密码	<input type="text"/>
			<input type="button" value="连接"/>

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

10.默认资源index.php

名称	修改日期	类型	大小
phpMyAdmin	2025/5/20 20:56	文件夹	
index.php	2010/9/22 17:16	phpfile	9 KB


11.MYSQL连接正确

MySQL 连接测试			
MySQL 服务器	<input type="text" value="localhost"/>	MySQL 数据库名	<input type="text" value="test"/>
MySQL 用户名	<input type="text" value="root"/>	MySQL 用户密码	<input type="password"/>
			<input type="button" value="连接"/>

MySQL 测试结果	
服务器 localhost	OK (8.0.40)
数据库 test	OK

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

12.进入phpMyAdmin



欢迎使用 phpMyAdmin

Language

中文 - Chinese simplified

登录

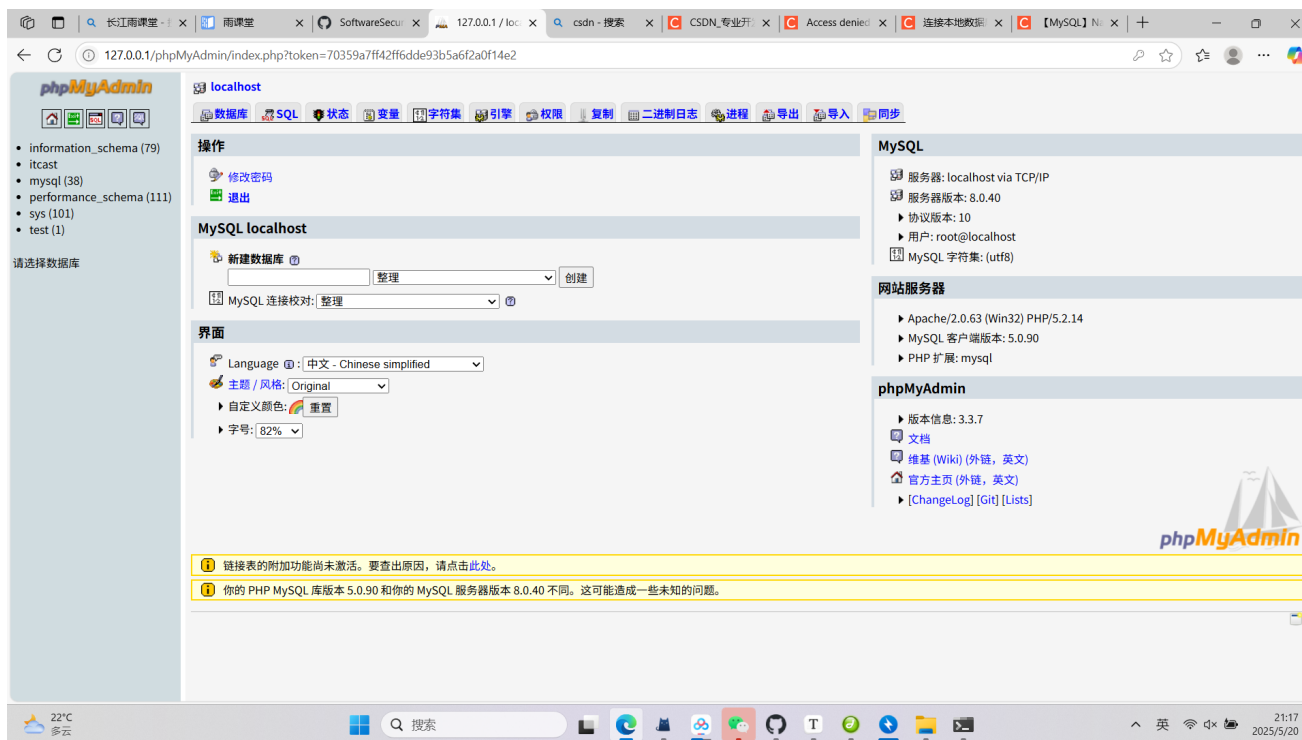
用户名:

密码:

