Web Dev Assignment Description - C13451458

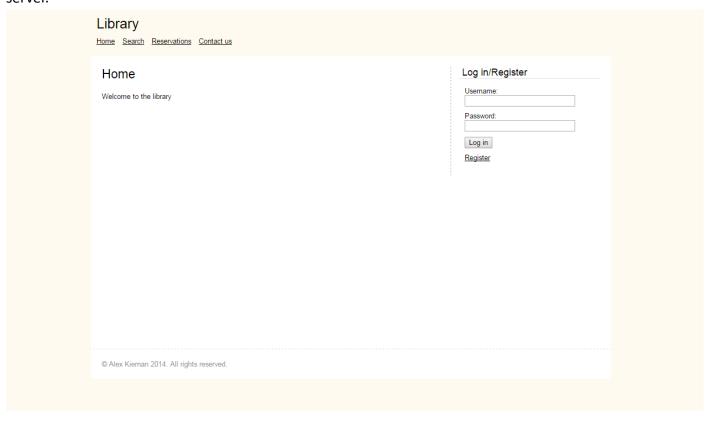
Overview

I broke my website into different PHP modules to allow for easy manipulation. Each page is comprised of a header, menu, sidebar and footer as well as the pages body. These elements persist throughout the website so the only elements that change are the body and the sidebar showing whether the user is logged in or not.

Description of pages

Index

The index page is the main splash page. The user could login from here on the sidebar. When a user signs in their session persists until they logout. The login feature has error checking such as wrong password. A new account could also be created from here. This directs the user to the new account page which takes into account the requirements for user data as outlined in the brief and sanitizes all inputted data sent to the server.

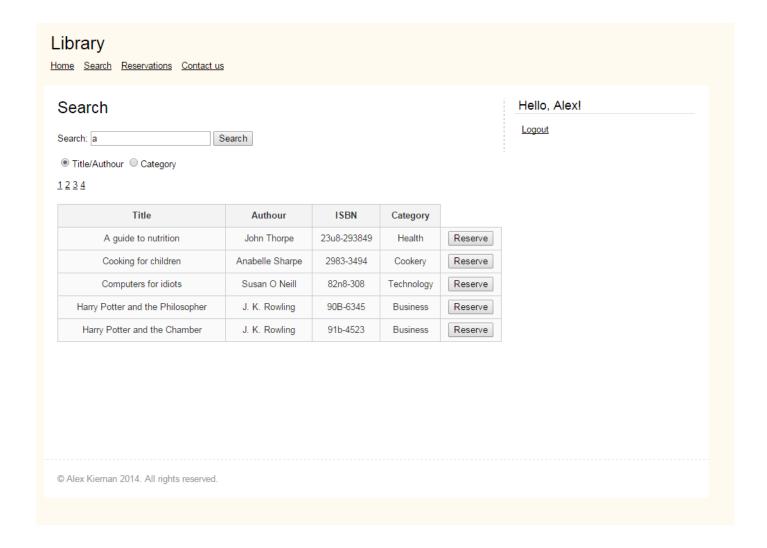


New Account

A user must enter all fields marked with a star. If the user enters a username that already exists an error message will display. A similar message appears for phone numbers that are not 10 digits and passwords that do not match or are less than 6 characters. When data is submitted it is sent using a POST method to a sql query which inserts the record into the database.

