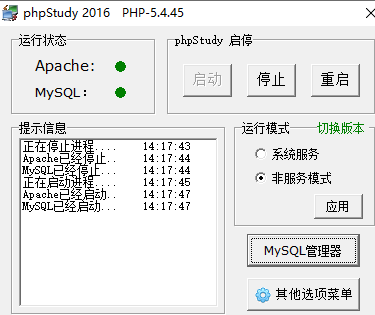
Web前端开发实现简易留言版功能

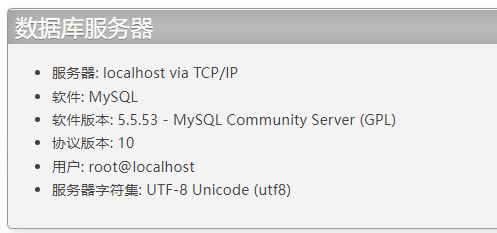
（1）系统功能：主页，注册，登录，留言。

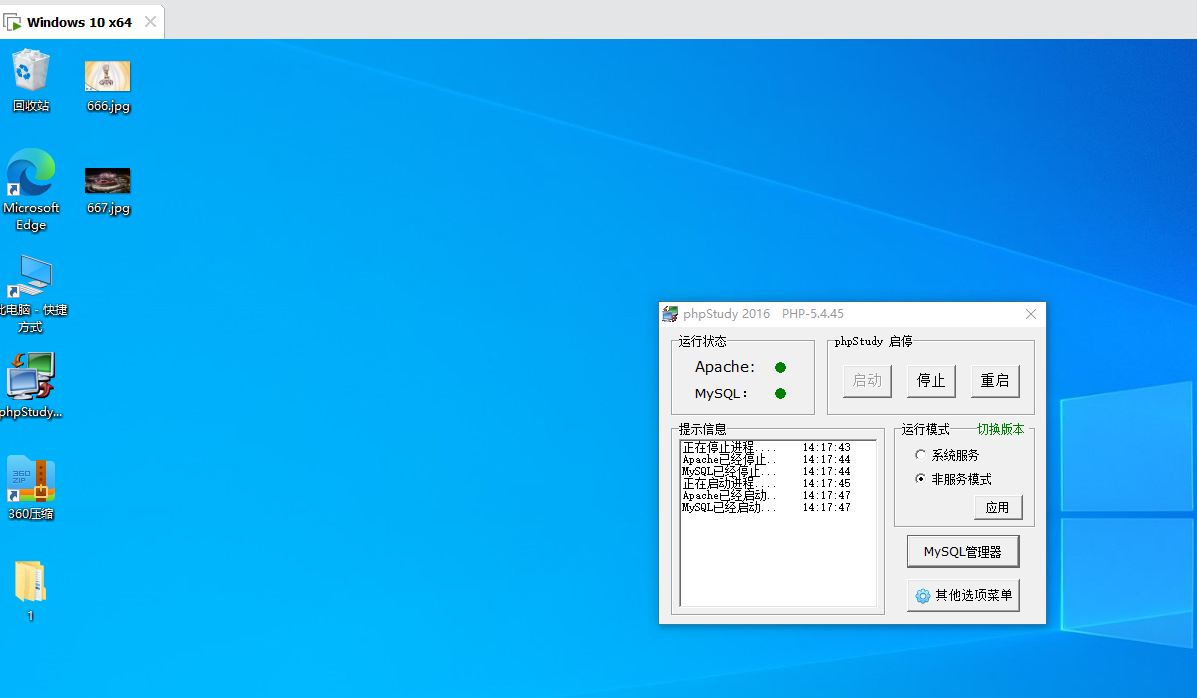
留言板环境及版本：PHP（版本：5.4.45）+Mysql （版本5.5.53）+windows10（虚拟机镜像）

留言板名称：“卡塔尔世界杯留言板”

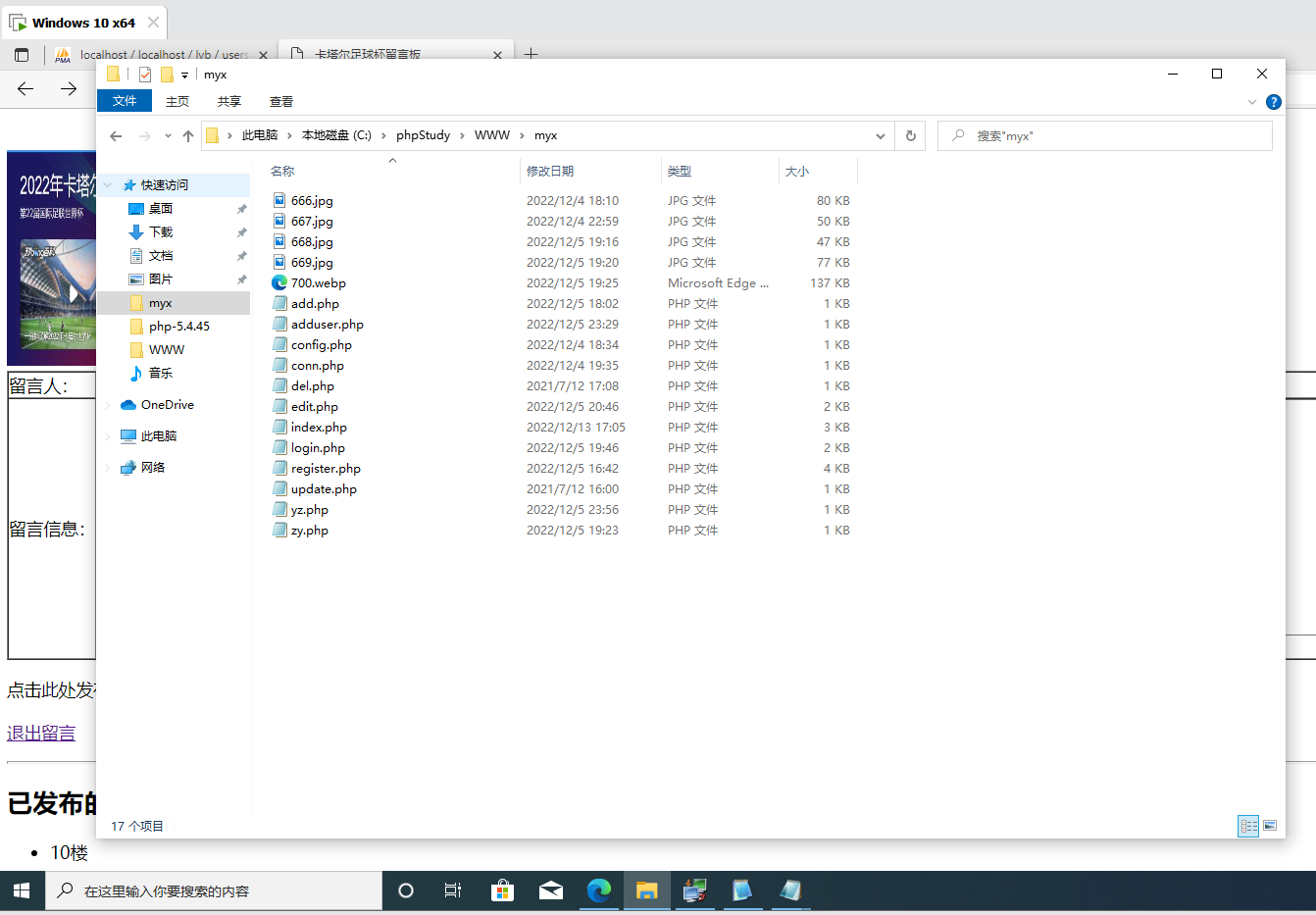
具体环境参数如下图所示：







留言板功能全部文件：



1、主页文件：zy.php

代码：

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>zhuye</title>

</head>

<body>

<pre>

<img src="668.jpg" width="380" height="150">

<h1>欢迎来到卡塔尔世界杯留言板 !</h1>

<a href="http://localhost/myx/register.php">还未注册？立即注册</a></br>

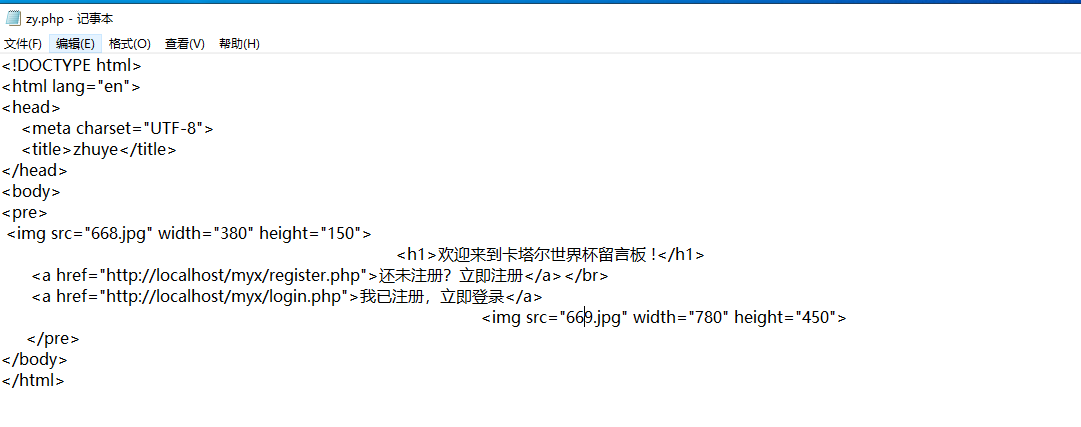
<a href="http://localhost/myx/login.php">我已注册，立即登录</a>

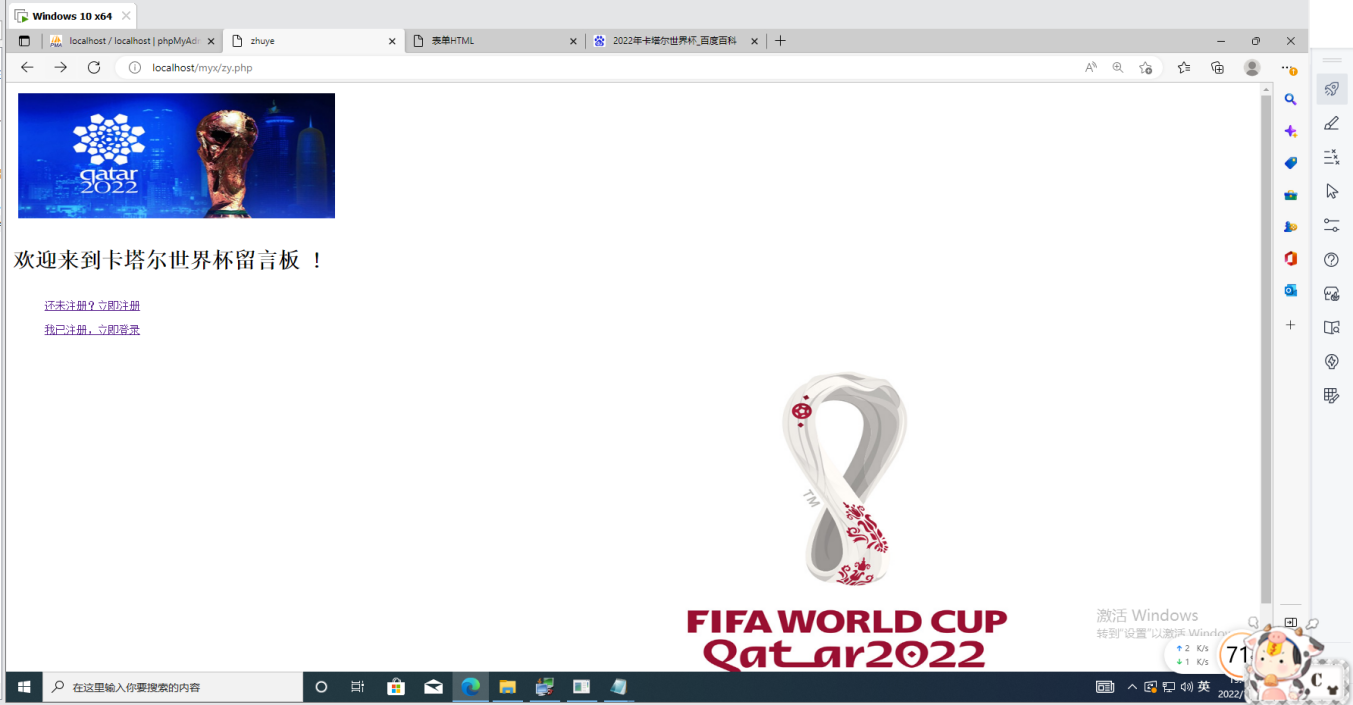
<img src="669.jpg" width="780" height="450">

</pre>

</body>

</html>





1. 注册功能：register.php（留言板用户注册页面）

代码：

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>表单HTML</title>

</head>

<body>

<img src="666.jpg" width="280" height="150">

<h1>卡塔尔世界杯留言板 </h1><form

action="./adduser.php"

method="POST"