执行

必须启用 Cookies 才能登录。

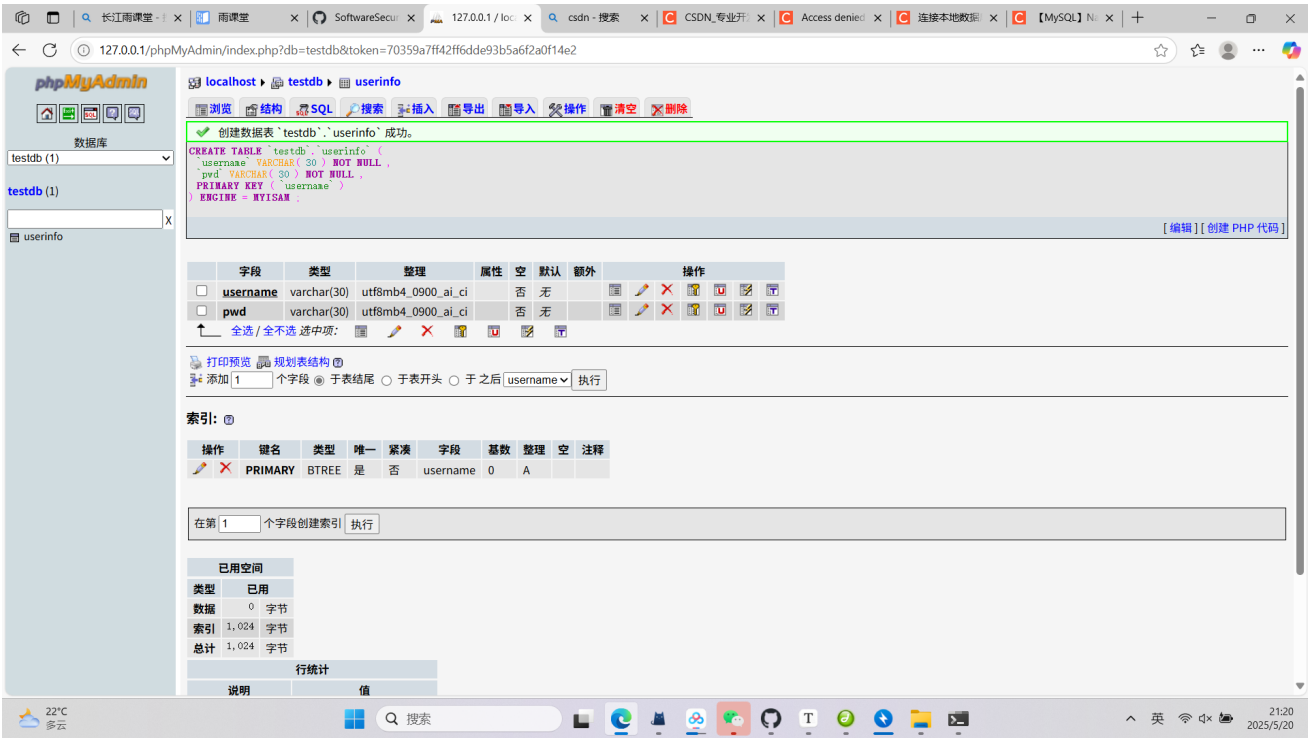
13.输入用户名和密码



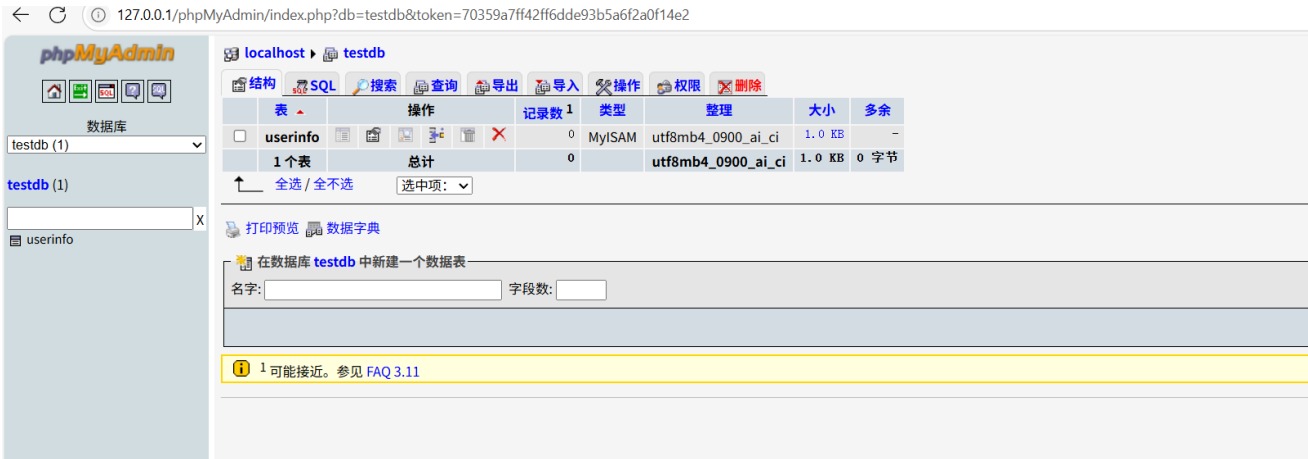
14.创建数据库 testDB 成功



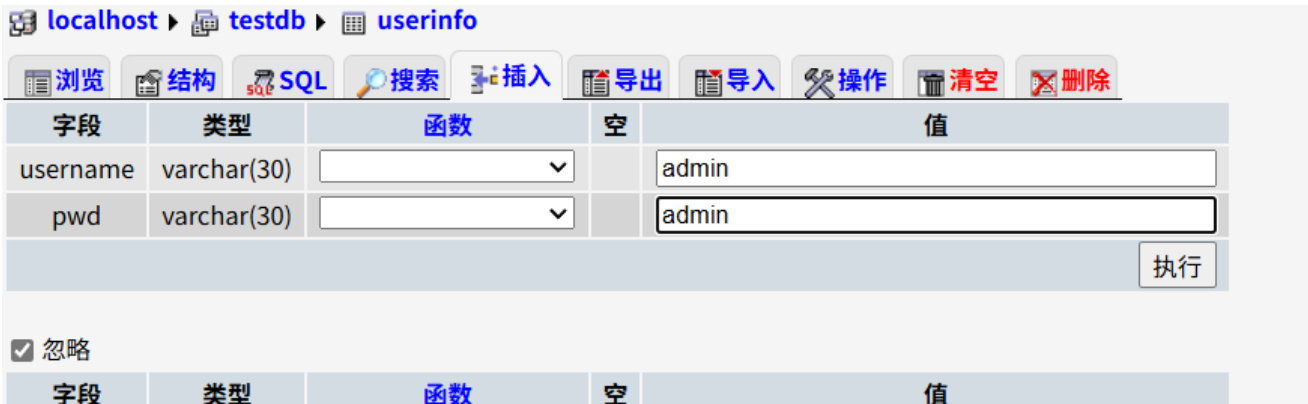
15.新建userinfo, 添加值username, pwd

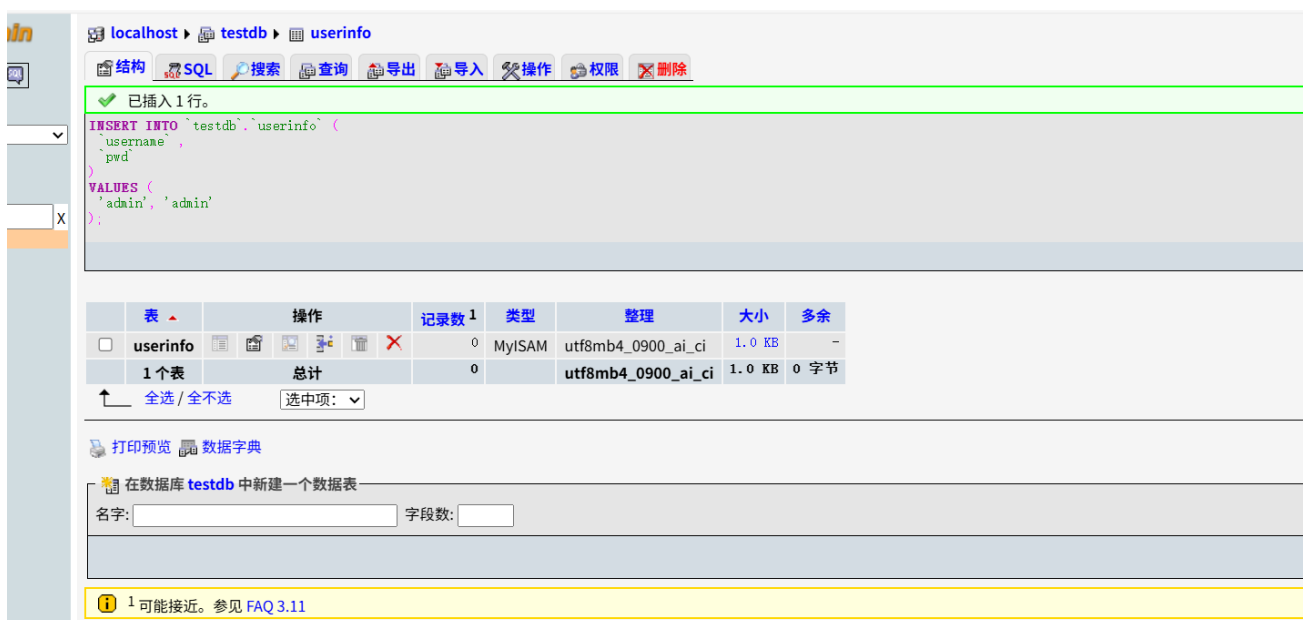


16.得到表



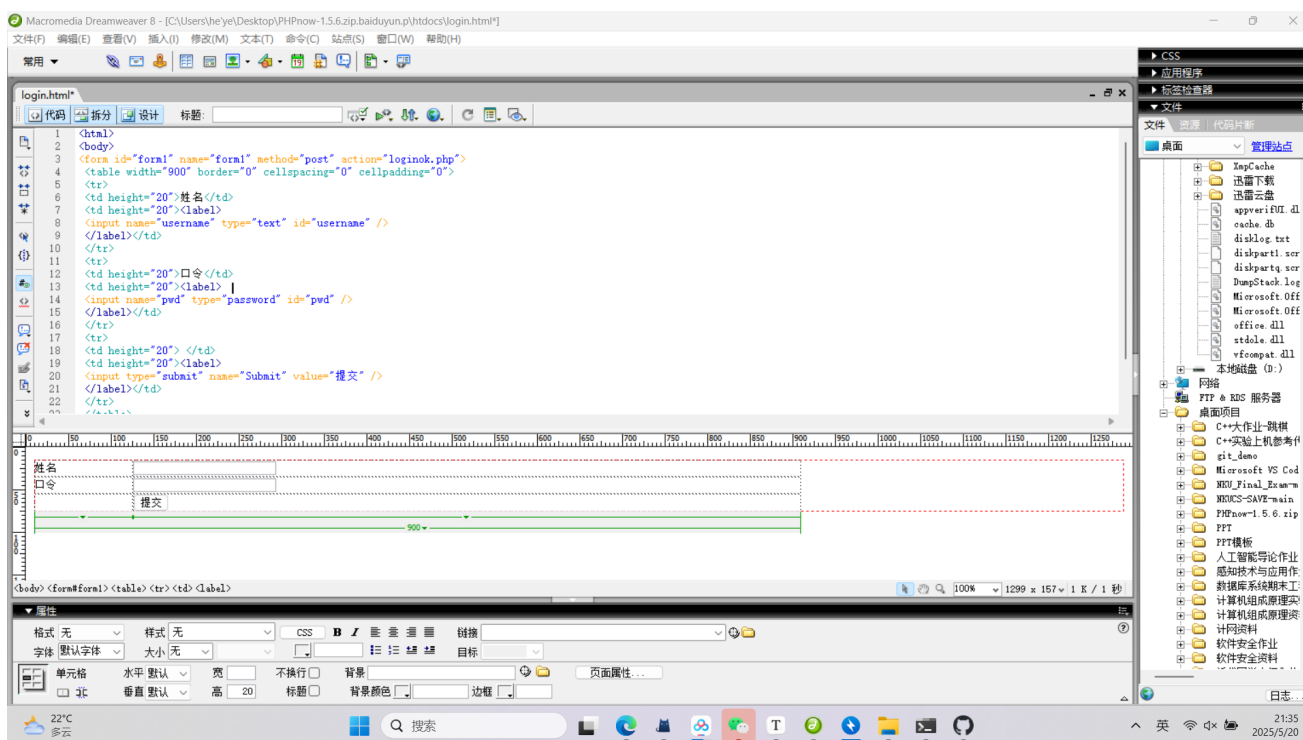
17.插入admin



