《漏洞利用及渗透测试基础》实验报告

姓名： 许健 学号：2013018 班级：信安班

**实验名称：**

WEB开发实践

**实验要求：**

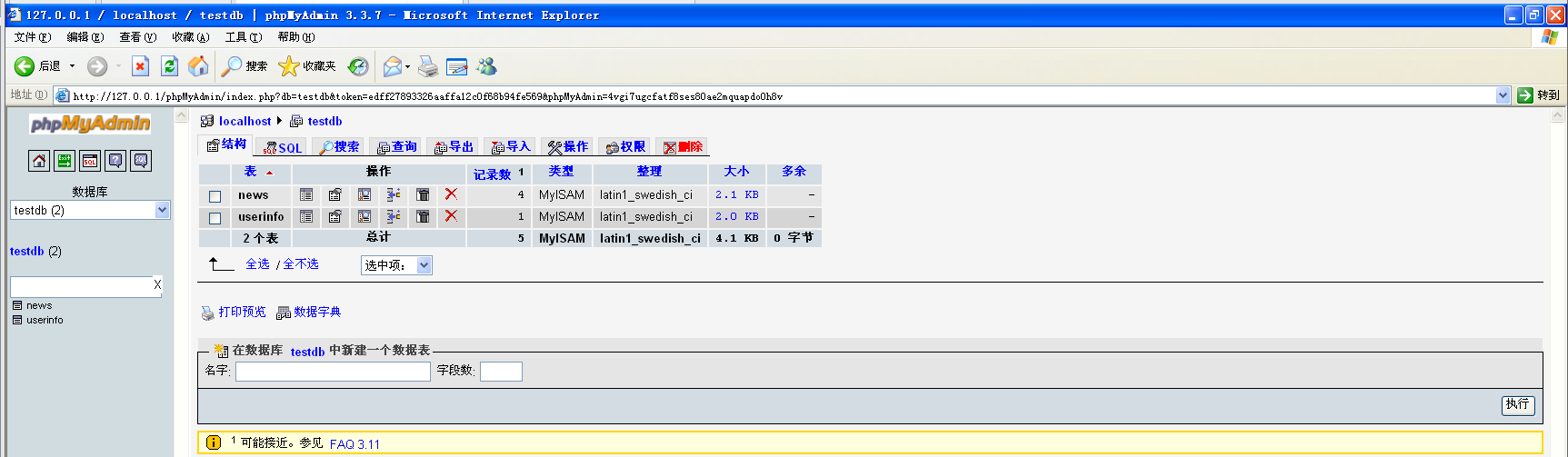
复现课本第十章的实验三(10.3.5节)：利用php，编写简单的数据库插入、查询和删除操作的示例。