><table border="1" cellspacing="0px" cellpadding="0px">

<tr>

<td>用户名：</td>

<td><input type="text" name="username"></td>

</tr>

<tr>

<td>密码:</td>

<td><input type="password" name="userpass1"></td>

</tr>

<tr>

<td>确认密码:</td>

<td><input type="password" name="userpass2"></td>

</tr>

<tr>

<td>性别：</td>

<td><label for="mingzi">男</label><input type="radio"name="1" id="mingzi"><label for="mingzi2">女</label><input type="radio" name="1" id="mingzi2"></td>

</tr>

<tr>

<td> 出生日期：</td>

<td><select>

<option selected="selected">2002</option>

<opyion>1998</opyion>

<opyion>1999</opyion>

<opyion>2000</opyion>

<opyion>2001</opyion>

<opyion>2002</opyion>

<option>2003</option>

<option>2004</option>

<opyion>2005</opyion>

</select>年<select>

<option selected="selected">1</option>

<option>2</option>

<option>3</option>

<option>4</option>

<option>5</option>

<option>6</option>

<option>7</option>

<option>8</option>

<option>9</option>

<option>10</option>

<option>11</option>

<option>12</option>

</select>月<select>

<option selected="selected">1</option>

<option>2</option>

<option>3</option>

<option>4</option>

<option>5</option>

<option>6</option>

<option>7</option>

<option>8</option>

<option>9</option>

<option>10</option>

<option>11</option>

<option>12</option>

<option>13</option>

<option>14</option>

<option>15</option>

<option>16</option>

<option>17</option>

<option>18</option>

<option>19</option>

<option>20</option>

<option>21</option>

<option>22</option>

<option>23</option>

<option>24</option>

<option>25</option>

<option>26</option>

<option>27</option>

<option>28</option>

<option>29</option>

<option>30</option>

<option>31</option>

</select>日</td>

</tr>

<tr>

<td> 个人简介：</td>

<td><input type="t" value="个人兴趣爱好，个人追求" maxlength="300" size="90"></td>

</tr>

<tr>

<td></td>

<td><input type="checkbox" checked="checked">我同意会员注册条款和会员加入标准</td>

</tr>

<tr>

<td>论坛承诺协议声明</td>

<td>

<h5>本人承诺：</h5>

<ul>

<li>自觉遵守网络安全相关规定</li>

<li>我已满足18岁</li>

<li>自觉维护论坛环境</li>

</ul>

</td>

</tr>

<tr>

<td></td>

<h3><td><input type="submit" name="usersubmit" value="免费注册"></td><h3>

</tr>

<tr>

<td></td>

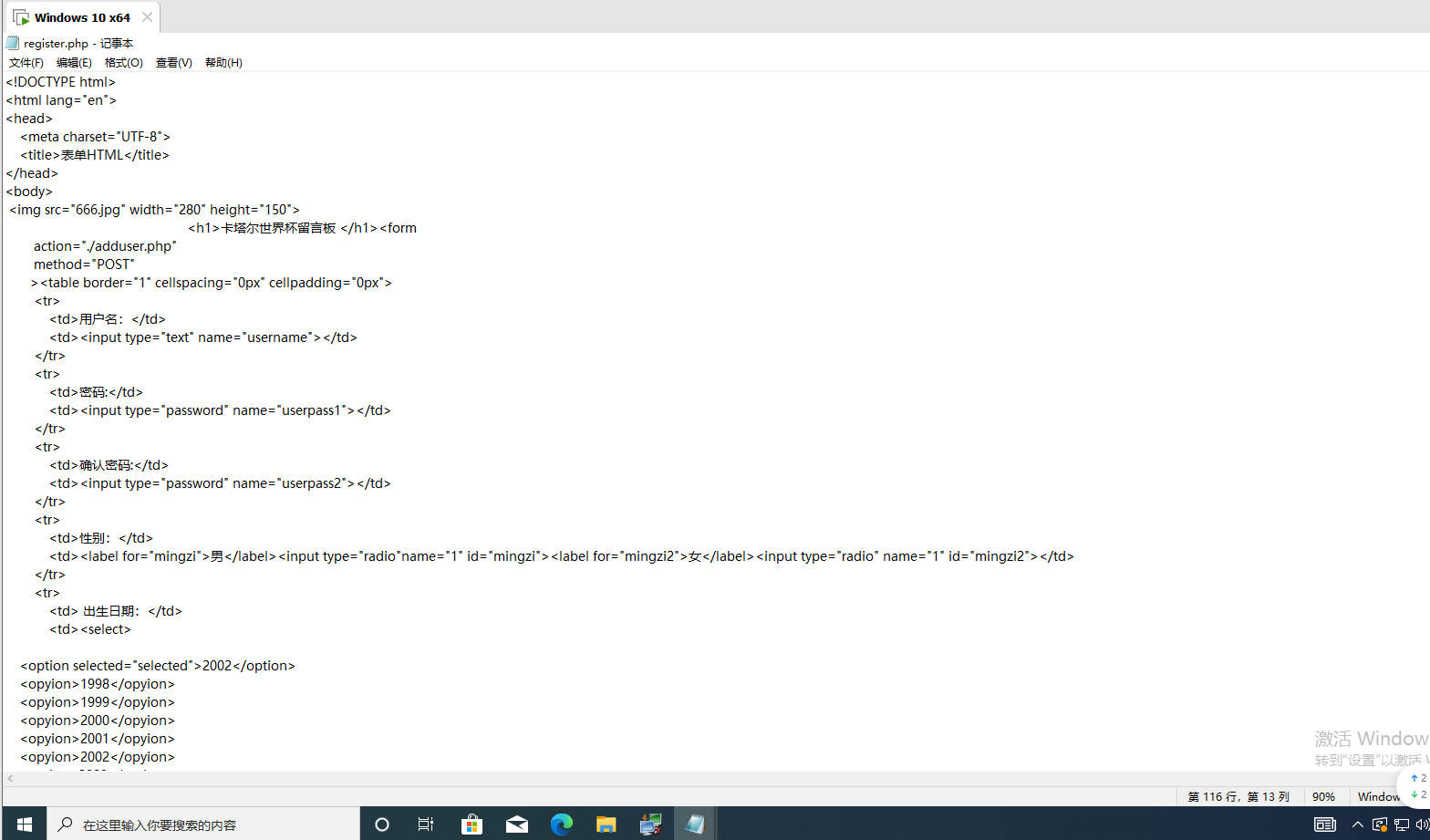
<td><a href="http://localhost/myx/login.php">我已注册，立即登录</td>

</tr>

</table>

</body>

</html>





1. 用户登录页面文件：login.php、后端用户数据验证文件:yz.php

Login.php代码：

<!DOCTYPE html>

<html>

<head>

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

<meta http-equiv="Pragma" content="no-cache">

<meta http-equiv="Cache-Control" content="no-cache">

<meta http-equiv="Expires" content="0">

<title>登录</title>

<link href="css/login.css" type="text/css" rel="stylesheet">

</head>

<body>

<div class="login">

<div class="message">卡塔尔论坛留言板用户登录</div>

<div id="darkbannerwrap"></div>

<form action="./yz.php" method="post" enctype="multipart/form-data">

<input name="action" value="register" type="hidden">

<pre>用户名：<input name="username" placeholder="用户名" required="" type="text">

密码：<input name="password" placeholder="密码" required="" type="password"></pre>

<hr class="hr15">

<input value="登录" style="width:50%;" type="submit">

<a href="./register.php" style="width: 50%">->还没有账号?点击此处注册<-</a>

<hr class="hr20">

<!-- 帮助 <a onClick="alert('请联系管理员')">忘记密码</a> -->

</form>

<pre>

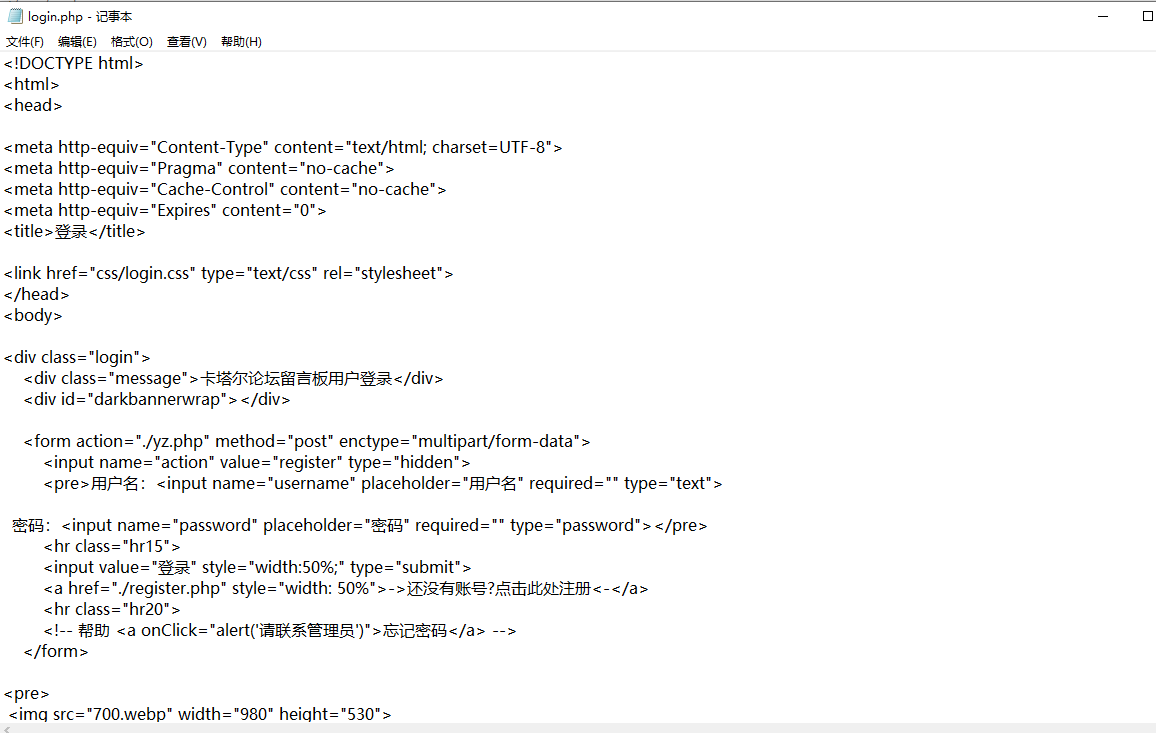
<img src="700.webp" width="980" height="530">

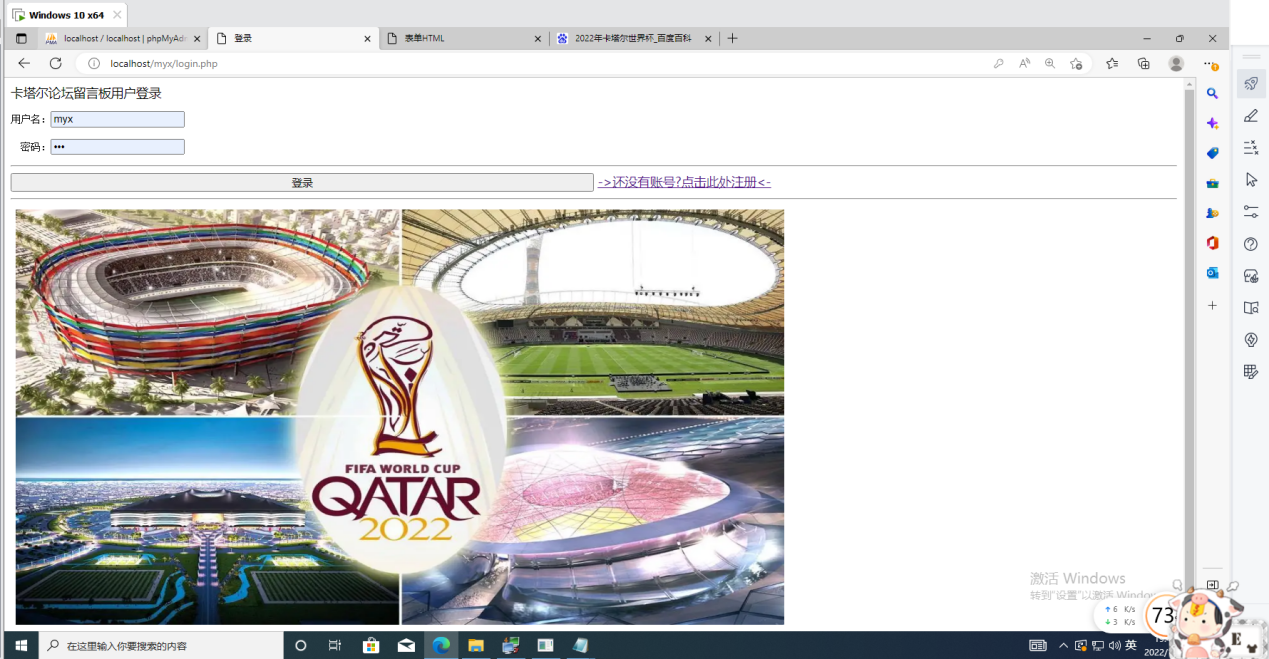
</pre>

</div>

</body>

</html>





yz.php(验证数据)