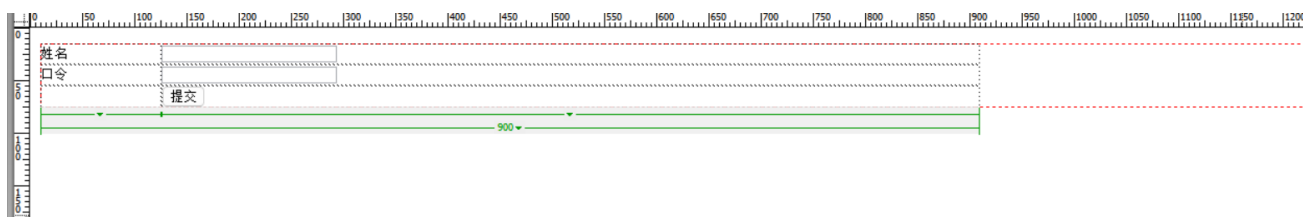


三、编写示例

1.打开Dreamweaver8新建html



2.编写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>

```

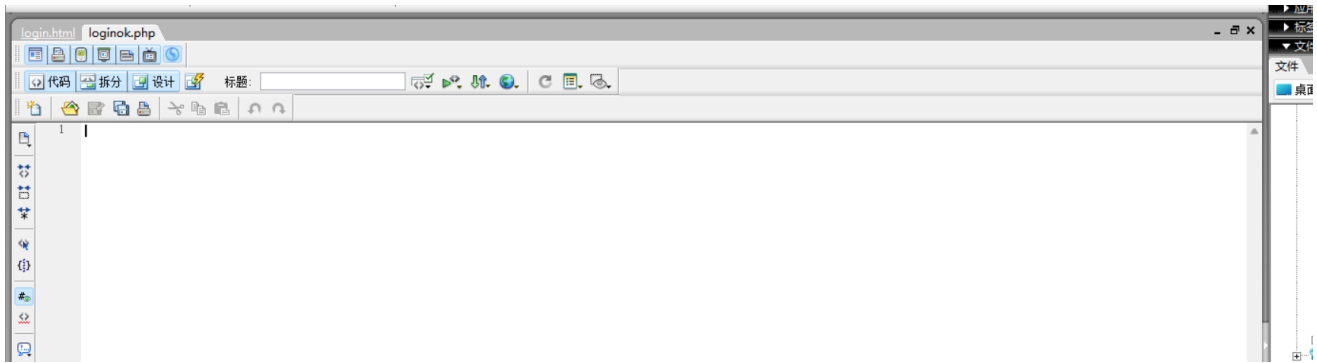
3.进入127.0.0.1/login.html



4.新建loginok.php

名称	修改日期	类型	大小
phpMyAdmin	2025/5/20 20:56	文件夹	
index.php	2010/9/22 17:16	phpfile	9 KB