基于课本的完整的例子，进一步了解WEB开发的细节

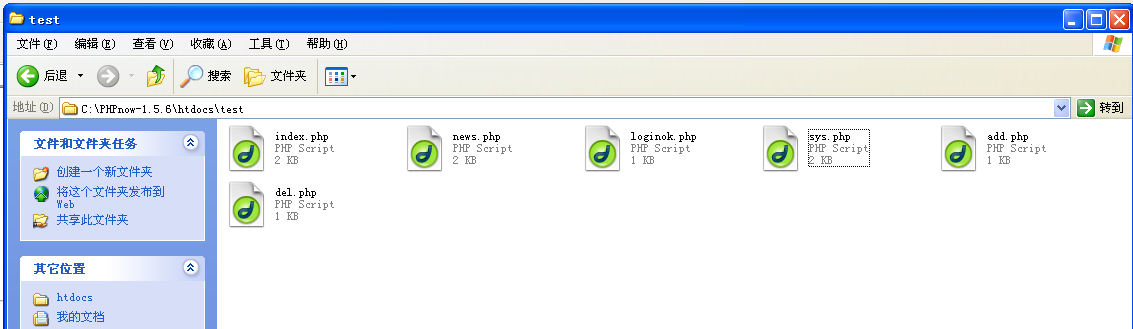
**实验过程：**

1. **实验复现**

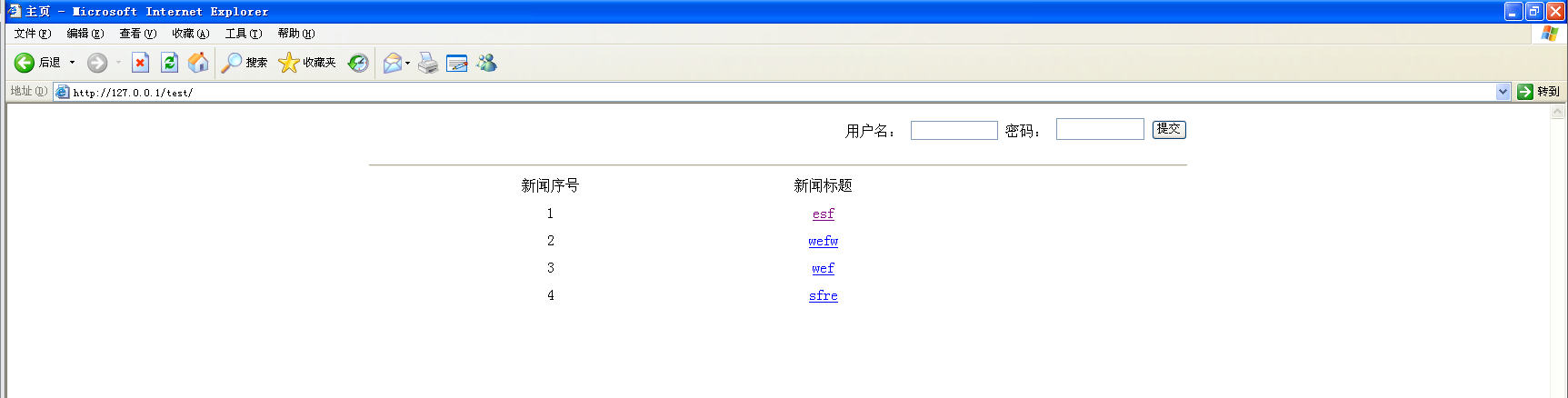
创建testdb数据库，添加表



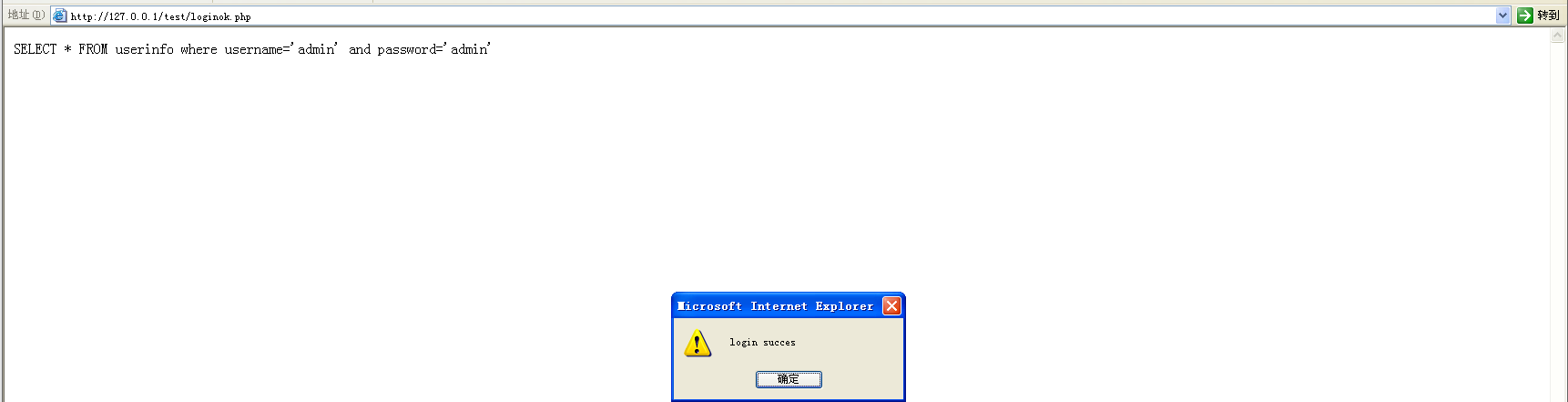
