《漏洞利用及渗透测试基础》实验报告

姓名：姜志凯 学号：2011937 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. 环境搭建：

本实验用到PHPnow。PHPnow是Win32下绿色免费的Apache + PHP + MySQL 环境套件包。简易安装、快速搭建支持虚拟主机的 PHP 环境。PHPnow 是绿色的，解压后执行 Setup.cmd 初始化，即可得到一个 PHP + MySQL 环境。然后就可以直接安装 Discuz!, PHPWind, DeDe, WordPress 等程序。

解压得到



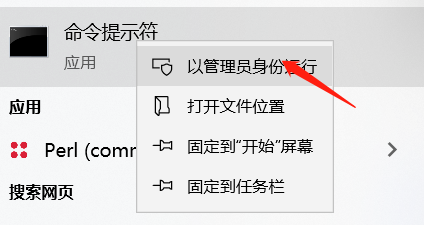
运行Setup.cmd





此时得到了一个PHP+MySQL环境。

执行Init.cmd（我用的是windows xp，所以没有安装apache服务器时管理员权限的问题，如果有则以管理员身份运行即可）



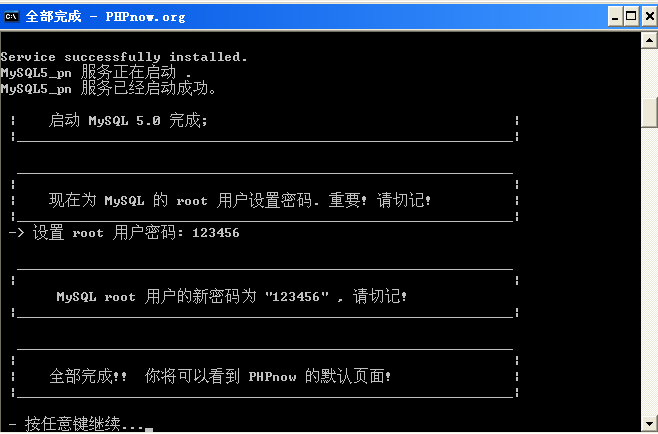
再到对应目录下执行init.cmd即可



设置MySQL账户root用户密码

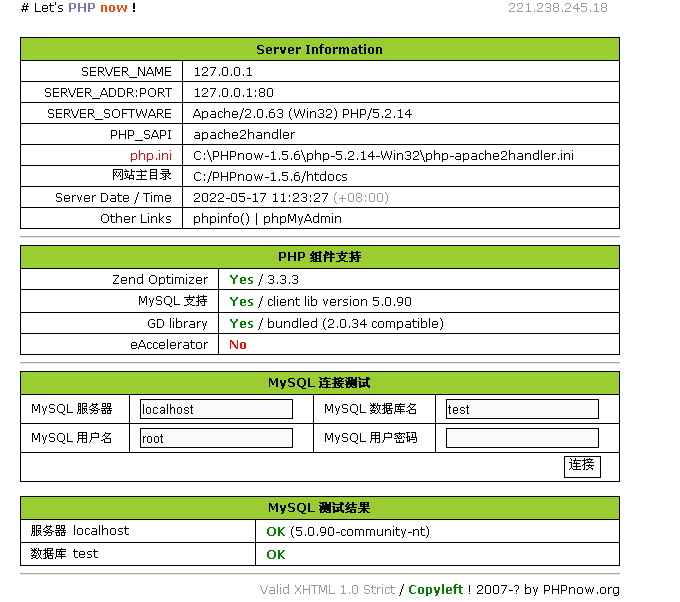


设置成功，并进入PHPnow默认界面



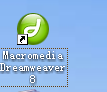


输入MySQL root用户密码测试连接



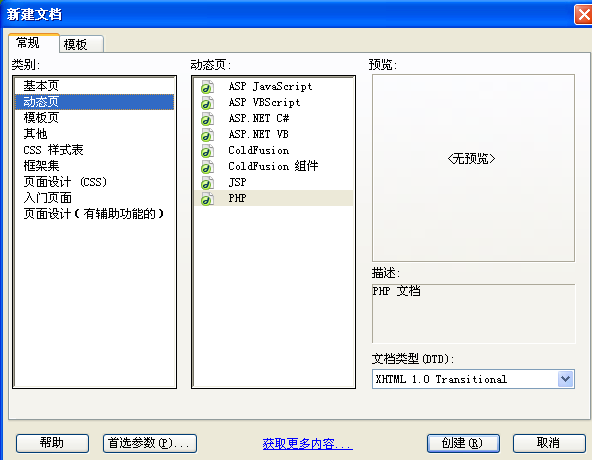
连接成功！

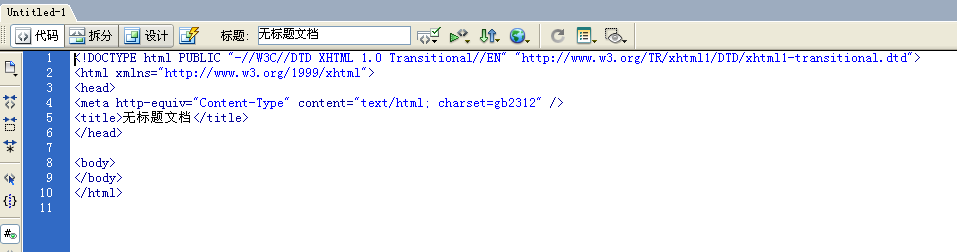
编写php代码会用到Dreamweaver，将Dreamerweaver压缩包解压，然后复制到xp系统按步骤进行安装即可。



