**Web安全项目报告**

题目： 图书馆管理系统

姓名： 刘 帅 201601060115

班级：信息安全16级1班

目录

[第一章 引言 3](#_Toc529461631)

[第二章 详细设计 4](#_Toc529461632)

[系统安全性 4](#_Toc529461633)

[**服务器** 4](#_Toc529461634)

[**数据库** 5](#_Toc529461635)

[角色权限 5](#_Toc529461636)

[**管理员用户** 5](#_Toc529461637)

[**普通用户** 5](#_Toc529461638)

[Web安全性 6](#_Toc529461639)

[密码 6](#_Toc529461640)

[退出 6](#_Toc529461641)

[输入验证 6](#_Toc529461642)

[会话管理 7](#_Toc529461643)

[功能 8](#_Toc529461644)

[管理并查看图书信息 8](#_Toc529461645)

[管理并查看读者信息 10](#_Toc529461646)

[借还图书 14](#_Toc529461647)

[修改密码 14](#_Toc529461648)

[重置密码 15](#_Toc529461649)

[借书卡挂失 15](#_Toc529461650)

[第三章 测试和演示 16](#_Toc529461651)

[第四章 总结 24](#_Toc529461652)

# 第一章 引言

在高校中，图书借阅是学生获取知识的一个很重要的途径，如何既能方便学生借书，又能减轻图书馆管理人员的工作负担、高效地完成图书借阅管理工作，是一件非常重要的事。

该项目主要目的是设计一套合理实用的图书馆管理系统，以对校内的图书信息、图书借阅信息进行统一集中的管理，对学生的个人信息、网上图书馆的登录账号、借阅卡的挂失情况进行统一细致的管理。同时该项目还具备一定的安全性，能够应对如sql注入、xss攻击等攻击方式，并将攻击方式写入日志。

该图书馆管理系统，能够实现在服务器端的图书借阅管理，能够提供方便快速的图书信息检索功能和便捷的图书借阅和归还功能，并且能够对图书信息和读者信息进行管理，方便管理员和读者的借阅处理。要求系统具备安全稳定、易于操作、人机交互界面方便美观等特点。

主要架构是通过Bootstrap搭建起整洁美观的前端操作界面，用php7.0来进行前端与后端数据库的信息交互、存储，利用开源的MySQL数据库对数据进行存储、查询、修改及删除。最后将Web应用搭建在Apache服务器上，实现对网络图书馆管理系统的访问和一系列操作。

# 第二章 详细设计

## 系统安全性

### **服务器**

服务器使用phpstudy中的Apache服务器，将服务器环境部署到本地。进行一系列的系统配置，提升服务器的安全性。

1. 隐藏版本信息。在Apache的ini配置文件中隐藏其版本信息，如：

ServerSignature Off

ServerTokens Prod

2.设置用户和组

User apache

Group apachegroup

window系统中创建apache用户，给予apache用户读取和执行所有文档和脚本目录的权限。对Apache的logs目录具有读/写/删除的权限。对httpd.exe二进制文件具有读取和执行的权限。在service.msc服务中选择Aapche属性，登录账号改为apache即可。

3. apache目录禁止访问

Indexes 的作用就是当该目录下没有 index.html文件时，就显示目录结构。 默认apache在当前目录下没有index.html入口就会显示目录。让目录暴露在外面是非常危险的事，如下操作禁止apache显示目录：Options FollowSymLinks

将Options Indexes FollowSymLinks中的Indexes 去掉，就可以禁止 Apache 显示该目录结构。

4.阻止用户修改系统设置

在Apache 服务器的配置文件中进行以下的设置，阻止用户建立、修改 .htaccess文件，防止用户超越能定义的系统安全特性。

### **数据库**

设置新的用户user，赋予user查询、插入、更新的权限

insert into user

(host, user, password,

select\_priv, insert\_priv, update\_priv)

values('localhost', 'guest',

password('guest123'), 'y', 'y', 'y');

在该用户操作下，创建数据库。从而确保数据库的安全性。

其次是保证数据库和操作系统为最新版本。防止黑客利用版本漏洞攻击数据库

## 角色权限

将登陆账户分为管理员用户和普通用户两种角色，具有不同的操作权限。

### **管理员用户**

1．管理员用户具有增加图书、修改图书信息、删除图书和查询全部图书操作的权限。

2．管理员用户具有增加读者、修改读者信息、删除读者和查询全部读者信息的权限。

3．管理员用户可对图书的借阅信息进行修改，查询图书归还状态，设置图书归还状态。

4．管理员用户可以修改管理员个人账户的密码，也可以重置普通用户的密码，重置普通用户的密码为’111111’

### **普通用户**

1. 普通用户具有查询馆藏图书借阅信息的权限。
2. 普通用户具有修改个人密码的权限。
3. 普通用户具有挂失借阅卡信息的权限。
4. 普通用户具有查询个人借阅信息的权限。

## Web安全性

### 密码

1. 存储

将密码以MD5的形式存储在MySQL数据库中，设定密码的最长长度为50。

1. 验证

在输入验证时，将post输入的密码转换为MD5的形式，以数据库中的密码进行对比。

1. 修改

对管理员用户和普通用户，都创建一个可以修改密码的页面。对两次输入进行判定，若两次输入一致，将数据库中的密码更新为传入字符串的MD5形式。

1. 重置

对管理员用户，创建一个重置密码的页面，使管理员可以重置普通用户的密码。而无需对数据库进行直接操作，提供一定的安全性。

### 退出

在导航栏中设置退出按钮。

退出链接到index.php页面，即登录页面。同时存储在session中的用户信息清除，注销用户信息。

**<?php  
include** (**'waf.php'**);  
  
*session\_start*();  
**if**(**isset**($\_SESSION[**'userid'**]))  
{  
 **unset**($\_SESSION[**'userid'**]);  
}  
**if**(**isset**($\_SESSION[**'captcha'**]))  
{  
 **unset**($\_SESSION[**'captcha'**]);  
}  
**?>**

### 输入验证

对所有的输入进行验证。首先创建一系列的验证规则，存储在waf.php文件中，在包含输入的文件中，引用waf.php，对所有的输入校验。而在关闭报错信息后，不会弹出任何与数据库，数据表有关的信息。攻击方式主要为sql注入，所以输入验证主要围绕sql注入展开。

包括攻击关键字检测：

**if**(*preg\_match*(**"/select**\b**|insert**\b**|update**\b**|drop**\b**|delete**\b**|dumpfile**\b**|outfile**\b**|load\_file|rename**\b**|floor**\(**|extractvalue|updatexml|name\_const|multipoint**\(**/i"**, $str)){  
 close();}

0x25检测：

**function** filter\_0x25($str){  
 **if**(*strpos*($str,**"%25"**) !== **false**){  
 $str = *str\_replace*(**"%25"**, **"%"**, $str);  
 **return** filter\_0x25($str);  
 }