首先设置编码为utf-8。通过$\_POST获取用户输入的用户名和密码，使用addslashes函数防止SQL注入。连接数据库，执行SQL语句查询用户名和密码是否匹配。使用mysqli\_fetch\_array函数获取查询结果的第一行数据。

判断用户名是否匹配且不为空，如果是，则跳转到留言板界面，并显示登录成功的提示信息；否则，显示登录失败的提示信息。

使用header函数设置跳转页面和刷新时间。

**Php代码：（yz.php:3~15行）**

<?php

header("content-type:text/html;charset=utf-8"); //设置编码

$username=addslashes($\_POST['username']);

$password=addslashes($\_POST['password']);

$conn=mysqli\_connect('127.0.0.1','root','root','lyb');

$sql="select\* from users where name='$username' and password='$password'";

$result=mysqli\_query($conn,$sql);

$a=mysqli\_fetch\_array($result);

if($a['name']==$username && $username!=''){

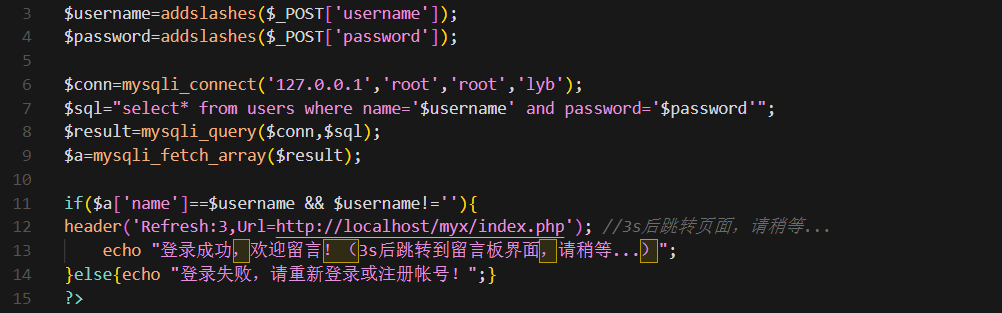
header('Refresh:3,Url=http://localhost/myx/index.php'); //3s后跳转页面，请稍等...

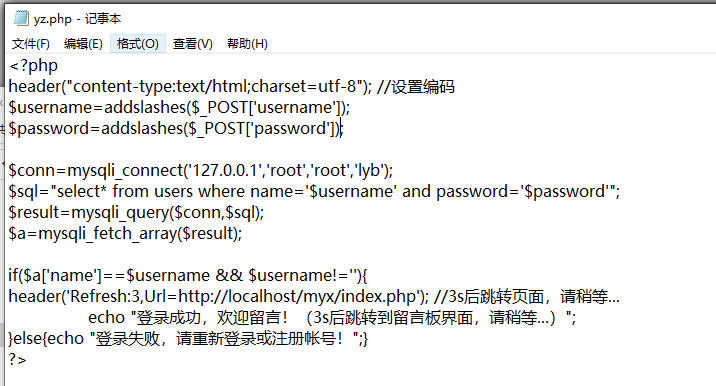
echo "登录成功，欢迎留言！（3s后跳转到留言板界面，请稍等...）";

}else{echo "登录失败，请重新登录或注册帐号！";}

?>

?>





1. 留言板功能文件:index.php（留言板） add.php(用于传递用户留言板内容)、edit.php（编辑留言板功能）、update.php(更新留言板)、del.php（删除留言）

Index.php代码是用来从数据库中获取最新的留言，并将其展示在网页上。代码首先执行一个SQL查询语句，从名为liuyan的表中选择所有的数据，并按照id字段进行降序排列。然后，通过$conn->query($sql)执行查询，并将结果存储在$result变量中。

接下来，代码检查查询结果的行数是否大于0，如果大于0，则表示有留言数据。然后，通过一个循环遍历每一行数据，使用$row变量来存储当前行的数据。在循环内部，代码使用PHP的echo语句将留言的相关信息输出到网页上，包括留言的楼层、内容、留言人、留言时间等。此外，代码还通过一个<img>标签显示了留言人的头像，并提供了编辑和删除留言的链接。

如果查询结果的行数为0，则表示暂无留言，代码通过echo语句

**Php代码：（index.php:40~67行）**

<?php

// 最新留言展示前面

$sql = "SELECT \* FROM `liuyan` ORDER BY `liuyan`.`id` DESC";

// ORDER BY `liuyan`.`id` DESC 加上这个是降序排列

$result = $conn->query($sql);

if($result->num\_rows>0){

//输出数据

while($row = $result->fetch\_assoc()){

// $result->fetch\_assoc()执行一次显示第一条，执行第二次显示第二条

?>

<li>

<p><?php echo $row["id"];?>楼</p>

<p>留言内容：<?php echo $row["text"];?></p>

<p>留言人：<?php echo $row["username"];?></p>

<p>留言时间：<?php echo $row["time"];?></p>

<img src="http://q1.qlogo.cn/g?b=qq&nk=<?php echo $row["text"];?>&s=640" alt="">

<p>

<a href="edit.php?id=<?php echo $row['id'];?>">编辑</a>

<a href="del.php?id=<?php echo $row['id'];?>">删除</a>

</p>

</li>

<?php

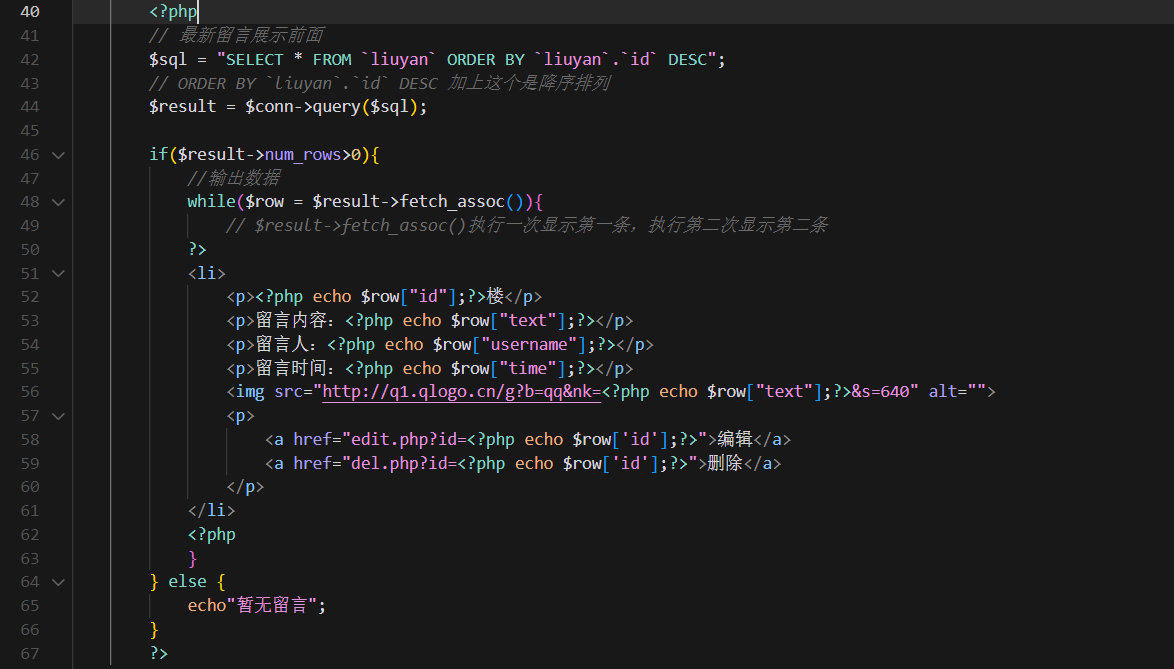
}

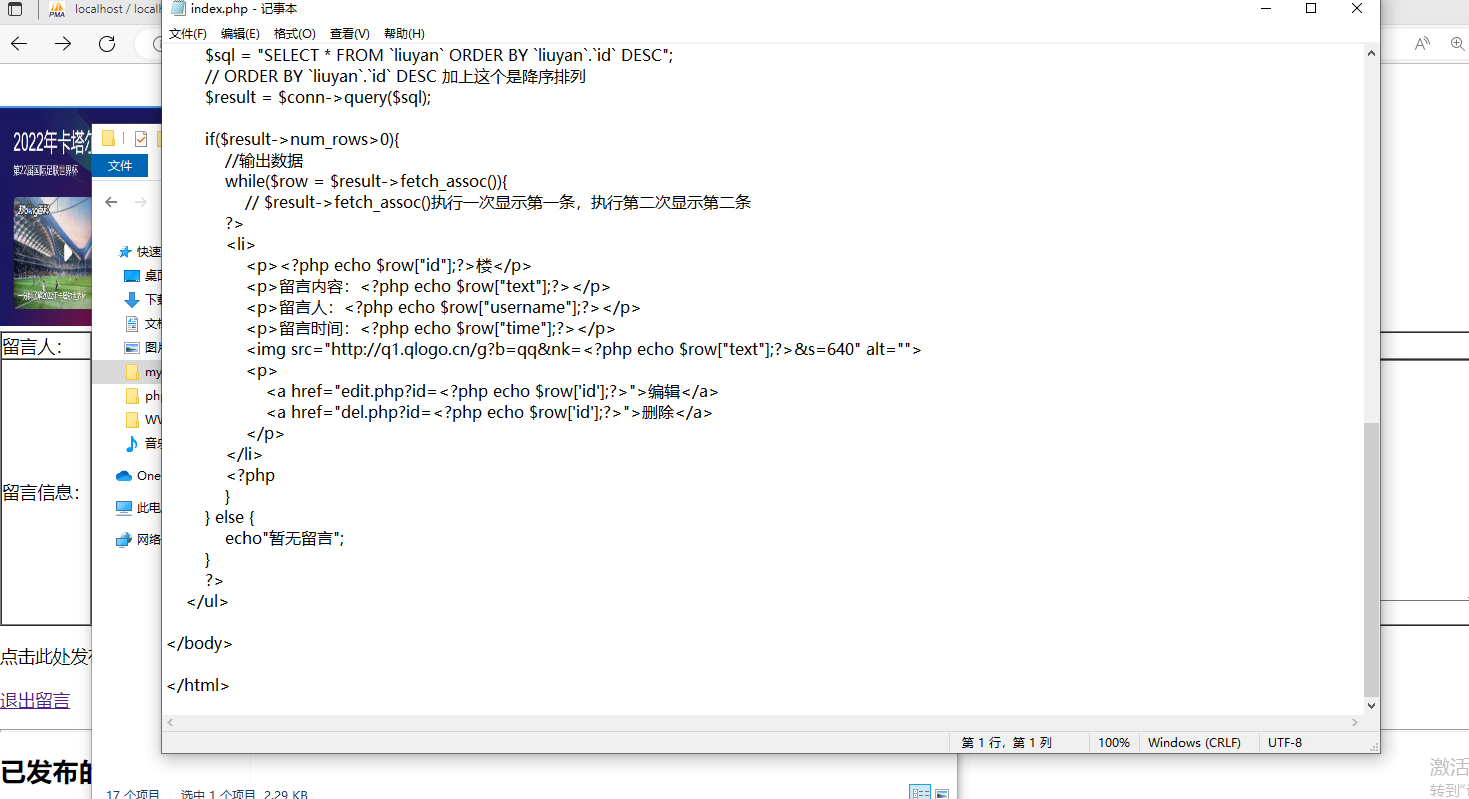
} else {

echo"暂无留言";

}

?>





add.php(用于传递用户留言板内容)代码

add.php(用于传递用户留言板内容)

处理用户注册的PHP脚本。

该代码通过使用isset()函数检查是否提交了名为usersubmit的表单。如果是，它从$\_POST超全局数组中获取username、userpass1和userpass2字段的值。

然后，它检查是否设置了所有必需的字段，并且用户输入的密码是否匹配。如果满足这些条件，它构建一个SQL查询，将用户的姓名和密码（使用md5()进行哈希处理）插入到users表中。如果查询执行失败，它会终止脚本并显示错误消息。否则，它设置一个刷新头部，在3秒后将用户重定向到登录页面，显示成功消息，并设置一个带有用户姓名的cookie。

如果表单没有被提交，该代码只是使用header()函数将用户重定向到register.php页面。

在选中的代码之后，有一些关闭的PHP标签和调用mysqli\_close()函数来关闭数据库连接。

**php代码：add.php(8-31行)**

<?php

echo "<hr />";

if(isset($\_POST['usersubmit'])){

$username=htmlspecialchars($\_POST['username']);

$userpass1=htmlspecialchars($\_POST['userpass1']);

$userpass2=htmlspecialchars($\_POST['userpass2']);

if(isset($username)&& isset($userpass1)&&isset($userpass2)&& $userpass1===$userpass2){

$sql="insert into users(name,password) values('".$username."','".md5($userpass1)."')";

if(!mysqli\_query($conn,$sql)){

die("sql语句有误");

}else{

header('Refresh:3,Url=http://localhost/myx/login.php'); //3s后跳转,请稍等...

echo "注册成功!正在跳转登陆页面,请稍等...";

setcookie("name",$username);

}

}else{

echo "注册信息有误，<a href='./register.php'>请重新注册 </a>";