文件->新建->动态页->php，创建，进入代码区编辑即可。



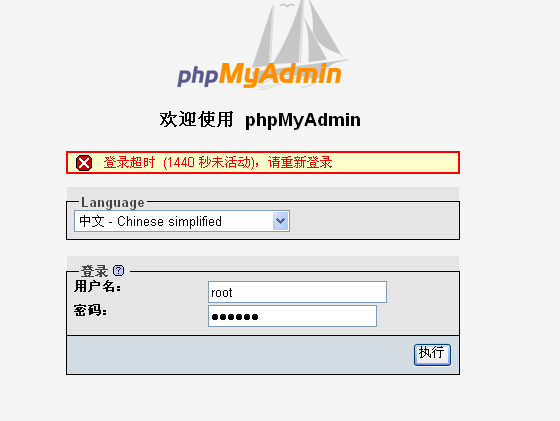




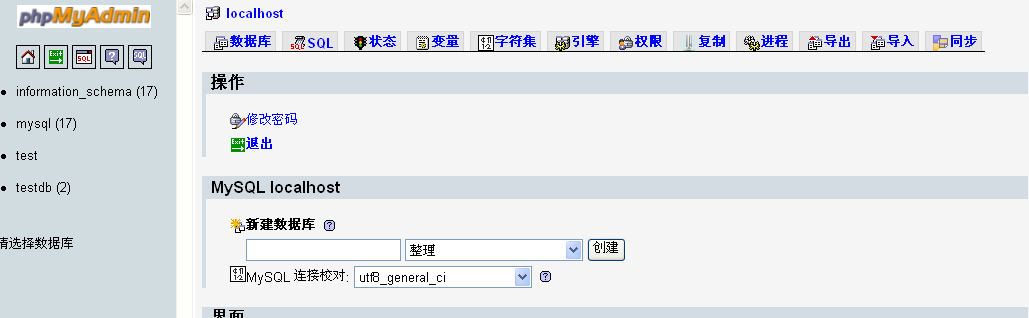
1. 利用php进行数据库的相关操作：

**先创建实验需要的数据库和表**

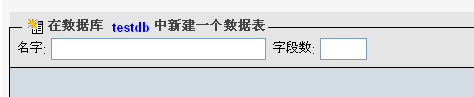
在PHPnow默认界面进入phpMyAdmin，登录

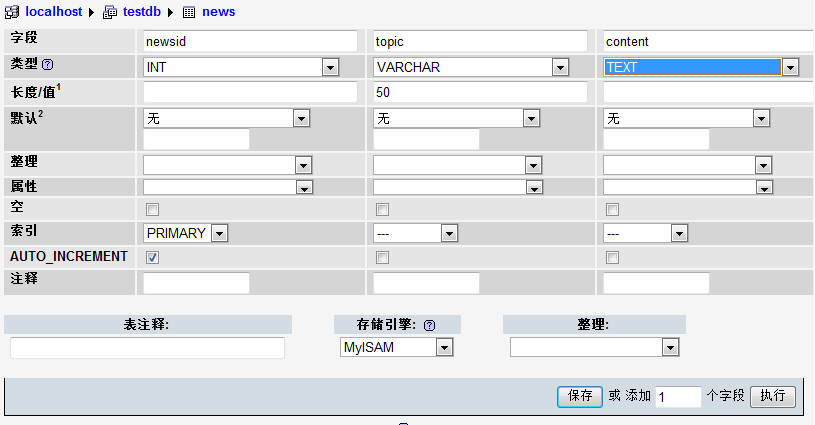


新建数据库testdb



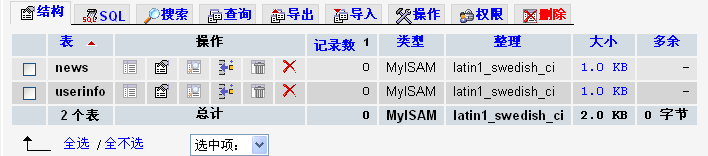