**else**{  
 **return** $str;  
 }  
}

检测不可见字符的截断和绕过效果：

**function** filter\_invisible($str){  
 **for**($i=0;$i<*strlen*($str);$i++){  
 $ascii = *ord*($str[$i]);  
 **if**($ascii>126 || $ascii < 32){ *//有中文这里要修改* **if**(!*in\_array*($ascii, **array**(9,10,13))){  
*// write\_attack\_log("interrupt");* close();  
 }**else**{  
 $str = *str\_replace*($ascii, **" "**, $str);  
 }  
 }  
 }  
 $str = *str\_replace*(**array**(**"`"**,**"|"**,**";"**,**","**), **""**, $str);  
 **return** $str;  
}

### 会话管理

1．对输入内容进行管理。

如输入用户信息时，除账号、密码等不可限定输入的内容，对可限定输入的内容限定其输入。在输入用户性别信息时，给予下拉框来限制用户的输入，下拉框中包含男、女两个选项。

2．防范xss攻击

将xss攻击中的关键字符替换为中文字符，从而对xss攻击进行防范。

**function** filter\_dangerous\_words($str){  
 $str = *str\_replace*(**"'"**, **"‘"**, $str);  
 $str = *str\_replace*(**"\""**, **"“"**, $str);  
 $str = *str\_replace*(**"<"**, **"《"**, $str);  
 $str = *str\_replace*(**">"**, **"》"**, $str);  
 **return** $str;  
}

## 功能

### 管理并查看图书信息

添加图书

**<?php  
  
if** ($\_SERVER[**"REQUEST\_METHOD"**] == **"POST"**)  
{  
 $nnam = $\_POST[**"nname"**];  
 $naut = $\_POST[**"nauthor"**];  
 $npubl = $\_POST[**"npublish"**];  
 $nisb = $\_POST[**"nISBN"**];  
 $nint = $\_POST[**"nintroduction"**];  
 $nlan = $\_POST[**"nlanguage"**];  
 $npri = $\_POST[**"nprice"**];  
 $npubd = $\_POST[**"npubdate"**];  
 $ncla = $\_POST[**"nclass\_id"**];  
 $npre = $\_POST[**"npressmark"**];  
 $nsta= $\_POST[**"nstate"**];  
  
  
  
 $sqla=**"insert into book\_info VALUES (NULL ,'**{$nnam}**','**{$naut}**','**{$npubl}**','**{$nisb}**','**{$nint}**','**{$nlan}**','**{$npri}**','**{$npubd}**',**{$ncla}**,**{$npre}**,**{$nsta} **)"**;  
 $resa=*mysqli\_query*($dbc,$sqla);  
  
  
 **if**($resa==1)  
 {  
 **echo "<script>alert('添加成功！')</script>"**;  
 **echo "<script>window.location.href='admin\_book.php'</script>"**;  
  
 }  
 **else** {  
 **echo "<script>alert('添加失败！请重新输入！');</script>"**;  
  
 }  
  
}  
**?>**

删除图书

**<?php***session\_start*();  
$userid=$\_SESSION[**'userid'**];  
**include** (**'mysqli\_connect.php'**);  
  
  
$delid=$\_GET[**'id'**];  
$sqla=**"select state a from book\_info where book\_id=**{$delid}**;"**;  
$resa=*mysqli\_query*($dbc,$sqla);  
$resulta=*mysqli\_fetch\_array*($resa);  
  
**if**($resulta[**'a'**]==1) {  
 $sql = **"delete from book\_info where book\_id=**{$delid} **;"**;  
 $res = *mysqli\_query*($dbc, $sql);  
  
 **if** ($res == 1) {  
 **echo "<script>alert('删除成功！')</script>"**;  
 **echo "<script>window.location.href='admin\_book.php'</script>"**;  
 }  
 **else** {  
 **echo "删除失败！"**;  
 **echo "<script>window.location.href='admin\_book.php'</script>"**;  
 }  
}  
**else** {  
 **echo "<script>alert('不能删除该图书！')</script>"**;  
 **echo "<script>window.location.href='admin\_book.php'</script>"**;  
}  
  
**?>**

修改图书信息

**<?php  
  
if** ($\_SERVER[**"REQUEST\_METHOD"**] == **"POST"**)  
{  
  
 $boid=$\_GET[**'id'**];  
 $nnam = $\_POST[**"nname"**];  
 $naut = $\_POST[**"nauthor"**];  
 $npubl = $\_POST[**"npublish"**];  
 $nisb = $\_POST[**"nISBN"**];  
 $nint = $\_POST[**"nintroduction"**];  
 $nlan = $\_POST[**"nlanguage"**];  
 $npri = $\_POST[**"nprice"**];  
 $npubd = $\_POST[**"npubdate"**];  
 $ncla = $\_POST[**"nclass\_id"**];  
 $npre = $\_POST[**"npressmark"**];  
 $nsta= $\_POST[**"nstate"**];  
  
  
  
 $sqla=**"update book\_info set name='**{$nnam}**',author='**{$naut}**',publish='**{$npubl}**',  
ISBN='**{$nisb}**',introduction='**{$nint}**',language='**{$nlan}**',price='**{$npri}**',pubdate='**{$npubd}**',  
class\_id=**{$ncla}**,pressmark=**{$npre}**,state=**{$nsta} **where book\_id=**$boid**;"**;  
 $resa=*mysqli\_query*($dbc,$sqla);  
  
  
 **if**($resa==1)  
 {  
  
 **echo "<script>alert('修改成功！')</script>"**;  
 **echo "<script>window.location.href='admin\_book.php'</script>"**;  
  
 }  
 **else** {  
 **echo "<script>alert('修改失败！请重新输入！');</script>"**;  
  
 }  
  
}  
  
  
**?>**

### 管理并查看读者信息

增加读者

**<?php  
  
if** ($\_SERVER[**"REQUEST\_METHOD"**] == **"POST"**)  
{  
 $nnid = $\_POST[**"nid"**];  
 $nnam= $\_POST[**"nname"**];  
 $nsex = $\_POST[**"nsex"**];  
 $nbir= $\_POST[**"nbirth"**];  
 $nadd= $\_POST[**"naddress"**];  
 $nnte = $\_POST[**"ntel"**];  
  
  
 $sqla=**"insert into reader\_info VALUES (**$nnid **,'**{$nnam}**','**{$nsex}**','**{$nbir}**','**{$nadd}**','**{$nnte}**')"**;  
 $sqlb=**"insert into reader\_card (reader\_id,name,passwd) VALUES(**$nnid **,'**{$nnam}**',md5('111111));"**;  
 $resa=*mysqli\_query*($dbc,$sqla);  
 $resb=*mysqli\_query*($dbc,$sqlb);  
  
  
 **if**($resa==1&&$resb==1)  
 {  
  
 **echo "<script>alert('读者添加成功！初始密码为111111')</script>"**;  
 **echo "<script>window.location.href='admin\_reader.php'</script>"**;  
  
