《漏洞利用及渗透测试基础》实验报告

姓名：沙璇 学号：1911562 班级：信息安全

**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。

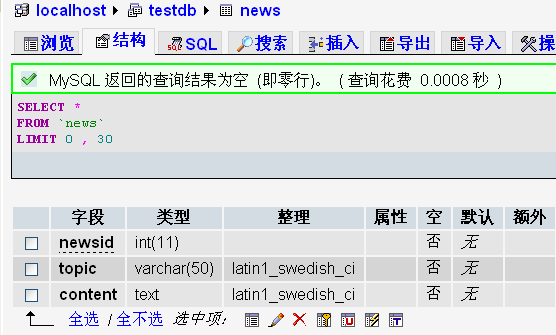
基于课本的完整的例子，进一步了解WEB开发的细节

**实验过程：**

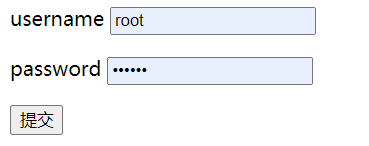
**①**在phpMyAdmin中新建数据库testdb并创建两个表

表1：News（newsid, topic, content）

表2：userinfo（username, password），结果如下图：

**②**在工作目录下新建login.html文件，用来编写用户登录页面布局，如下图：



**③**数据库插入（add.php）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");

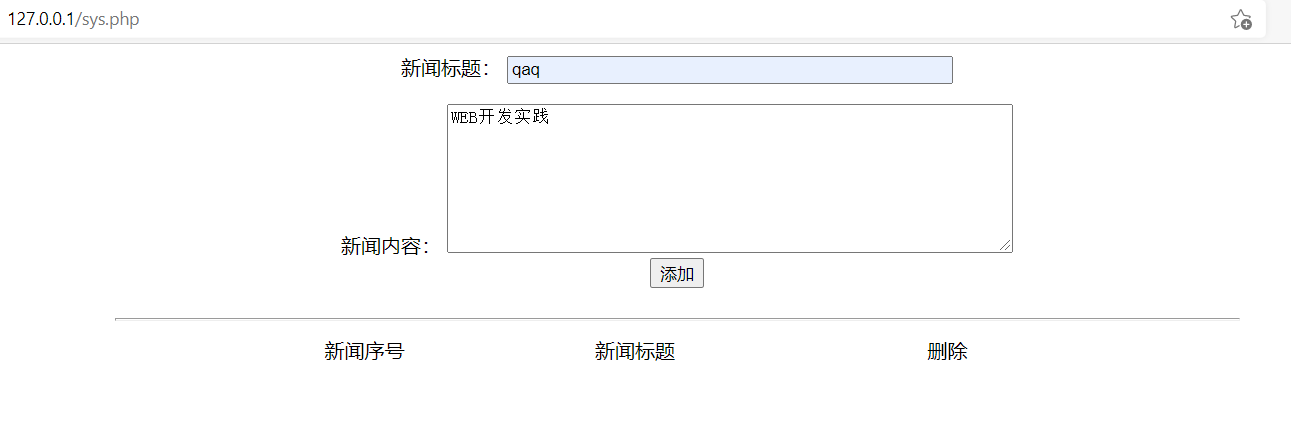
history.back();

</script>

<?php

}

?>

运行

显示：

观察数据库中记录：

插入成功！

*②删除（del.php）操作*

<?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();

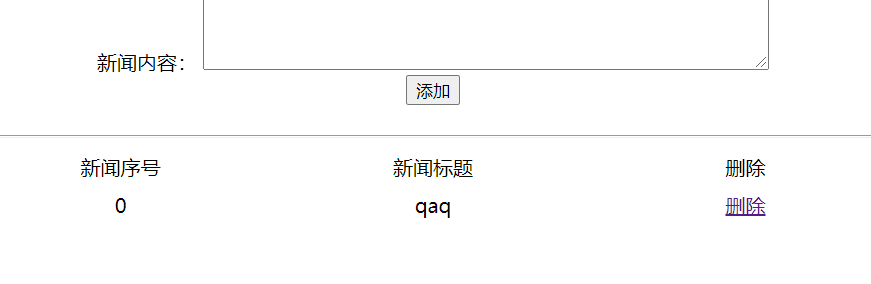
</script>

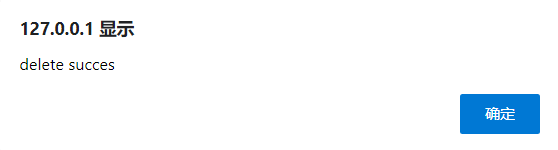
<?php }

?>

**④**数据库删除操作如下

点击页面上删除按钮：



显示：

删除成功

**⑤**查询（news.php）操作

<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>

<table width="432" height="59" border="1">

<tr>

<td width="92"><div align="center">id</div></td>

<td width="317"><div align="center">topic</div></td>

</tr>

<?php

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

$SQLStr = "select newsid,topic 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><?php echo $row[0]; ?></td>

<td><a href="see.php?newsid=<?php echo $row[0];?>"><?php echo $row[1];?>

</a></td>

</tr>

<?php

}

}

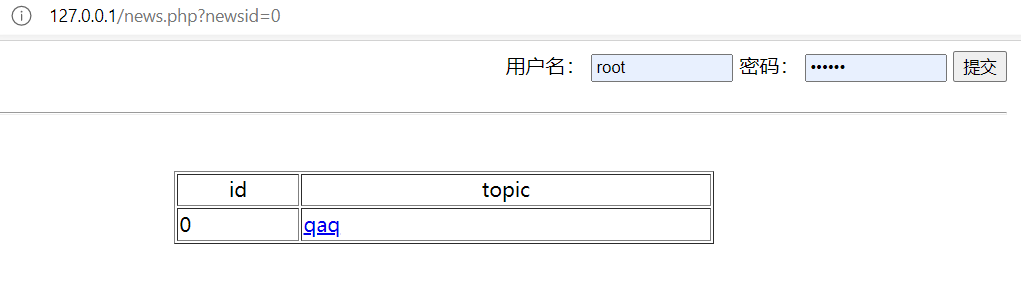
?>

</table>

</body>

</html>

地址框内输入127.0.0.1/news.php?newsid=0，对id为0的新闻进行检索



点击标题即可查看内容

查询成功

**心得体会：**PHP 是一种免费的脚本语言，主要用途是处理动态网页，也包含了命令行运行接口。是 一种解释性语言。PHP 语句被包含在 PHP 标记里面，PHP 标记外的语句都被直接输出。包括在 PHP 标记中的语句被解析，在其外的语句原样输出并且接受 PHP 语句的控制。