《漏洞利用及渗透测试基础》实验报告

姓名：管昀玫 学号：2013750 班级：计科一班

**实验名称：**

WEB开发实践

**实验要求：**

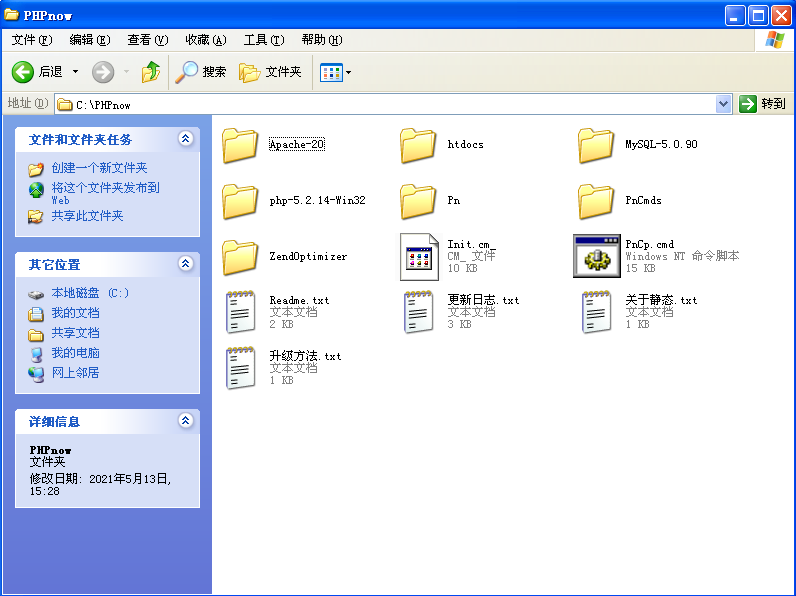
复现课本第十章的实验三(10.3.5节):利用php，编写简单的数据库插入、查询和删除

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

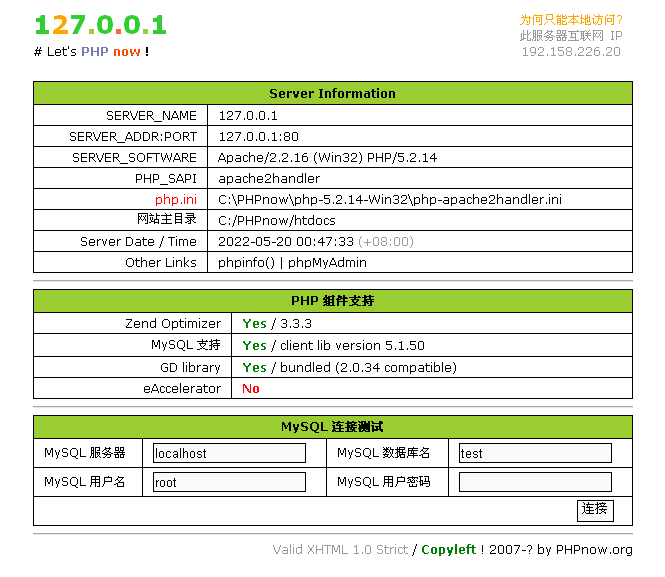
**实验过程：**

1. 实验准备

在Windows xp系统中解压PHPnew并运行setup.cmd，得到如下文件夹

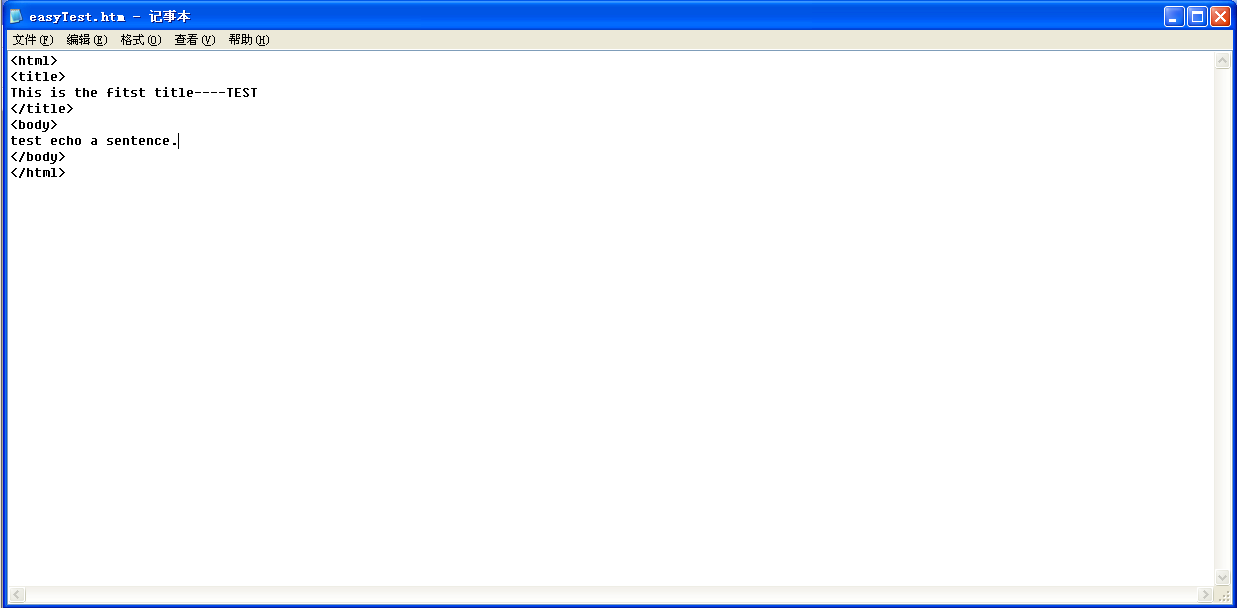


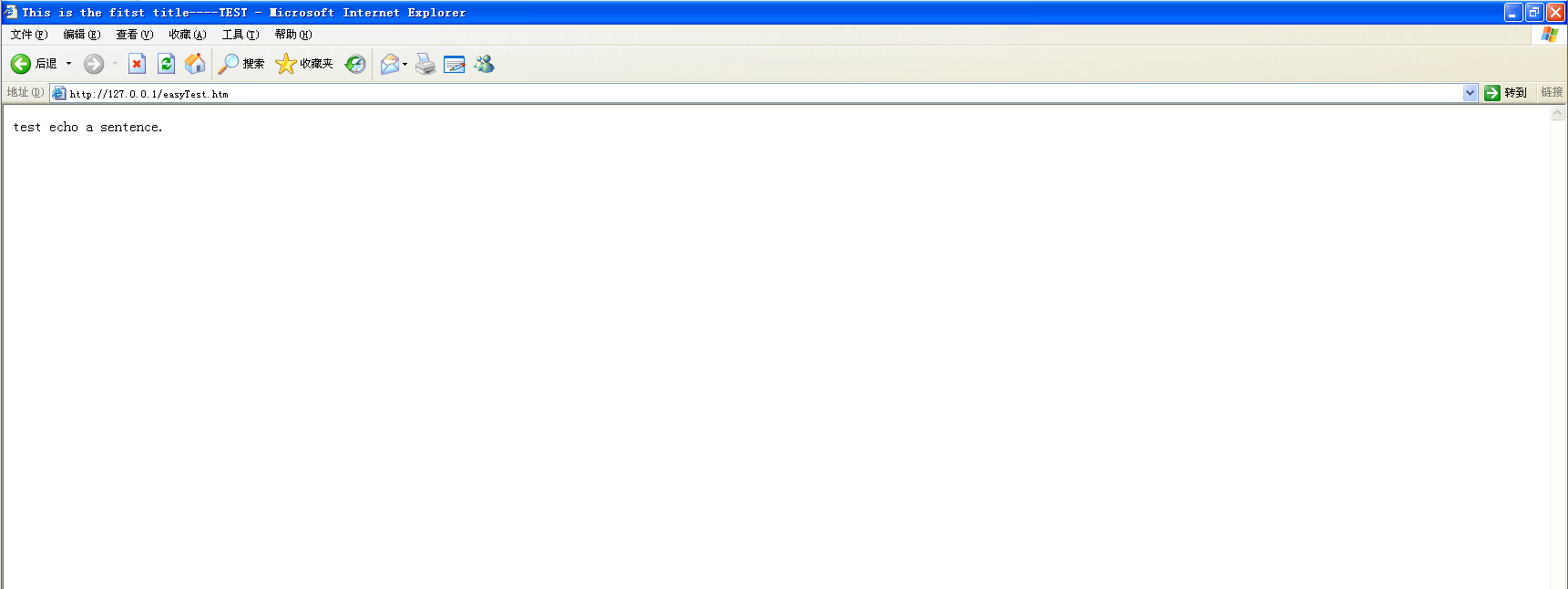
点击PnCp.cmd，选择序号20，启动PHPnow；打开网页，访问127.0.0.1，得到