在数据库中新建两张表news和userinfo，并分别设置相应的属性字段







点击保存，不要执行，否则会加一个字段

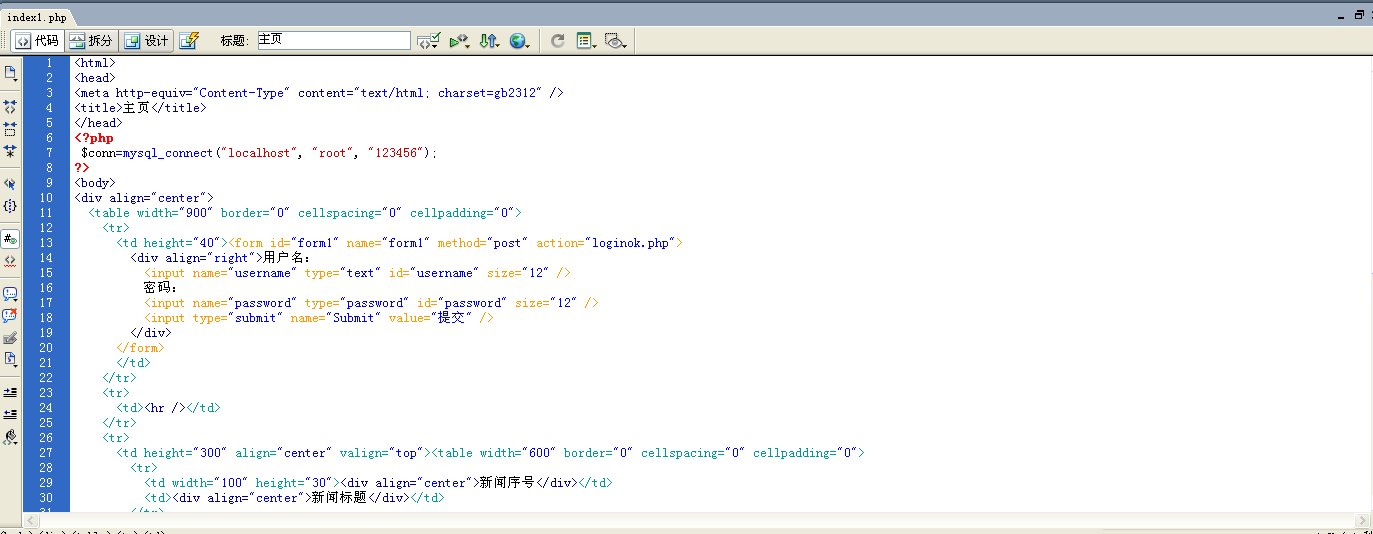


至此，实验需要用到的数据库建立完毕！

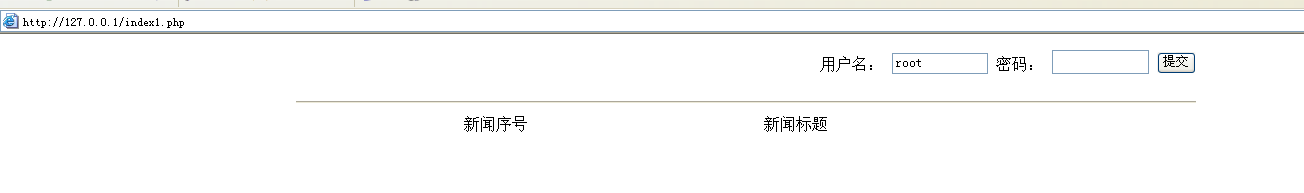
**用Dreamweaver编写php，实现数据库的相关操作**

编写好php文件后，保存至网站主目录htdocs下，在网页url后直接加上文件名就可以执行动态脚本。

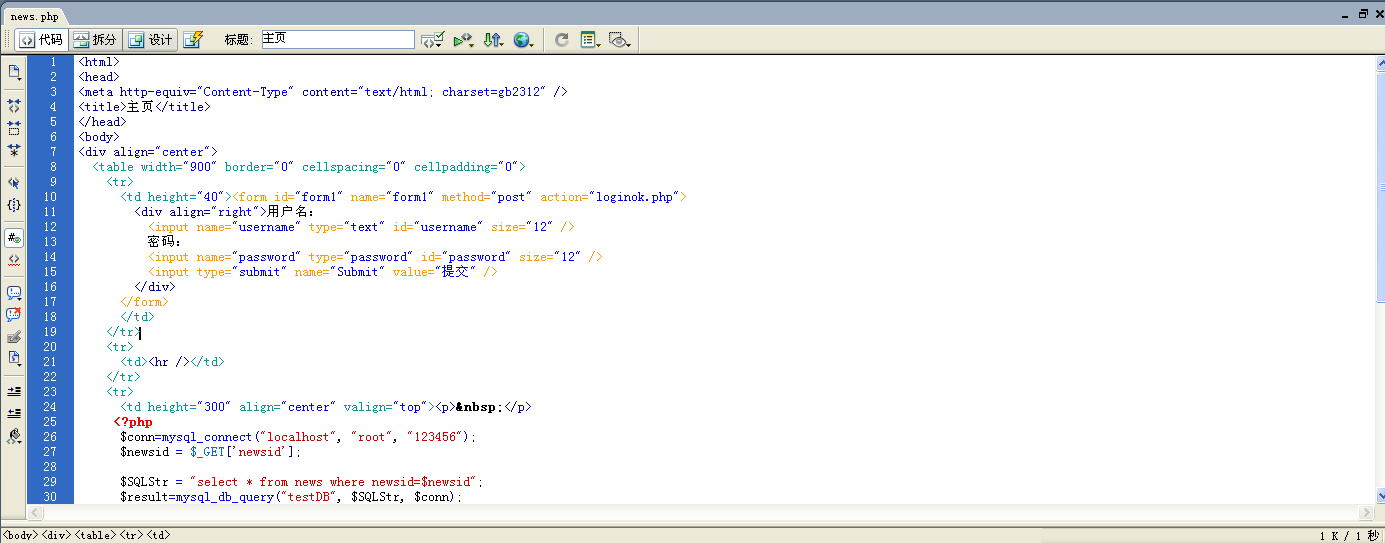
（1）编写index1.php，允许用户查看新闻和进行登录（要先登录才可以查看新闻内容）