login.html	2025/5/20 21:39	Firefox HTML D...	1 KB
loginok.php	2025/5/20 21:45	phpfile	0 KB

5.打开loginok.php



6.写loginok.php

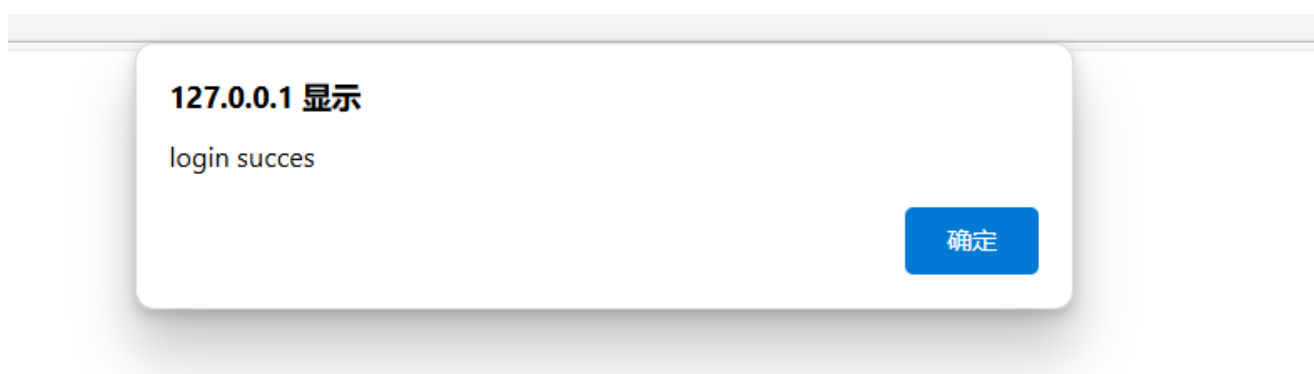
```
<?php
$loginok=0;
$conn=mysql_connect("localhost", "root", "123456");
$username = $_POST['username'];
$pwd = $_POST['pwd'];
$SQLStr = "SELECT * FROM userinfo where username='$username' and password='$pwd'";
echo $SQLStr;
$result=mysql_db_query("testDB", $SQLStr, $conn);
if ($row=mysql_fetch_array($result))//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 succes");
window.location.href="sys.php";
</script>
<?php
}
else{
?>
<script>
alert("login failed");
history.back();
</script>
<?php
}