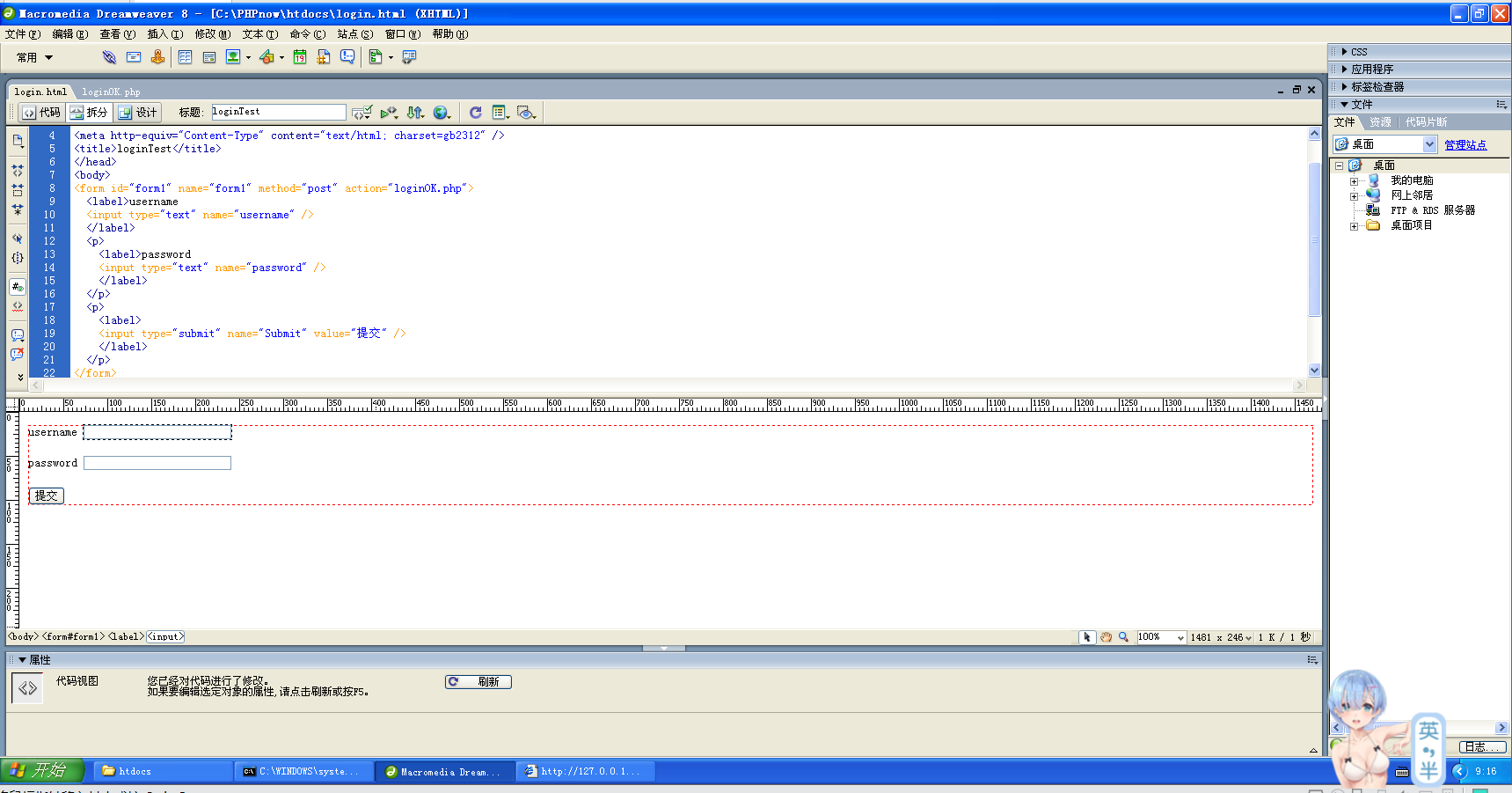
1. 简单测试网页效果

在htdocs的文件夹下编写一个简单的htm脚本，查看效果





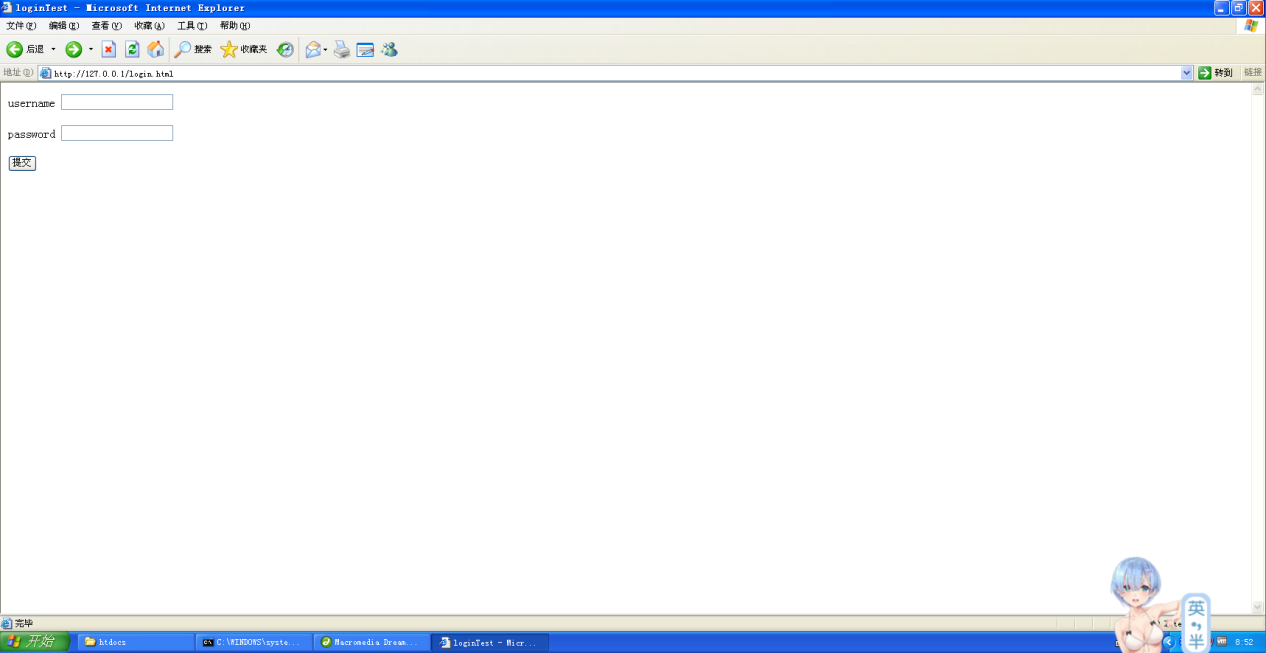
使用dreamweaver创建一个同于提交用户名账号密码的login.html，存储到PHPnow\htdocs下（因为htdocs是PHPnow的web应用的根目录），并把他的action设置为loginOK.php，form设置为post（意为当前网页不是一个静态网页，他会将一个post传输到loginOK.php进行处理）



