

《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

```
管理员: 初始化 PHPnow 1.5.6-1 - Apache 2.0 + PHP + MySQL 5.0

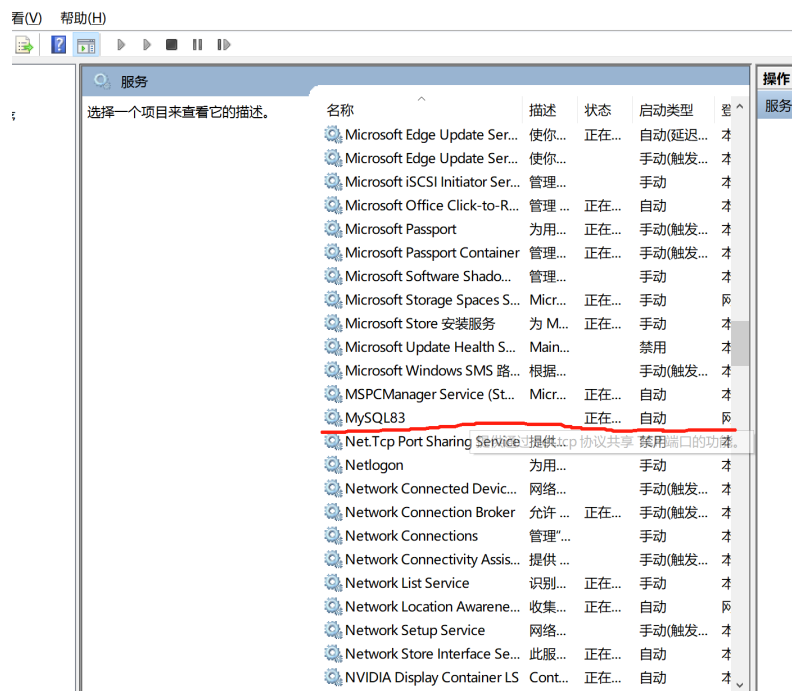
D:\Tools\PHPnow>init

##### PHPnow.org - 绿色免费的 PHP 环境套件 #####

端口 3306 已被 "MySQL" (mysqld.exe PID 6272) 使用!

1 - MySQL 使用其他端口(不推荐)
2 - 重试 (端口已被释放 或 程序已退出)
```

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



关闭后，可以正常安装、初始化。

```
管理员: 全部完成 - PHPnow.org

正在启动 MySQL 5.0 ...

Service successfully installed.
MySQL5_pn 服务正在启动 .
MySQL5_pn 服务已经启动成功。

启动 MySQL 5.0 完成:

现在为 MySQL 的 root 用户设置密码. 重要! 请切记!
-> 设置 root 用户密码: glgldsk.

MySQL root 用户的新密码为 "glgldsk.", 请切记!

全部完成!! 你将可以看到 PHPnow 的默认页面!

- 按任意键继续...
```

2. 然后，我们登录 127.0.0.1 可以查看当前的页面窗口如下：

127.0.0.1

Let's PHP now !

为何只能本地访问?

此服务器互联网 IP

180.213.85.253

Server Information	
SERVER_NAME	127.0.0.1
SERVER_ADDR:PORT	127.0.0.1:80
SERVER_SOFTWARE	Apache/2.0.63 (Win32) PHP/5.2.14
PHP_SAPI	apache2handler
php.ini	D:\Tools\PHPnow-1.5.6\php-5.2.14-Win32\php-apache2handler.ini
网站主目录	D:\Tools\PHPnow-1.5.6\htdocs
Server Date / Time	2024-06-07 18:20:43 (+08:00)
Other Links	phpinfo() phpMyAdmin

PHP 组件支持	
Zend Optimizer	Yes / 3.3.3
MySQL 支持	Yes / client lib version 5.0.90
GD library	Yes / bundled (2.0.34 compatible)
eAccelerator	No

MySQL 连接测试			
MySQL 服务器	<input type="text" value="localhost"/>	MySQL 数据库名	<input type="text" value="test"/>
MySQL 用户名	<input type="text" value="root"/>	MySQL 用户密码	<input type="password"/>
<input type="button" value="连接"/>			

Valid XHTML 1.0 Strict / Copyleft ! 2007-? by PHPnow.org

先进行测试链接，输入 MySQL 的用户密码：

127.0.0.1

Let's PHP now !

