《漏洞利用及渗透测试基础》实验报告

姓名：申宗尚 学号：2213924 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. 首先，进行phpnow的下载和安装

文本

描述已自动生成

这里遇到了一个问题：3306端口已被占用，因此在计算机管理页面中找到Mysql服务并关闭，从而空出3306端口进行phpnow的运行

图形用户界面, 文本

描述已自动生成

关闭后，可以正常安装、初始化。

文本

描述已自动生成

1. 然后，我们登录127.0.0.1可以查看当前的页面窗口如下：

图形用户界面

中度可信度描述已自动生成

先进行测试链接，输入MySQL的用户密码：

图片包含 应用程序

描述已自动生成

测试结果OK，说明数据库也已经正常连接。

3.然后，点击phpMyAdmin进入管理员界面：

图形用户界面, 应用程序

描述已自动生成

创建新数据库testdb作为我们网页的数据库，并且在其中加入两张表News(newsid, topic, content), userinfo(username, password)

图形用户界面

描述已自动生成

创建News表

图形用户界面

中度可信度描述已自动生成

创建News成功

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

创建userinfo成功

4. 然后，我们在php\htdocs目录下创建新文件夹web，代表我们需要制作的网页，并在其中加入我们写好并修改的php文件：

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

Add.php 实现新闻库的增

图形用户界面, 文本, 应用程序

描述已自动生成

Del.php 实现新闻库的删

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

Index.php 实现用户界面的登录

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

News.php 实现登录后界面的新闻列表显示

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

Loginok.php 实现登录判断

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

Sys.php 实现整个页面的功能

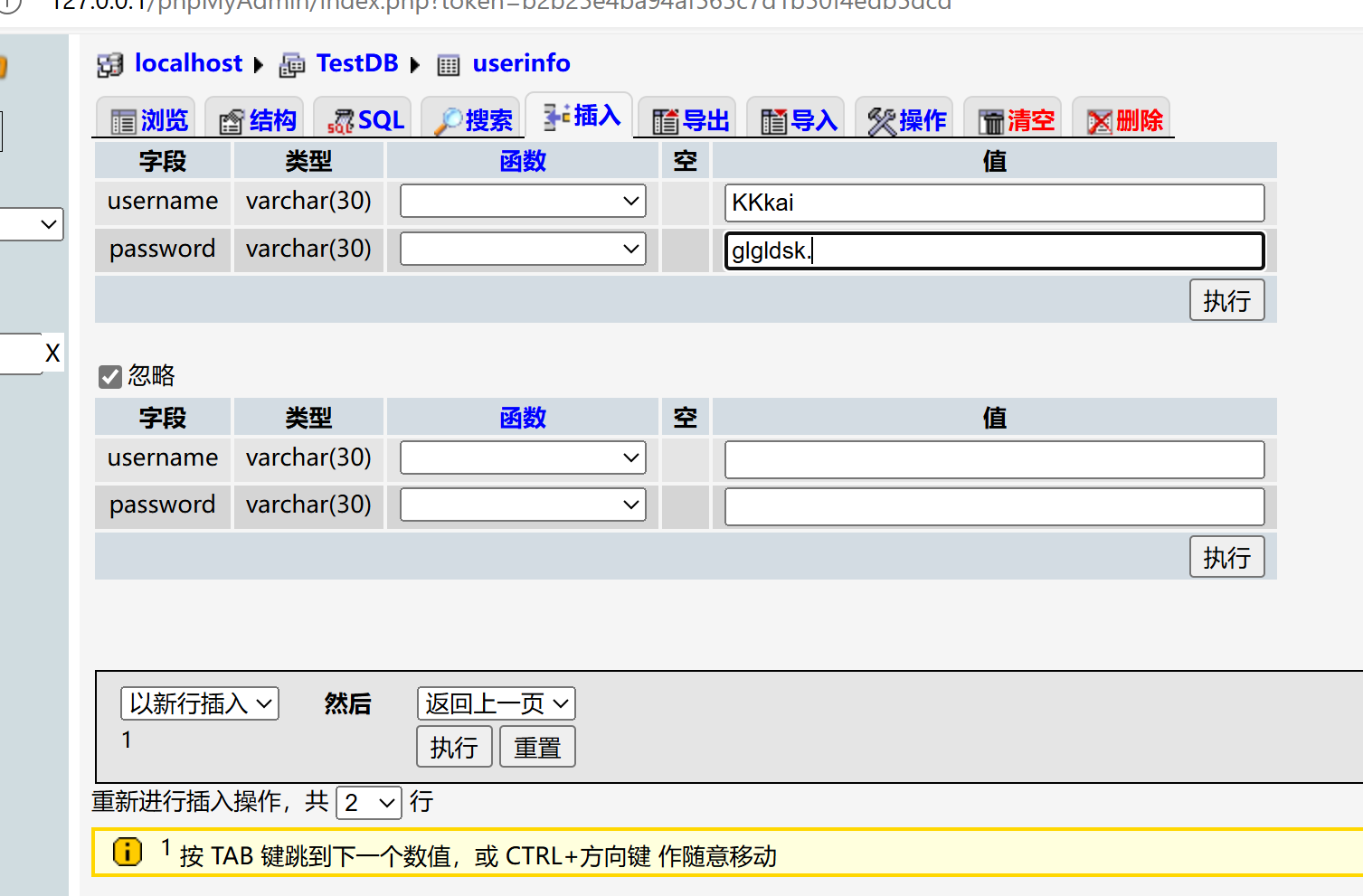
5. 创建完web目录下的php文件后，我们登录127.0.0.1/web

可以看到以下界面：

图形用户界面, 应用程序

描述已自动生成

为了成功登录，我们还是先返回phpadmin界面，向userinfo表中插入一条用户信息，我们使用这条信息的账号密码进行登录：



图形用户界面, 文本, 应用程序

描述已自动生成

成功登录

图形用户界面, 应用程序

描述已自动生成

然后可以看到主页面，如图，有新闻标题，新闻内容和添加键，下面有一列信息树Treeview，分别显示新闻序号、新闻标题和删除功能，实现查询。

首先，我们尝试添加操作：

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

添加这条新闻

形状, 矩形

中度可信度描述已自动生成

显示添加成功

图形用户界面, 文本, 应用程序

描述已自动生成

可以在下面的页面看到刚插入的新闻，插入成功

然后，我们尝试删除操作，选择上面新闻右边的删除

形状, 矩形

描述已自动生成

提示删除成功图形用户界面, 文本, 应用程序

描述已自动生成

下面的信息树少了我们刚插入的新闻

从而，实现了增、查询、删操作，实验成功。

**心得体会：**

在本次实验中，我实践、并从零搭建了数据库系统和网页前端显示，利用 PhpNow工具来搭建，学习了处理动态网页的脚本语言PHP并接触了前端语言JavaScript。在前端与后端数据库管理系统交互的过程中我遇到了一些连接失败和非正常查询和操作的问题，但都在探究下最终解决，而且我还注意到我们的输入获取字符串并没有对内容进行处理、限制，这也就为攻击者提供了可乘之机。另一方面，我发现我们URL直接会显示用户的敏感信息，在登录过程中，如果用户的用户名和密码以明文形式传输，那么黑客可以轻松地获取到这些信息，从而冒充用户登录系统。另外，如果用户没有对输入的数据进行过滤和验证，恶意用户还可以利用 URL 参数执行 SQL 注入攻击，通过篡改 URL 参数中的数据，向数据库中插入恶意代码或者获取敏感数据，从而对系统造成严重威胁。