 }  
 **else** {  
 **echo "<script>alert('添加失败！请重新输入！');</script>"**;  
  
 }  
  
}  
  
**?>**

修改读者信息

**<?php  
  
if** ($\_SERVER[**"REQUEST\_METHOD"**] == **"POST"**)  
{  
  
 $readid=$\_GET[**'id'**];  
  
 $nnid = $\_POST[**"nid"**];  
 $nnam= $\_POST[**"nname"**];  
 $nsex = $\_POST[**"nsex"**];  
 $nbir= $\_POST[**"nbirth"**];  
 $nadd= $\_POST[**"naddress"**];  
 $nnte = $\_POST[**"ntel"**];  
  
  
  
 $sqla=**"update reader\_info set reader\_id=**{$nnid}**,name='**{$nnam}**',sex='**{$nsex}**',  
birth='**{$nbir}**',address='**{$nadd}**',telcode='**{$nnte}**' where reader\_id=**$readid**;"**;  
 $resa=*mysqli\_query*($dbc,$sqla);  
 $sqlc=**"update reader\_card set name='**{$nnam}**' where reader\_id=**$readid**;"**;  
 $resc=*mysqli\_query*($dbc,$sqlc);  
  
 **if**($resa==1)  
 {  
  
 **echo "<script>alert('修改成功！')</script>"**;  
 **echo "<script>window.location.href='admin\_reader.php'</script>"**;  
  
 }  
 **else** {  
 **echo "<script>alert('修改失败！请重新输入！');</script>"**;  
  
 }  
  
}  
  
  
**?>**

删除读者信息

**<?php***session\_start*();  
$userid=$\_SESSION[**'userid'**];  
**include** (**'mysqli\_connect.php'**);  
  
  
$delid=$\_GET[**'id'**];  
$sqla=**"select** *count***(***\****) a from lend\_list where reader\_id=**{$delid} **and back\_date is NULL;"**;  
$resa=*mysqli\_query*($dbc,$sqla);  
$resulta=*mysqli\_fetch\_array*($resa);  
  
**if**($resulta[**'a'**]==0) {  
 $sqla = **"delete from reader\_card where reader\_id=**{$delid} **;"**;  
 $sqlb = **"delete from reader\_info where reader\_id=**{$delid} **;"**;  
 $resa = *mysqli\_query*($dbc, $sqla);  
 $resb = *mysqli\_query*($dbc, $sqlb);  
  
 **if** ($resa == 1 && $resb == 1) {  
 **echo "<script>alert('删除成功！')</script>"**;  
 **echo "<script>window.location.href='admin\_reader.php'</script>"**;  
 }  
 **else** {  
 **echo "删除失败！"**;  
 **echo "<script>window.location.href='admin\_reader.php'</script>"**;  
 }  
}  
**else** {  
 **echo "<script>alert('不能删除该读者！')</script>"**;  
 **echo "<script>window.location.href='admin\_reader.php'</script>"**;  
}  
  
**?>**

查看读者信息

**<?php** $sqla=**"select** *count***(***\****) a from lend\_list where reader\_id=**{$userid} **and back\_date is NULL;"**;  
  
 $resa=*mysqli\_query*($dbc,$sqla);  
 $resulta=*mysqli\_fetch\_array*($resa);  
 **echo "您目前共借阅**{$resulta[**'a'**]}**本书。"**;  
 **?>**

**<?php**$sqlb=**"select DATE\_ADD(lend\_date,INTERVAL 1 MONTH) AS yhrq from lend\_list where reader\_id=**{$userid} **and back\_date is NULL;"**;  
$counta=0;  
$resb=*mysqli\_query*($dbc,$sqlb);  
  
**foreach** ($resb **as** $row){  
 **if**(*strtotime*(*date*(**"y-m-d"**))>*strtotime*($row[**'yhrq'**])) $counta++;  
};  
  
**if**($counta==0) **echo "您当前没有超期且未归还的书。"**;  
**else echo "有**{$counta}**本书已超期，请您及时归还"**;  
  
  
**?>**

### 借还图书

**<?php**$sqle=**"select sernum from lend\_list where book\_id=**{$bookid}**"**;  
$rese=*mysqli\_query*($dbc,$sqle);  
$resulte=*mysqli\_fetch\_array*($rese);  
  
$sqlc=**"update lend\_list set back\_date=NOW() where sernum=**{$resulte[**'sernum'**]}**;"**;  
$sqld=**"UPDATE book\_info set state=1 where book\_id=**{$bookid}**;"**;  
$resc=*mysqli\_query*($dbc,$sqlc);  
$resd=*mysqli\_query*($dbc,$sqld);  
  
**if**($resc==1 && $resd==1)  
**echo"<script>alert('还书成功！');window.location.href='admin\_book.php'; </script>"**;  
**else echo"<script>alert('还书失败！');window.location.href='admin\_book.php'; </script>"**;  
**?>**

### 修改密码

**<?php  
  
if** ($\_SERVER[**"REQUEST\_METHOD"**] == **"POST"**)  
{  
 $passa = $\_POST[**"pass1"**];  
 $passb = $\_POST[**"pass2"**];  
**if**($passa==$passb){  
 $sql=**"update reader\_card set passwd='**{$passa}**' where reader\_id=**{$userid}**"**;  
 $res=*mysqli\_query*($dbc,$sql);  
 **if**($res==1)  
 {  
 **echo "<script>alert('密码修改成功！请重新登陆！')</script>"**;  
 **echo "<script>window.location.href='index.php'</script>"**;  
 }  
  
}  
**else**{  
 **echo "<script>alert('两次输入密码不同，请重新输入！')</script>"**;  
  