为何只能本地访问?
此服务器互联网 IP
180.213.85.253

Server Information	
SERVER_NAME	127.0.0.1
SERVER_ADDR:PORT	127.0.0.1:80
SERVER_SOFTWARE	Apache/2.0.63 (Win32) PHP/5.2.14
PHP_SAPI	apache2handler
php.ini	D:\Tools\PHPnow-1.5.6\php-5.2.14-Win32\php-apache2handler.ini
网站主目录	D:/Tools/PHPnow-1.5.6/htdocs
Server Date / Time	2024-06-07 18:23:01 (+08:00)
Other Links	phpinfo() phpMyAdmin

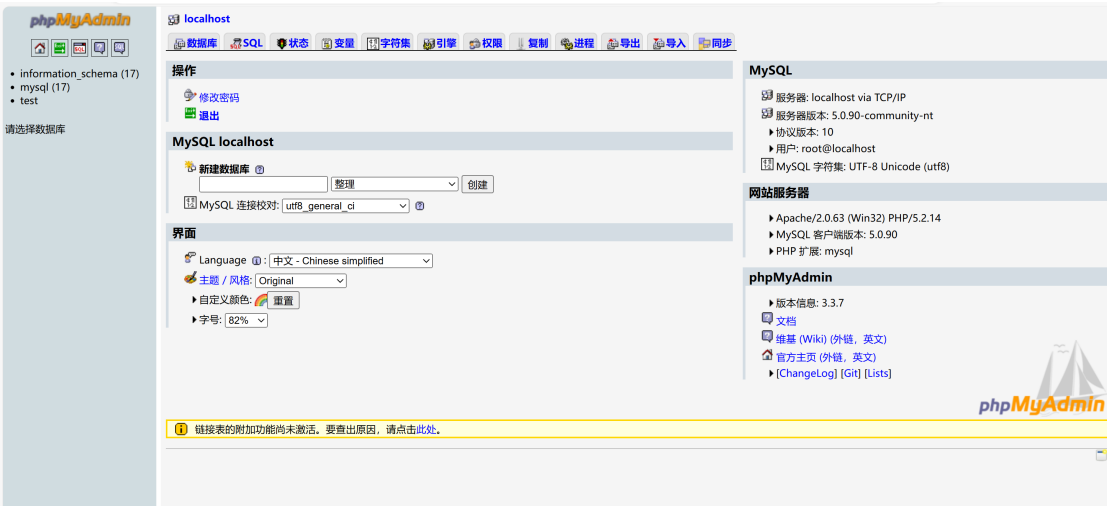
PHP 组件支持	
Zend Optimizer	Yes / 3.3.3
MySQL 支持	Yes / client lib version 5.0.90
GD library	Yes / bundled (2.0.34 compatible)
eAccelerator	No

MySQL 连接测试			
MySQL 服务器	localhost	MySQL 数据库名	test
MySQL 用户名	root	MySQL 用户密码	
<div>连接</div>			

MySQL 测试结果	
服务器 localhost	OK (5.0.90-community-nt)
数据库 test	OK

Valid XHTML 1.0 Strict / Copyleft ! 2007-? by PHPnow.org

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：



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)

localhostTestDBNews

字段	newsid	topic	content
类型	INT	VARCHAR	TEXT
长度/值 ¹	50		
默认 ²	无	无	无
整理			
属性			
空	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
索引	---	---	---
AUTO_INCREMENT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
注释			

表注释:

存储引擎: MyISAM

整理:

保存或添加1个字段执行

¹ 如字段类型是 "enum" 或 "set", 请使用以下的格式输入: 'a','b','c'...

