

```
1: <?php
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:     <?php if ($_SESSION["authenticated"]) { ?>
26:       You are logged in!
27:     <br />
28:     <a href="logout.php">log out</a>
29:   <?php } else { ?>
30:     You are not logged in!
31:   <?php } ?>
32:   </h3>
33:   <br />
34:   <b>Login Demos</b>
35:   <ul>
36:     <li><a href="login5a.php">version 5a</a></li>
37:     <li><a href="login6a.php">version 6a</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>
```

```
1: <?php
2:
3:     // Here are some MySQL login credentials
4:     define("HOST", "localhost");
5:     define("USER", "danallan_lecture");
6:     define("PASS", "welcome$");
7:
8:     // define the database name
9:     define("DB", "danallan_lecture");
```

```
1: <?php
2:
3:     // Here are some MySQL login credentials
4:     define("HOST", "localhost");
5:     define("USER", "danallan_lecture");
6:     define("PASS", "12345");
7:
8:     // define the database name
9:     define("DB", "danallan_lecture");
```

```
1: <?php
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:     * Dan Armendariz
10:    * Computer Science E-75
11:    * Harvard Extension School
12:    */
13:
14:    // get MySQL login data
15:    require "include.php";
16:
17:    // enable sessions
18:    session_start();
19:
20:    // if username and password were submitted, check them
21:    if (isset($_POST["user"]) && isset($_POST["pass"]))
22:    {
23:        // connect to database
24:        if (($connection = mysql_connect(HOST, USER, PASS)) === FALSE)
25:            die("Could not connect to database");
26:
27:        // select database
28:        if (mysql_select_db(DB, $connection) === FALSE)
29:            die("Could not select database");
30:
31:        // prepare SQL
32:        $sql = sprintf("SELECT * FROM users1 WHERE user='%s'",
33:            mysql_real_escape_string($_POST["user"]));
34:
35:        // execute query
36:        $result = mysql_query($sql);
37:        if ($result === FALSE)
38:            die("Could not query database");
39:
40:        // check whether we found a row
41:        if (mysql_num_rows($result) == 1)
42:        {
43:            // fetch row
44:            $row = mysql_fetch_assoc($result);
45:
46:            // check password
47:            if ($row["pass"] == $_POST["pass"])
```

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

```
1: <?php
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:  * Dan Armendariz
10:  * Computer Science E-75
11:  * Harvard Extension School
12:  */
13:
14: // get MySQL login data
15: require "include.php";
16:
17: // enable sessions
18: session_start();
19:
20: // if username and password were submitted, check them
21: if (isset($_POST["user"]) && isset($_POST["pass"]))
22: {
23:     // connect to database
24:     if (($connection = mysql_connect(HOST, USER, PASS)) === FALSE)
25:         die("Could not connect to database");
26:
27:     // select database
28:     if (mysql_select_db(DB, $connection) === FALSE)
29:         die("Could not select database");
30:
31:     // prepare SQL
32:     $sql = sprintf("SELECT 1 FROM users1 WHERE user='%s' AND pass='%s'",
33:         mysql_real_escape_string($_POST["user"]),
34:         mysql_real_escape_string($_POST["pass"]));
35:
36:     // execute query
37:     $result = mysql_query($sql);
38:     if ($result === FALSE)
39:         die("Could not query database");
40:
41:     // check whether we found a row
42:     if (mysql_num_rows($result) == 1)
43:     {
44:         // remember that user's logged in
45:         $_SESSION["authenticated"] = TRUE;
46:
47:         // redirect user to home page, using absolute path, per
```

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

```
1: <?php
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:  * Dan Armendariz
10:  * Computer Science E-75
11:  * Harvard Extension School
12:  */
13:
14: // get MySQL login data
15: require "include.php";
16:
17: // enable sessions
18: session_start();
19:
20: // if username and password were submitted, check them
21: if (isset($_POST["user"]) && isset($_POST["pass"]))
22: {
23:     // connect to database
24:     if (($connection = mysql_connect(HOST, USER, PASS)) === FALSE)
25:         die("Could not connect to database");
26:
27:     // select database
28:     if (mysql_select_db(DB, $connection) === FALSE)
29:         die("Could not select database");
30:
31:     // prepare SQL
32:     $sql = sprintf("SELECT 1 FROM users2 WHERE user='%s' AND pass=PASSWORD('%s')",
33:         mysql_real_escape_string($_POST["user"]),
34:         mysql_real_escape_string($_POST["pass"]));
35:
36:     // execute query
37:     $result = mysql_query($sql);
38:     if ($result === FALSE)
39:         die("Could not query database");
40:
41:     // check whether we found a row
42:     if (mysql_num_rows($result) == 1)
43:     {
44:         // remember that user's logged in
45:         $_SESSION["authenticated"] = TRUE;
46:
47:         // redirect user to home page, using absolute path, per
```