}  
  
}  
**?>**

### 重置密码

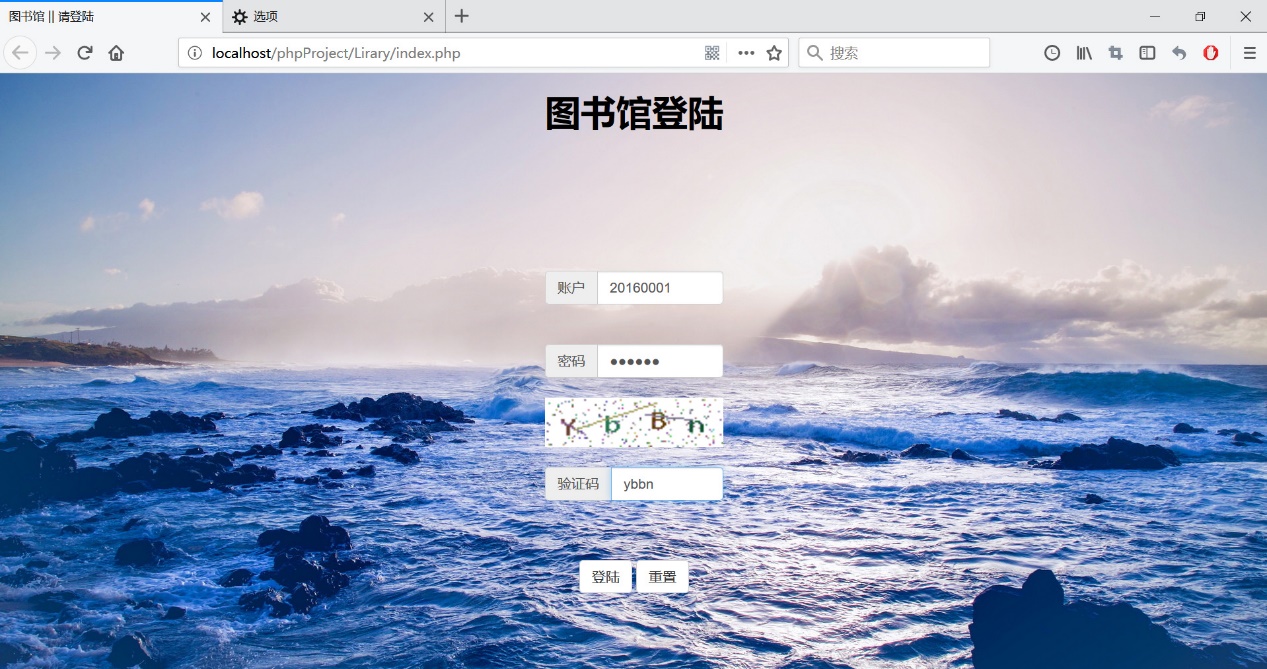
**<?php***session\_start*();  
$userid=$\_SESSION[**'userid'**];  
**include** (**'mysqli\_connect.php'**);  
  
  
$sql=**"update reader\_card set passwd = md5('111111') where reader\_id=**{$userid}**"**;  
$res=*mysqli\_query*($dbc,$sql);  
**if**($res==1)  
{  
 **echo "<script>alert('密码重置成功!')</script>"**;  
 **echo "<script>window.location.href='admin\_init\_password.php'</script>"**;  
}  
**else**{  
 **echo "<script>alert('密码重置失败!')</script>"**;  
 **echo "<script>window.location.href='admin\_init\_password.php'</script>"**;  
}  
  
**?>**

### 借书卡挂失

**<?php***session\_start*();  
$userid=$\_SESSION[**'userid'**];  
**include** (**'mysqli\_connect.php'**);  
  
$state=$\_GET[**'id'**];  
  
**if**($state==1){  
 $sql=**"update reader\_card set card\_state=0 where reader\_id=**{$userid}**"**;  
 $res=*mysqli\_query*($dbc,$sql);  
  
 **if**($res==1)  
 {  
 **echo"<script>alert('挂失成功！')</script>"**;  
 **echo "<script>window.location.href='reader\_guashi.php'</script>"**;  
 }  
 **else** {  
 **echo"<script>alert('挂失失败！')</script>"**;  
 **echo "<script>window.location.href='reader\_guashi.php'</script>"**;  
 }  
  
}  
**else**{  
  
 $sqla=**"update reader\_card set card\_state=1 where reader\_id=**{$userid}**"**;  
 $resa=*mysqli\_query*($dbc,$sqla);  
  
 **if**($resa==1)  
 {  
 **echo"<script>alert('取消挂失成功！')</script>"**;  
 **echo "<script>window.location.href='reader\_guashi.php'</script>"**;  
 }  
 **else** {  
 **echo"<script>alert('取消挂失失败！')</script>"**;  
 **echo "<script>window.location.href='reader\_guashi.php'</script>"**;  
 }  
}  
  