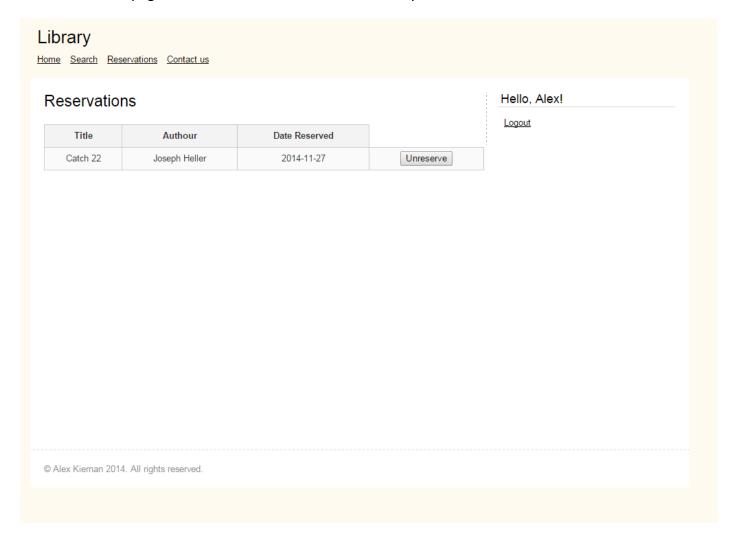
Search

The search page allows the user to search by author/title or by category. The sql query can accept complete or near complete queries. The results are displayed in a table which then allows a user who is logged in to reserve a book. If a book is not able to be reserved it is marked as unavailable. If more than five results are returned the data continues on another page, the user can easily navigate between each page.



Reservations

The reservations page allows a user to see and unreserve any reserved books linked to their account.