?>
```

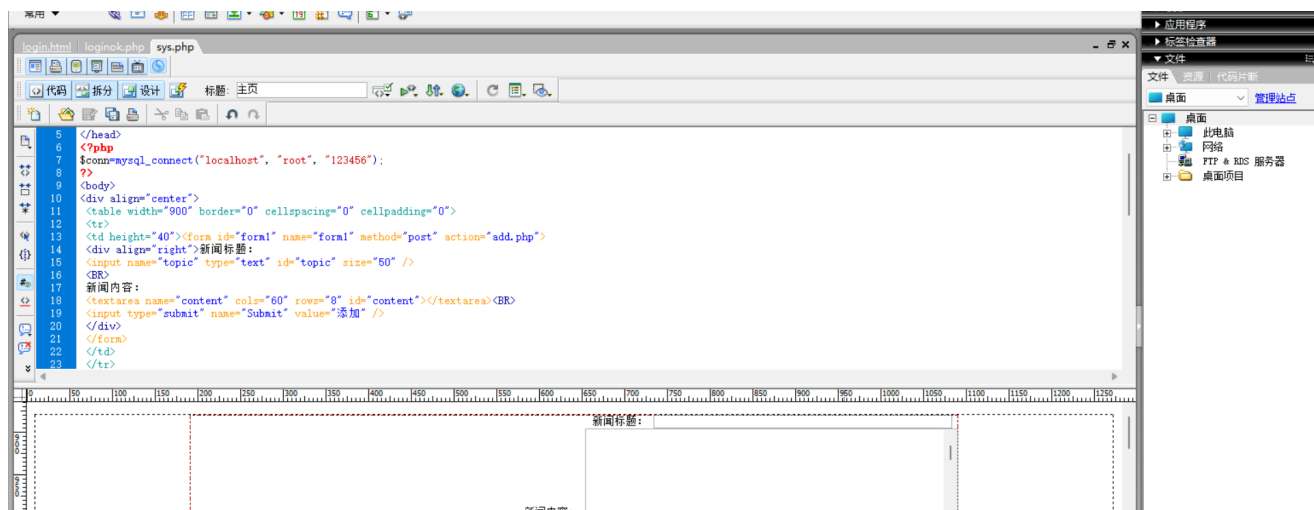
7.如果输入错误



8.输入正确



9.写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);
?>