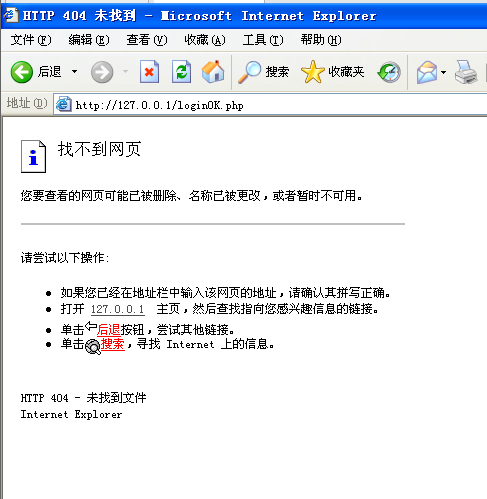
在上面的页面中，定义了一个form表单。表单是一个包含表单元素的区域。表单区域里包含了两个文本框（<input>）、一个确认按钮(submit) 。确认按钮的作用是当用户单击确认按钮时，表单的内容会被传送到另一个文件。而表单的动作属性(action)定义了目的文件的文件名。由动作属性定义的这个文件通常会对接收到的输入数据进行相关的处理。

在上面的表单中，定义了接受表单输入的处理文件为“loginok.php”，而method属性指定了与服务器进行信息交互的方法为POST。（POST一般用于更新资源信息）。