<u>Code</u>

```
Index
<?php
include 'core/init.php';
include 'includes/overall/overall_header.php';
?>
<h1>Home</h1>
Welcome to the library
<?php include 'includes/overall_footer.php'; ?>
Login
<?php
// Logic
include 'core/init.php';
if (empty($_POST) === false) {
          $username = $_POST['username'];
          $password = $_POST['password'];
         // error checking
         if (empty($username) === true || empty($password) === true)
                   $errors[] = 'You need to enter a username and password';
         } else if (user_exists($username) === false) {
                   $errors[] = 'Username does not exist';
         }
         else
         {
                   // more error checking
                   if (strlen($password) > 6) {
                             $errors[] = 'Password too long';
                   // call login function with submitted data
                   $login = login($username, $password);
                   if ($login === false) {
                             $errors[] = 'Username and password combination is incorrect';
                   } else {
                             // set the user session and login
                             $_SESSION['username'] = $login;
                             header('Location: index.php');
                             exit();
                   }
} else {
          $errors[] = 'No data recieved';
}
// Output
include 'includes/overall/overall_header.php';
if (empty($errors) === false) {
?>
          <h2>Login failed:</h2>
<?php
          echo output_errors($errors);
include 'includes/overall/overall footer.php';
Logout
<?php
session_start();
session_destroy();
header('Location: index.php');
Register
<?php
include 'core/init.php';
```

```
include 'includes/overall/overall header.php';
// error reporting
if (empty($_POST) === false)
         // check all fields contain data
          $required_fields = array('username', 'password', 'password_again', 'firstName', 'lastName', "AddressLine1", 'AddressLine2', 'city',
'telephone', 'mobile');
         foreach ($ POST as $key => $value) { // loop through each value and check each one
                    if (empty($value) && in_array($key, $required_fields) === true) { // if a field is empty AND is in array generate error
                              $errors[] = "All fields are required!";
                              break 1;
          // check conditions for fields
          if (empty($errors) === true) {
                    if (user exists($ POST['username']) === true) {
                             $errors[] = 'Sorry, the username \'' . $_POST['username'] . '\' is already taken.';
                    if (preg\_match("/\s/", \$\_POST['username']) == true) {
                              $errors[] = "Your username must not contain any spaces";
                    if (strlen($ POST['password']) != 6) {
                              $errors[] = 'Your password must be 6 characters';
                    if ($_POST['password'] !== $_POST['password_again']) {
                              $errors[] = 'Your passwords do not match';
                    if (strlen($_POST['mobile']) != 10) {
                              $errors[] = 'Mobile number must be 10 digits!';
                    if (is_numeric($_POST['mobile']) == false) {
                              $errors[] = 'Mobile number must be a number';
<h1>Register</h1>
<?php
// recieves success passed by header
if (isset($ GET['success']) && empty($ GET['success'])) {
          echo 'You have been registered!';
}
else
{
         // post data for register user or output errors
          if (empty($_POST) === false && empty($errors) === true) {
                    $register_data = array (
                              'username'
                                                            => $_POST['username'],
                              'password'
                                                            => $_POST['password'],
                              'firstName'
                                                 => $_POST['firstName'],
                              'lastName'
                                                            => $ POST['lastName'],
                              'AddressLine1'
                                                 => $ POST['AddressLine1'],
                                                 => $_POST['AddressLine2'],
                              'AddressLine2'
                              'city'
                                                            => $ POST['city'],
                                                            => $_POST['telephone'] ,
                              'telephone'
                              'mobile'
                                                 => $_POST['mobile']
                    // function to register data with query
                    register_user($register_data);
                    // send success and break
                    header('Location: register.php?success');
                    exit();
          } else if (empty($errors) === false) {
                    echo output errors($errors);
}
```

```
<form action="" method="post">
        <1i>
                          Username*:<br>
                          <input type="text" name="username">
                 </i>
                          Password*:<br>
                          <input type="password" name="password">
                 <1i>
                          Password again*:<br>
                          <input type="password" name="password_again">
                 <1i>
                          First name*:<br>
                          <input type="text" name="firstName">
                 </i>
                          Last name*:<br>
                          <input type="text" name="lastName">
                 <1i>
                          Address Line 1*:<br>
                          <input type="text" name="AddressLine1">
                 <1i>
                          Address Line 2*:<br>
                          <input type="text" name="AddressLine2">
                 </i>
                          City*:<br>
                          <input type="text" name="city">
                 <1i>
                          Telephone*:<br>
                          <input type="text" name="telephone">
                 </i>
                          Mobile*:<br>
                          <input type="text" name="mobile">
                 <1i>
                          <input type="submit" value="Register">
                 </form>
<?php
include 'includes/overall_footer.php';
?>
Search
<?php
include 'core/init.php';
include 'includes/overall/overall_header.php';
?>
<h1>Search</h1>
<form action="" method="get">
        <label>
                 Search:
                 <input type="text" name="keywords">
        </label>
        <input type="submit" value="Search">
        <br><br>
                 <input type="radio" name="criteria" value="TitleAuthour">Title/Authour
                 <input type="radio" name="criteria" value="Category">Category
</form>
```

```
<br>
```

```
<?php
if (isset($_GET['keywords']) && isset($_GET['keywords'])) {
         $keywords = $_GET['keywords'];
         $criteria = $_GET['criteria'];
         if ($criteria == "TitleAuthour") {
                   $sql =
                                      SELECT books.*, categories.categoryDesc
                                                FROM books
                                                LEFT JOIN categories
                                                ON books.categoryID = categories.categoryID
                                                WHERE bookTitle LIKE '%{$keywords}%' OR authour LIKE '%{$keywords}%'
                                       ");
         else if ($criteria == "Category") {
                                      SELECT books.*, categories.categoryDesc
                   $sql =
                                                FROM books
                                                LEFT JOIN categories
                                                ON books.categoryID = categories.categoryID
                                                WHERE categories.categoryDesc LIKE '%{$keywords}%'
                                       ");
         else {
                                      SELECT books.*, categories.categoryDesc
                   $sql =
                                                FROM books
                                                LEFT JOIN categories
                                                ON books.categoryID = categories.categoryID
                                                WHERE bookTitle LIKE '%{$keywords}%' OR authour LIKE '%{$keywords}%' OR
categories.categoryDesc LIKE '%{$keywords}%'
         }
         $result = mysql query($sql);
         $row = mysql_fetch_assoc($result);
         // number of results to show per page
         $per_page = 5;
         // figure out the total pages in the database
         $total_results = mysql_num_rows($result);
         $total_pages = ceil($total_results / $per_page);
         // check if the 'page' variable is set in the URL
         if (isset($_GET['page']) && is_numeric($_GET['page']))
                   $show_page = $_GET['page'];
                   // make sure the $show_page value is valid
                   if ($show_page > 0 && $show_page <= $total_pages)
                             $start = ($show_page -1) * $per_page;
                             $end = $start + $per_page;
                   else
                   {
                             // error - show first set of results
                             $start = 0;
                             $end = $per_page;
                   }
         }
         else
                   // if page isn't set, show first set of results
                   $start = 0;
                   $end = $per_page;
         }
         // display pagination
```