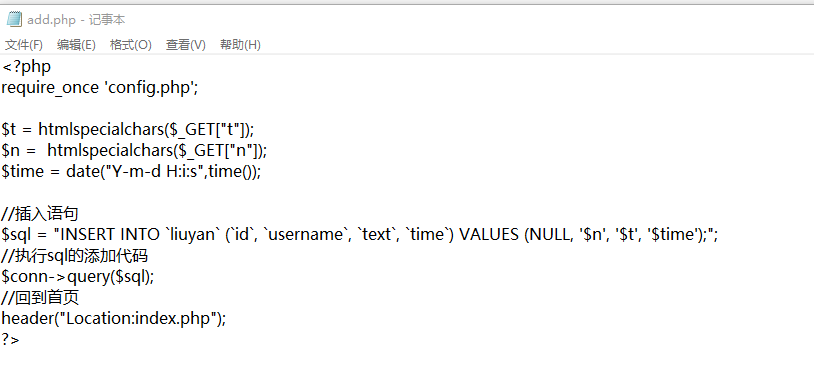
}

}else{

header("location:./register.php");

}





edit.php（编辑留言板功能）

通过GET方法获取传递过来的id参数，并将其赋值给变量$id。接下来，使用该id查询数据库表liuyan，获取对应的留言信息。

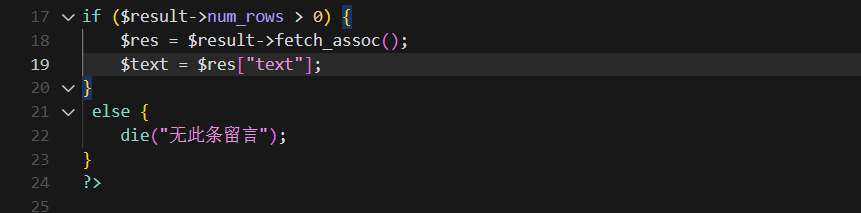
如果查询结果中存在记录（即$result->num\_rows > 0），则将查询结果的第一行数据赋值给变量$res，并从中提取出text字段的值，赋给变量$text。

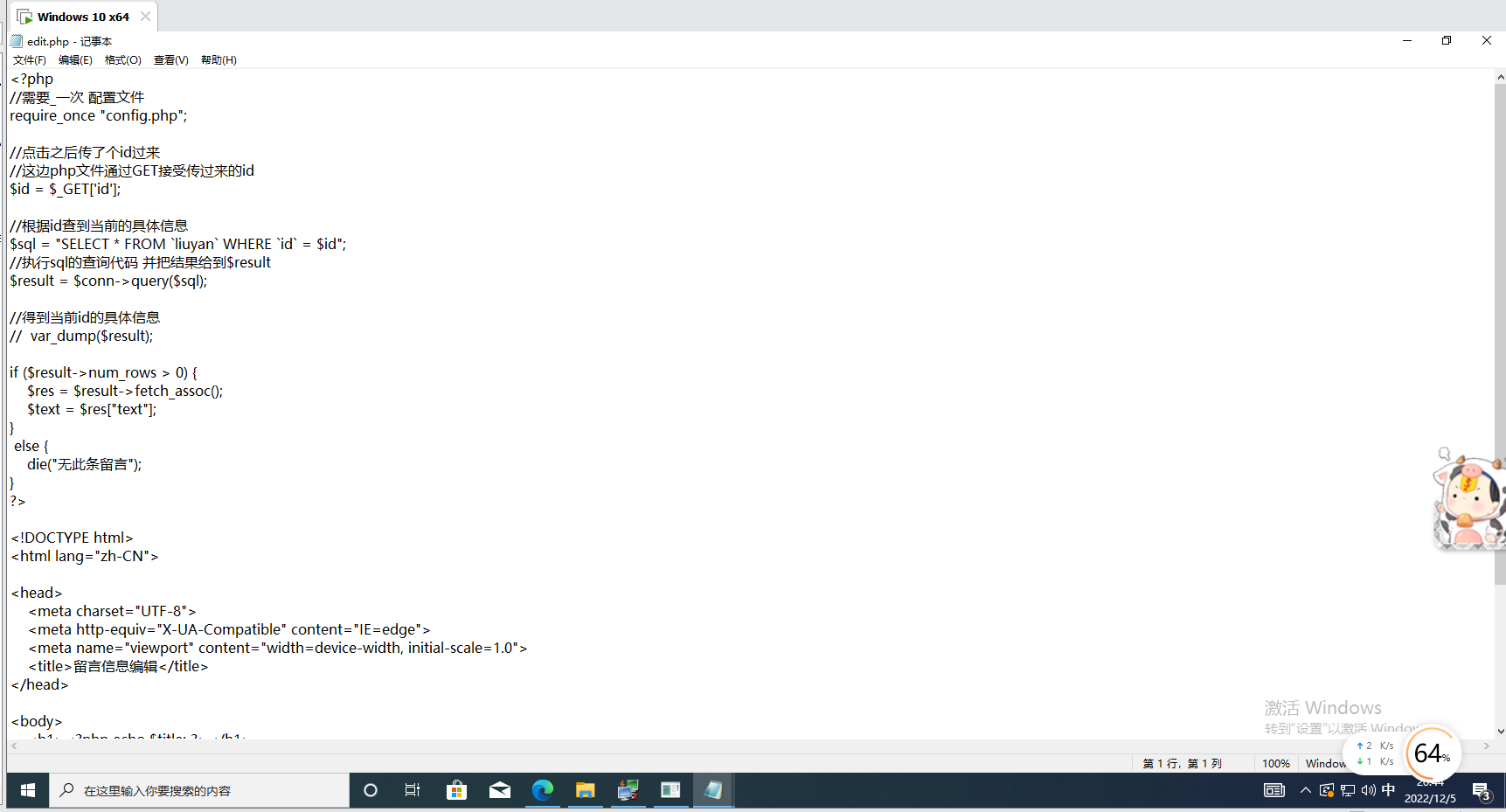
如果查询结果为空（即没有对应的留言记录），则输出错误信息"无此条留言"并终止脚本的执行。

接下来的代码是HTML部分，用于显示编辑留言的表单。在表单中，使用$title变量显示标题，使用$id变量显示楼层号，并将$res['id']赋值给隐藏的输入字段i，将$res["text"]赋值给文本域textarea的内容。