查看效果

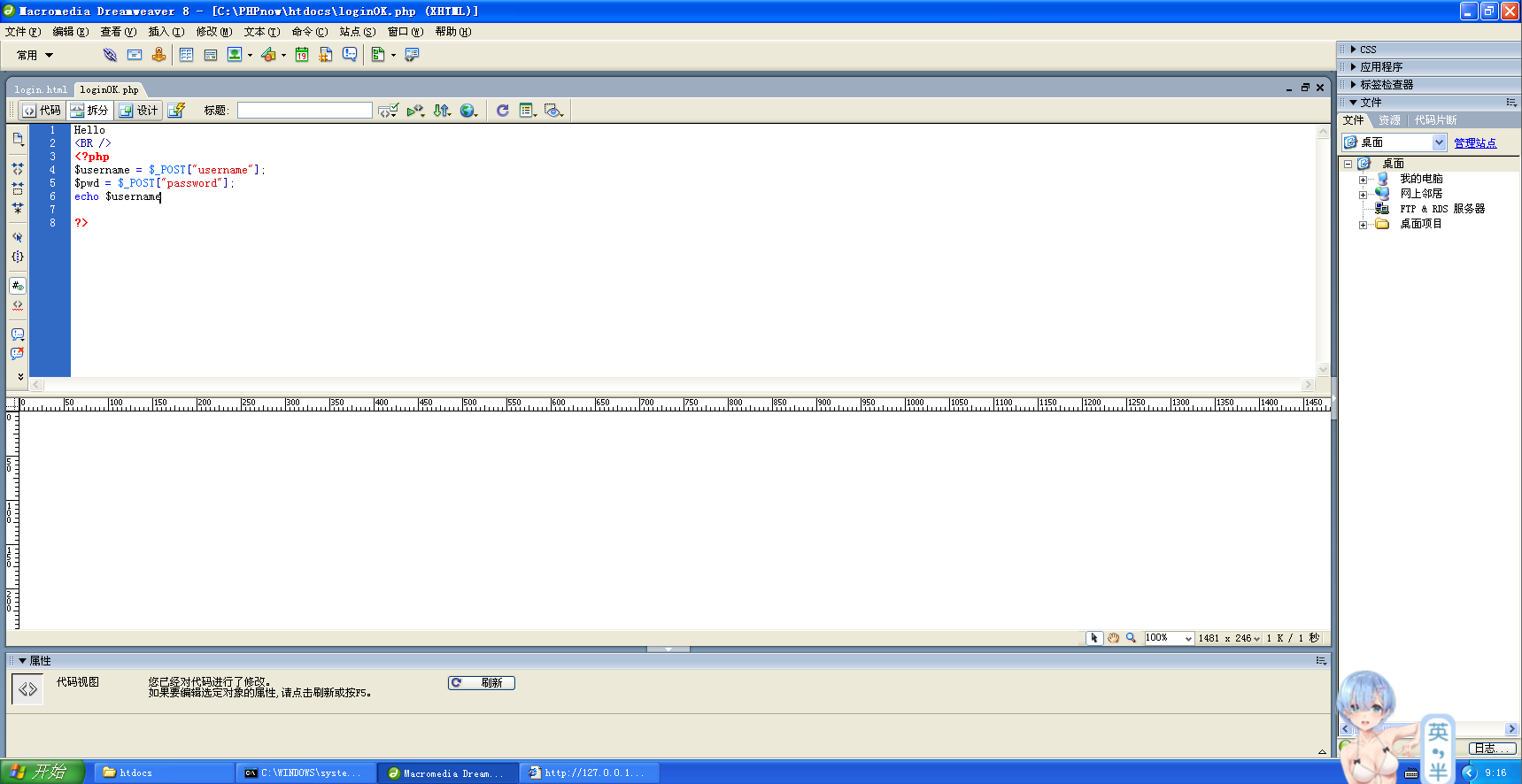


点击提交按钮后

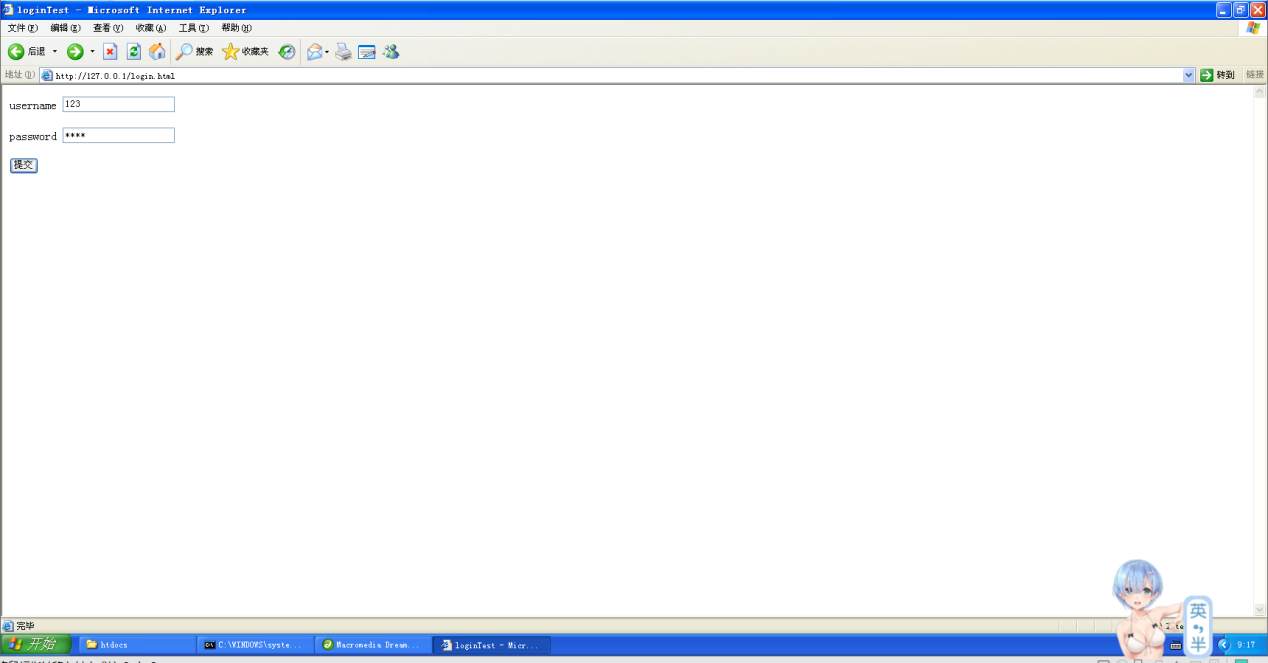


从URL可以看到使用loginOK.php进行了响应，但是此时还没有写loginOK.php，所以无法找到相应的网页进行处理

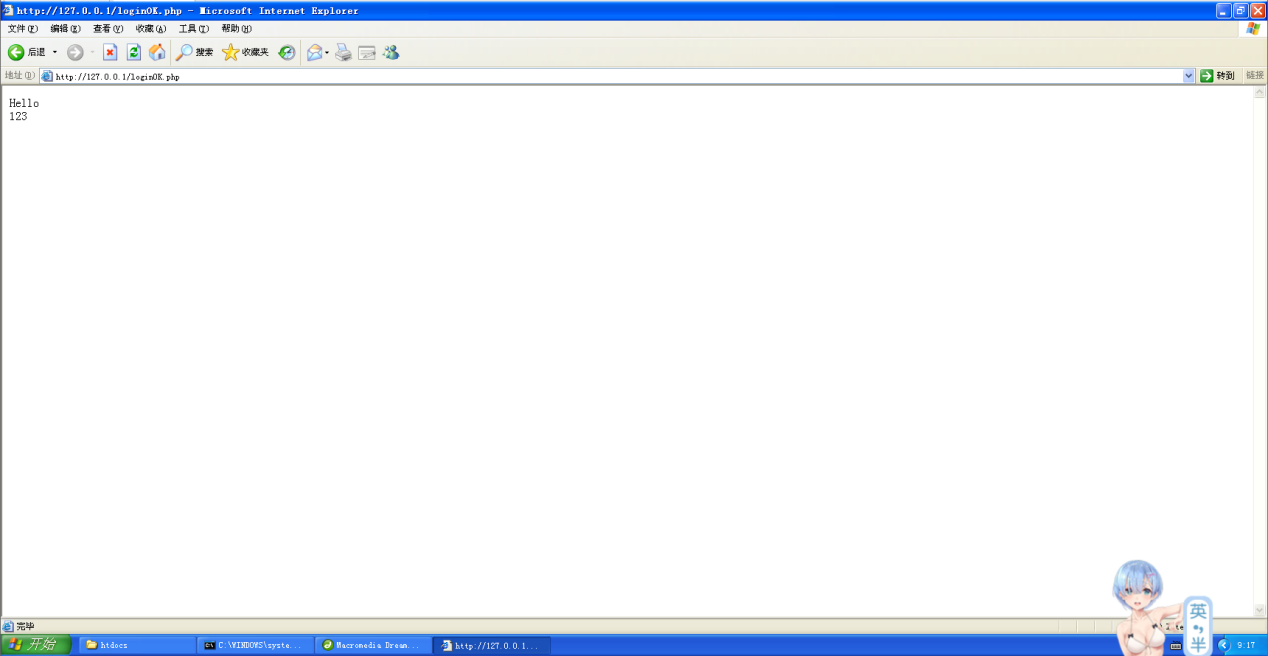
编写loginOK.php



再次输入用户名密码提交查看效果



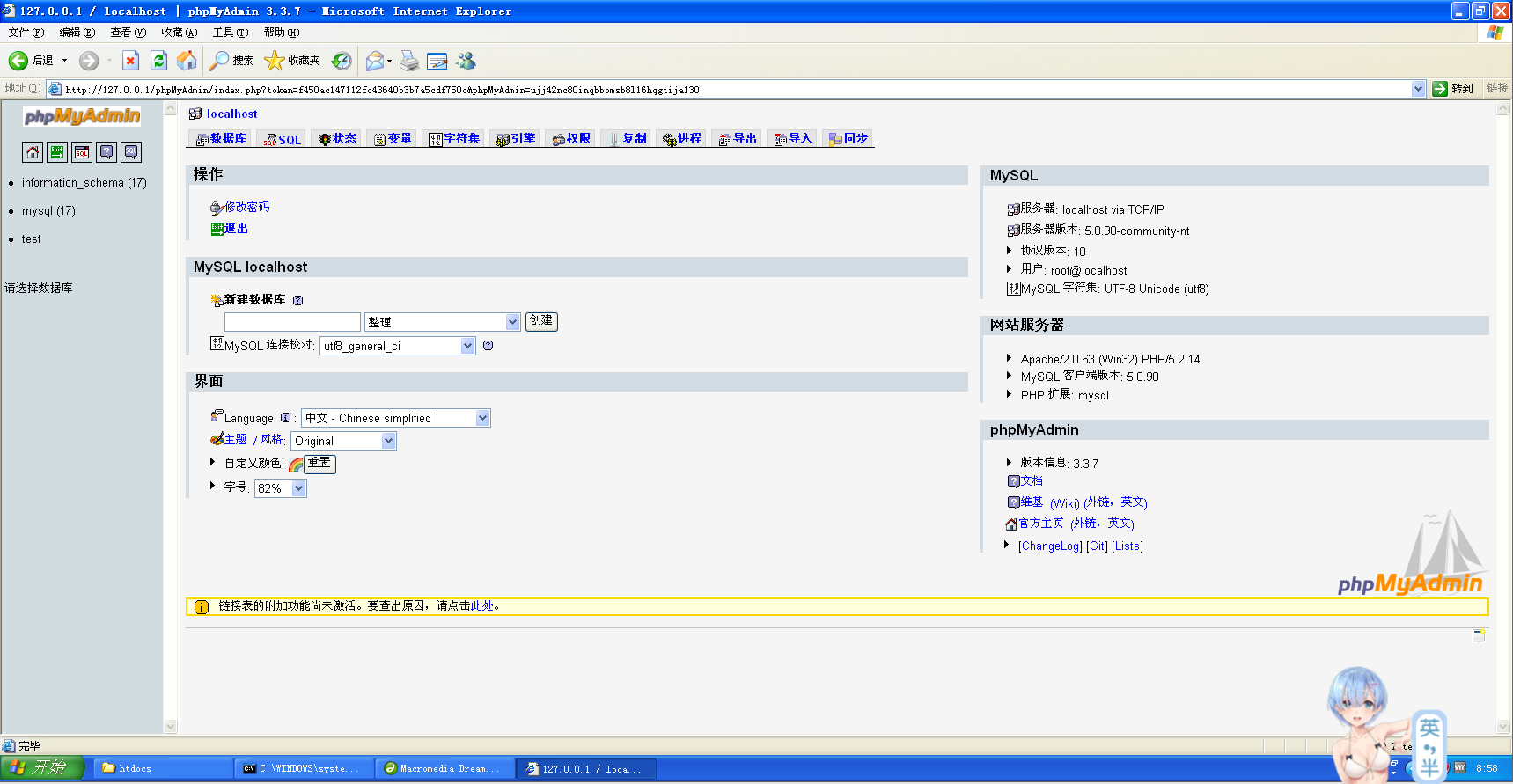
点击提交得到



响应成功

1. 创建数据库

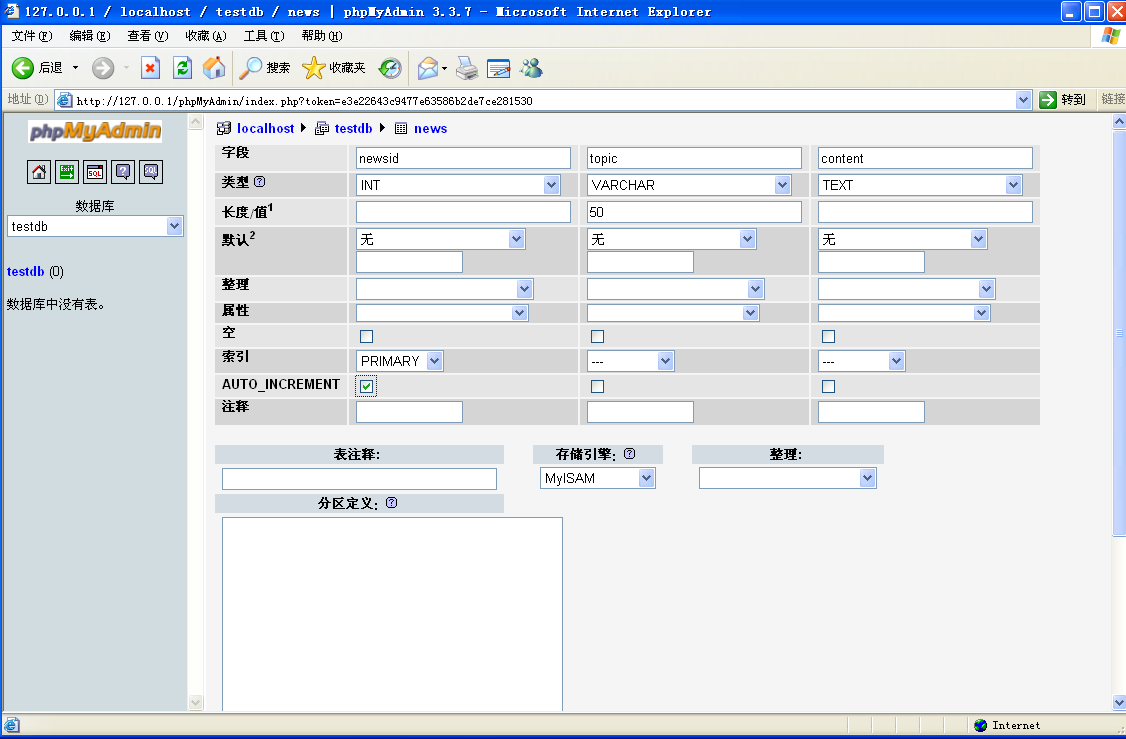
进入到Myadmin下