for (\$i = 1; \$i <= \$total_pages; \$i++)

```
{
                  echo "<a href='search.php?&keywords=$keywords&criteria=$criteria&page=$i'>$i</a>";
         echo "";
         // display data in table
         echo "";
         echo " Title Authour ISBN Category ";
         // loop through results of database query, displaying them in the table
         for ($i = $start; $i < $end; $i++)
         {
                  // make sure that PHP doesn't try to show results that don't exist
                  if ($i == $total_results) { break; }
                           echo "";
                           echo '' . mysql_result($result, $i, 'bookTitle') . '';
                           echo '' . mysql_result($result, $i, 'authour') . '';
                           echo '' . mysql_result($result, $i, 'ISBN') . '';
                           echo '' . mysql_result($result, $i, 'categoryDesc') . '';
                           echo '';
                           if(mysql_result($result, $i, 'reserved') == 'N')
                  {
                           $ISBN = mysql result($result, $i, 'ISBN');
                  <form method="post" action="">
                           <button type="submit" name="ISBN" value=" <?php echo "$ISBN" ?> ">Reserve</button>
                  </form><?php
                  else
                  echo "Unavailable";
                  echo '';
                           echo "";
         // close table>
         echo "";
         // pagination
}
?>
Reserve
<?php
if (isset($_POST['ISBN']) && isset($_SESSION["username"])) {
         \$string = preg\_replace('/\s+/', ", \$\_POST['ISBN']);
         $username = $_SESSION['username'];
         mysql_query ("
                           UPDATE books
                                              SET reserved = 'Y'
                                              WHERE ISBN = '$string'
                                     ");
                           INSERT INTO reservations
         mysql_query ("
                                              VALUES ('$string', '$username', CURDATE())
         header('Location: '.$_SERVER['REQUEST_URI']);
2>
<?php include 'includes/overall_footer.php'; ?>
Functions
<?php
function array_sanitize(&$item) {
         $item = mysql_real_escape_string($item);
}
function sanitize($data) {
         return mysql_real_escape_string($data);
}
```

```
function output errors($errors) {
          $output = array();
         foreach($errors as $error) {
                   $output[] = '' . $error . '';
          return ''. implode(", $output). '';
?>
<?php
function ISBN exists($ISBN) {
          $ISBN = sanitize($ISBN);
          return (mysql result(mysql query("SELECT COUNT(ISBN) FROM reservations WHERE ISBN = '$ISBN'"),0) == 1)? true: false;
function register user($register data) {
          array_walk($register_data, 'array_sanitize');
          $fields = '`' . implode('`, `', array_keys($register_data)) . '`'; // fields to insert data
          $data = '\" . implode('\', \", $register_data) . '\"; // values
          mysql query("INSERT INTO users ($fields) VALUES ($data) ");
}
function user data($username) {
          $data = array();
          $func_num_args = func_num_args();
          $func_get_args = func_get_args();
          if ($func_num_args >= 1) {
                   unset($func_get_args[0]); // removes actual username which is first element in array
                   $fields = implode(', ', $func_get_args) . "; // implode returns a string from array with seperators
                   $data = mysql_fetch_assoc(mysql_query("SELECT $fields FROM users WHERE username = '$username' ")); // returns an
array that corresponds to the fetched rows
                   return($data);
function logged_in() {
          return (isset($_SESSION['username']) ? true : false); // return
function user exists($username) {
          $username = sanitize($username);
          return (mysql_result(mysql_query("SELECT COUNT(username) FROM users WHERE username = '$username'"),0) == 1)? true : false;
function login($username, $password) {
         // return username or false
          return (mysql_result(mysql_query("SELECT COUNT(`username`) FROM `users` WHERE `username`='$username' AND
`password`='$password' "), 0)==1) ? $username : false;
?>
Extras
<aside>
          <?php
          $check = logged in();
          if ($check === true) {
                   include 'includes/widgets/widget_logged_in.php';
          } else {
                   include 'includes/widgets/widget_login.php';
          2>
</aside>
<footer>
          © Alex Kiernan 2014. All rights reserved.
</footer>
<head>
  <title>Home</title>
  <meta charset="UTF-8">
```

```
<link rel="stylesheet" href="css/stylio.css">
</head>
<header>
 <h1 class="logo">Library</h1>
 <?php include 'includes/menu.php'; ?>
 <div class="clear"></div>
</header>
<nav>
 <a href="index.php">Home</a>
   <a href="search.php">Search</a>
   <a href="reservations.php">Reservations</a>
    <a href="contact.php">Contact us</a>
 </nav>
<!doctype html>
<html>
<?php include 'includes/head.php'; ?>
<body>
        <?php include 'includes/header.php'; ?>
 <div id="container">
        <?php include 'includes/aside.php' ?>
  </div>
        <?php include 'includes/footer.php'; ?>
</body>
</html>
```