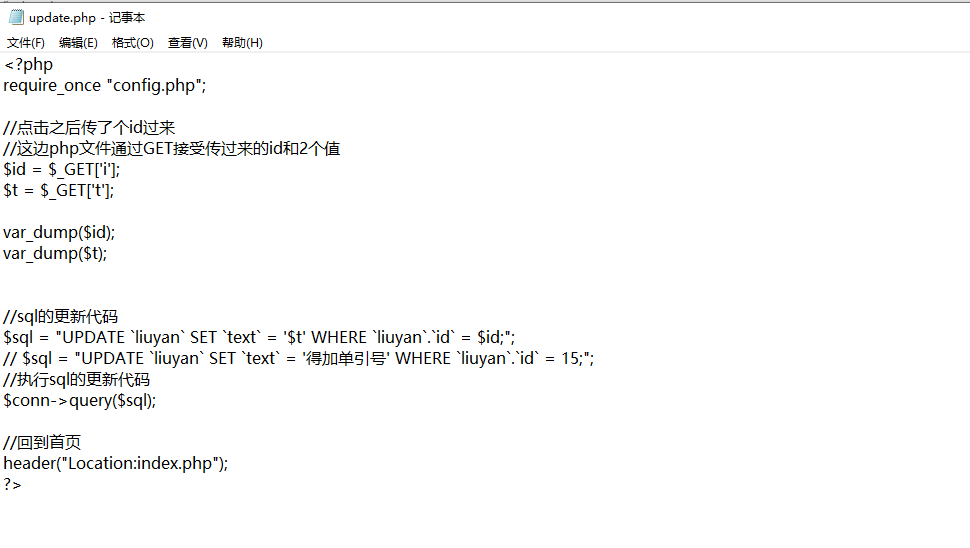
最后，提交表单时将数据发送到update.php页面进行更新。

**Php代码：（edit.php:17~24行）**

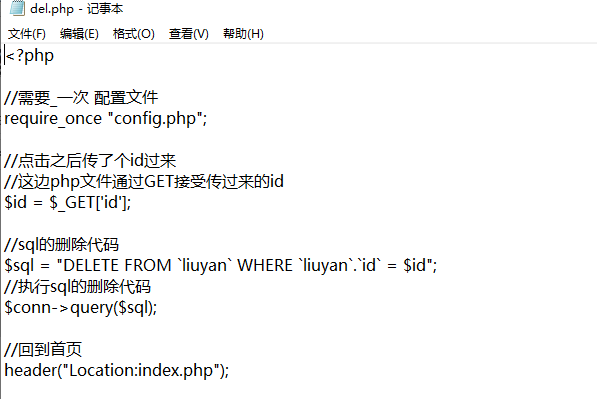


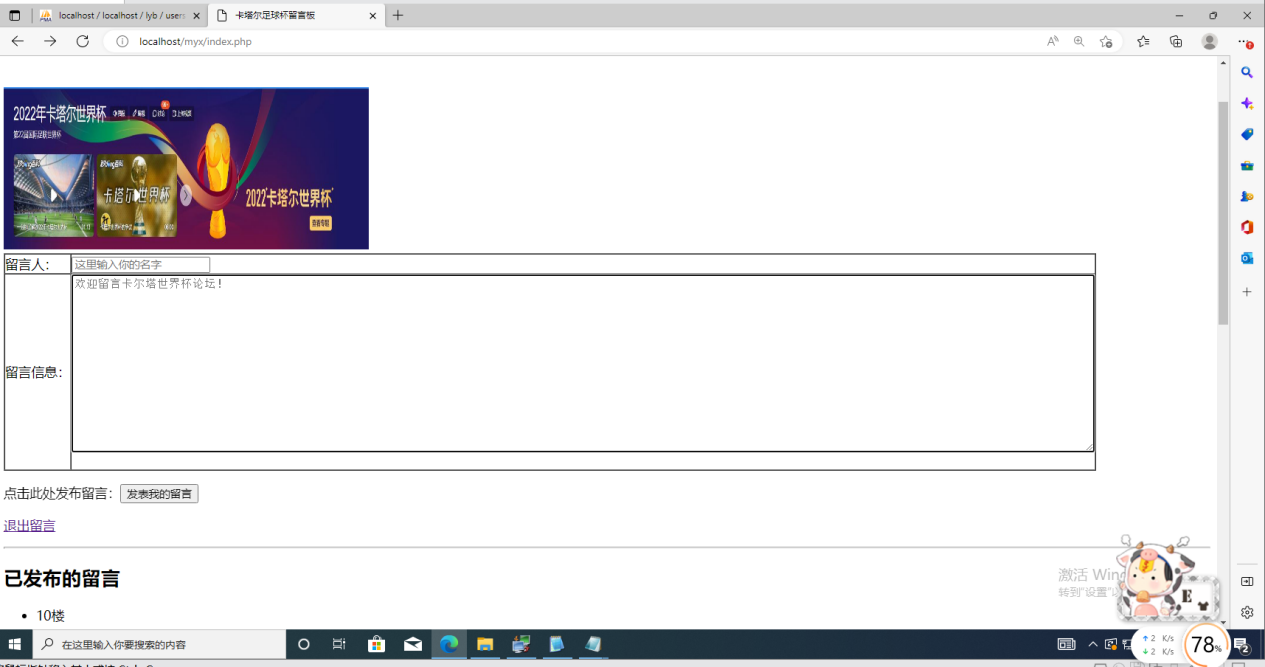


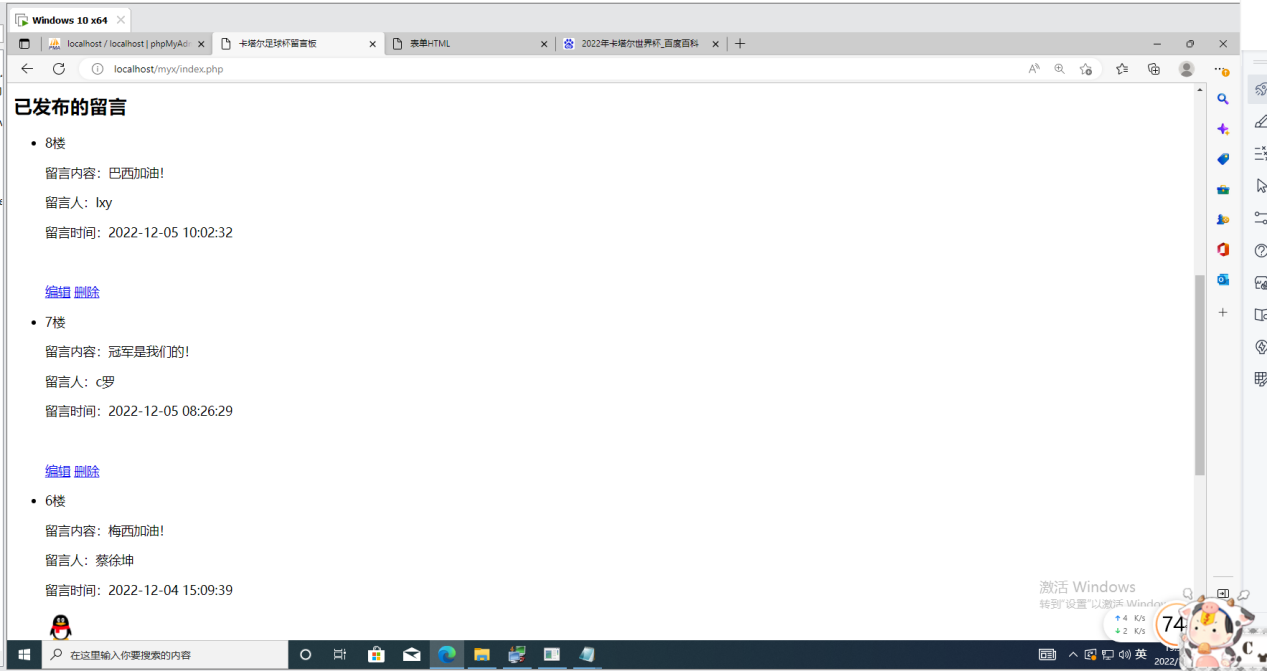
update.php(更新留言板)代码：



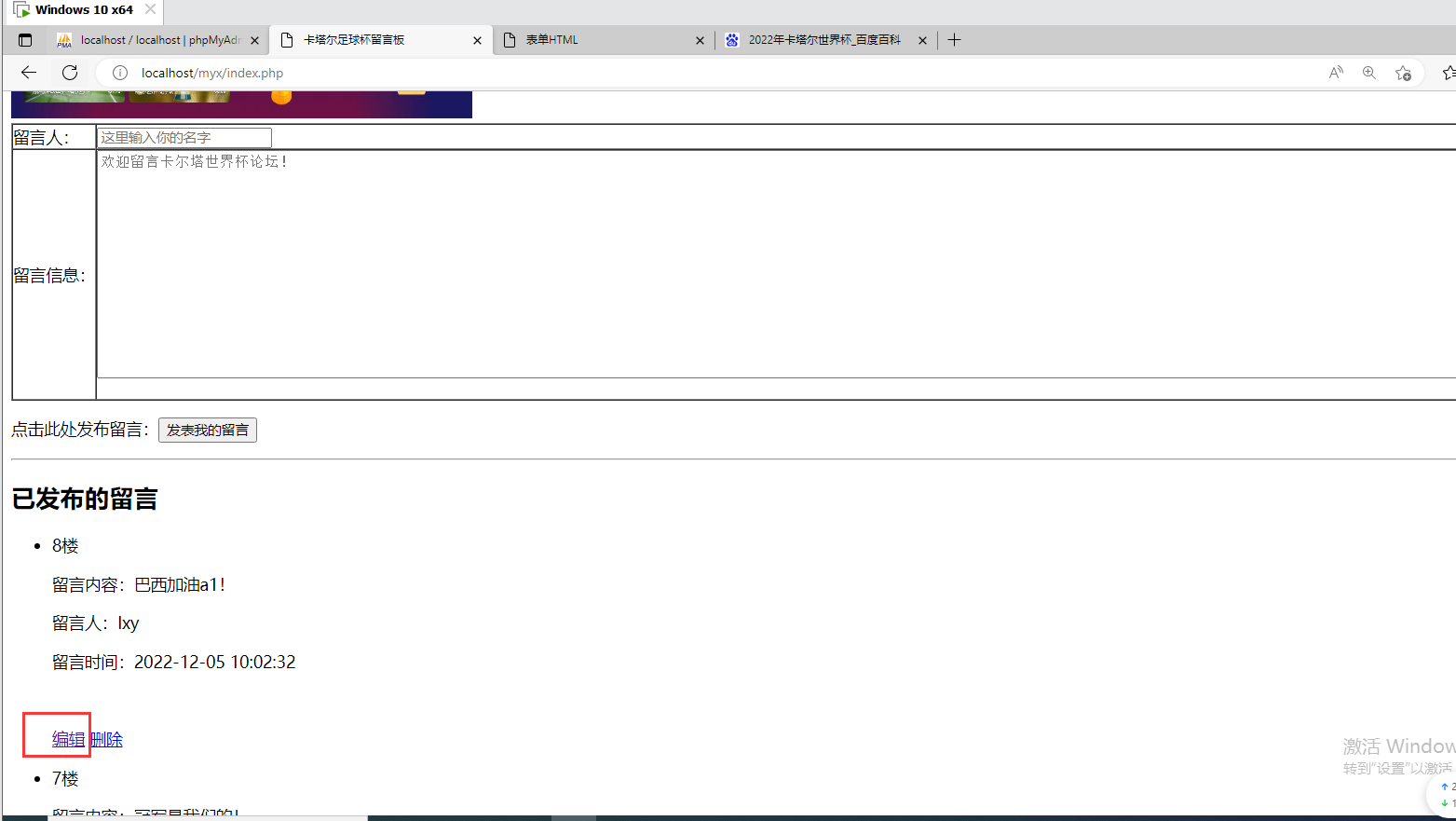
del.php（删除留言）代码：



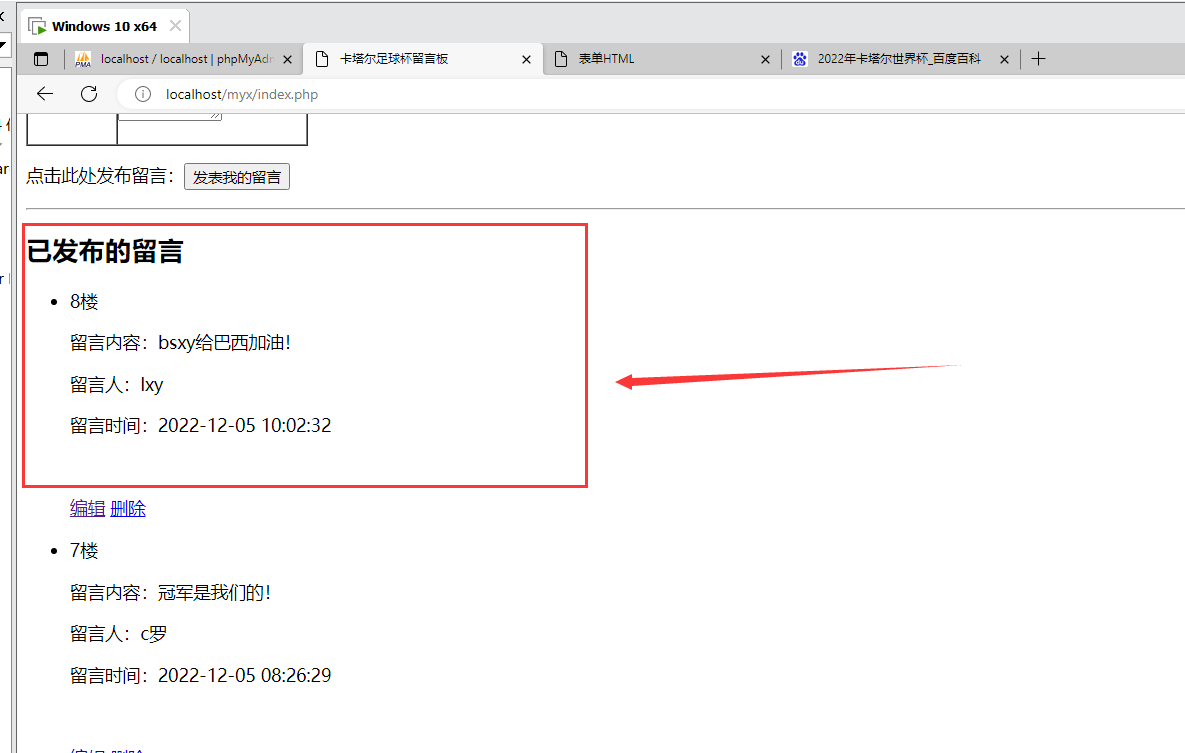




设置了更改留言内容功能：

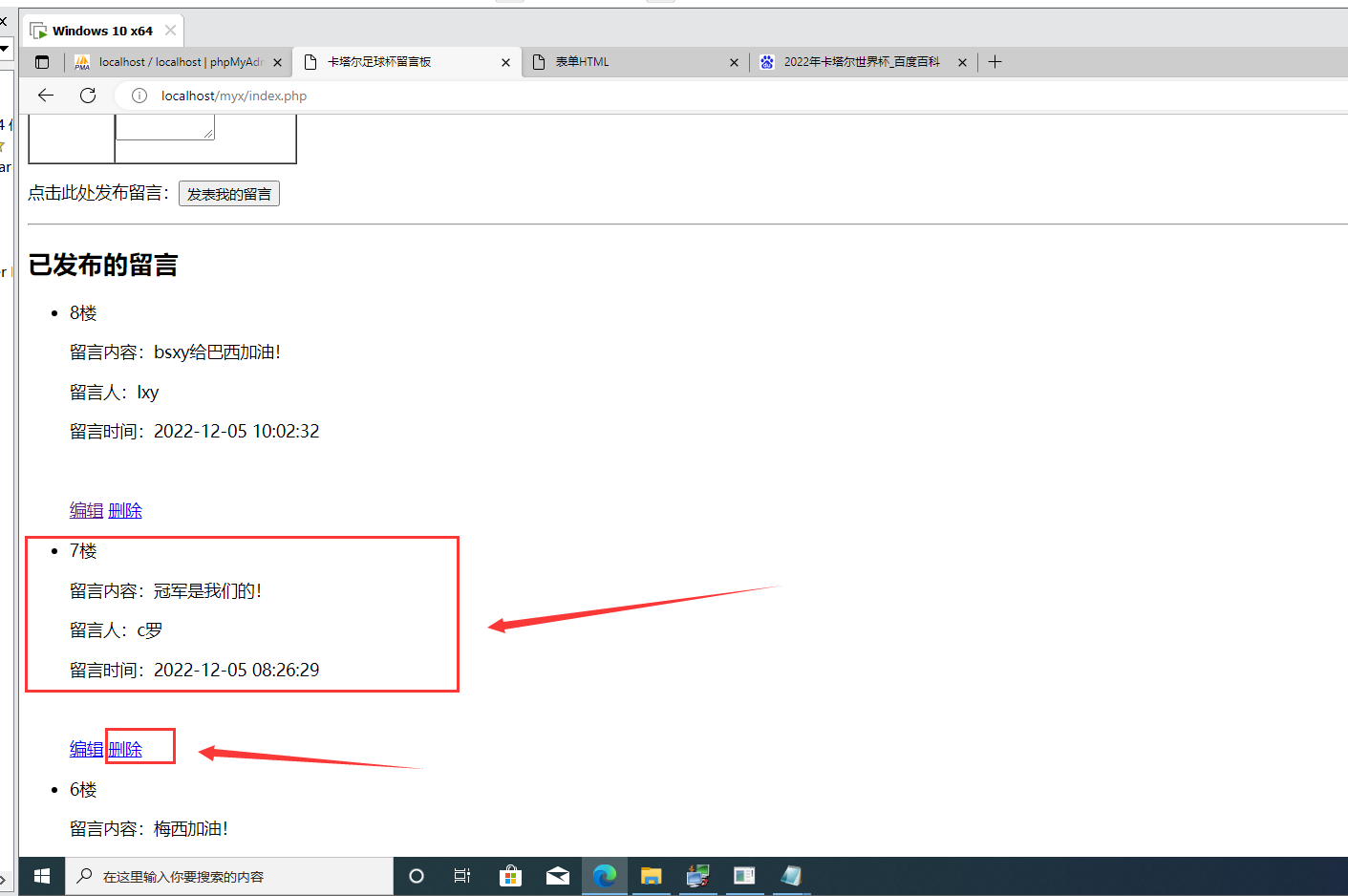






设置了删除留言功能：

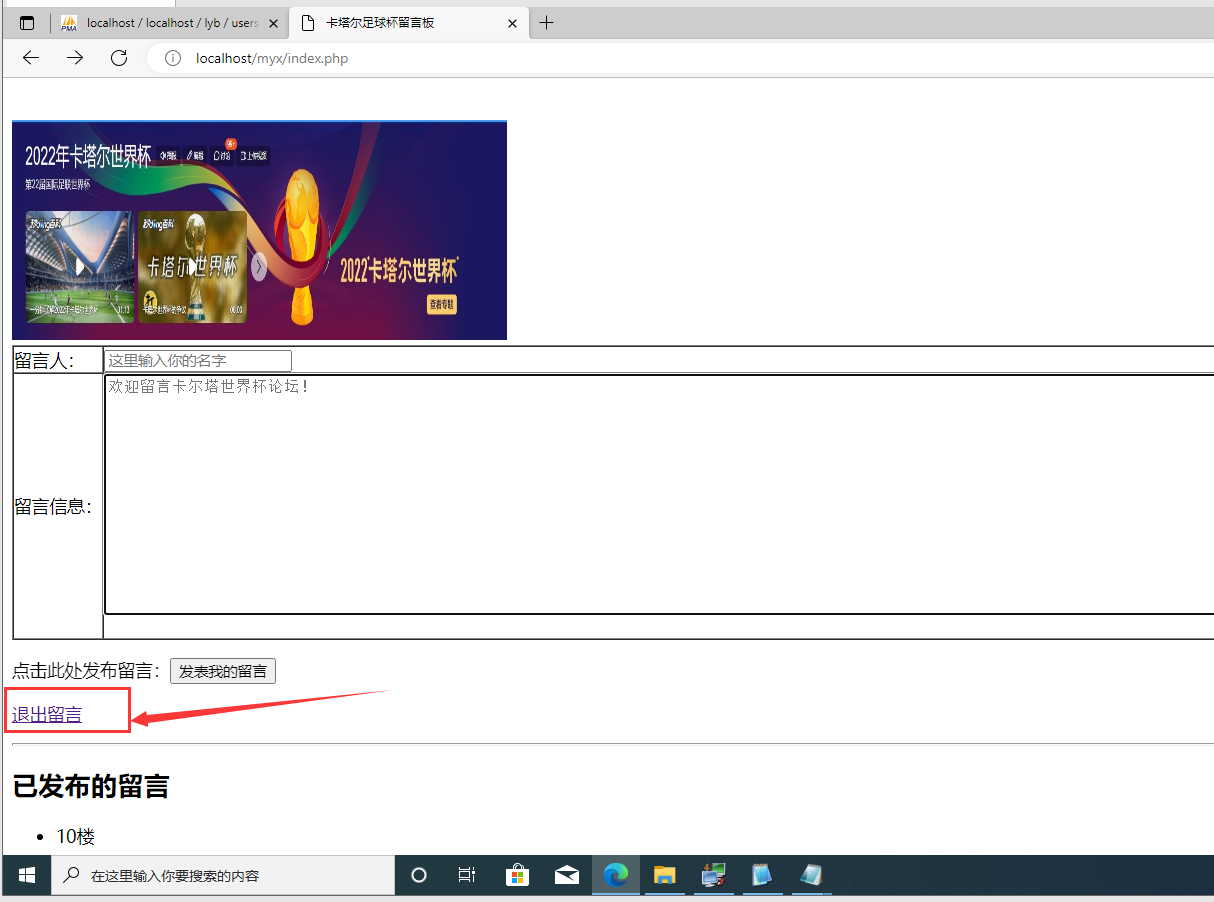
方框是要删除的留言：



点击删除后发现留言已删除：



留言后可选择退出留言板个人登录：



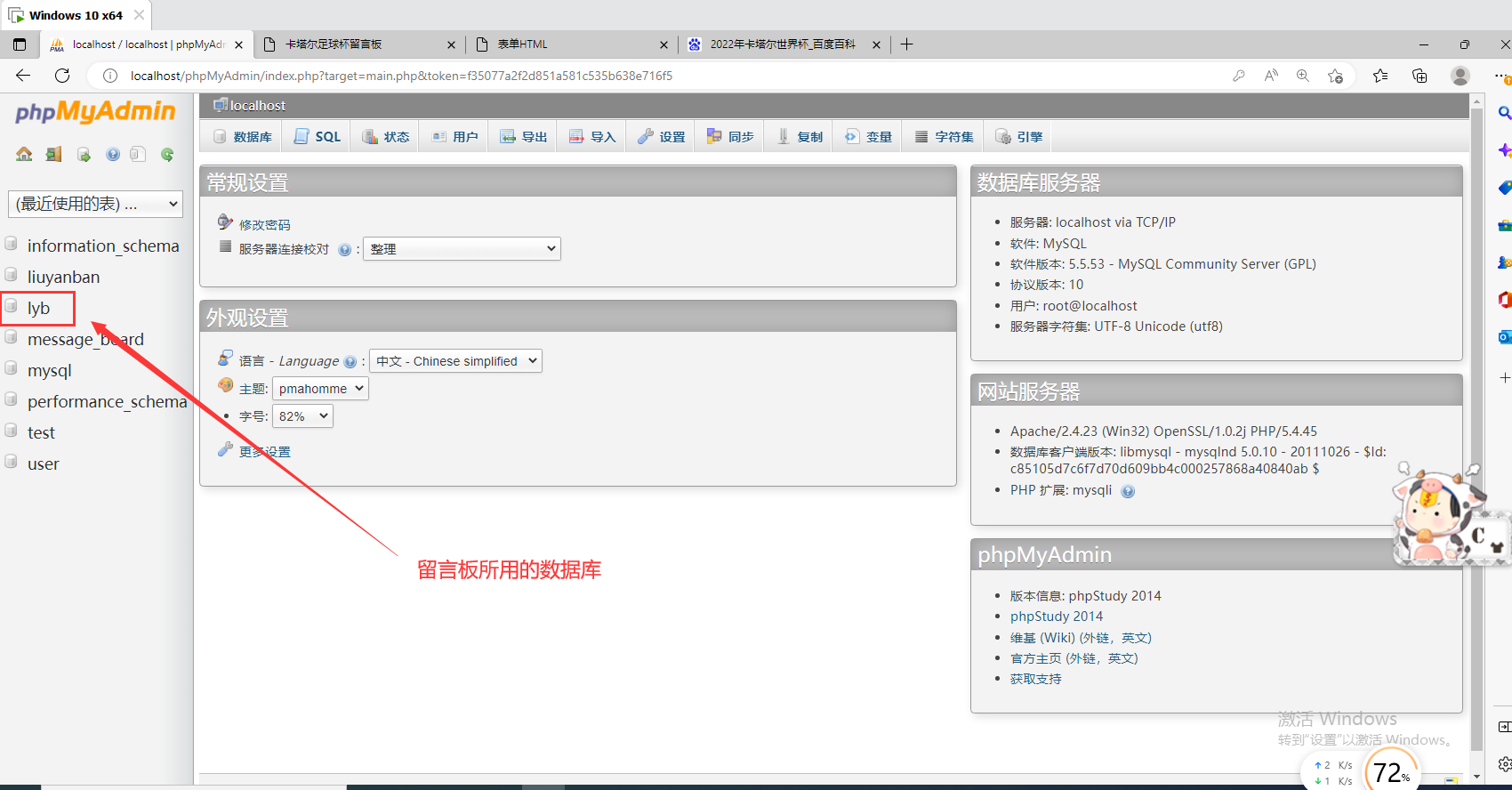
1. 实现与数据库的连接，通过POST提交数据存储与数据输出。

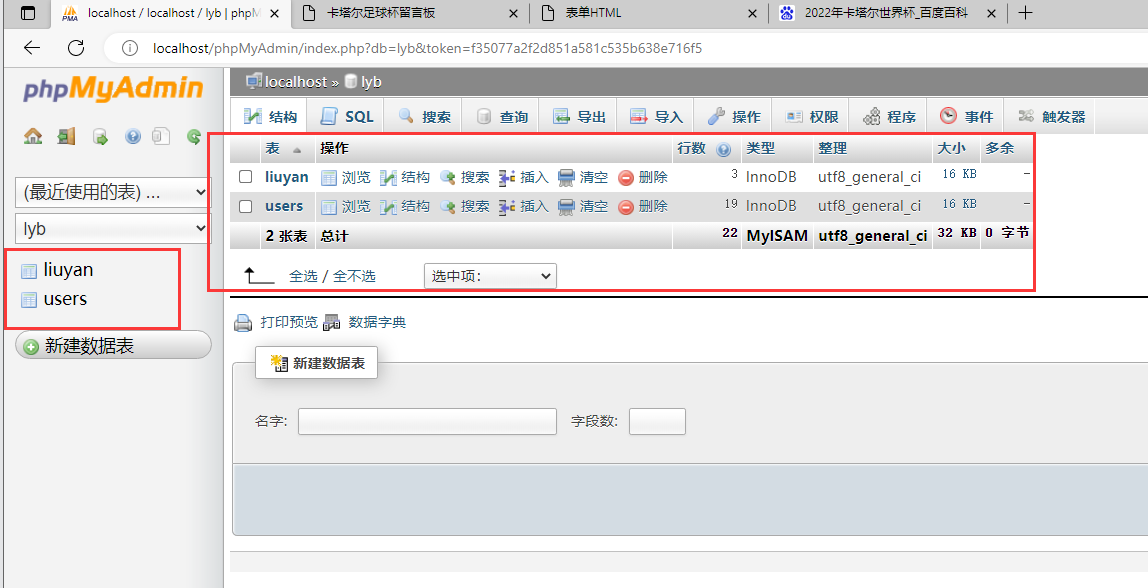
mysql数据库用户:root,密码：root