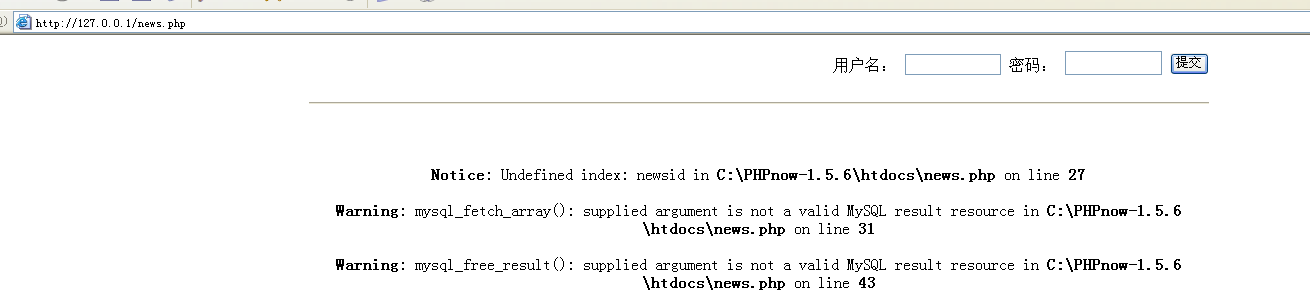


在浏览器上直接访问

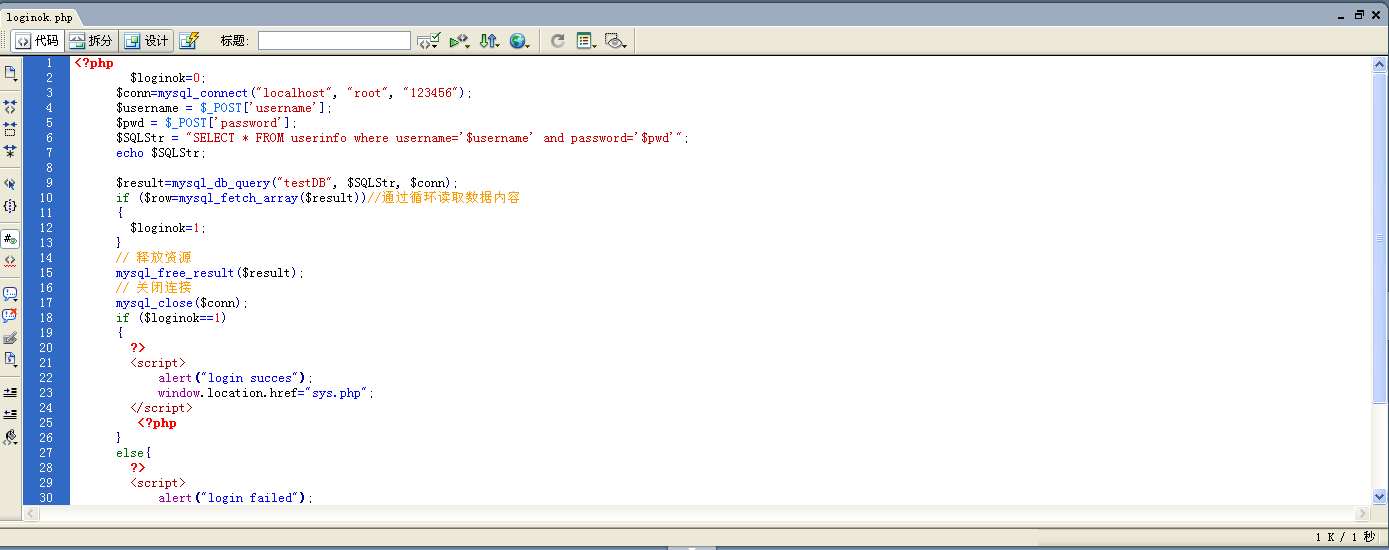


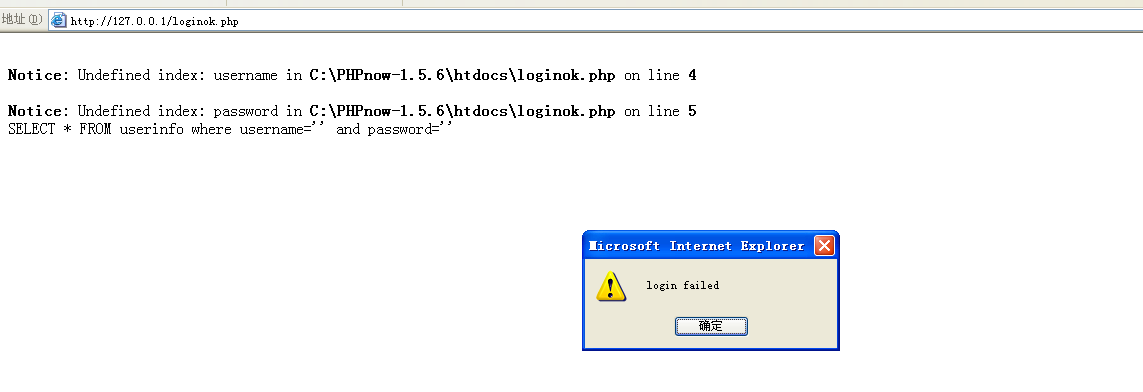
1. 编写news.php，根据传入的id查看新闻内容（得先登录，才能进行下一步操作）





