home.php

lectures/5/src/login/

```
 1: <?
 2:     /**
 3:      * home.php
 4:      *
 5:      * A simple home page for these login demos.
 6:      *
 7:      * David J. Malan
 8:      * Computer Science E-75
 9:      * Harvard Extension School
10:      */
11:
12:     // enable sessions
13:     session_start();
14: ?>
15:
16: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional
.dtd">
17:
18: <html xmlns="http://www.w3.org/1999/xhtml">
19:   <head>
20:     <title>Home</title>
21:   </head>
22:   <body>
23:     <h1>Home</h1>
24:     <h3>
25:       <? if ($_SESSION["authenticated"]) { ?>
26:         You are logged in!
27:         <br />
28:         <a href="logout.php">log out</a>
29:       <? } else { ?>
30:         You are not logged in!
31:       <? } ?>
32:     </h3>
33:     <br />
34:     <b>Login Demos</b>
35:     <ul>
36:       <li><a href="login5.php">version 5</a></li>
37:       <li><a href="login6.php">version 6</a></li>
38:       <li><a href="login7.php">version 7</a></li>
39:       <li><a href="login8.php">version 8</a></li>
40:     </ul>
41:   </body>
42: </html>
```

include.php

lectures/5/src/login/

```
1: <?
2:
3:     // do some stuff
4:
```

```
 1: <?
 2:     /**
 3:      * login5.php
 4:      *
 5:      * A simple login module that checks a username and password
 6:      * against a MySQL table with no encryption.
 7:      *
 8:      * David J. Malan
 9:      * Computer Science E-75
10:      * Harvard Extension School
11:      */
12:
13:     // enable sessions
14:     session_start();
15:
16:     // connect to database
17:     if (($connection = mysql_connect("", "", "")) === FALSE)
18:         die("Could not connect to database");
19:
20:     // select database
21:     if (mysql_select_db("", $connection) === FALSE)
22:         die("Could not select database");
23:
24:     // if username and password were submitted, check them
25:     if (isset($_POST["user"]) && isset($_POST["pass"]))
26:     {
27:         // prepare SQL
28:         $sql = sprintf("SELECT * FROM users WHERE user='%s'",
29:                        mysql_real_escape_string($_POST["user"]));
30:
31:         // execute query
32:         $result = mysql_query($sql);
33:         if ($result === FALSE)
34:             die("Could not query database");
35:
36:         // check whether we found a row
37:         if (mysql_num_rows($result) == 1)
38:         {
39:             // fetch row
40:             $row = mysql_fetch_assoc($result);
41:
42:             // check password
43:             if ($row["pass"] == $_POST["pass"])
44:             {
45:                 // remember that user's logged in
46:                 $_SESSION["authenticated"] = TRUE;
47:
```



```
48:                 // redirect user to home page, using absolute path, per
49:                 // http://us2.php.net/manual/en/function.header.php
50:                 $host = $_SERVER["HTTP_HOST"];
51:                 $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
52:                 header("Location: http://$host$path/home.php");
53:                 exit;
54:             }
55:         }
56:     }
57: ?>
58:
59: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional
.dtd">
60:
61: <html xmlns="http://www.w3.org/1999/xhtml">
62:   <head>
63:     <title>Log In</title>
64:   </head>
65:   <body>
66:     <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
67:       <table>
68:         <tr>
69:           <td>Username:</td>
70:           <td>
71:             <input name="user" type="text" /></td>
72:         </tr>
73:         <tr>
74:           <td>Password:</td>
75:           <td><input name="pass" type="password" /></td>
76:         </tr>
77:         <tr>
78:           <td></td>
79:           <td><input type="submit" value="Log In" /></td>
80:         </tr>
81:       </table>
82:     </form>
83:   </body>
84: </html>
```

```
 1: <?
 2:     /**
 3:      * login6.php
 4:      *
 5:      * A simple login module that checks a username and password
 6:      * against a MySQL table with no encryption by asking for a binary answer.
 7:      *
 8:      * David J. Malan
 9:      * Computer Science E-75
10:      * Harvard Extension School
11:      */
12:
13:     // enable sessions
14:     session_start();
15:
16:     // connect to database
17:     if (($connection = mysql_connect("", "", "")) === FALSE)
18:         die("Could not connect to database");
19:
20:     // select database
21:     if (mysql_select_db("", $connection) === FALSE)
22:         die("Could not select database");
23:
24:     // if username and password were submitted, check them
25:     if (isset($_POST["user"]) && isset($_POST["pass"]))
26:     {
27:         // prepare SQL
28:         $sql = sprintf("SELECT 1 FROM users WHERE user='%s' AND pass='%s'",
29:                        mysql_real_escape_string($_POST["user"]),
30:                        mysql_real_escape_string($_POST["pass"]));
31:
32:         // execute query
33:         $result = mysql_query($sql);
34:         if ($result === FALSE)
35:             die("Could not query database");
36:
37:         // check whether we found a row
38:         if (mysql_num_rows($result) == 1)
39:         {
40:             // remember that user's logged in
41:             $_SESSION["authenticated"] = TRUE;
42:
43:             // redirect user to home page, using absolute path, per
44:             // http://us2.php.net/manual/en/function.header.php
45:             $host = $_SERVER["HTTP_HOST"];
46:             $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
47:             header("Location: http://$host$path/home.php");
```



```
48:             exit;
49:         }
50:     }
51: ?>
52:
53: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional
.dtd">
54:
55: <html xmlns="http://www.w3.org/1999/xhtml">
56:   <head>
57:     <title>Log In</title>
58:   </head>
59:   <body>
60:     <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
61:       <table>
62:         <tr>
63:           <td>Username:</td>
64:           <td>
65:             <input name="user" type="text" /></td>
66:         </tr>
67:         <tr>
68:           <td>Password:</td>
69:           <td><input name="pass" type="password" /></td>
70:         </tr>
71:         <tr>
72:           <td></td>
73:           <td><input type="submit" value="Log In" /></td>
74:         </tr>
75:       </table>
76:     </form>
77:   </body>
78: </html>
```

```
 1: <?
 2:     /**
 3:      * login7.php
 4:      *
 5:      * A simple login module that checks a username and password
 6:      * against a MySQL table with weak encryption (well, a weak hash).
 7:      *
 8:      * David J. Malan
 9:      * Computer Science E-75
10:      * Harvard Extension School
11:      */
12:
13:     // enable sessions
14:     session_start();
15:
16:     // connect to database
17:     if (($connection = mysql_connect("", "", "")) === FALSE)
18:         die("Could not connect to database");
19:
20:     // select database
21:     if (mysql_select_db("", $connection) === FALSE)
22:         die("Could not select database");
23:
24:     // if username and password were submitted, check them
25:     if (isset($_POST["user"]) && isset($_POST["pass"]))
26:     {
27:         // prepare SQL
28:         $sql = sprintf("SELECT 1 FROM users WHERE user='%s' AND pass=PASSWORD('%s')",
29:                        mysql_real_escape_string($_POST["user"]),
30:                        mysql_real_escape_string($_POST["pass"]));
31:
32:         // execute query
33:         $result = mysql_query($sql);
34:         if ($result === FALSE)
35:             die("Could not query database");
36:
37:         // check whether we found a row
38:         if (mysql_num_rows($result) == 1)
39:         {
40:             // remember that user's logged in
41:             $_SESSION["authenticated"] = TRUE;
42:
43:             // redirect user to home page, using absolute path, per
44:             // http://us2.php.net/manual/en/function.header.php
45:             $host = $_SERVER["HTTP_HOST"];
46:             $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
47:             header("Location: http://$host$path/home.php");
```



```
48:             exit;
49:         }
50:     }
51: ?>
52:
53: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional
.dtd">
54:
55: <html xmlns="http://www.w3.org/1999/xhtml">
56:   <head>
57:     <title>Log In</title>
58:   </head>
59:   <body>
60:     <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
61:       <table>
62:         <tr>
63:           <td>Username:</td>
64:           <td>
65:             <input name="user" type="text" /></td>
66:         </tr>
67:         <tr>
68:           <td>Password:</td>
69:           <td><input name="pass" type="password" /></td>
70:         </tr>
71:         <tr>
72:           <td></td>
73:           <td><input type="submit" value="Log In" /></td>
74:         </tr>
75:       </table>
76:     </form>
77:   </body>
78: </html>
```

```
 1: <?
 2:     /**
 3:      * login8.php
 4:      *
 5:      * A simple login module that checks a username and password
 6:      * against a MySQL table with strong encryption (but insecure secret).
 7:      *
 8:      * David J. Malan
 9:      * Computer Science E-75
10:      * Harvard Extension School
11:      */
12:
13:     // enable sessions
14:     session_start();
15:
16:     // connect to database
17:     if (($connection = mysql_connect("", "", "")) === FALSE)
18:         die("Could not connect to database");
19:
20:     // select database
21:     if (mysql_select_db("", $connection) === FALSE)
22:         die("Could not select database");
23:
24:     // if username and password were submitted, check them
25:     if (isset($_POST["user"]) && isset($_POST["pass"]))
26:     {
27:         // prepare SQL
28:         $sql = sprintf("SELECT 1 FROM users WHERE user='%s' AND pass=AES_ENCRYPT('%s', 'secret')",
29:                        mysql_real_escape_string($_POST["user"]),
30:                        mysql_real_escape_string($_POST["pass"]));
31:
32:         // execute query
33:         $result = mysql_query($sql);
34:         if ($result === FALSE)
35:             die("Could not query database");
36:
37:         // check whether we found a row
38:         if (mysql_num_rows($result) == 1)
39:         {
40:             // remember that user's logged in
41:             $_SESSION["authenticated"] = TRUE;
42:
43:             // redirect user to home page, using absolute path, per
44:             // http://us2.php.net/manual/en/function.header.php
45:             $host = $_SERVER["HTTP_HOST"];
46:             $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
47:             header("Location: http://$host$path/home.php");
```



```
48:             exit;
49:         }
50:     }
51: ?>
52:
53: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional
.dtd">
54:
55: <html xmlns="http://www.w3.org/1999/xhtml">
56:   <head>
57:     <title>Log In</title>
58:   </head>
59:   <body>
60:     <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
61:       <table>
62:         <tr>
63:           <td>Username:</td>
64:           <td>
65:             <input name="user" type="text" /></td>
66:         </tr>
67:         <tr>
68:           <td>Password:</td>
69:           <td><input name="pass" type="password" /></td>
70:         </tr>
71:         <tr>
72:           <td></td>
73:           <td><input type="submit" value="Log In" /></td>
74:         </tr>
75:       </table>
76:     </form>
77:   </body>
78: </html>
```