```




















10.写数据库表news

127.0.0.1/phpMyAdmin/index.php?db=testdb&token=7bc7659b478d68e88b9ee19409b3d9c4

localhost ▸ testdb ▸ news

已成功修改表 news





```
ALTER TABLE `news` CHANGE `content` `content` TEXT CHARACTER SET utf8mb4 COLLATE utf8mb4_0900_ai_ci NOT NULL;
```

字段	类型	整理	属性	空	默认	额外	操作
<input type="checkbox"/> newsid	int			否	无	AUTO_INCREMENT	     
<input type="checkbox"/> topic	varchar(50)	utf8mb4_0900_ai_ci		否	无		     
<input type="checkbox"/> content	text	utf8mb4_0900_ai_ci		否	无		     

打印预览 规划表结构

添加 1 个字段 于表结尾 于表开头 于之后 newsid 执行

索引:

操作	键名	类型	唯一	紧凑	字段	基数	整理	空	注释
 	PRIMARY	BTREE	是	否	newsid	0	A		
 	newsid	BTREE	否	否	newsid	0	A		

索引 PRIMARY 和 newsid 可能是相同的, 其中一个将被删除

在第 1 个字段创建索引 执行

11.写add.php用于增加新闻

login.html | loginok.php | sys.php | add.php

代码 拆分 设计 标题:

```
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', '$content')";
7 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>
```

```
<?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
}

?>

```

12.新闻界面

新闻标题:

新闻内容:

添加

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in
C:\Users\he'ye\Desktop\PHPnow-1.5.6.zip\baiduyun.p\htdocs\sys.php on line 38

13.写del.php用于删除新闻

```

login.html | loginok.php | sys.php | add.php | del.php
代码 拆分 设计 标题:
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 ?>

```

```

<?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)

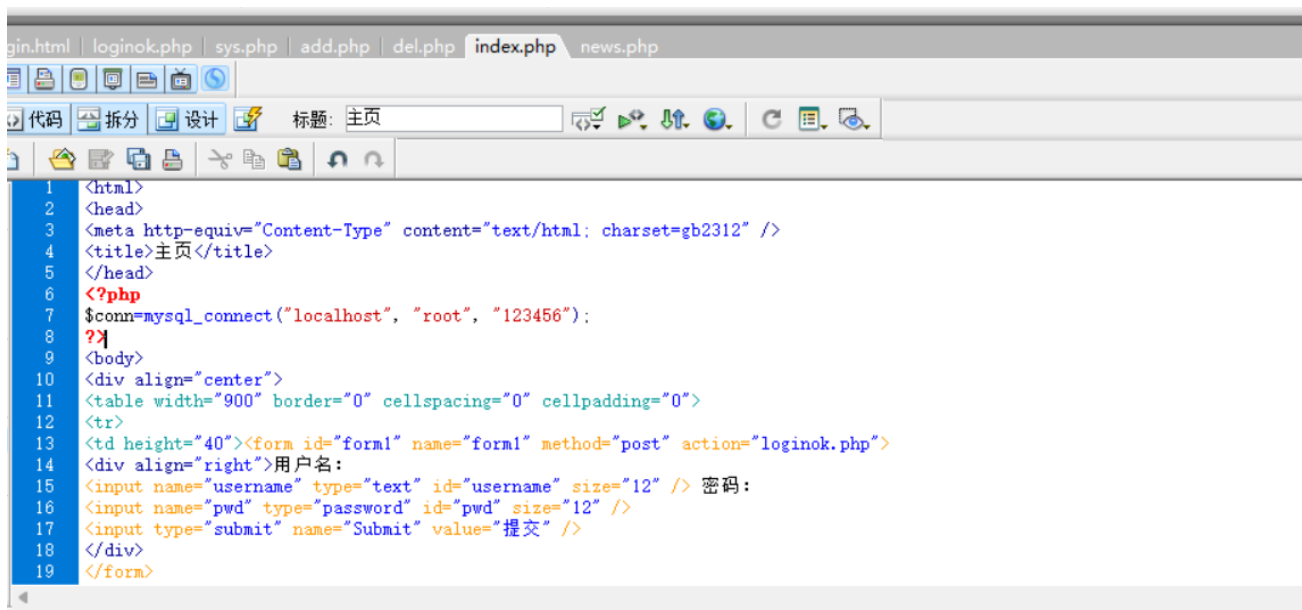
```

```

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