编写php文件



尝试运行index.php



可以看到页面，登录账号（在userinfo中已经创建的账号）



看到弹窗，显示登陆成功

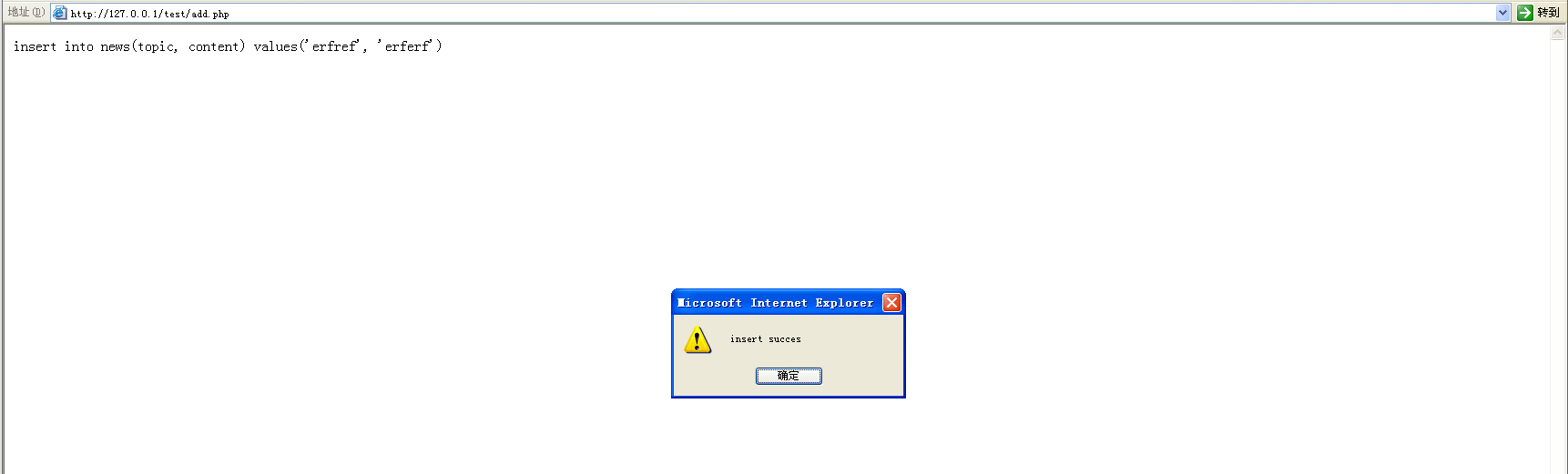
可以看到URL发生变化，跳转到loginok.php，后面不显示？...