留言板数据库名称:lyb

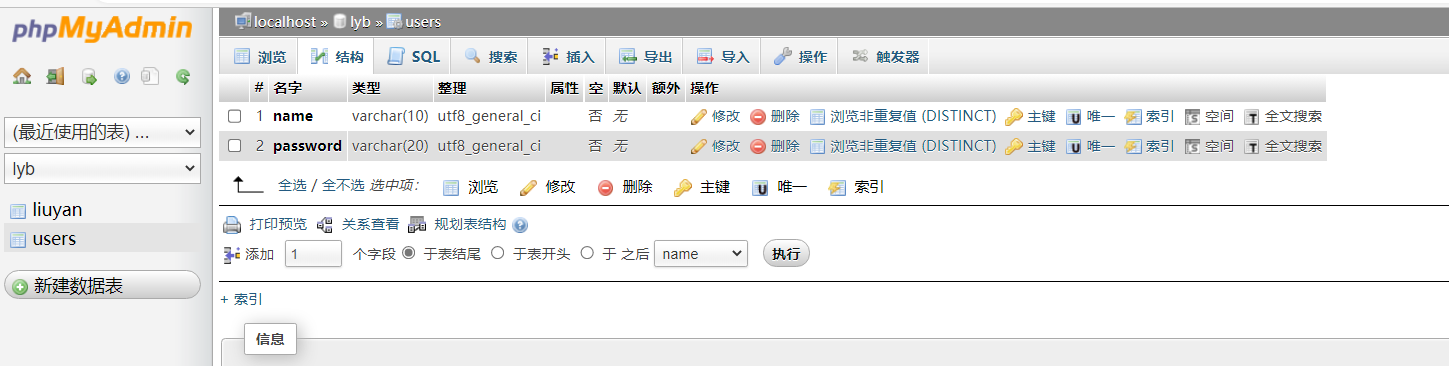
数据库lyb有两个表，一个是users用户表，里面包含账号密码,

另一个表是liuyan 用于存储用户在留言板发步的数据。





users表结构：



liuyan表结构：



**conn.php和config.php两个文件实现与数据库的连接：**

coon.php代码：

<?php

// 连接数据库(地址,用户名,密码,数据库名)

$servername="localhost";

$username="root";

$password="root";

$dbname="lyb";

// 创建链接

$conn = new mysqli($servername,$username,$password,$dbname);

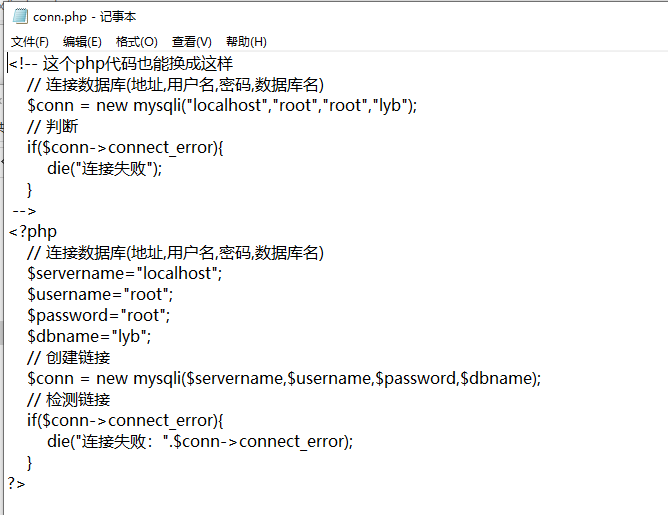
// 检测链接

if($conn->connect\_error){

die("连接失败：".$conn->connect\_error);

}

?>



config.php代码（这个是配置文件）：

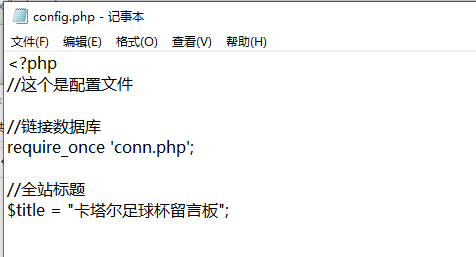
<?php

//链接数据库

require\_once 'conn.php';

//全站标题

$title = "卡塔尔足球杯留言板";

