**《软件安全》实验报告**

姓名：禹相祐 学号：2312900 班级：计算机科学与技术

**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. **环境配置：**
2. **书本实验的复现：**

下面我们复现课本的10.3.5节，用php编写一个简单的数据库并实现数据的插入、查询和删除，一共可以分为八个步骤，如下所示。

**2.1 数据库的建立**

我们首先打开phpMyAdmin进行登录，登陆后如图：

然后建立表News(newsid,topic,content)和表userinfo(username,password),建立后如图：

**2.2 login.html编写**

首先先是登陆的部分，源代码如下：

<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>

我们打开html的网页，运行结果如图：

**2.3 loginok.php编写**

此处用来当用户输入正确的账号密码后，系统能够顺利载入下一个页面。我们首先为userinfo表中插入一条数据(admin,123456)方便进行验证，如图：

源代码如下：

<?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

}

?>

验证如图：

**2.4 sys.php编写**

此处用于在用户登陆后，能够上传新闻，包括标题、内容等，还能删除新闻，源代码如下：

<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", "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);

?>

效果如下图：

**2.5 add.php编写**

此处用于将sys.php传来的新闻的标题和内容添加到数据库中，源代码如下：

<?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

}

?>

我们尝试往其中插入一条news，观察器能否正常存入sys.php，如图：

**2.6 del.php编写**

此处用于将新闻从sys.php和数据库中同时删除，源代码如下：

<?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

}

?>

我们尝试删除第一条新闻，如图：

**2.7 index.php编写**

此处使得用户可以查看已经有的新闻并且点击链接能查看内容，源代码如下：

<html>

<head>

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

<title>主页</title>

</head>

<?php

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

?>

运行如图：

**2.8 news.php编写**

此处使得在点击新闻标题后能够显示新闻内容，源代码如下：

<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>

**心得体会：**

啊啊啊