因为我们使用的是post而不是get的方式

然后跳转到sys.php界面

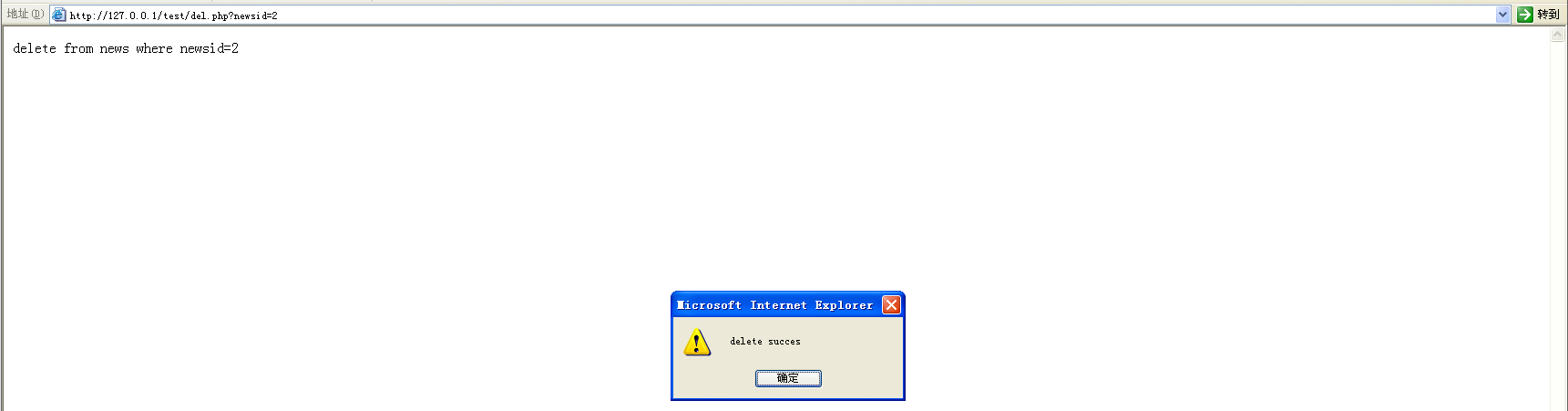


在这里可以插入数据，同时会显示已经有的数据，可以删除，我们尝试插入一条数据

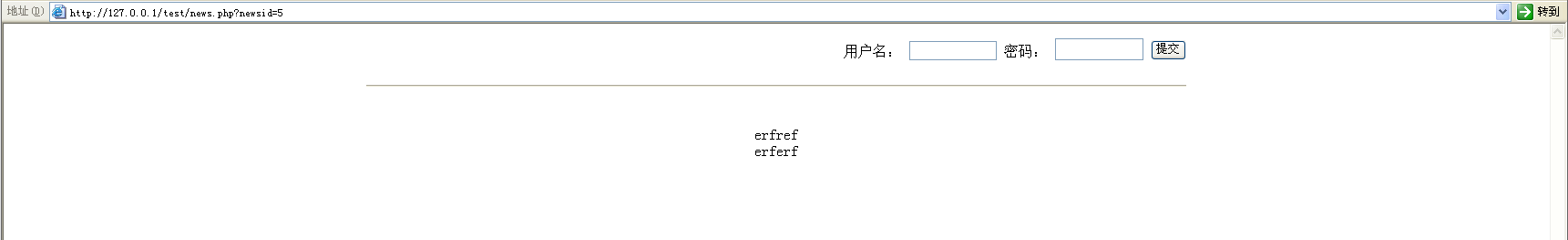


跳转到add.php，显示插入成功，之后会跳转回到sys.php页面

同理我们可以删除数据，点击删除按钮会跳转到del.php页面



回到index.php，点击新闻标题，可以跳转到news.php，查看新闻内容



1. **Php代码解析**

前面我们展示了动态网页之间的跳转，实现新闻的插入删除与查看，这实际是建立在php脚本语言与MySql数据库交互的基础上

下面讲解php脚本代码中的重点部分

1. index.php（允许用户查看新闻和进行登录）

|  |
| --- |
| 连接数据库  <?php  $conn=mysql\_connect("localhost", "root", "123456");  ?>  创建表单，选择“post”的方式，事件发生时会跳转到“loginok.php”  <form id="form1" name="form1" method="post" action="loginok.php">  输入用户名和密码，密码type是“password”，不会显示防止信息泄露  创建submit提交按钮  <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>  SQL查询，通过循环读取数据内容  $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))  跳转到news.php  <a href="news.php?newsid=<?php echo $row[0] ?> " > <?php echo $row[1] ?>  使用完数据库要释放资源，并关闭连接  // 释放资源  mysql\_free\_result($result);  // 关闭连接  mysql\_close($conn); |

1. news.php（根据传入的id查看新闻内容）

|  |
| --- |
| GET读取内容，输出查询记录  <?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>";  } |

1. loginok.php（判断用户登录是否成功）

|  |
| --- |
| 通过post读取输入的账号和密码，SQL语句用于比较账号和密码，读取到则说明登陆成功  感觉这里可以写SQL注入语句，如果userinfo表中有一个管理员账号administrators，则可以构造注入语句，注释掉密码；或者' 'or 1 = 1 -- and password='，后果可想而知  但是通过尝试，我发现他的防护机制是将特殊字符进行转义，从而避免sql注入的方式  $username = $\_POST['username'];  $pwd = $\_POST['password'];  $SQLStr = "SELECT \* FROM userinfo where username='$username' and password='$pwd'";  echo $SQLStr; |

1. sys.php（系统管理界面）

|  |
| --- |
| 事件发生跳转到add.php  <td height="40"><form id="form1" name="form1" method="post" action="add.php">  Topic构造文本框，content构造文本域textarea  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" />  读取循环内容，添加删除按钮，事件发生跳转到del.php  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>  <a href="del.php?newsid=<?php echo $row[0] ?> " > 删除 </a> |

1. add.php（新闻添加）

|  |
| --- |
| mysql\_query比较适合更新和删除语句，其返回值是boolean，可以校验执行成功与失败  $topic = $\_POST['topic'];  $content = $\_POST['content'];  $SQLStr = "insert into news(topic, content) values('$topic', '$content')";  echo $SQLStr;  $result=mysql\_query($SQLStr); |

1. del.php（新闻删除）

|  |
| --- |
| GET读取输入的参数  $newsid = $\_GET['newsid'];  $SQLStr = "delete from news where newsid=$newsid";  echo $SQLStr;  $result=mysql\_query($SQLStr);  嵌套php和javaScript，通过result字段判断删除是否成功  if ($result)  {  ?>  <script>  alert("delete succes");  window.location.href="sys.php";  </script>  <?php  }  else{  ?>  <script>  alert("delete failed");  history.back();  </script>  <?php  } |

1. **实验遇到问题**

# php网页显示无法连接服务器错误,phpmyadmin报错原因及解决方法：无法在发生错误时创建会话，请检查 PHP 或网站服务器日志，并正确配置 PHP 安装。

查询发现phpmyadmin需要写session文件，但session目录没有相应权限所以报错“…发生错误时创建会话…”，错误信息里说明是session相关的，只是这个错误信息太简略了，不容易轻易看明白。

到服务器上修改php.ini，以前没有配置session.save\_path的。于是C盘建一个session目录c:\tempfolder\phpsession，给phpmyadmin站点的web用户赋读写权限，在php.ini里加上一条

**session.save\_path=”c:\tempfolder\phpsession”**

再次进入 phpmyadmin站点，终于看到了久违的登录页面了。

1. 只能插入一条数据的错误

开始做实验，发现我的add.php只能插入一条数据，再添加就会显示“add failed”,检查脚本代码发现没有错误，但是newsid字段应该是要自动更新加一的，代码中是没有的

于是打开testdb数据库检查news表，果然发现newsid字段忘记勾选auto\_increament

添加之后恢复正常

**实验心得：**

初步熟悉开发一个网页的基本流程，以及php的一些基本语法，以及如何连接数据库等等，对于实验中遇到的问题可以自己查询解决，解决问题能力得到提升。