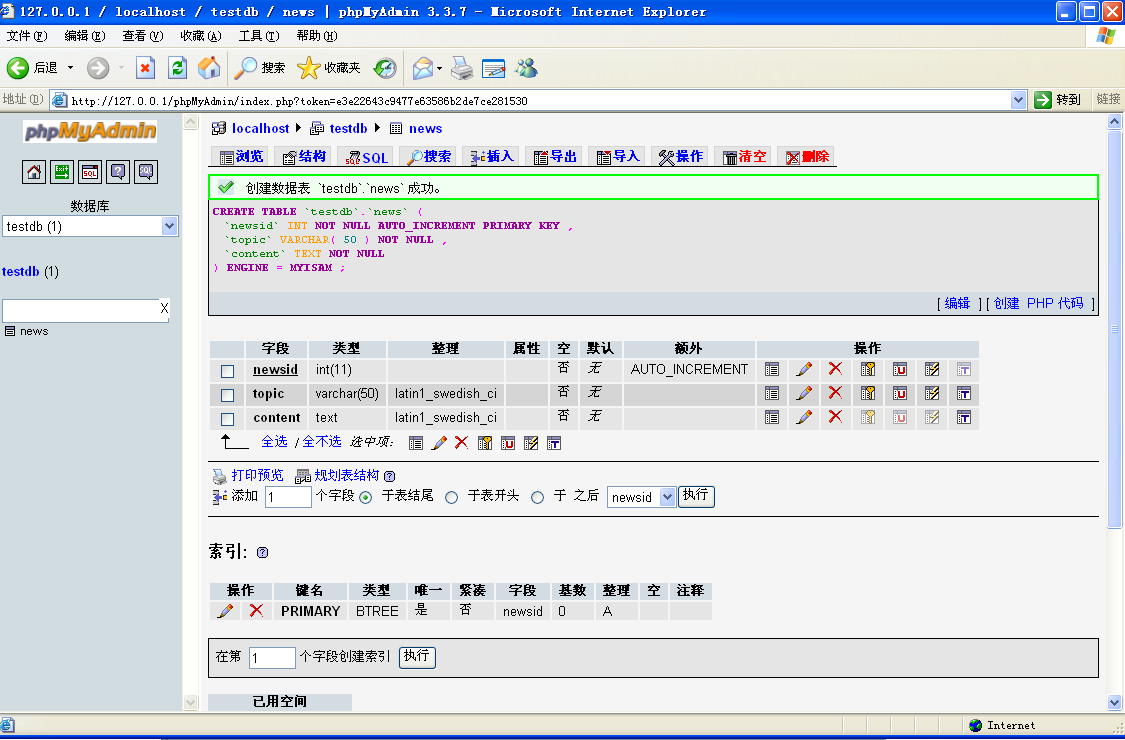
数据库：TestDB

表1：News（newsid, topic, content）

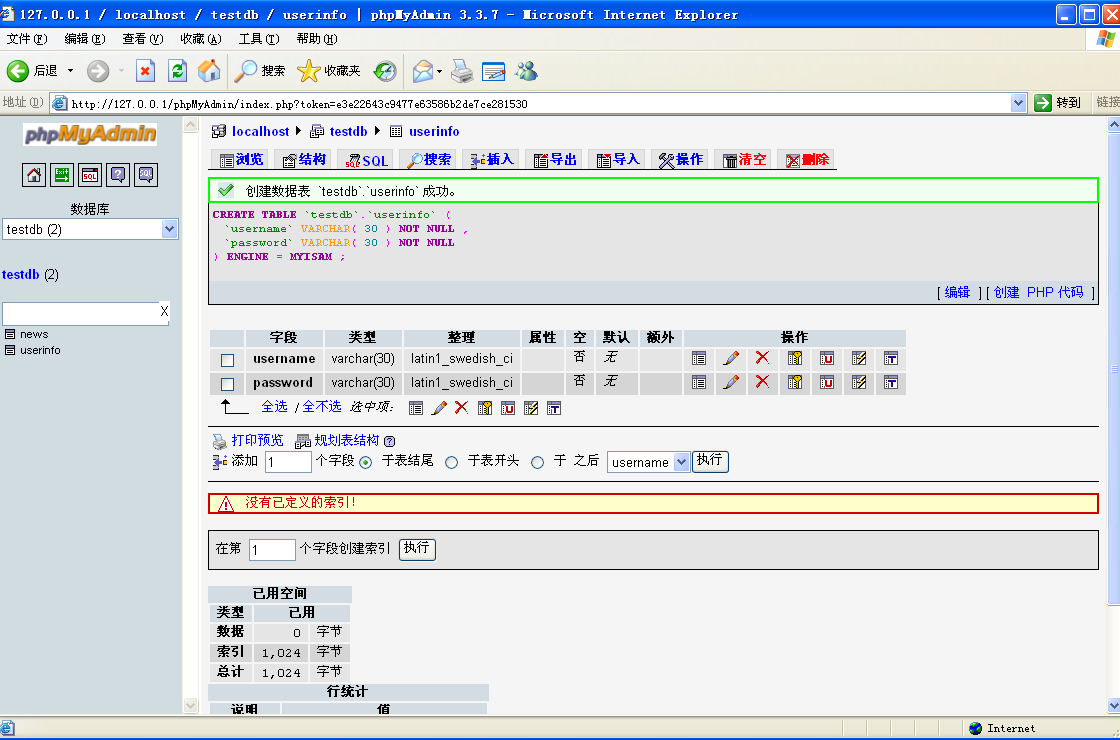
表2：userinfo（username, password）

在phpMyAdmin中建表如下：

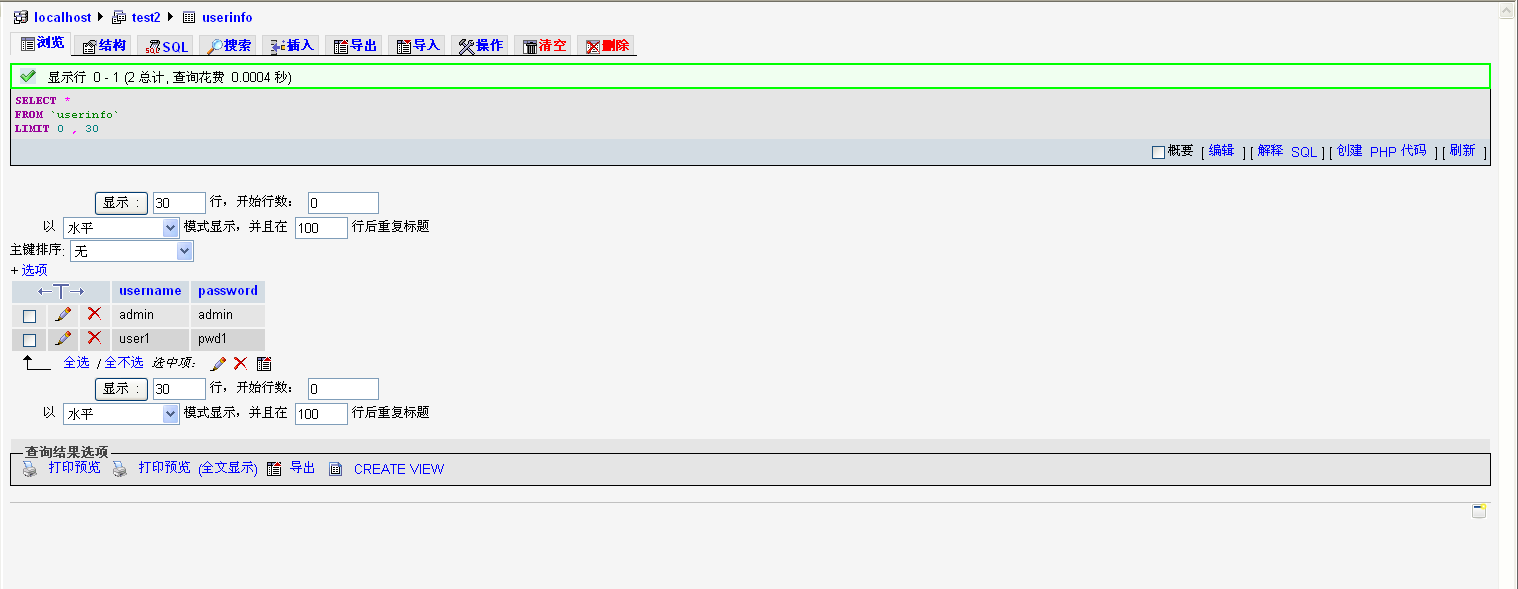
创建成功



之后再创建一个userinfo的表，用于之后数据库操作的测试



1. 数据库操作
   1. 插入



插入两个用户，第一个用户名密码都是admin

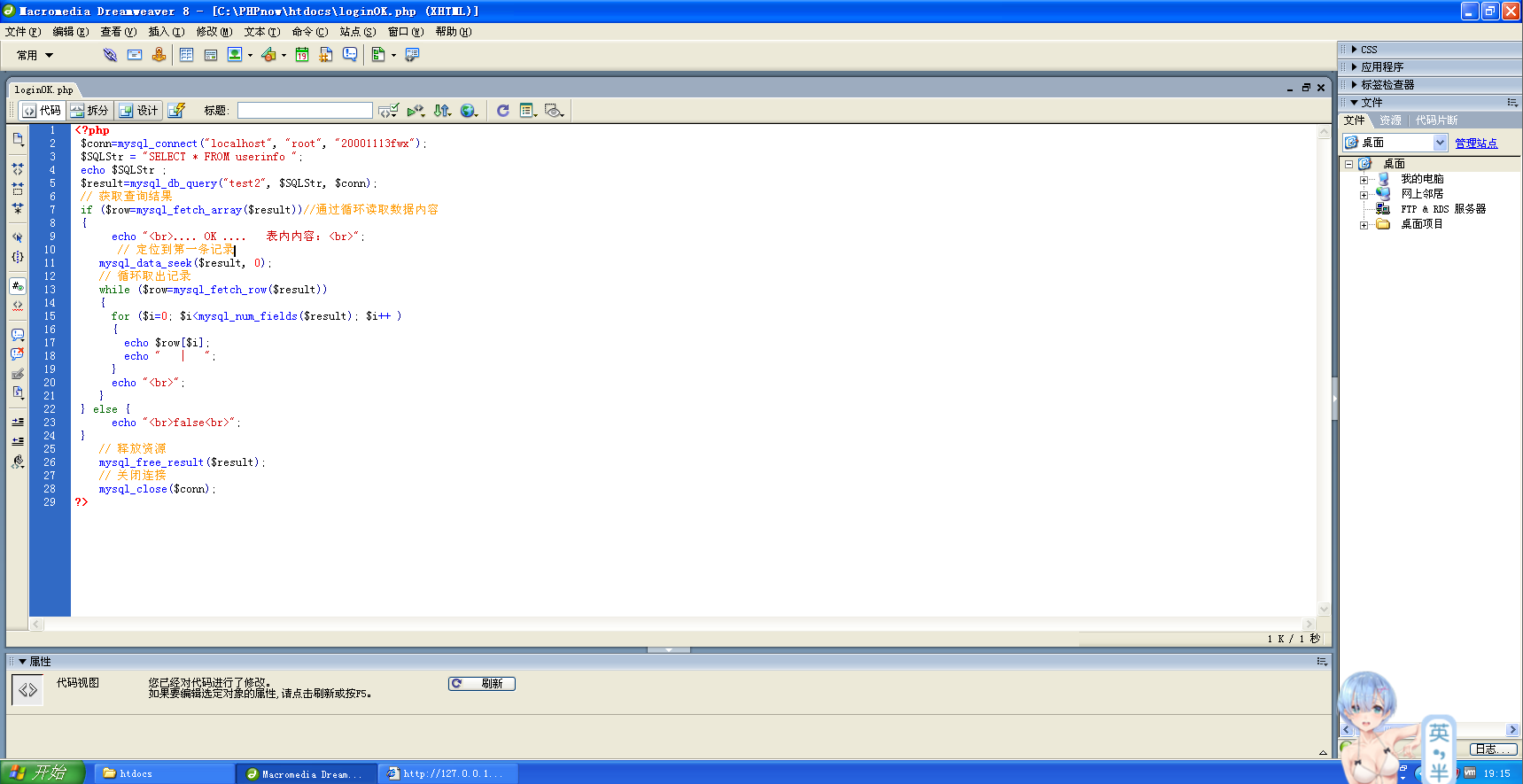
第二个用户名是user1，密码是pwd1

创建相关PHP文件：（总共6个，此处略）