```

14.写index.php用于查看新闻



新闻标题:

新闻内容:

新闻序号	新闻标题	删除
1	holiday	删除

```

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>主页</title>
</head>
<?php
$conn=mysql_connect("localhost", "root", "123456");
?>

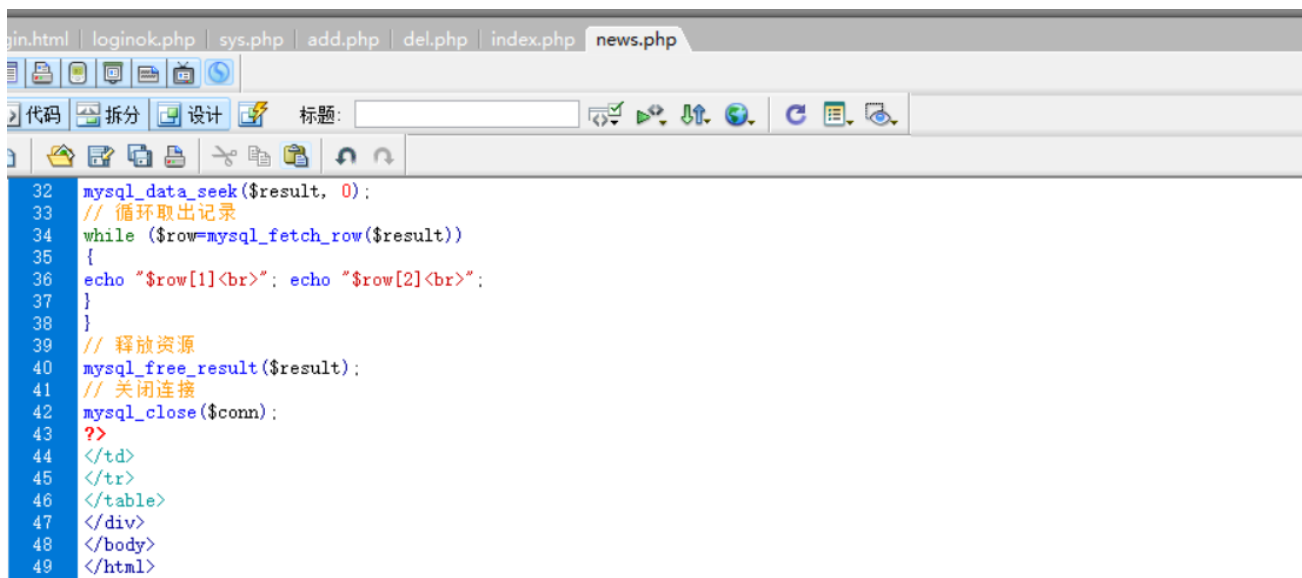
```

```

<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="pwd" type="password" id="pwd" 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);
?>

```

15.写news.php点击



```
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>
```

```
<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>
```

心得体会：

通过本次实验，我深入理解了PHP与MySQL结合进行Web开发的基本流程和方法。实验过程中，我学会了如何搭建开发环境，包括安装Dreamweaver和PHPnow，并成功创建了数据库和表。在编写代码时，我体会到了SQL注入问题的潜在风险，尤其是在构造SQL语句时，直接将用户输入拼接到SQL语句中可能会导致安全漏洞。未来，我将学习如何使用参数化查询等更安全的方法来避免此类问题。此外，通过实际操作，我对Web开发中的表单处理、页面跳转和动态内容生成有了更直观的认识，为后续学习更复杂的Web开发技术奠定了基础。