logout.php

lectures/5/src/login/

```
 1: <?
 2:     /**
 3:      * logout.php
 4:      *
 5:      * A simple logout module for all of our login modules.
 6:      *
 7:      * David J. Malan
 8:      * Computer Science E-75
 9:      * Harvard Extension School
10:      */
11:
12:     // enable sessions
13:     session_start();
14:
15:     // delete cookies, if any
16:     setcookie("user", "", time() - 3600);
17:     setcookie("pass", "", time() - 3600);
18:
19:     // log user out
20:     setcookie(session_name(), "", time() - 3600);
21:     session_destroy();
22: ?>
23:
24: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional
.dtd">
25:
26: <html xmlns="http://www.w3.org/1999/xhtml">
27:   <head>
28:     <title>Log Out</title>
29:   </head>
30:   <body>
31:     <h1>You are logged out!</h1>
32:     <h3><a href="home.php">home</a></h3>
33:   </body>
34: </html>
```

lolcat.php

lectures/5/src/lolcat/

```
 1:
 2: <!DOCTYPE html PUBLIC
 3:      "-//W3C//DTD XHTML 1.0 Transitional//EN"
 4:      "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
 5:
 6: <html xmlns="http://www.w3.org/1999/xhtml">
 7:   <head>
 8:     <title>Lolcat of teh Day</title>
 9:   </head>
10:   <body>
11:     <div align="center" style="padding: 20px;">
12:       <h1>Lolcat of teh Day</h1>
13:       <?
14:
15:           $xml = new SimpleXMLElement(file_get_contents("http://feedproxy.google.com/ICanHasCheezburger?format=xml"
));
16:           $item = $xml->channel->item[0];
17:           preg_match("/^.* - (.*)</", $item->description, $matches);
18:           $alt = htmlspecialchars($matches[1], ENT_QUOTES);
19:           $link = $item->link;
20:           foreach ($item->children("http://search.yahoo.com/mrss/") as $content)
21:           {
22:               $attributes = $content->attributes();
23:               $src = $attributes["url"];
24:           }
25:           print("<a href='{$link}'><img alt='{$alt}' border='0' src='{$src}' /></a>");
26:
27:       ?>
28:     </div>
29:   </body>
30: </html>
31:
```

csv.php

lectures/5/src/lunch/development/

```
 1: <?
 2:
 3:     // ensure complete form was submitted
 4:     if (!isset($_POST["name"]) || !isset($_POST["item"]))
 5:     {
 6:         header("Location: http://www.cs75.net/lectures/5/src/lunch/lunch.php");
 7:         exit;
 8:     }
 9:
10:     // open CSV file for appending
11:     $handle = fopen("orders.csv", "a");
12:
13:     // acquire exclusive lock
14:     flock($handle, LOCK_EX);
15:
16:     // add order to CSV file
17:     $order = array($_POST["name"], $_POST["item"]);
18:     fputcsv($handle, $order);
19:     fclose($handle);
20:
21: ?>
22:
23: <!DOCTYPE html PUBLIC
24:      "-//W3C//DTD XHTML 1.0 Transitional//EN"
25:      "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
26:
27: <html xmlns="http://www.w3.org/1999/xhtml">
28:   <head>
29:     <title>Lunch</title>
30:   </head>
31:   <body>
32:     One <?= $_POST["item"] ?> for <?= $_POST["name"] ?>, coming right up!
33:   </body>
34: </html>
```