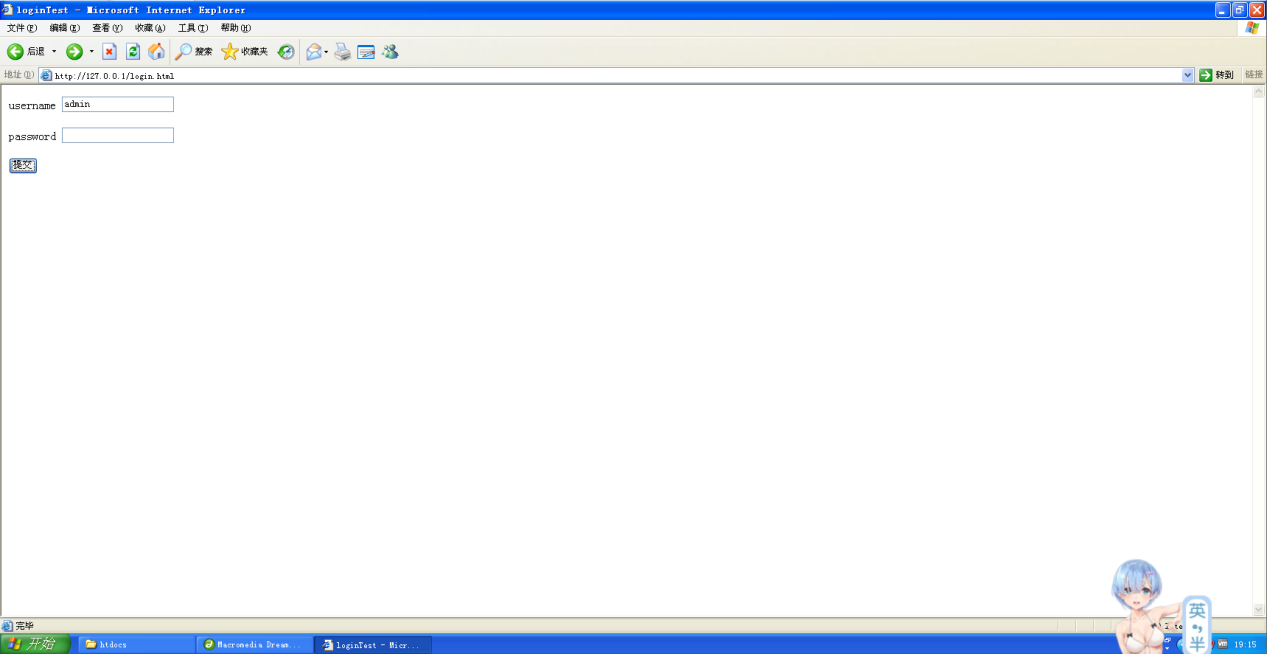


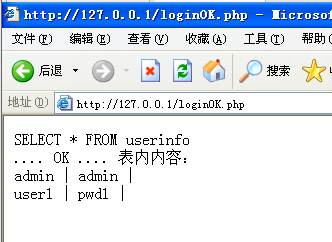
* 1. 查询（登录）

编写查询代码

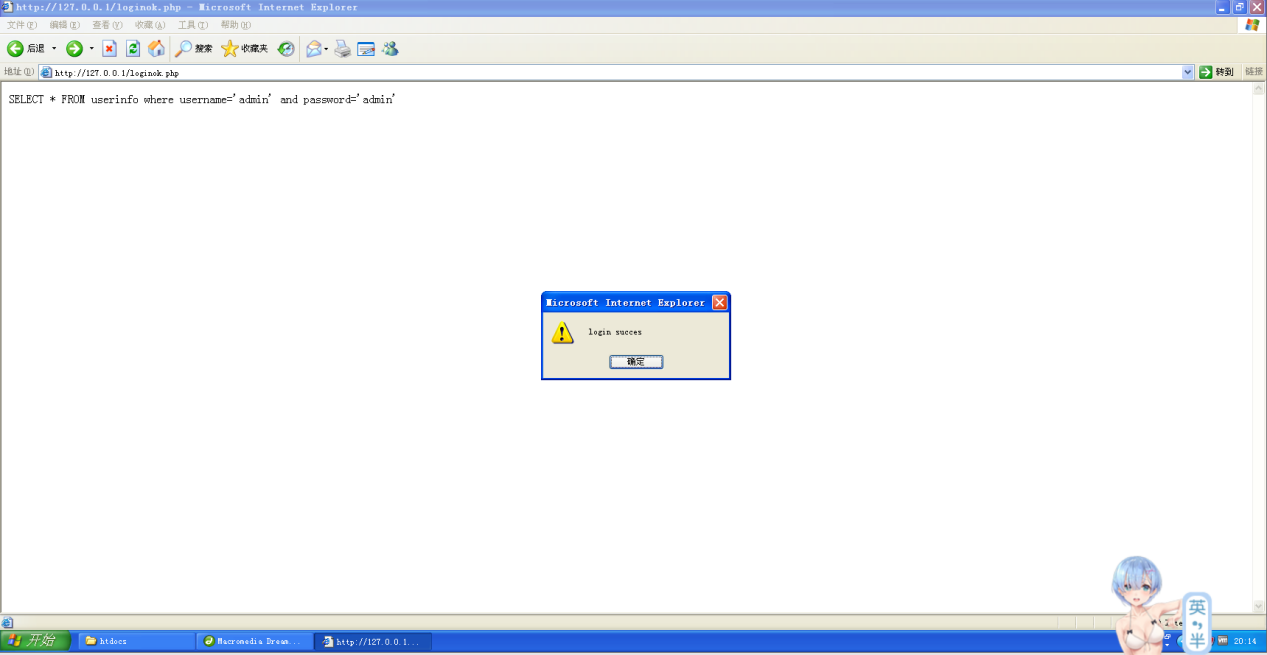


测试输入





更换新的登录

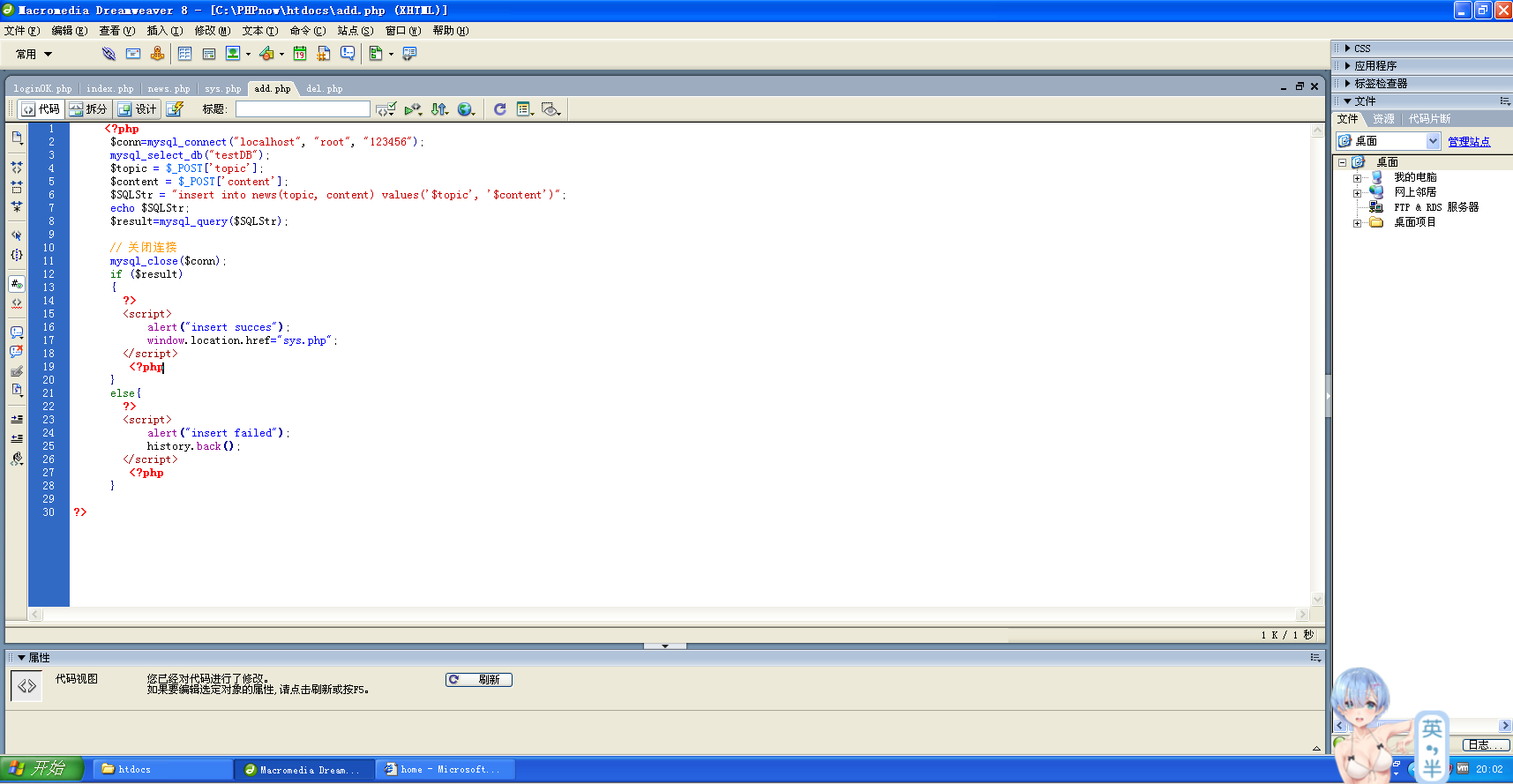


* 1. 插入

进入 sys.php 后，“添加”写好的新闻标题和内容，会跳转到 add.php，更新 news

表中的信息。

编写代码如下



插入新闻标题为123，新闻内容为Hello world

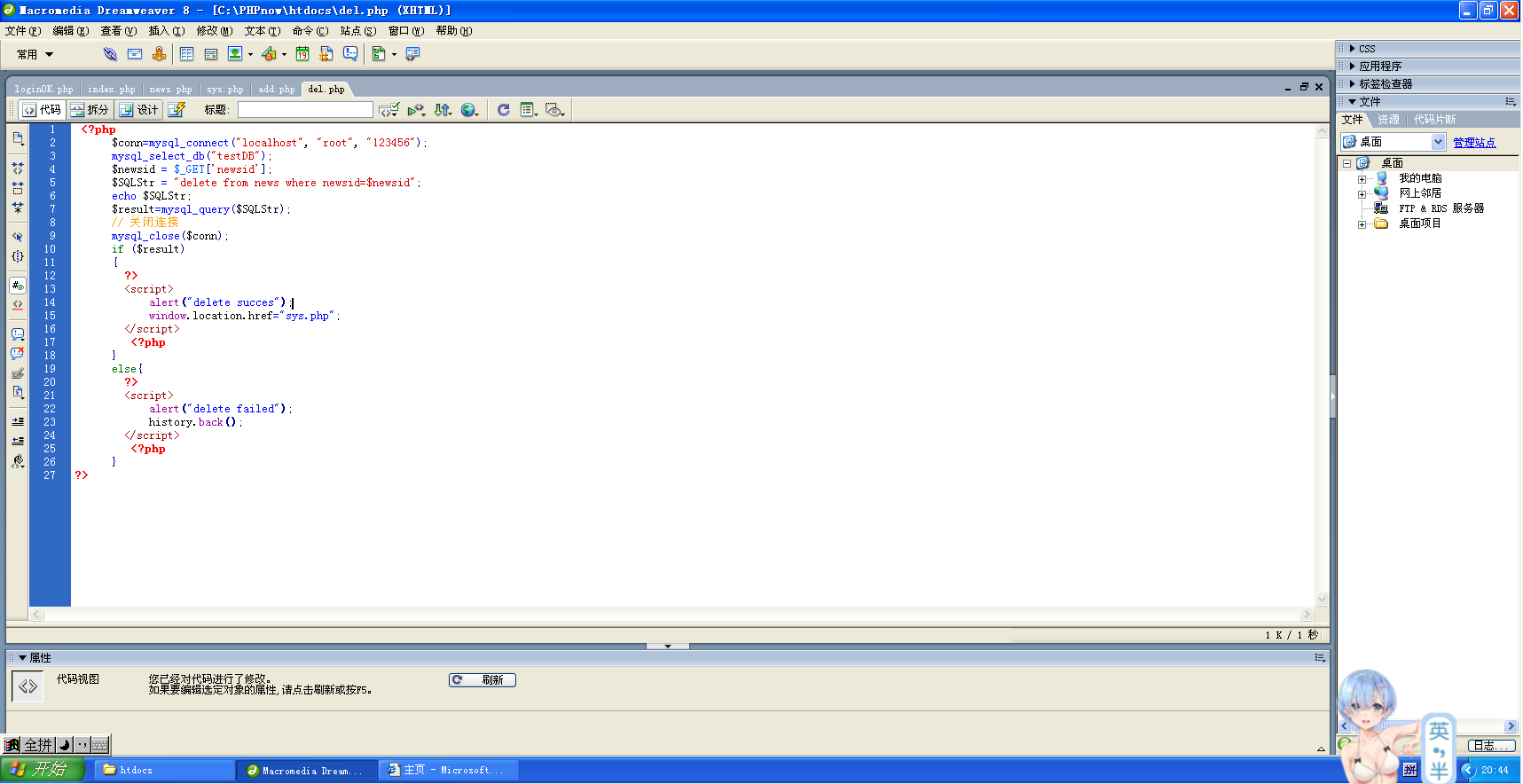
插入成功



* 1. 删除