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

```
1: <?php
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:  * Dan Armendariz
10:  * Computer Science E-75
11:  * Harvard Extension School
12:  */
13:
14: // get MySQL login data
15: require "include.php";
16:
17: // enable sessions
18: session_start();
19:
20: // if username and password were submitted, check them
21: if (isset($_POST["user"]) && isset($_POST["pass"]))
22: {
23:     // connect to database
24:     if (($connection = mysql_connect(HOST, USER, PASS)) === FALSE)
25:         die("Could not connect to database");
26:
27:     // select database
28:     if (mysql_select_db(DB, $connection) === FALSE)
29:         die("Could not select database");
30:
31:     // prepare SQL
32:     $sql = sprintf("SELECT 1 FROM users3 WHERE user='%s' AND pass=AES_ENCRYPT('%s', 'secret')",
33:         mysql_real_escape_string($_POST["user"]),
34:         mysql_real_escape_string($_POST["pass"]));
35:
36:     // execute query
37:     $result = mysql_query($sql);
38:     if ($result === FALSE)
39:         die("Could not query database");
40:
41:     // check whether we found a row
42:     if (mysql_num_rows($result) == 1)
43:     {
44:         // remember that user's logged in
45:         $_SESSION["authenticated"] = TRUE;
46:
47:         // redirect user to home page, using absolute path, per
```

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

```
1: <?php
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>
```

```

1: -- phpMyAdmin SQL Dump
2: -- version 2.11.4
3: -- http://www.phpmyadmin.net
4: --
5: -- Host: localhost
6: -- Generation Time: Jul 08, 2009 at 09:37 PM
7: -- Server version: 5.0.45
8: -- PHP Version: 5.2.5
9:
10: SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";
11:
12: --
13: -- Database: 'autox'
14: --
15:
16: -- -----
17:
18: --
19: -- Table structure for table 'cars'
20: --
21:
22: CREATE TABLE 'cars' (
23:   'id' mediumint(9) unsigned NOT NULL auto_increment,
24:   'make' varchar(20) NOT NULL,
25:   'model' varchar(20) NOT NULL,
26:   'year' year(4) NOT NULL,
27:   'class' tinyint(4) unsigned NOT NULL,
28:   PRIMARY KEY ('id')
29: ) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=5 ;
30:
31: --
32: -- Dumping data for table 'cars'
33: --
34:
35: INSERT INTO 'cars' VALUES(1, 'Ford', 'Pinto', 1975, 5);
36: INSERT INTO 'cars' VALUES(2, 'Volkswagen', 'Beetle', 1971, 4);
37: INSERT INTO 'cars' VALUES(4, 'Porsche', '911 GT3 RS', 2008, 1);
38:
39: -- -----
40:
41: --
42: -- Table structure for table 'drivers'
43: --
44:
45: CREATE TABLE 'drivers' (
46:   'id' int(11) unsigned NOT NULL auto_increment,
47:   'name' varchar(255) NOT NULL,