lunch.php

lectures/5/src/lunch/development/

```
 1: <?
 2:     $xml = new SimpleXMLElement(file_get_contents("menu.xml"));
 3: ?>
 4:
 5: <!DOCTYPE html PUBLIC
 6:      "-//W3C//DTD XHTML 1.0 Transitional//EN"
 7:      "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
 8:
 9: <html xmlns="http://www.w3.org/1999/xhtml">
10:   <head>
11:     <title>Lunch</title>
12:   </head>
13:   <body>
14:     <form action="sqlite.php" method="post">
15:       <b>Name:</b> <input name="name" type="text" /> <input type="submit" value="Submit Order" />
16:       <br /><br />
17:       <table border="0">
18:         <? foreach ($xml->xpath("/menu/category[@name='Specialty Sandwiches']/item") as $item): ?>
19:           <tr>
20:             <td valign="top"><input id="<?= $item["name"] ?>" name="item" type="radio" value="<?= $item["name"] ?>"
/></td>
21:             <td>
22:               <label for="<?= $item["name"] ?>">
23:                 <b><?= $item["name"] ?></b>
24:                 <br />
25:                 <?= $item ?>
26:               </label>
27:             </td>
28:           </tr>
29:         <? endforeach ?>
30:       </table>
31:     </form>
32:   </body>
33: </html>
```

sqlite.php

lectures/5/src/lunch/development/

```
 1: <?
 2:
 3:     // ensure complete form was submitted
 4:     if (!isset($_POST["name"]) || !isset($_POST["item"]))
 5:     {
 6:         header("Location: http://www.cs75.net/lectures/5/src/lunch/lunch.php");
 7:         exit;
 8:     }
 9:
10:     try
11:     {
12:         // open database
13:         $dbh = new PDO("sqlite:orders.db");
14:         $dbh->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
15:
16:         // prepare fields
17:         $name = $dbh->quote($_POST["name"]);
18:         $item = $dbh->quote($_POST["item"]);
19:
20:         // insert order
21:         $dbh->exec("INSERT INTO orders (name, item) VALUES($name, $item)");
22:     }
23:     catch (PDOException $e)
24:     {
25:         die($e->getMessage());
26:     }
27:
28: ?>
29:
30: <!DOCTYPE html PUBLIC
31:      "-//W3C//DTD XHTML 1.0 Transitional//EN"
32:      "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
33:
34: <html xmlns="http://www.w3.org/1999/xhtml">
35:   <head>
36:     <title>Lunch</title>
37:   </head>
38:   <body>
39:     One <?= $_POST["item"] ?> for <?= $_POST["name"] ?>, coming right up!
40:   </body>
41: </html>
```

xml.php

lectures/5/src/lunch/development/

```
 1: <?
 2:
 3:     // ensure complete form was submitted
 4:     if (!isset($_POST["name"]) || !isset($_POST["item"]))
 5:     {
 6:         header("Location: http://www.cs75.net/lectures/5/src/lunch/lunch.php");
 7:         exit;
 8:     }
 9:
10:     // open XML file for reading + writing
11:     $handle = fopen("orders.xml", "r+");
12:
13:     // acquire exclusive lock
14:     flock($handle, LOCK_EX);
15:
16:     // read contents of XML file
17:     $contents = fread($handle, filesize("orders.xml"));
18:
19:     // build DOM out of contents
20:     $xml = new SimpleXMLElement($contents);
21:
22:     // add order
23:     $order = $xml->addChild("order");
24:     $order->addChild("name", $_POST["name"]);
25:     $order->addChild("item", $_POST["item"]);
26:
27:     // overwrite original XML file
28:     rewind($handle);
29:     fwrite($handle, $xml->asXML());
30:     fclose($handle);
31: ?>
32:
33: <!DOCTYPE html PUBLIC
34:      "-//W3C//DTD XHTML 1.0 Transitional//EN"
35:      "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
36:
37: <html xmlns="http://www.w3.org/1999/xhtml">
38:   <head>
39:     <title>Lunch</title>
40:   </head>
41:   <body>
42:     One <?= $_POST["item"] ?> for <?= $_POST["name"] ?>, coming right up!
43:   </body>
44: </html>
```