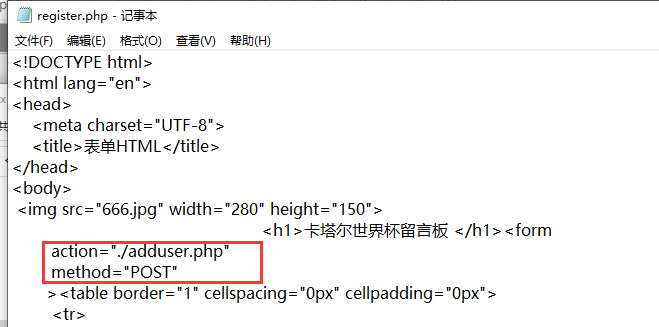


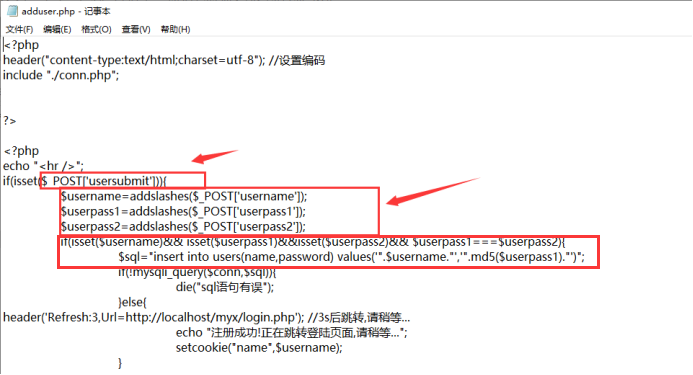
通过递交POST提交数据存储与数据输出

**Php代码：（register.php:10~29行）**

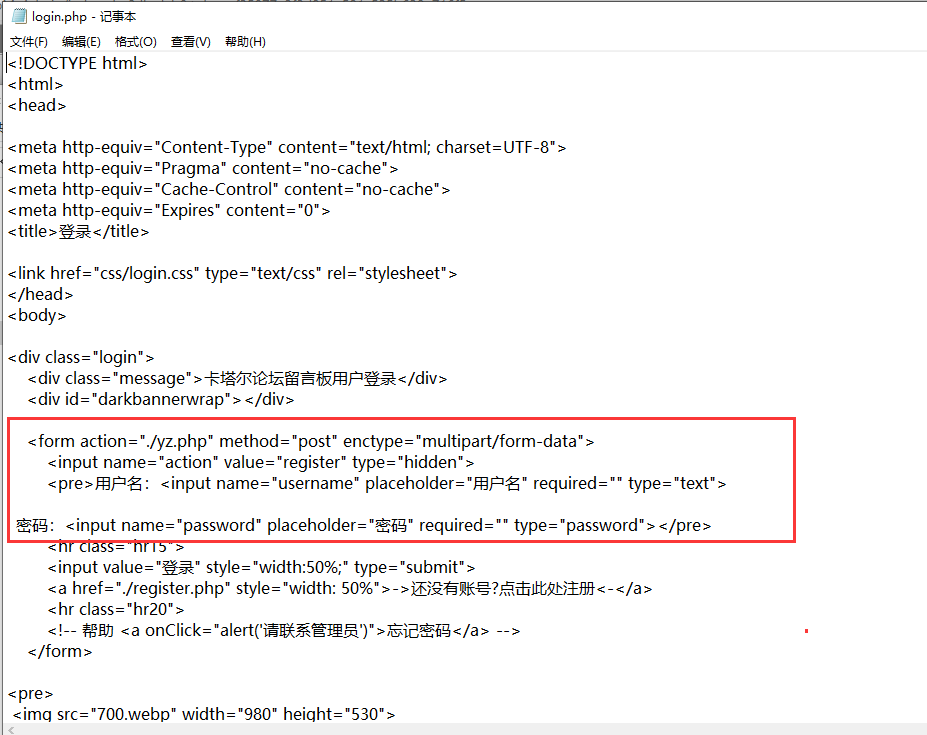
表单的提交地址是./adduser.php，使用POST方法进行提交。表单中包含了一个包含边框的表格，表格中有多个行（<tr>）和列（<td>）。每一行包含一个表单字段的标签和输入框。







登录时通过post将变量username和password参数传递给后实现数据验证，后端mysql数据库验证是否存在该用户，若存在即可登录留言板，不存在则无法登陆：

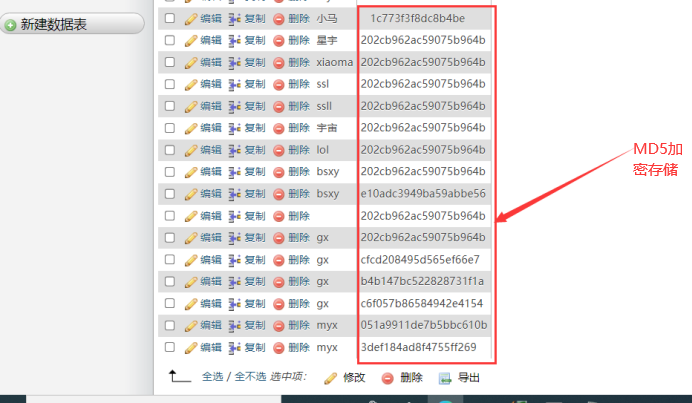
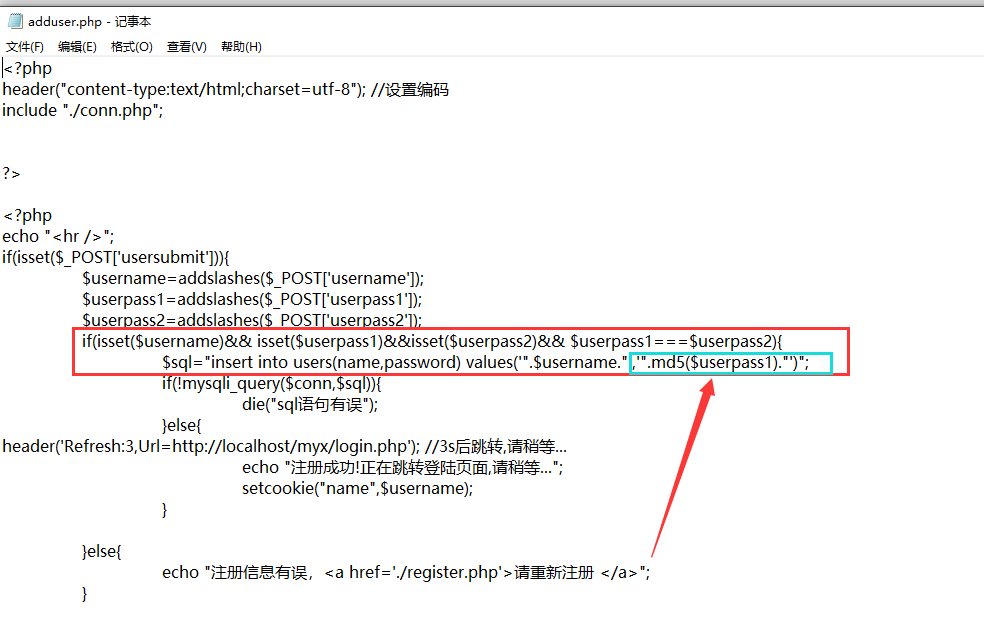




1. 利用加密算法实现加密存储，掌握使用Cookie知识。

利用MD5加密算法实现加密存储：

对存储到mysql数据库中的用户密码采用MD5加密存储：



 Cookie是由服务器端产生并发送给客户端浏览器的，浏览器会将发送过来的Cookie存储到某个文件中，随后再一次请求时，会自动带着存储的Cookie一并请求到服务器端

php中cookie可以用来实现自动填写该用户的用户名和密码，以及判断是否是第一次登录。cookie是一种服务器留在用户计算机上的小文件。当同一台计算机通过浏览器请求页面时，这台计算机将会发送cookie。

Cookie的创建十分简单，只要用户的浏览器支持 Cookie 功能，就可以使用 PHP 内建的函数来建立一个新的Cookie。在PHP中通过 setcookie() 函数创建 Cookie。



cookie中设置了HttpOnly属性，程序(JS脚本、Applet等)将无法读取到Cookie信息  
在php.ini配置文件中进行cookie只读设置的开启：

#搜索session.cookie\_httponly =

session.cookie\_httponly = On

PHP代码中开启：

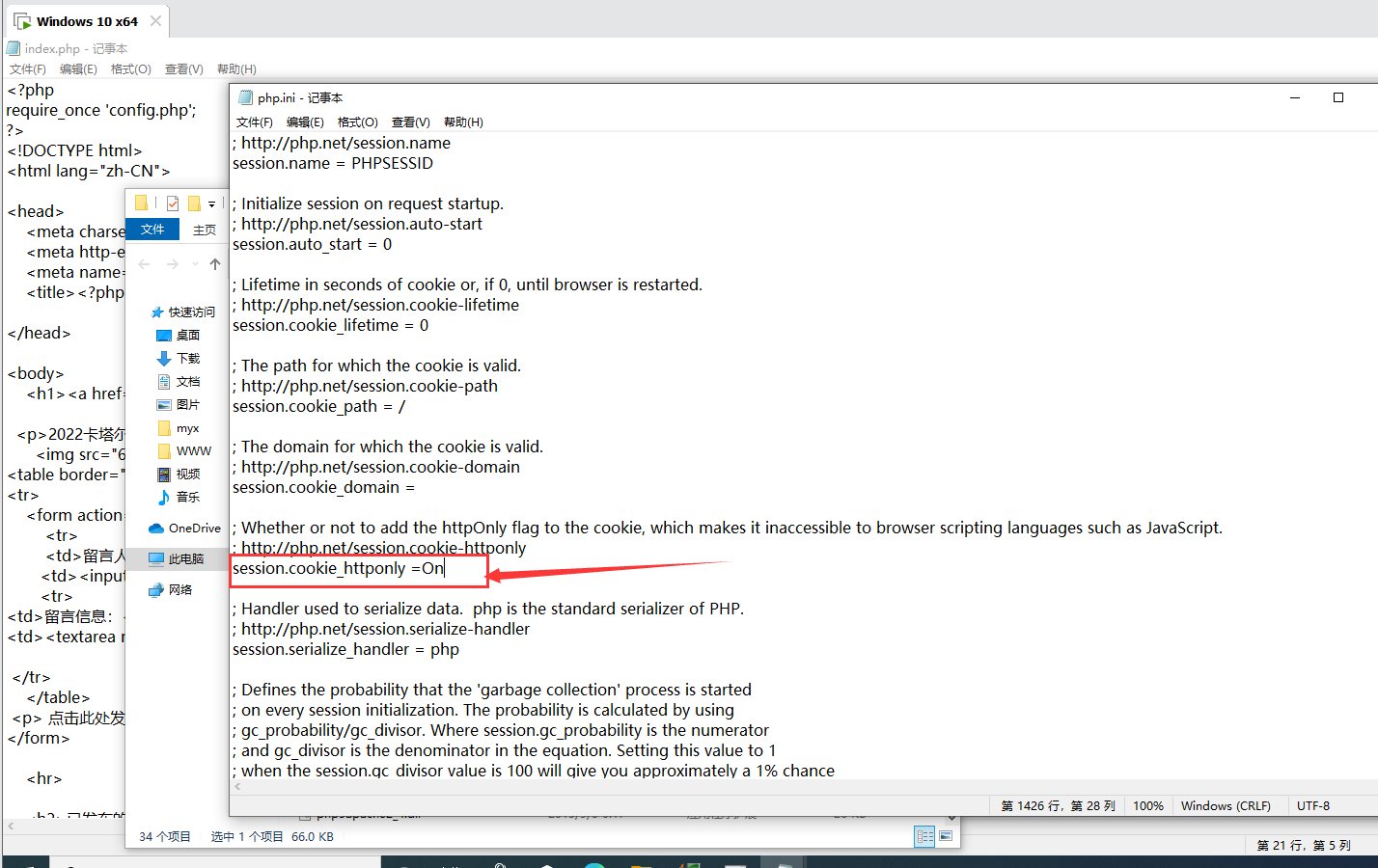
<?php

ini\_set("session.cookie\_httponly", 1);

// or

session\_set\_cookie\_params(0, NULL, NULL, NULL, TRUE);

?>



1. 利用web网站漏洞原理，使用函数对相关数据进行过滤处理。

sql注入：就是通过把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。

具体来说，它是利用现有应用程序，将恶意的SQL命令注入到后台数据库引擎执行的能力，它可以通过在Web表单中输入（恶意）SQL语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行SQL语句。

通过启用php.ini配置文件中的相关选项，就可以将大部分想利用SQL注入漏洞的骇客拒绝于门外。常用的安全函数有：  
1、mysql\_real\_escape\_string()  
2、addslashes()

1. htmlspecialchars()过滤  
    这些函数的作用：  
    mysql\_real\_escape\_string – [转义](https://so.csdn.net/so/search?q=%E8%BD%AC%E4%B9%89&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/xuxiaopang0417/article/details/_blank) SQL 语句中使用的字符串中的特殊字符，并考虑到 连接的当前字符集 ！