进入 sys.php 后，点击“删除”，会跳转到 del.php，删除 news 表中的信息。

编写代码如下



测试删除

屏幕显示delete from news where newsid=3

删除操作成功（此处忘了截图）

**心得体会：**

Http定义了与服务器交互的不同方法，最基本的方法有4种，分别是GET、POST、PUT、DELETE。URL全称是资源描述符，我们可以这样认为：一个URL地址，它用于描述一个网络上的资源，而HTTP中的GET、POST、PUT、DELETE就对应着对这个资源的查、改、增、删4个操作。GET一般用于获取/查询资源信息，而POST一般用于更新资源信息，早期的系统由于不支持DELETE，因此PUT和DELETE用的较少。

具体的，POST和GET的区别如下：

* GET请求的数据会附在URL之后（就是把数据放置在HTTP协议头中），以?分割URL和传输数据，参数之间以&相连，如：login.action?name=sean&password=123。
* POST把提交的数据则放置在是HTTP包的包体中。POST的安全性要比GET的安全性高。这里的安全不仅仅是通过URL就可以作数据修改，还包含更多的安全含义，比如：通过GET提交数据，用户名和密码将明文出现在URL上，因为登录页面有可能被浏览器缓存、其他人查看浏览器的历史纪录，那么别人就可以拿到你的账号和密码了；除此之外，使用GET提交数据还可能会造成跨站请求伪造攻击(CSRF，Cross-site request forgery)。

这节课上知识丰富，不仅能学到漏洞相关的知识，还能一下子学习多门语言。熟悉了php、HTML、Mysql这几门语言，了解了网页编写的一些基础知识，让我对于动态、静态、网页交互、post和get请求有了更加深刻的了解。