《漏洞利用及渗透测试基础》实验报告

姓名：孙蕗 学号：2112060 班级：信息安全1班

**实验名称：**

WEB开发实践

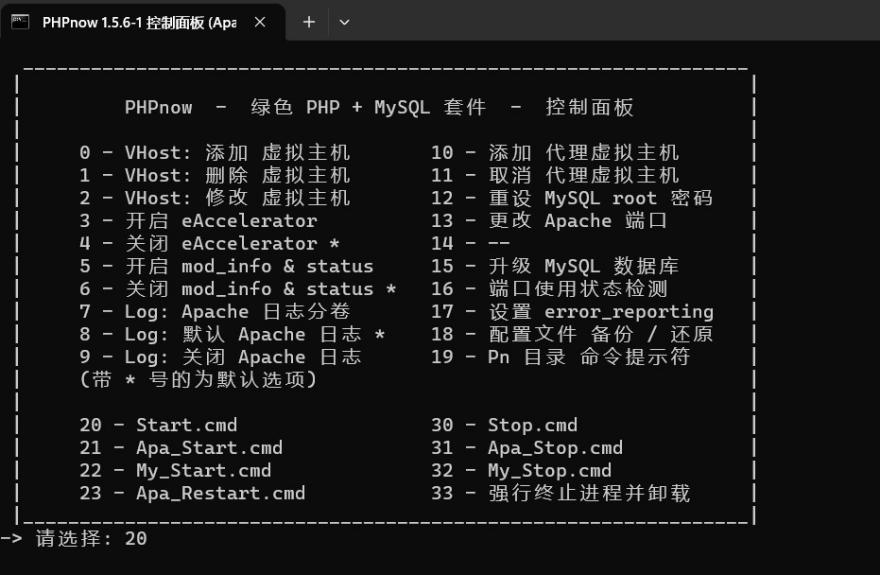
**实验要求：**

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、查询和删除操作的事例。

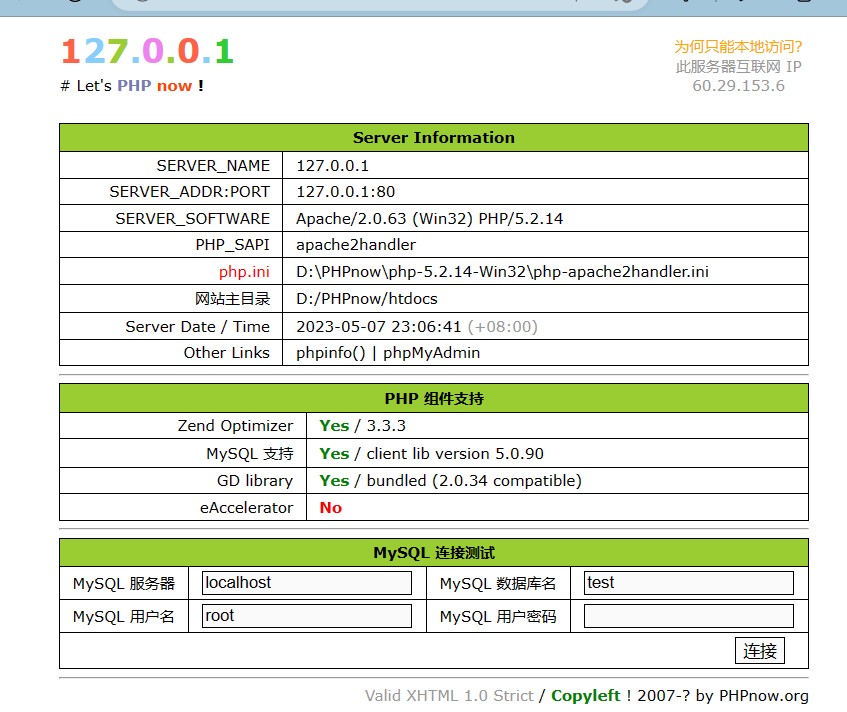
基于课本的完整的例子，进一步了解WEB开发的细节。

**实验过程：**

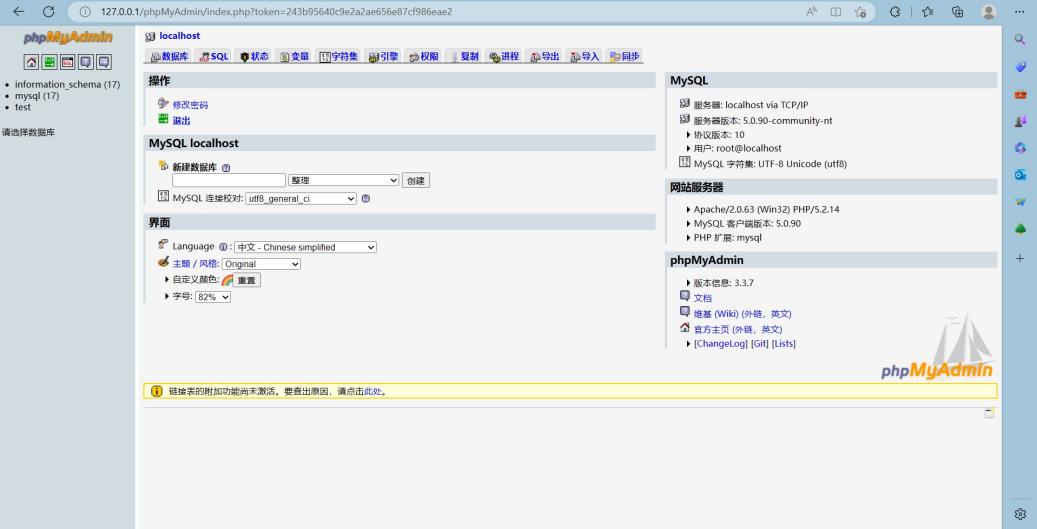
1. **安装phpnow**
2. 下载安装包，点击Pncp cmd，选择20



1. 打开网页，访问127.0.0.1如下，点击phpMyAdmin，将进入数据库管理界面，可以自行创建数据库、表以及录入数据等

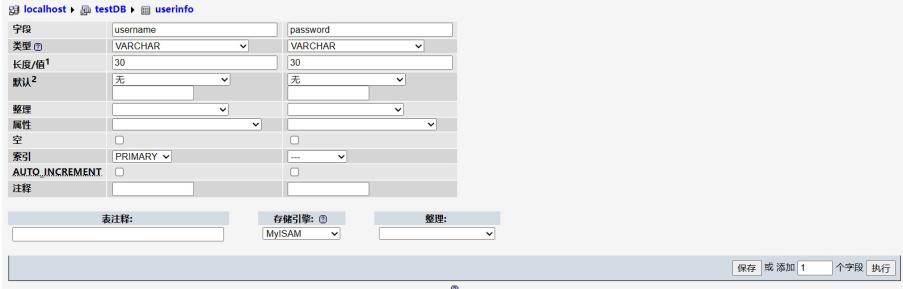


1. 进入数据库管理界面，可以自行创建数据库、表以及录入数据等



1. 建表





1. 代码
2. index.php

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<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="forml" name="forml" 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))//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);

?>

1. news.php

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>主页</title>

</head>

<body>

<div align="center">

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

<tr>

<td height="40">

<form id="forml" name="forml" 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>

1. loginok.php

<?php

$loginok=0;

$conn=mysql\_connect("localhost","root","123456");

$username=$\_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

}

?>

1. sys.php

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="texthtml; charset=utf-8" />

<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="forml" name="forml" 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="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>

<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 herf="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);

?>

1. 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 success");

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

</script>

<?php

}

else{

?>

<script>

alert("insert failed");

history.back();

</script>

<?php

}

?>

1. 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 success");

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

</script>

<?php

}

else{

?>

<script>

alert("delete failed");

history.back();