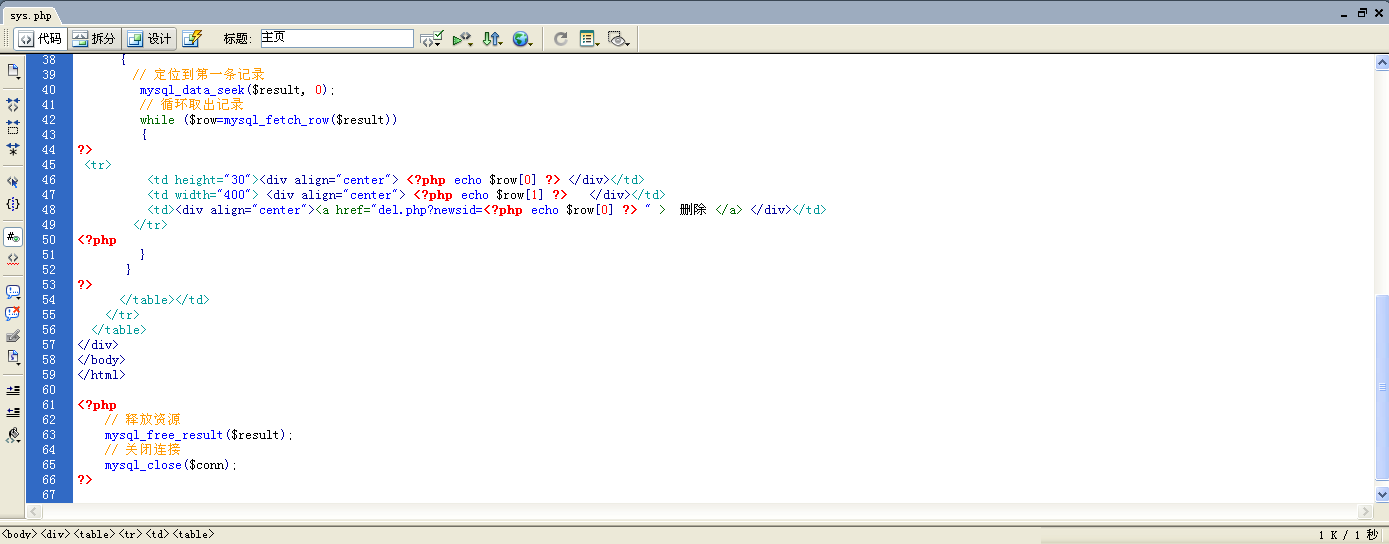
1. 编写loginok.php，判断用户登录是否成功

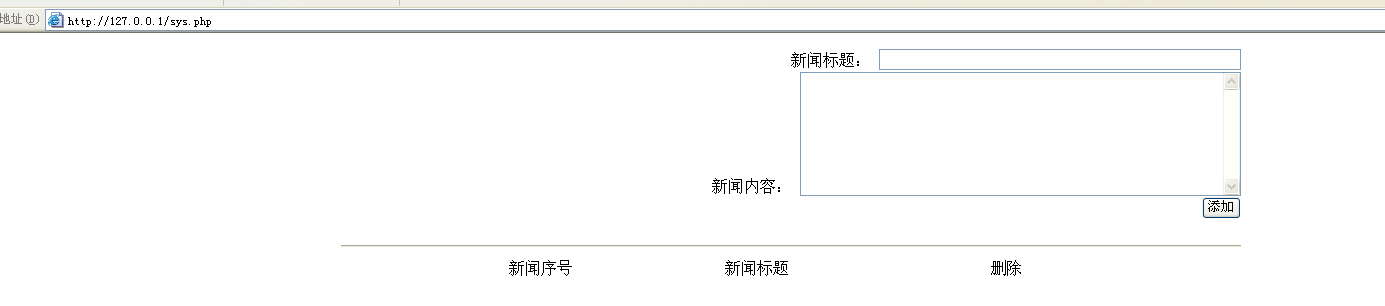




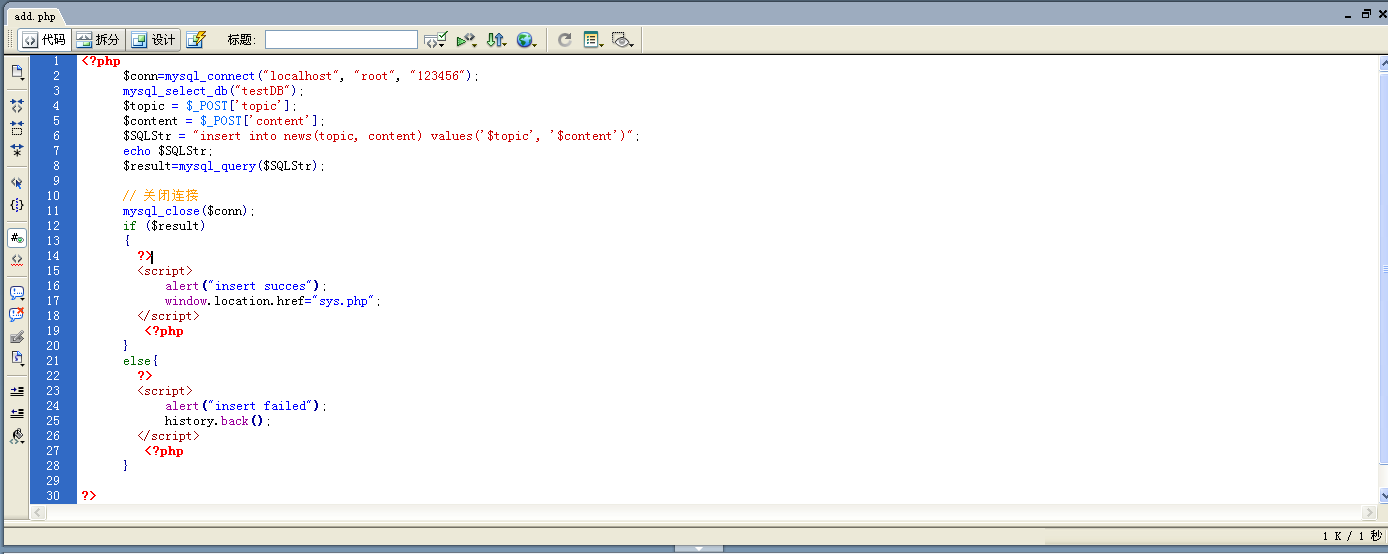
此时还未登录，没有登录成功（这是一个提示界面，不会单独运行，在别的界面登陆后会有这个提示）