**?>**

# 第三章 测试和演示

首先是图书馆的登录界面

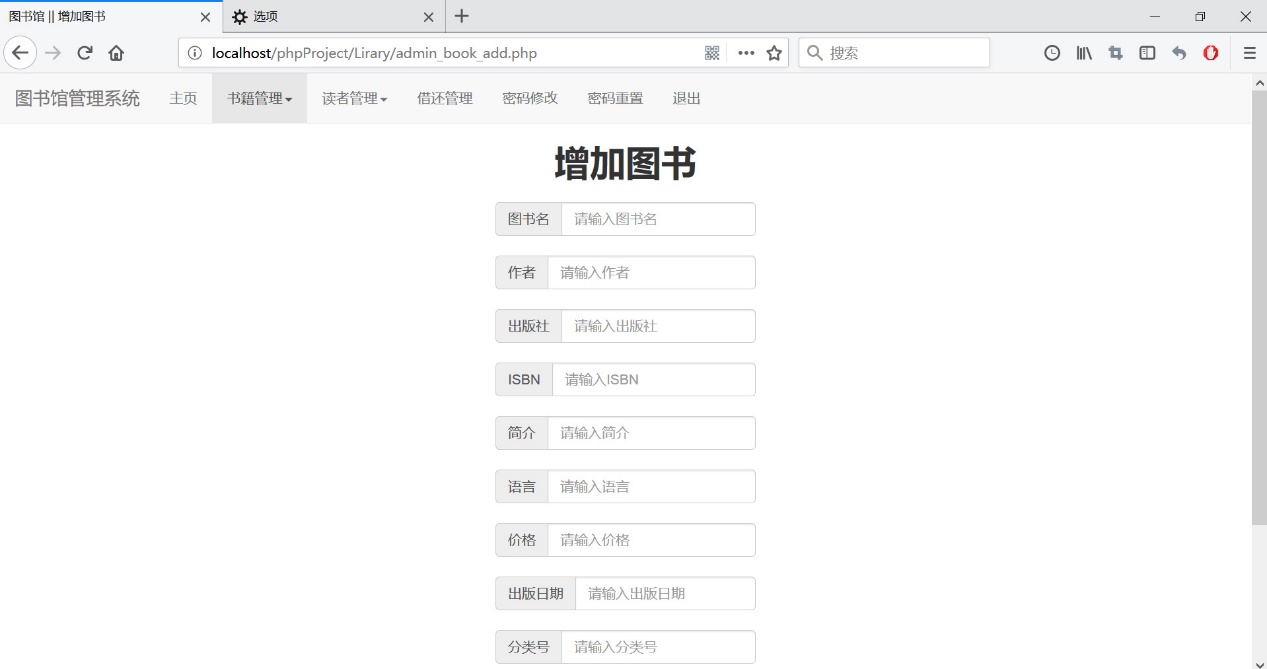


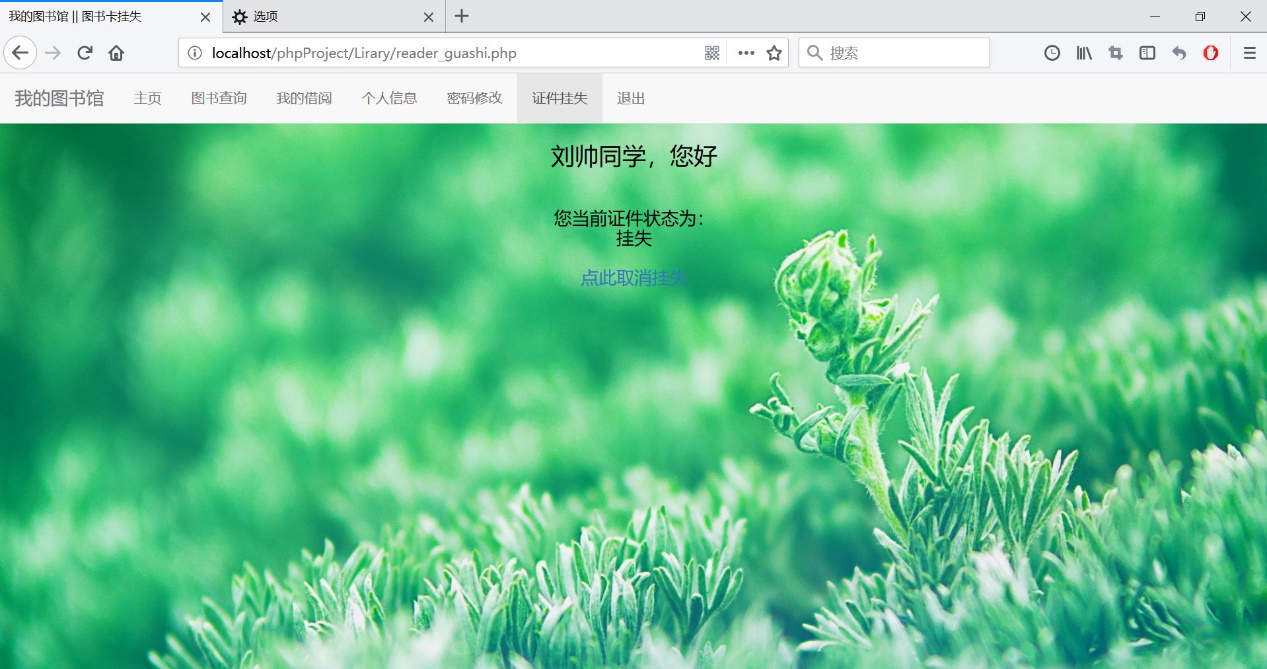
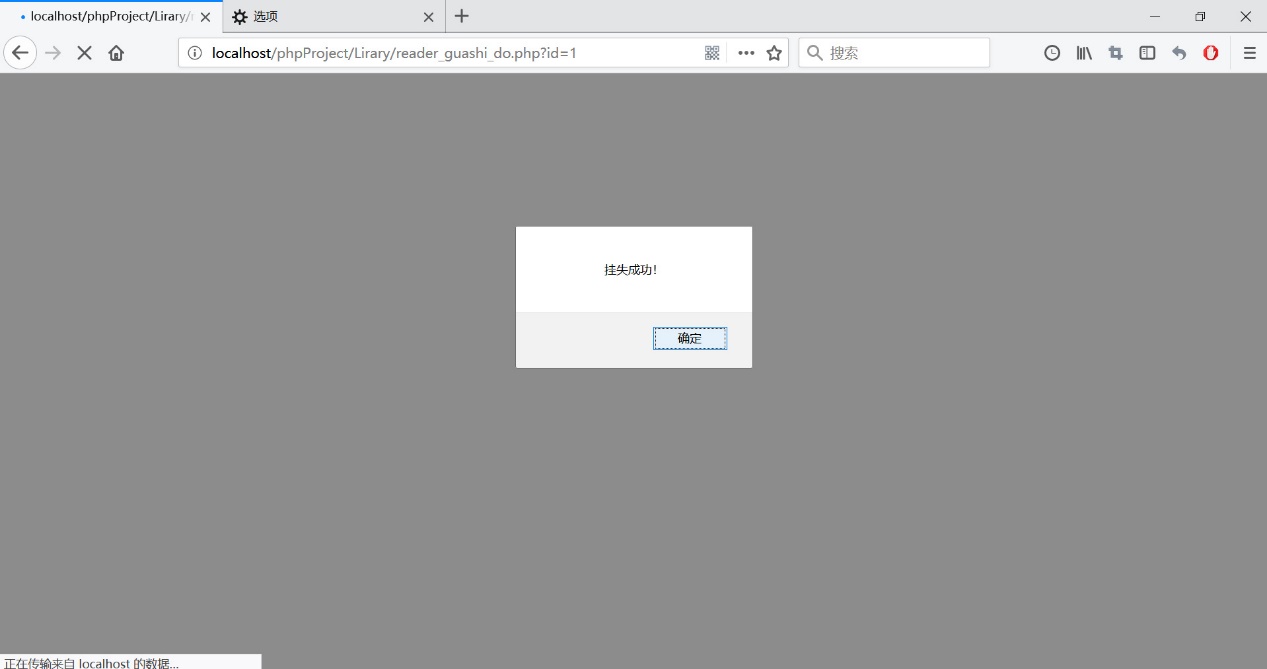
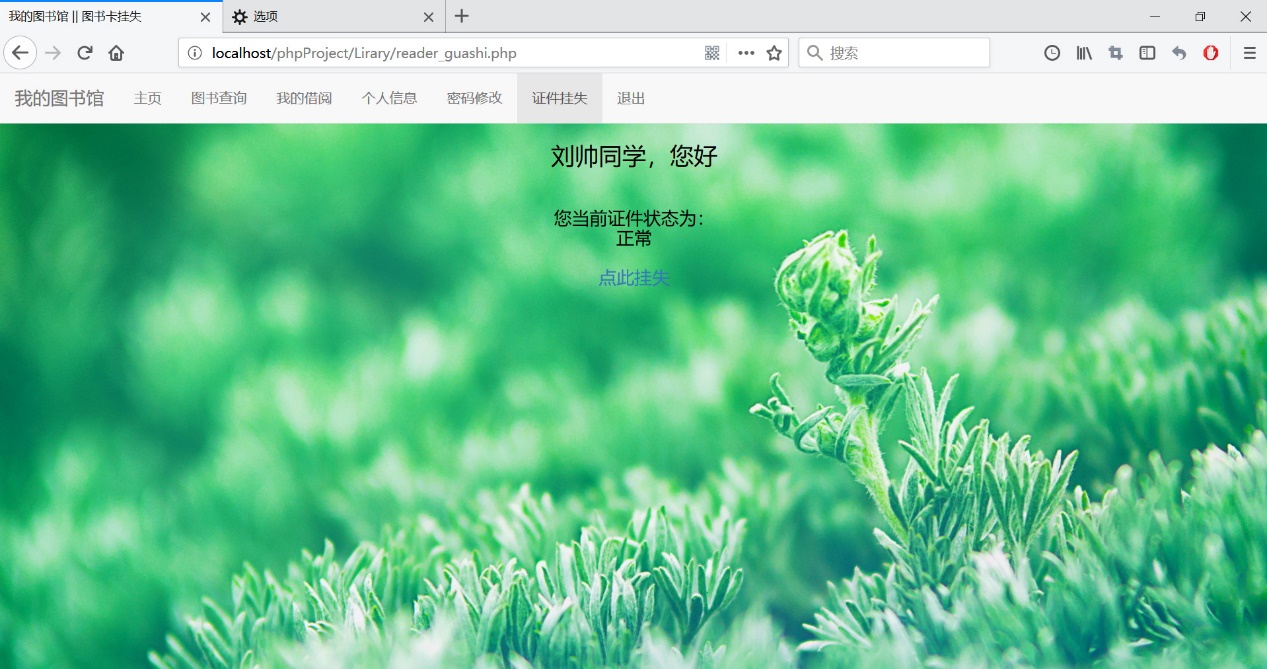
