PHP
and MVC Architecture

Build a better website

Class 4: Security and Permissions

Logging in, logging out and user-specific permissions

Passwords and Model

Create Blogger -- models/blogger.php

md5 is a function that scrambles data

```
public static function create ($fields) {
    $date = date ("Y-m-d H:i:s");
    $fields = Model::cleanData($fields);

    $password = md5($fields['password'], false);

    $sql = 'INSERT INTO bloggers (username, email, password,
        date_created)VALUES ("' . $fields['username'] . '", "' .
        $fields['email'] . '", "'. $password .'", "'. $date .'")';
    $results = Model::insert($sql);
    return $results;
}
```

You will have to add a similar line in the update function in the model

Passwords and Controllers

Update blogger -- controllers/blogger.php

```
if (isset($_POST['update_blogger'])){
    if($_POST['password']==''){
        Blogger::edit($_POST, $_POST['id']);
    }
    else if($_POST['password']!='' && $_POST['old_password']!=''){
        $blogger = Blogger::getOne($_POST['id']);
        $old_password = md5($_POST['old_password'], false);
        if($old_password == $blogger['password']){
           Blogger::edit($_POST, $_POST['id']);
        }
        else{
          $warning = 'Old password does not match password in the
database';
    }
   }
   else{
    $warning = 'You must provide an old password to change passwords.'
   }
}
```

Logging in and Starting Sessions

Config and models/blogger.php

```
session_start();
```

```
public static function login ($fields){
    $fields = Model::cleanData($fields);
  $password = md5($fields['password'], false);
   $sql = 'SELECT * FROM bloggers WHERE username = "'.
$fields['username'] . '" and password = "' .$password. '"  LIMIT 1';
   $results = Model::select($sql);
   if($results){
      return $results[0];
   }
   else{
      return false;
   }
}
```

Logging in and Starting Sessions

controllers/blogger.php

$_SESSION

```
if(isset($_POST['login_blogger'])){
    if($_POST['username']!='' && $_POST['password']!=''){
        $blogger = Blogger::login($_POST);
        if($blogger){
            $_SESSION['user_id'] = $blogger['id'];
        }
        else{
            $warning = 'No blogger with that username and database exists in
our database';
        }
    }
   else{
      $warning = 'Please enter both username and password';
   }
}
```

Logging in and Starting Sessions

views/blogger/list.php

```
<div id= "login-blogger">
    <form action="<?php echo htmlentities($_SERVER['PHP_SELF']); ?>"
method="post">
        <label>Username</label><input type="text" name ="username"/>
        <label>Password</label><input type="password" name ="password"/>
        <input type = "hidden" value ="true" name="login_blogger"/>
        <button type = "submit" value="Login" class="edit"><img
class="icon" src='/public/images/add.png'/><div class="button-text">
Login</div></button>
    </form>
</div>
```

Logging out and ending sessions

controllers/blogger.php & views/blogger/list.php

```
if(isset($_POST['logout_blogger'])){
    unset($_SESSION['user_id']);
}

<div id= "logout-blogger">
        <p class="warning">Are you sure you want to logout?</p>
        <form action="<?php echo htmlentities($_SERVER['PHP_SELF']); ?>"
method="post">
            <input type = "hidden" value ="true" name="logout_blogger"/>
            <button type = "submit" value="Logout" class="delete"><img
class="icon" src='/public/images/delete.png'/><div class="button-text">
Logout</div></button>
        </form>
    </div>
```

Using Sessions

controllers/blogger.php

```
if (isset($_POST['update_blogger'])){
  if(isset($_SESSION['user_id']) && $_SESSION['user_id']==$_POST['id']){
    ///all the code we wrote before
  }
  else{
    $warning = 'Sorry, you do not have permissions to edit that user';
  }
 }

if (isset($_POST['delete_blogger'])) {
  if(isset($_SESSION['user_id']) && $_SESSION['user_id']==$_POST['id']){
     Blogger::destroy($_POST['id']);
  }
  else{
     $warning = 'Sorry, you do not have permissions to delete that
user';
  }
}
```

Using Sessions

controllers/post.php

```
if (isset($_POST['create_post'])){
  if(isset($_SESSION['user_id'])){
     $_POST['user_id'] = $_SESSION['user_id'];
     Post::create($_POST);
  }
  else{
     $warning = 'Sorry, you must be logged in to submit a post';
  }
}
```

Using Sessions

controllers/post.php

```
if (isset($_POST['update_post'])){
  if(isset($_SESSION['user_id']) && $_SESSION['user_id']==
$_POST['user_id']){
      Post::edit($_POST, $_POST['id']);
  }
  else{
      $warning = 'Sorry, you do not have permissions to edit that post';
  }
}
```

Using Sessions

controllers/post.php

```
if (isset($_POST['delete_post'])) {
    if(isset($_SESSION['user_id']) && $_SESSION['user_id']==
$_POST['user_id']){
        Post::destroy($_POST['id']);
    }
    else{
        $warning = 'Sorry, you do not have permissions to delete that
post';
    }
}
```

Using Sessions

views/posts/list.php

```
<?php if(!isset($_SESSION['user_id'])): ?>
  <div id = "login" class="edit">
    <img class="icon" src='/public/images/pencil.png'/>
    <div class="button-text"> Login</div>
  </div>
<?php else: ?>
   <div id = "logout" class="delete">
    <img class="icon" src='/public/images/delete.png'/>
    <div class="button-text"> Logout</div>
  </div>
<?php endif;?>
```

Frameworks and CMS

CMS:

Wordpress, Drupal, Omeka, Collective Access

Frameworks:

Kohana, CodeIgniter, Symfony, CakePHP, Zend

Books and Resources

php.net

Learning PHP, MySQL and Javascript (Robin Nixon)

PHP for the Web: QuickStart Guide (Larry Ulman)

http://www.w3schools.com/php/default.asp

http://net.tutsplus.com/tutorials/php/20-ways-to-save-kittens-and-learn-php/

Questions?