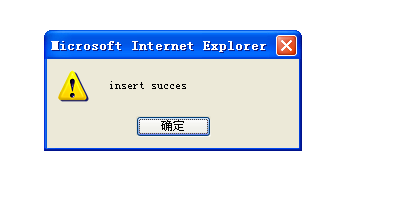
1. 编写sys.php，系统管理界面

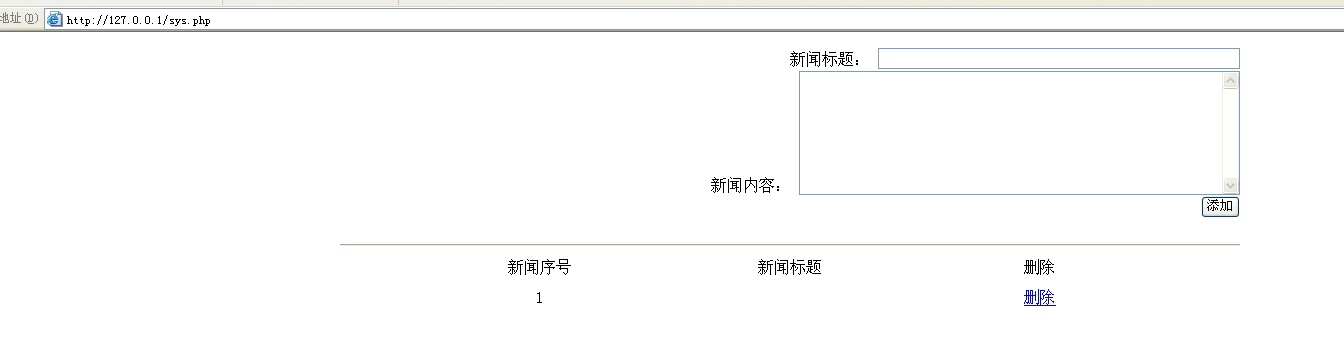




1. 编写add.php，新闻添加

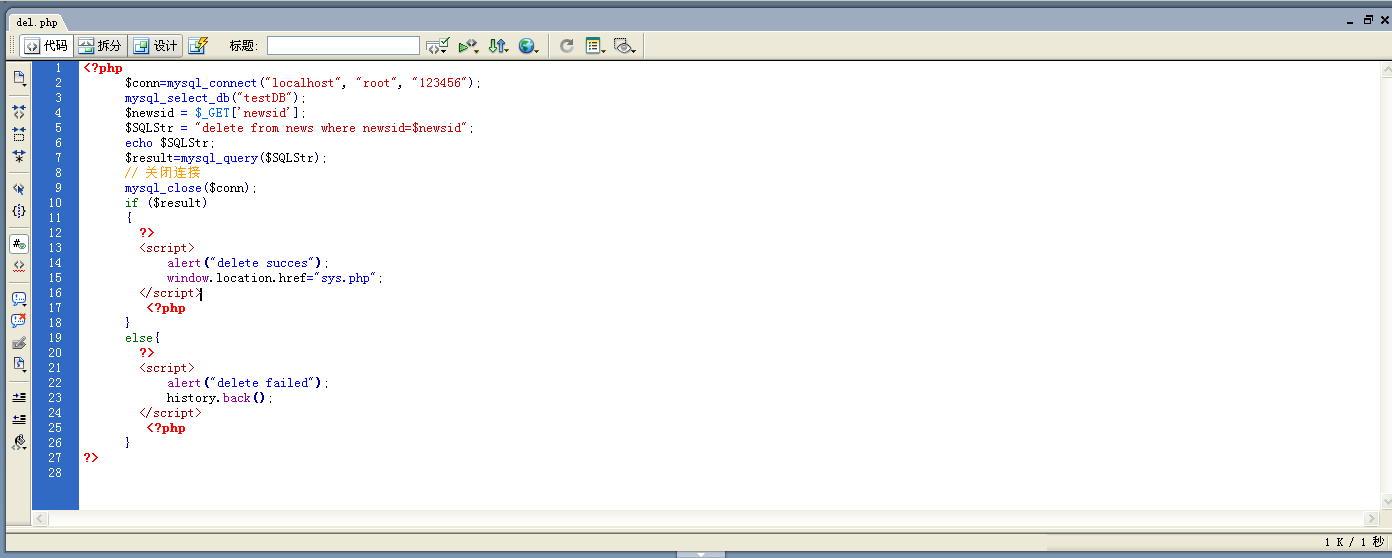


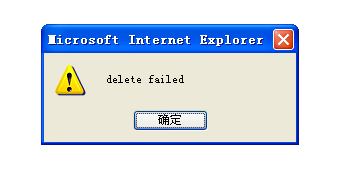




注意，通过这个脚本插入内容需要修改add.php中的代码，将newid和content修改为要添加的值即可，新闻序号自增1。

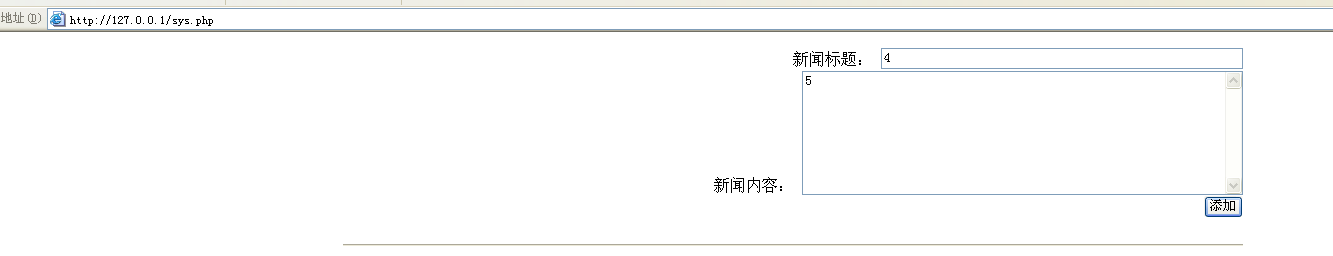
1. 编写del.php，删除新闻

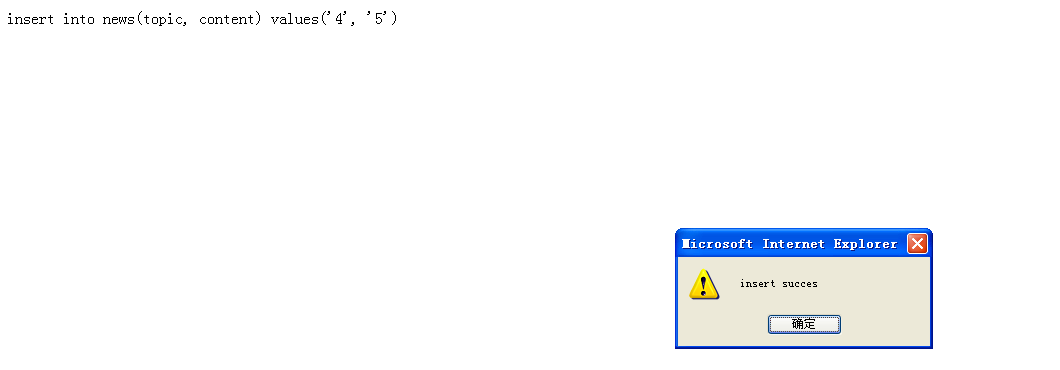


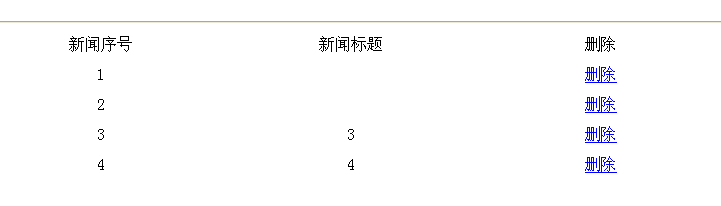


在del.php代码中修改newsid为要删除的新闻id，就能通过这个脚本删除对应ID的新闻。（示例中给newsid赋的值在数据库中不存在，所以显示删除失败）

1. 也可以通过系统管理页面直接添加新闻