</script>

<?php

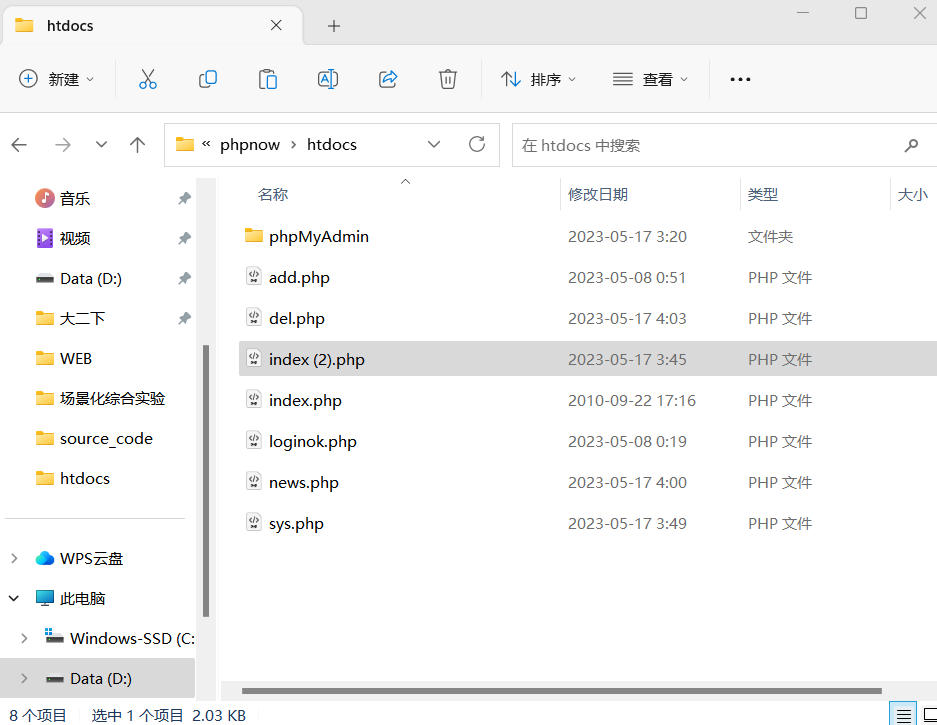
}

?>

1. 连接测试，连接成功

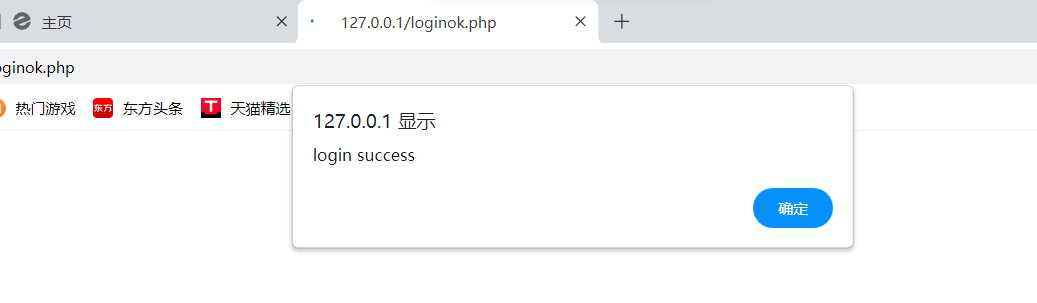


1. php文件添加到phpnow下的htdocs文件夹



1. **测试**
2. 登录是否成功

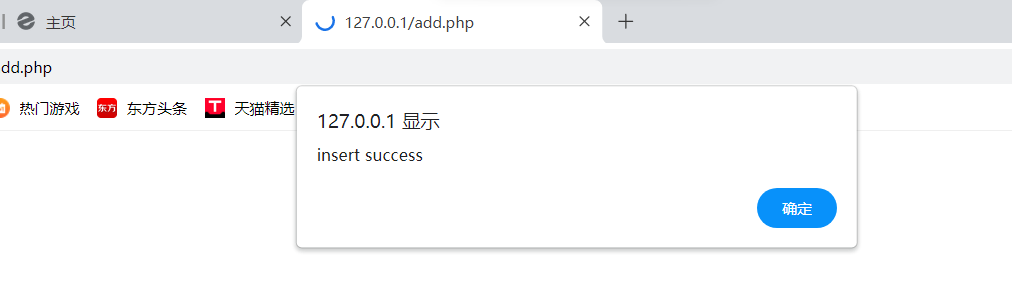




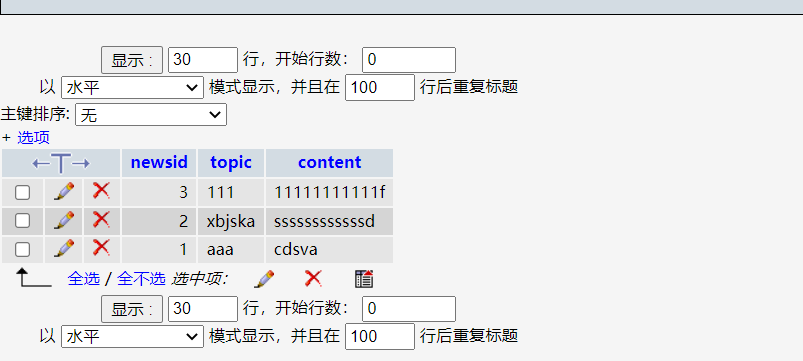
1. 系统管理界面



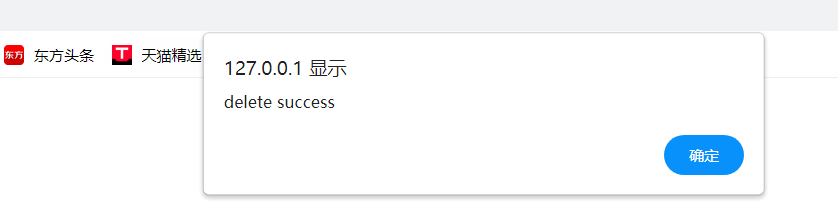
1. 添加新闻

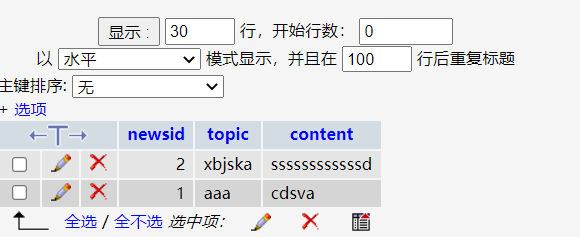






1. 删除







**心得体会：**

PHP是一种免费脚本语言，主要用途是处理静态网页，也包含命令行运行接口。PHP语法与C/C++、java、perl、asp、jsp有相通支出，并且还加上了自己的语法。PHP是一种面向html的解析语言，包括在PHP标记中的语句被解析，在其外的语句原样输出并接受PHP语句的控制。

学习了PHP语言的语法规则，包括注释、变量解析等，并连接数据库，利用SQL语句进行数据库的插入查询删除等操作。