² 对于默认值, 请只输入单个值. 不要加反斜杠或引号, 请用此格式: a

创建 News 表

localhostTestDBNews

浏览结构SQL搜索插入导出导入操作清空删除

创建数据表 'TestDB`.`News` 成功.

```
CREATE TABLE `TestDB`.`News` (
  `newsid` INT NOT NULL,
  `topic` VARCHAR( 50 ) NOT NULL,
  `content` TEXT NOT NULL,
) ENGINE = MYISAM ;
```

	字段	类型	整理	属性	空	默认	额外	操作
<input type="checkbox"/>	newsid	int(11)			否	无		
<input type="checkbox"/>	topic	varchar(50)	latin1_swedish_ci		否	无		
<input type="checkbox"/>	content	text	latin1_swedish_ci		否	无		

全选 / 全不选 选中项:

打印预览 规划表结构

添加1个字段于表结尾于表开头于之后newsid执行

没有已定义的索引!

创建 News 成功

localhostTestDBuserinfo

浏览结构SQL搜索插入导出导入操作清空删除

创建数据表 'TestDB`.`userinfo` 成功.

```
CREATE TABLE `TestDB`.`userinfo` (
  `username` VARCHAR( 30 ) NOT NULL,
  `password` VARCHAR( 30 ) NOT NULL,
) ENGINE = MYISAM ;
```

	字段	类型	整理	属性	空	默认	额外	操作
<input type="checkbox"/>	username	varchar(30)	latin1_swedish_ci		否	无		
<input type="checkbox"/>	password	varchar(30)	latin1_swedish_ci		否	无		

全选 / 全不选 选中项:

打印预览 规划表结构

添加1个字段于表结尾于表开头于之后username执行

没有已定义的索引!

在第1个字段创建索引执行

已用空间

类型	已用
数据	0 字节
索引	1,024 字节
总计	1,024 字节

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：



```
add.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

<?php
$conn = mysql_connect("localhost", "root", "glgldsk.");
mysql_select_db("testdb", $conn); // 第二个参数应该是数据库连接句柄

$topic = $_POST['topic'];
$content = $_POST['content'];

$SQLStr = "INSERT INTO news(topic, content) VALUES ('$topic', '$content')";
echo $SQLStr . "<br>";

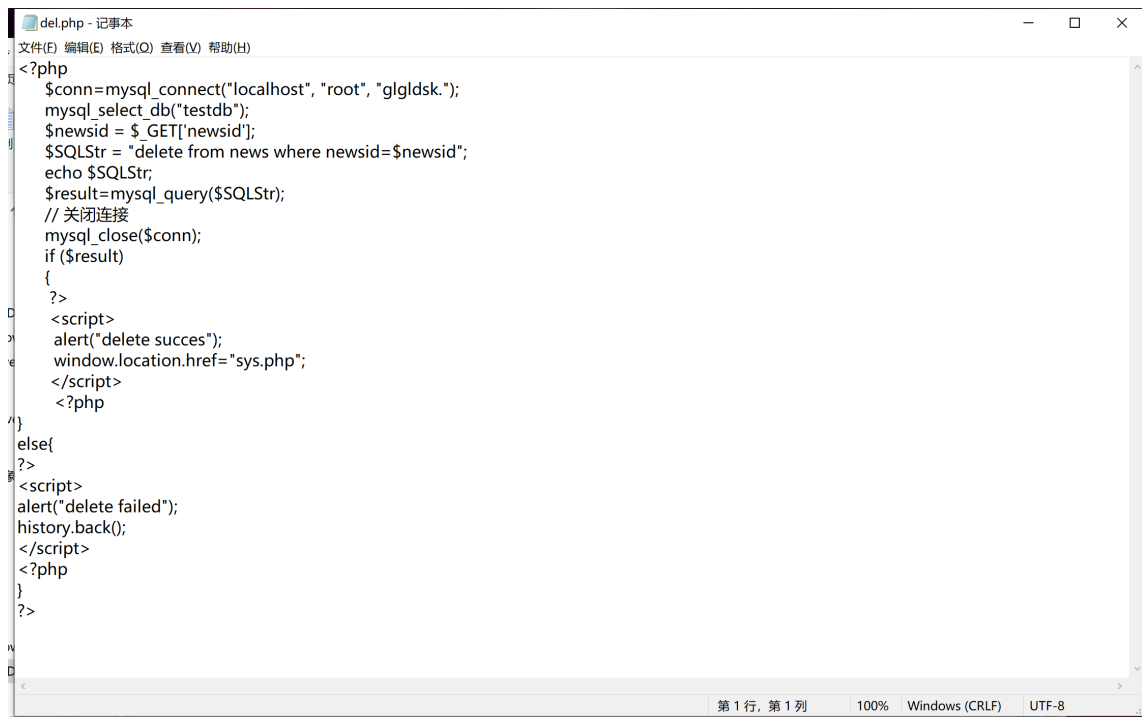
$result = mysql_query($SQLStr);

if (!$result) {
    die('Invalid query: ' . mysql_error());
}

// 关闭连接
mysql_close($conn);

if ($result) {
    ?>
    <script>
        alert("insert success");
        window.location.href = "sys.php";
    </script>
    <?php
    } else {
    ?>
    <script>
        alert("insert failed");
    </script>
    <?php
    }
    ?>
```