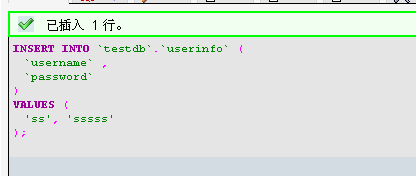




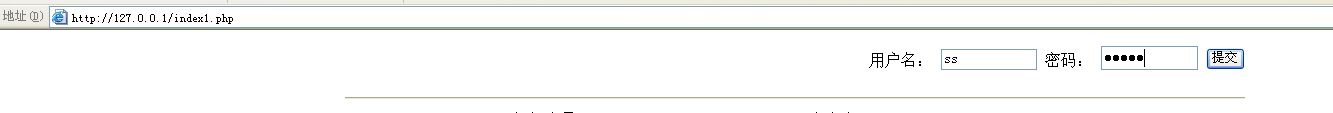
1. 为数据库创建一个用户

向userinfo中插入一个记录，即一个用户

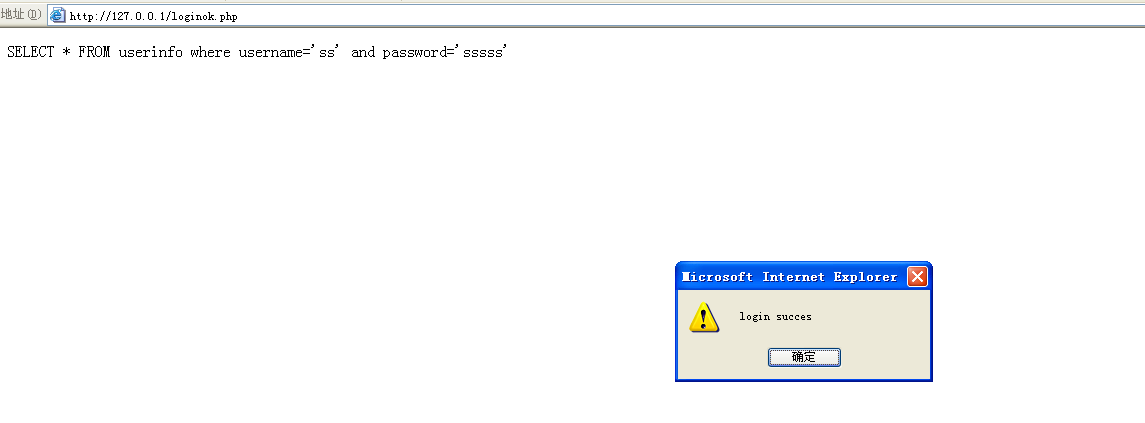




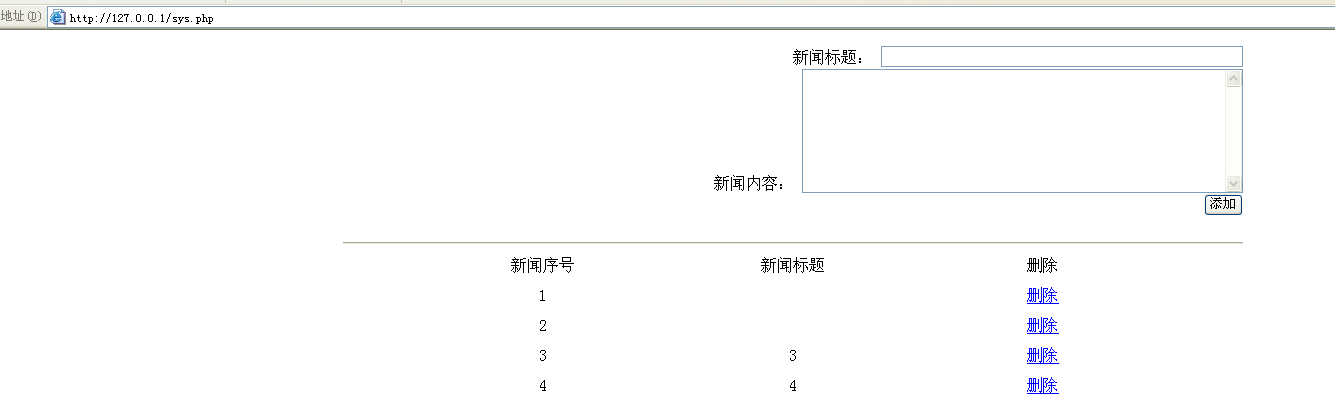
到index1.php或news.php中进行登录



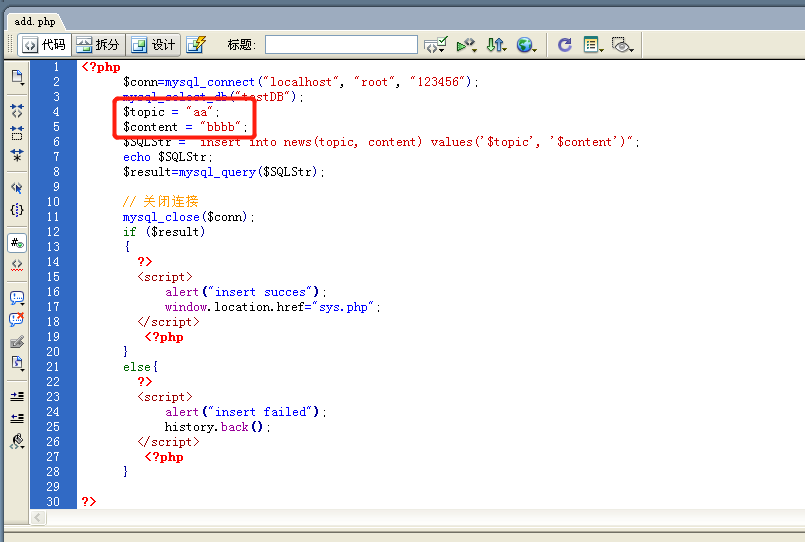
显示loginok.php的界面



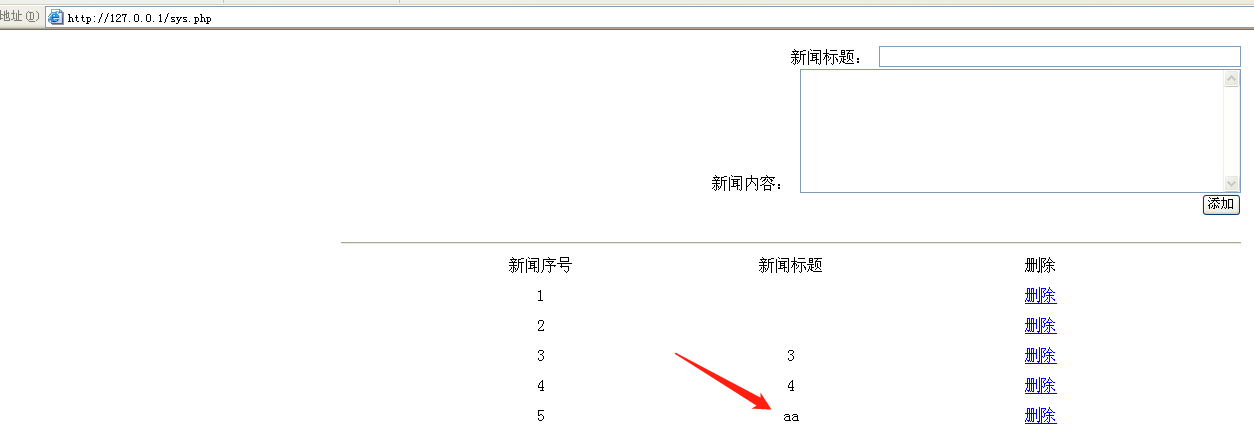
确定后会进入系统管理系统，允许用户查看新闻和添加新闻



也可以用脚本add.php对数据库进行插入，用del.php对数据库指定新闻id进行删除。







这就是本次实验的全部内容！

**心得体会：**

总结：网站都是以文件的形式存在的，可以通过向服务器请求来访问网站文件的各级内容，这个过程是通过路径来访问的。

PHPnow就是一个Apache+PHP+MySQL的环境套件包，Setup后就会在原文件夹里产生一个网页主文件htdocs，这里包含创建的网站的信息，各种子级页面。Init后，会安装Apache，是一个Web服务器，产生一个网页文件的url，通过浏览器访问这个url可以得到htdocs中的内容，包括静态或动态的脚本，即这里访问的网站的内容，就在自己的电脑里。还包含MySQL文件夹，可以使用数据库管理系统phpMyAdmin，创建数据库并进行相关操作。

所以用Dreamweaver编写php文件，保存到htdocs文件夹中，在通过浏览器访问url后加上文件名的网址，就可以执行这个php文件了，可以使静态也可以是动态脚本。

注意：

本机如果装有MySQL，会出现MySQL端口被占用的情况，所以可以使用虚拟机实验；

Win7以上系统在安装Apache时会出现没有管理员权限的问题，解决方法是找到cmd.exe，右键以管理员身份运行，然后找到Init.cmd执行即可；

通过动态脚本的执行可以更改网站的内容，还可以通过cookie直接跳过登录界面，如果我知道登陆后的界面对应的php文件名，在没有防护措施的情况下，应该可以跳过登录直接访问。

此外，通过本实验，掌握了多个汇编语言的用法