```

```

48:   'age' smallint(6) NOT NULL,
49:   'year_started' year(4) NOT NULL,
50:   PRIMARY KEY ('id')
51: ) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=5 ;
52:
53: --
54: -- Dumping data for table 'drivers'
55: --
56:
57: INSERT INTO 'drivers' VALUES(1, 'John Harvard', 27, 2006);
58: INSERT INTO 'drivers' VALUES(2, 'Jane Harvard', 30, 2004);
59: INSERT INTO 'drivers' VALUES(3, 'John Smith', 18, 2008);
60: INSERT INTO 'drivers' VALUES(4, 'Jane Doe', 32, 2000);
61:
62: -- -----
63:
64: --
65: -- Table structure for table 'events'
66: --
67:
68: CREATE TABLE 'events' (
69:   'id' int(10) unsigned NOT NULL auto_increment,
70:   'date' datetime NOT NULL,
71:   'description' varchar(255) NOT NULL,
72:   PRIMARY KEY ('id')
73: ) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=3 ;
74:
75: --
76: -- Dumping data for table 'events'
77: --
78:
79: INSERT INTO 'events' VALUES(1, '2009-06-27 14:30:36', 'Held at Devens Airport in Ayer, MA. Dry conditions in the mo
rning but pouring rain in the afternoon.');
```

```

80: INSERT INTO 'events' VALUES(2, '2009-07-04 14:32:13', 'A sunny and warm 4th of July autocross.');
```

```

81:
82: -- -----
83:
84: --
85: -- Table structure for table 'times'
86: --
87:
88: CREATE TABLE 'times' (
89:   'driver_id' int(11) unsigned NOT NULL,
90:   'event_id' int(11) unsigned NOT NULL,
91:   'car_id' mediumint(8) unsigned NOT NULL,
92:   'am_run1' decimal(6,3) NOT NULL,
93:   'am_run2' decimal(6,3) NOT NULL,

```

```
94: 'pm_run1' decimal(6,3) NOT NULL,
95: 'pm_run2' decimal(6,3) NOT NULL,
96: PRIMARY KEY ('driver_id','event_id','car_id')
97: ) ENGINE=MyISAM DEFAULT CHARSET=latin1;
98:
99: --
100: -- Dumping data for table 'times'
101: --
102:
103: INSERT INTO 'times' VALUES(4, 1, 3, 68.043, 64.001, 72.023, 71.120);
104: INSERT INTO 'times' VALUES(1, 1, 1, 72.560, 70.230, 76.540, 75.890);
105: INSERT INTO 'times' VALUES(4, 2, 4, 50.060, 45.780, 45.455, 43.223);
```

```
1: -- phpMyAdmin SQL Dump
2: -- http://www.phpmyadmin.net
3:
4: SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";
5:
6: -- -----
7:
8: --
9: -- Table structure for table 'users1'
10: --
11:
12: CREATE TABLE 'users1' (
13: 'user' varchar(8) NOT NULL,
14: 'pass' varchar(8) NOT NULL,
15: PRIMARY KEY ('user')
16: ) ENGINE=MyISAM DEFAULT CHARSET=latin1;
17:
18: --
19: -- Dumping data for table 'users1'
20: --
21:
22: INSERT INTO 'users1' VALUES('jharvard', 'crimson');
23: INSERT INTO 'users1' VALUES('jane', 'crimson');
24:
```



```
1: -- phpMyAdmin SQL Dump
2: -- http://www.phpmyadmin.net
3:
4: SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";
5:
6: -- -----
7:
8: --
9: -- Table structure for table 'users2'
10: --
11:
12: CREATE TABLE 'users2' (
13:   'user' varchar(8) NOT NULL,
14:   'pass' varchar(255) NOT NULL,
15:   PRIMARY KEY ('user')
16: ) ENGINE=MyISAM DEFAULT CHARSET=latin1;
17:
18: --
19: -- Dumping data for table 'users2'
20: --
21:
22: INSERT INTO 'users2' VALUES('jharvard', '*02A501BC718BBD7927FC5805D858811E3C3F1825');
23:
```

```
1: -- phpMyAdmin SQL Dump
2: -- http://www.phpmyadmin.net
3:
4: SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";
5:
6: -- -----
7:
8: --
9: -- Table structure for table 'users3'
10: --
11:
12: CREATE TABLE 'users3' (
13:   'user' varchar(8) NOT NULL,
14:   'pass' varbinary(255) NOT NULL,
15:   PRIMARY KEY ('user')
16: ) ENGINE=MyISAM DEFAULT CHARSET=latin1;
17:
18: --
19: -- Dumping data for table 'users3'
20: --
21:
22: INSERT INTO 'users3' VALUES('jharvard', 'ÃĤ$g&ÂiÂ\213Â«-Z\024dÂ\217Â»Â\2264i');
```