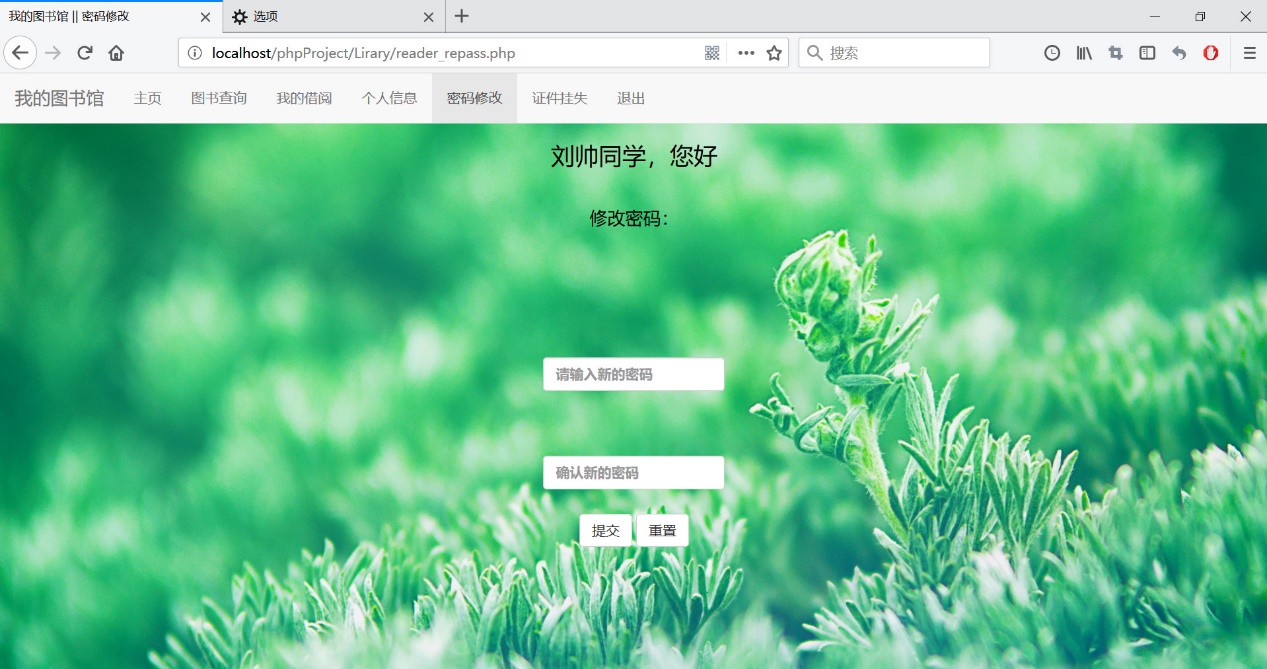
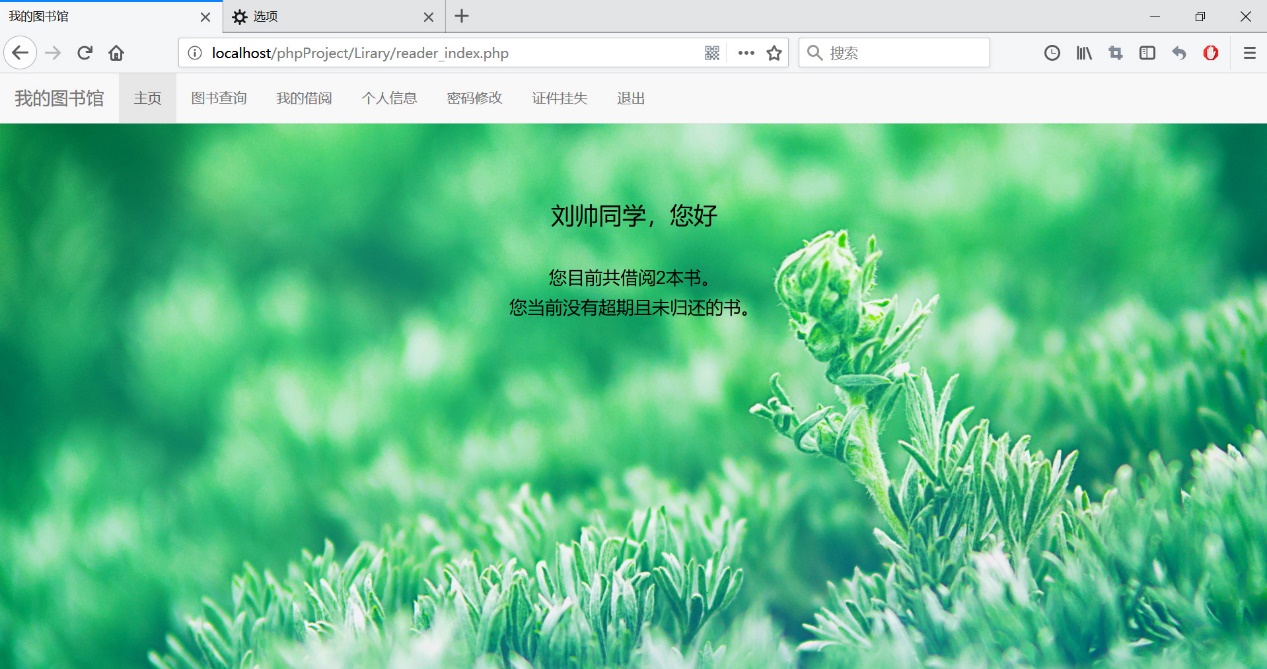
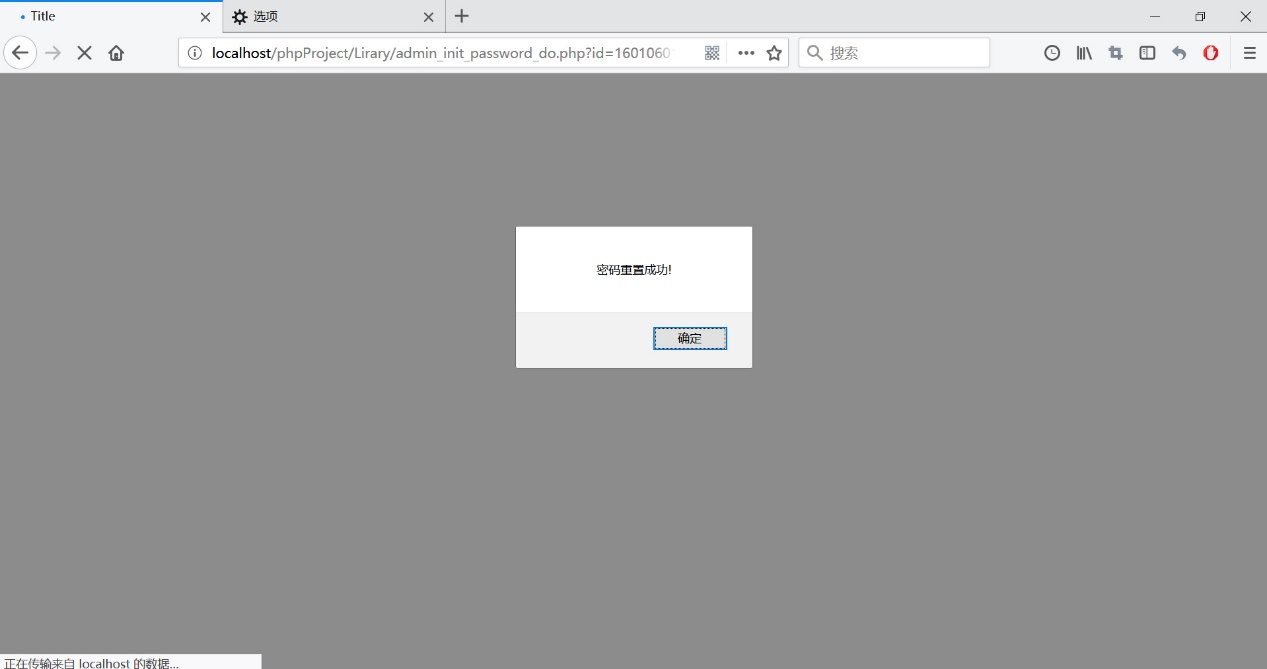
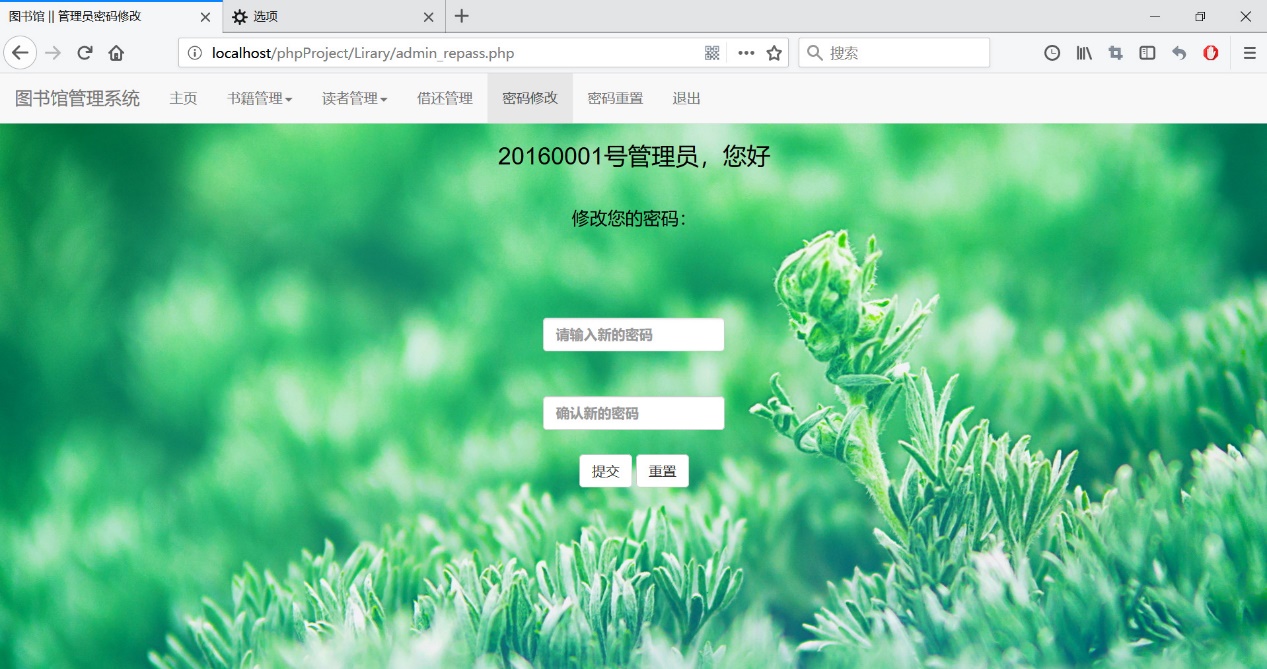
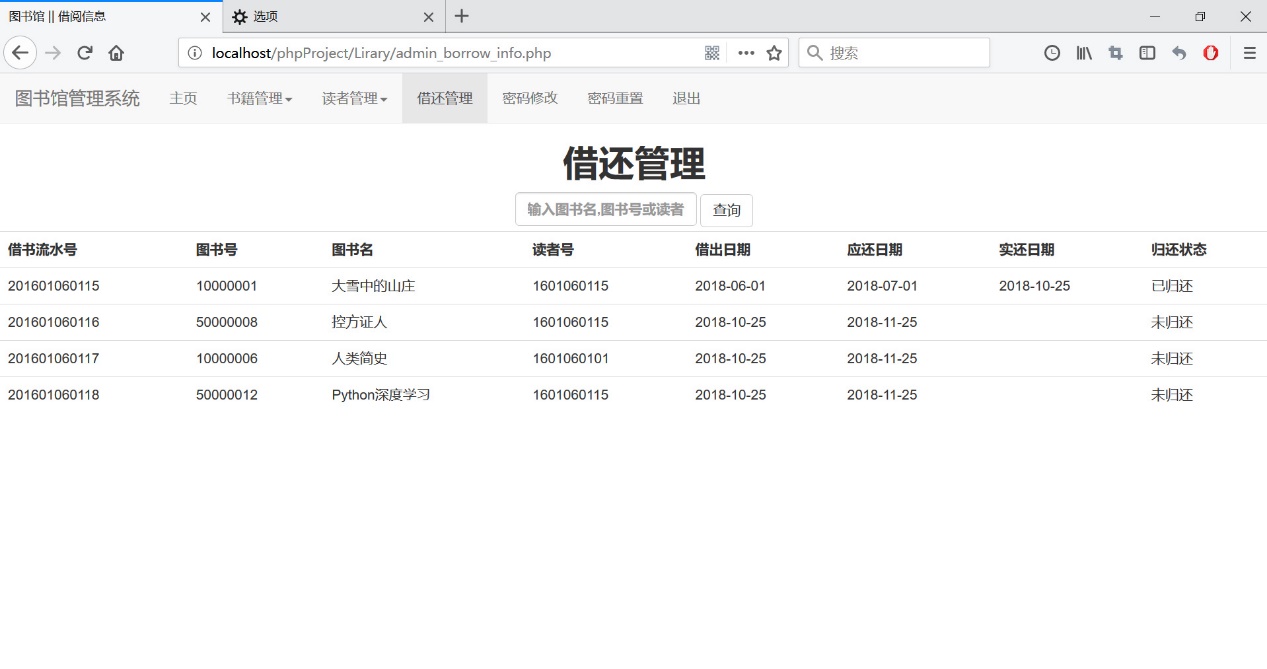