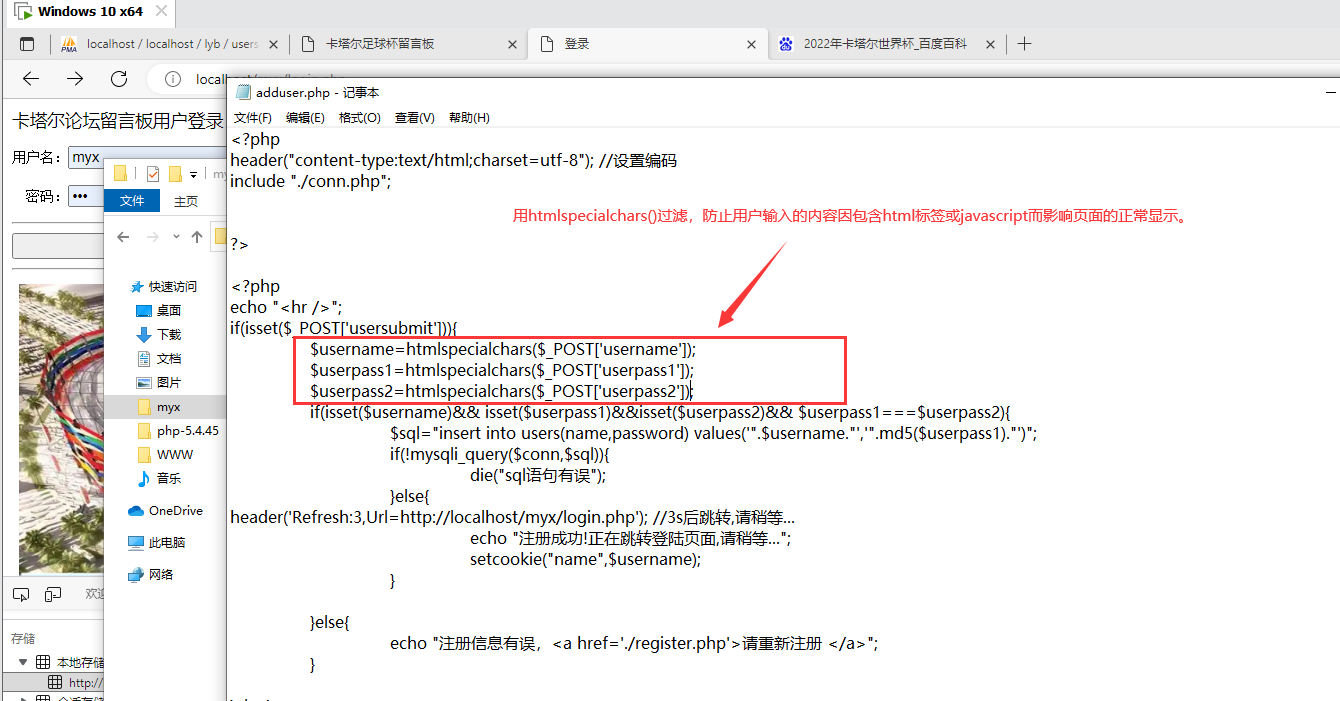
mysql\_real\_escape\_string()和addslashes()函数都是对数据中的 单引号、双引号进行转义！也就是防止sql注入！  
当前的字符集是单字节的话，这两个函数作用相同，都可以起到转义过滤的作用。

用htmlspecialchars()过滤，防止用户输入的内容因包含html标签或javascript而影响页面的正常显示。  
可以用htmlspecialchars()过滤其中的 & " < >，输出的时候用htmlspecialchars()函数输出，能有效应对一些xss攻击，也可以转换html代码为实体，更安全一些。

另一方面也能在一定程度上应对XSS攻击。  
例如PHP代码：  
$username=htmlspecialchars($\_POST['username']);

$userpass1=htmlspecialchars($\_POST['userpass1']);

$userpass2=htmlspecialchars($\_POST['userpass2']);



在PHP中，专门用于转义的内置函数，它就是 addslashes()，addslashes 使用反斜线引用字符串；返回字符串，该字符串为了数据库查询语句等的需要在某些字符前加上了反斜线。这些字符是单引号（’）、双引号（”）、反斜线（\）与 NUL（NULL 字符）。

不要对已经被 magic\_quotes\_gpc 转义过的字符串使用 addslashes()，因为这样会导致双层转义。遇到这种情况时可以使用函数 get\_magic\_quotes\_gpc() 进行检测。

魔术引号是程序自动将进入PHP脚本的数据进行转意的过程。当打开时，所有的 '（单引号），"（双引号），\（反斜线）和 NULL 字符都会被自动加上一个反斜线进行[转义](https://so.csdn.net/so/search?q=%E8%BD%AC%E4%B9%89&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/weixin_50464560/article/details/_blank)。和 addslashes() 函数的作用完全相同。

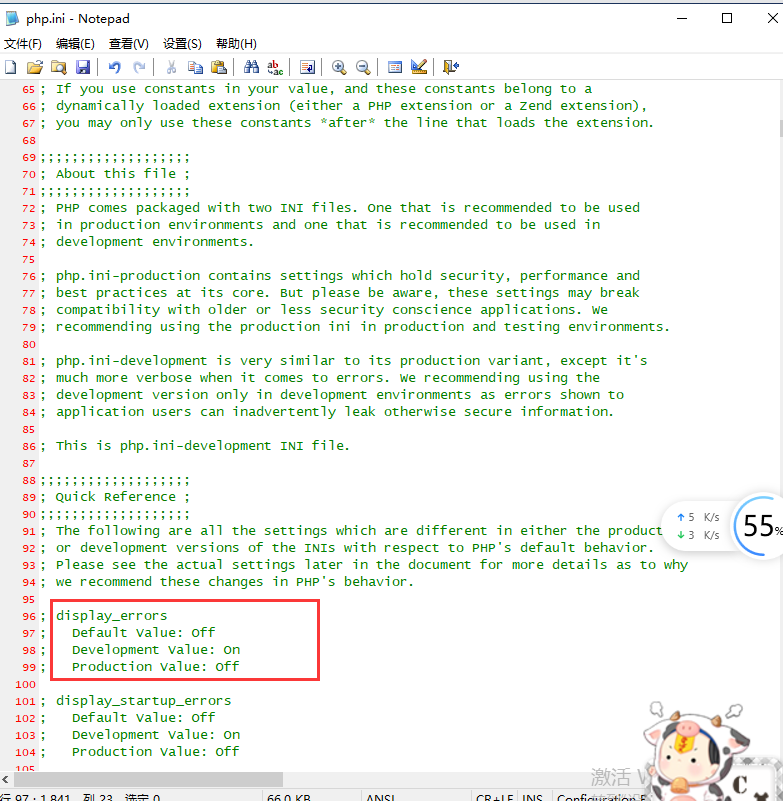
当初是为了阻止SQL注入的需要引入了魔法引号，对于开发者有一定好的好友，但在使用的时候也带来很多的不便，现在有了更多更好的方案来替代，所以如果还是在php 5.3.0或php 5.3.0之前的版本做开发应该尽量避免使用魔法引号，php 5.4.0以后已经移除了。  
 我们用addslashe()函数对用户输入的账号和密码进行过滤，语法: string addslashes(string str); //str为含有需转义字符的字符串：



应对sql报错注入：

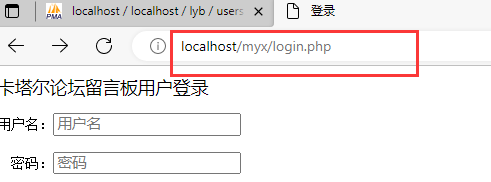
如果WEB网站开启了错误显示，攻击者就可以通过反复调整发送的参数、查看页面打印的错误信息，推测出WEB网站使用的数据库和开发语言等重要信息。错误回显可以暴露出非常多的敏感信息，为攻击者下一步攻击提供便利

为了防止报错信息被攻击者直接看到，设置display\_errors=Off：

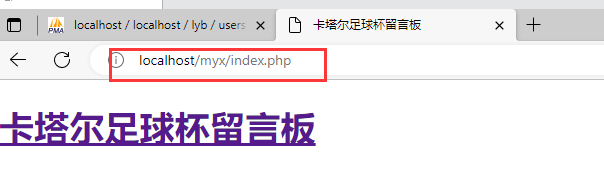
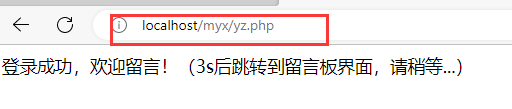


防止sql注入关键的一步是找到页面与数据库产生交互的地方.

用户登录界面的url:



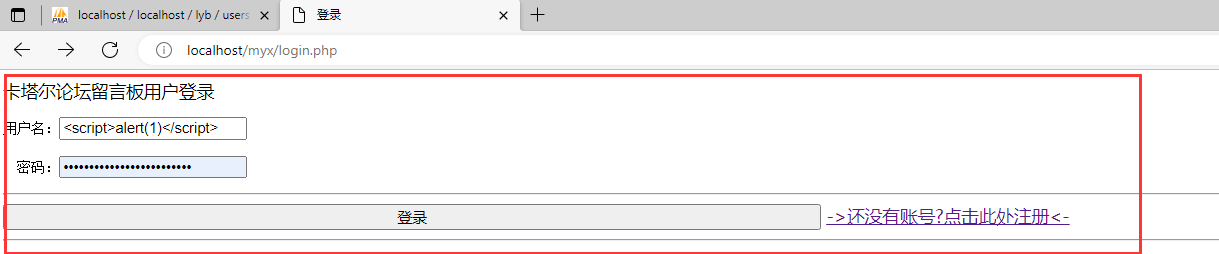
登陆成功及跳转留言板的url：



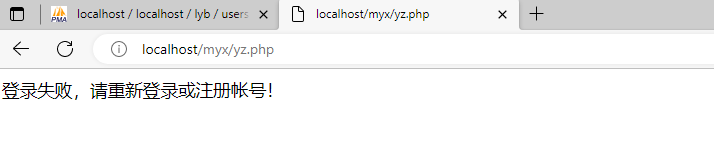
url后跟的就是没有类似参数id=1，’ ? ’ 这种的传参。一般来讲 ’ ? '的内容都是用户可控的。若不存在能够与数据库产生交互的地方，那么sql注入也就自然无处下手了，这样就能够比较有效的防止一些sql注入。

再试试一些简单的xss攻击：

<script>alert(1)</script> —— 测试是否存在XSS的常用语句，刷新之后若还有弹窗，说明为存储型XSS



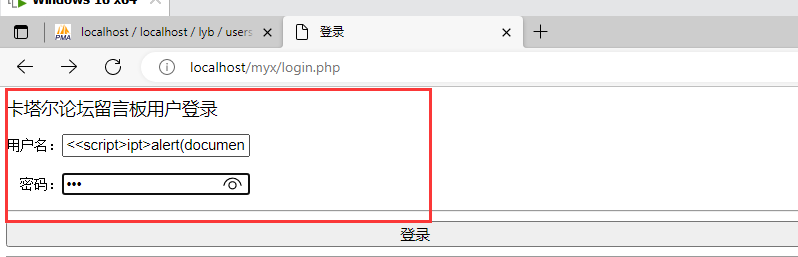
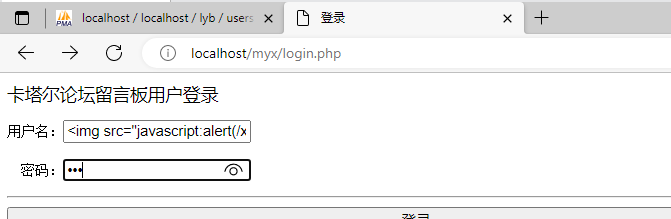
没有alert弹窗:



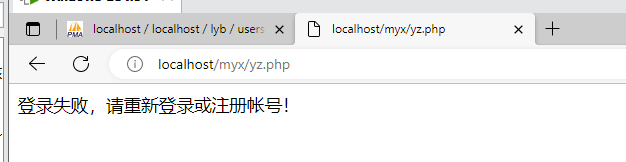
试试这两种：

<img src="javascript:alert(/xss/)">

<<script>ipt>alert(document.cookie)</scri<script>pt>

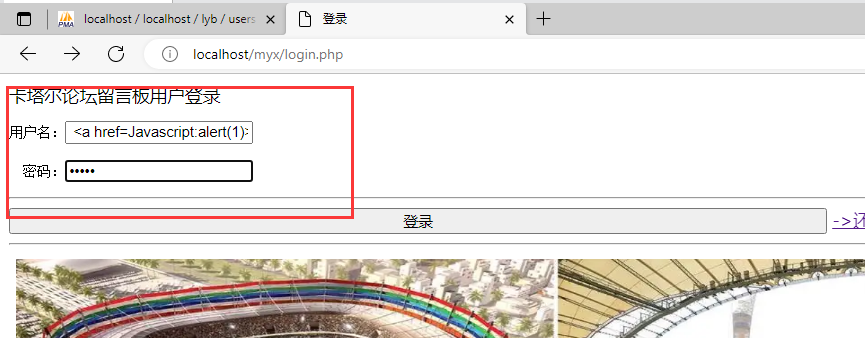


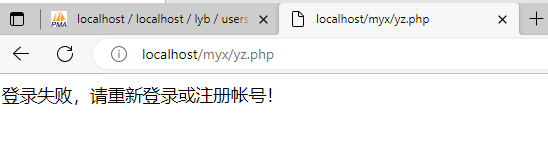
都是不行



试试伪协议：

伪协议： <a href=Javascript:alert(1)>123</a>





还是不行，说明这个web留言板对于一些sql注入和xss攻击都是比较有效的。