Add. php 实现新闻库的增



```
del.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

<?php
$conn=mysql_connect("localhost", "root", "glgldsk.");
mysql_select_db("testdb");
$newsid = $_GET['newsid'];
$SQLStr = "delete from news where newsid=$newsid";
echo $SQLStr;
$result=mysql_query($SQLStr);
// 关闭连接
mysql_close($conn);
if ($result)
{
    ?>
    <script>
        alert("delete succes");
        window.location.href="sys.php";
    </script>
    <?php
}
else{
    ?>
    <script>
        alert("delete failed");
        history.back();
    </script>
    <?php
}
    ?>
```

Del. php 实现新闻库的删


```
sys.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
  <title>主页</title>
</head>
<?php
$conn = mysql_connect("localhost", "root", "glgldsk.");
?>
<body>
  <div align="center">
    <table width="900" border="0" cellspacing="0" cellpadding="0">
      <tr>
        <td height="40">
          <form id="form1" name="form1" method="post" action="add.php">
            <div align="right">
              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" />
            </div>
          </form>
        </td>
      </tr>
      <tr>
        <td><hr /></td>
      </tr>
      <tr>
        <td height="300" align="center" valign="top">
```

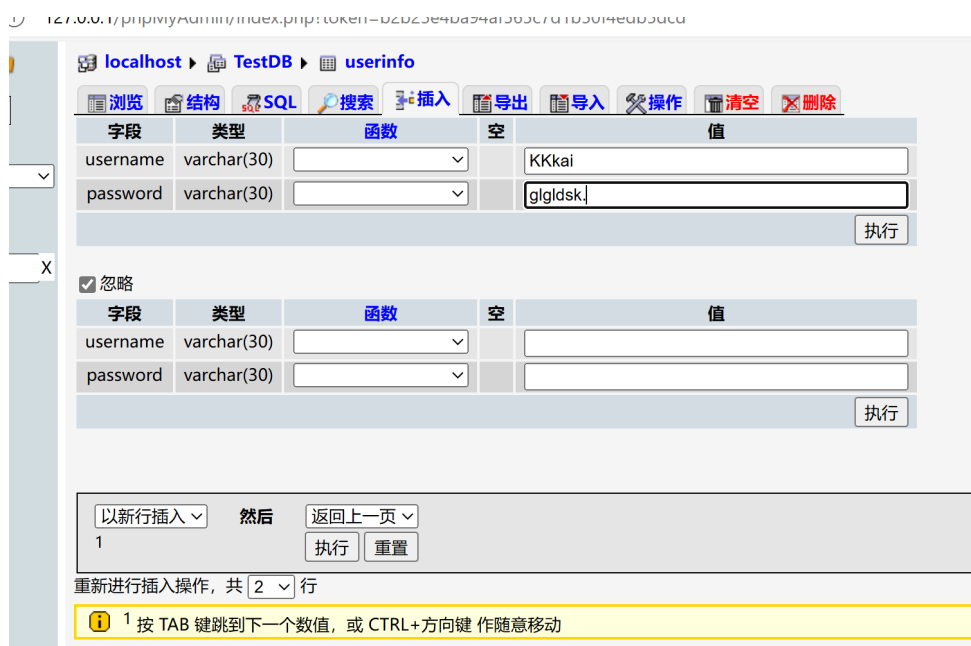
Sys.php 实现整个页面的功能

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：



新闻序号	新闻标题
------	------

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：



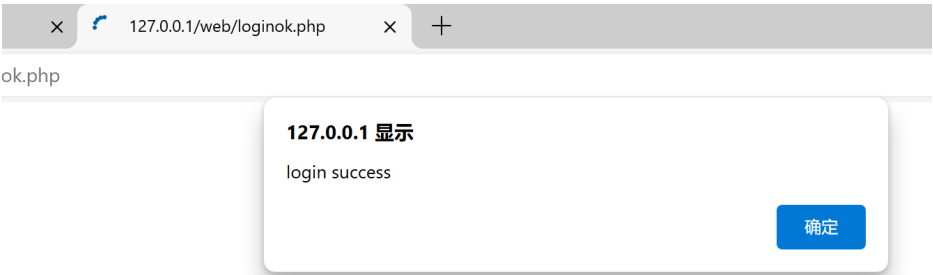
字段	类型	函数	空	值
username	varchar(30)			KKkai
password	varchar(30)			glgldsk.