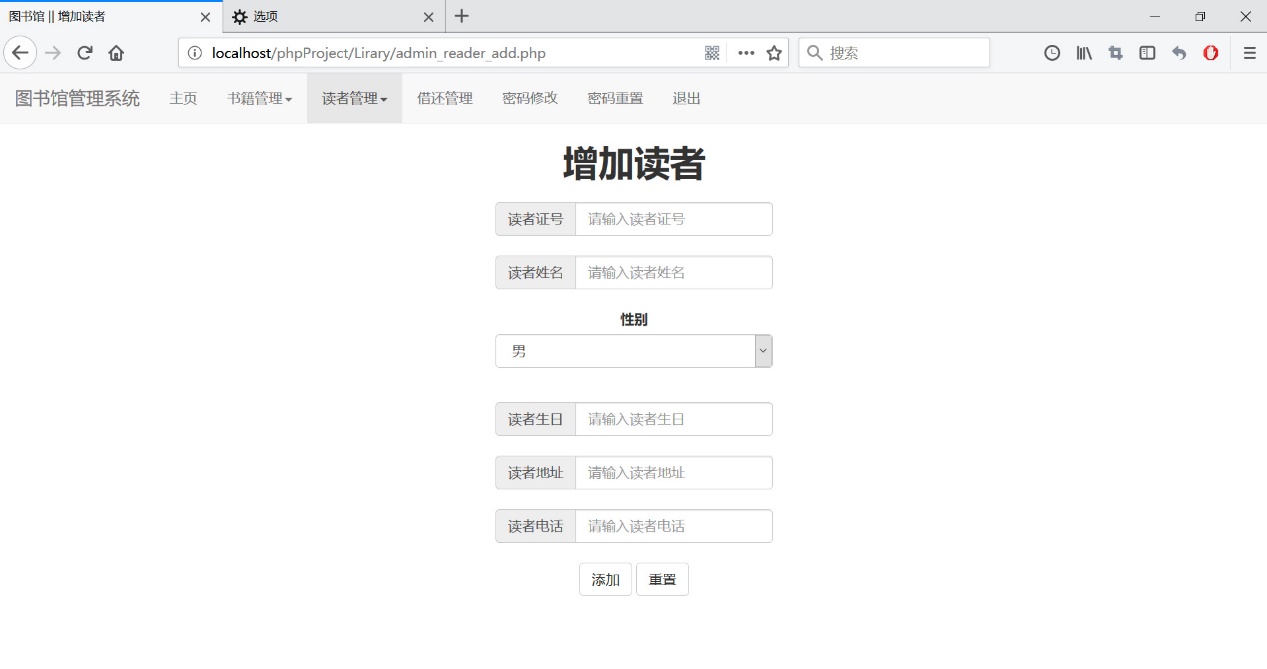
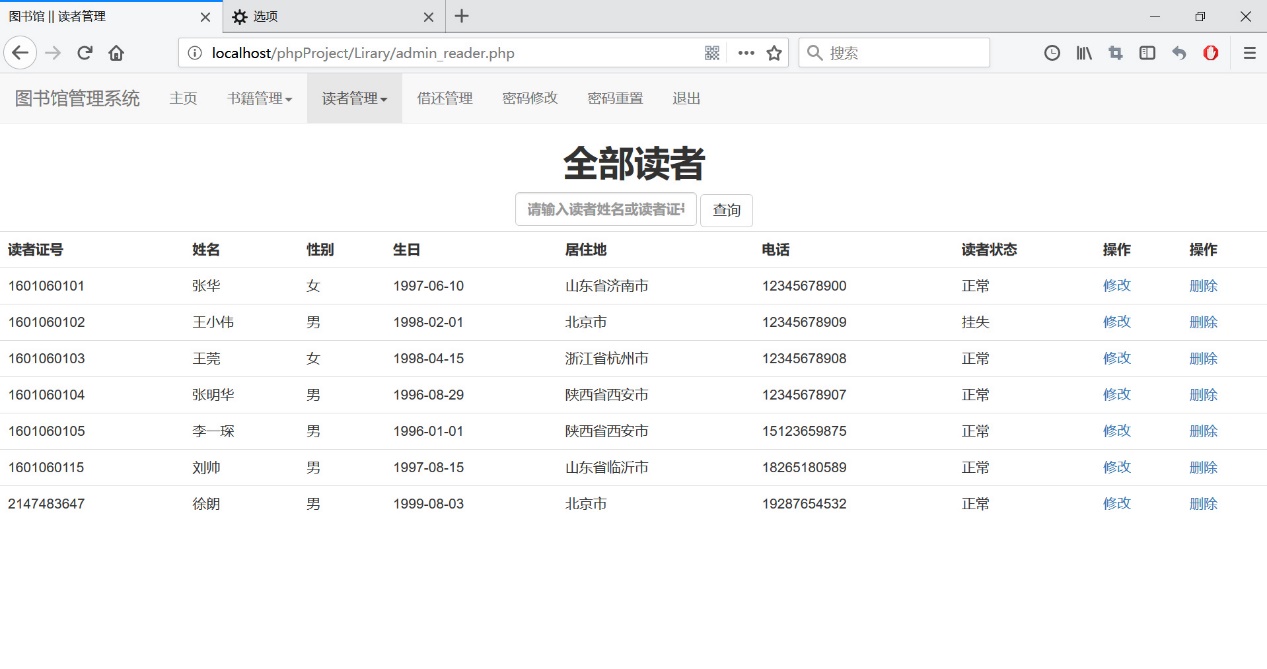
登录管理员账号，进入到图书馆主页



查看全部书籍

增加图书



查看读者

# 第四章 总结

通过此次项目实训，了解了网络攻击的方式，如包括不仅限于sql注入、目录包含、xss攻击等。同时学习防范上述攻击的方式，并应用到此次项目当中。学习了twitter的bootstrap框架，对整个页面的导航栏和一些表单进行重新设计，使页面具有扁平化的感受，更具科技感。

应用php、MySQL、Apache、bootstrap开发了网络图书管理系统，具有较为整洁的交互页面，具备一定的安全性防范网络攻击，同时可以对图书、用户信息进行增删改查等操作。

在此次项目的实现过程中，能够快速地了解所需要的技术，并快速学习技术。学习实例，通过使用来掌握技术方法，同时练习了实际编码能力。