以新行插入 然后 返回上一页

1 执行 重置

重新进行插入操作，共 2 行

1 按 TAB 键跳到下一个数值，或 CTRL+方向键 作随意移动



成功登录

A screenshot of a web browser window. The address bar shows '127.0.0.1/web/sys.php'. The page has a title '成功登录'. Below the title, there is a form with two input fields: '新闻标题:' and '新闻内容:'. The '新闻内容:' field is a larger text area. To the right of the '新闻内容:' field is a small button labeled '添加'. Below the form, there is a table with three columns: '新闻序号', '新闻标题', and '删除'.

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：

A screenshot of a web browser window. The address bar shows '127.0.0.1/web/sys.php'. The page has a title '成功登录'. Below the title, there is a form with two input fields: '新闻标题:' and '新闻内容:'. The '新闻标题:' field contains the text 'this is a title'. The '新闻内容:' field contains the text 'this is the content'. To the right of the '新闻内容:' field is a small button labeled '添加'. Below the form, there is a table with three columns: '新闻序号', '新闻标题', and '删除'.

添加这条新闻

A screenshot of a web browser window. The address bar shows '127.0.0.1/web/sys.php'. Below the browser window, there is a white modal box with a blue border. Inside the modal, the text '127.0.0.1 显示' is in bold, followed by 'insert success'. At the bottom right of the modal is a blue button with the text '确定'.

显示添加成功

新闻标题:

新闻内容:

添加

新闻序号	新闻标题	删除
0	this is a title	删除

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

127.0.0.1 显示

delete succes

确定

提示删除成功

b/sys.php

新闻标题:

新闻内容:

添加

新闻序号	新闻标题	删除
------	------	----

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。