```
<?
    /**
     * home.php
     *
     * A simple home page for these login demos.
     *
     * David J. Malan
     * Computer Science E-75
     * Harvard Extension School
     */

    // enable sessions
    session_start();
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Home</title>
  </head>
  <body>
    <h1>Home</h1>
    <h3>
      <? if ($_SESSION["authenticated"]) { ?>
        You are logged in!
        <br />
        <a href="logout.php">log out</a>
      <? } else { ?>
        You are not logged in!
      <? } ?>
    </h3>
    <br />
    <b>Login Demos</b>
    <ul>
      <li><a href="login1.php">version 1</a></li>
      <li><a href="login2.php">version 2</a></li>
      <li><a href="login3.php">version 3</a></li>
      <li><a href="login4.php">version 4</a></li>
      <li><a href="login5.php">version 5</a></li>
      <li><a href="login6.php">version 6</a></li>
      <li><a href="login7.php">version 7</a></li>
      <li><a href="login8.php">version 8</a></li>
      <li><a href="login9.php">version 9</a></li>
    </ul>
  </body>
</html>
```

```
<?
    /**
     * login1.php
     *
     * A simple login module.
     *
     * David J. Malan
     * Computer Science E-75
     * Harvard Extension School
     */

    // enable sessions
    session_start();

    // were this not a demo, these would be in some database
    define("USER", "jharvard");
    define("PASS", "crimson");

    // if username and password were submitted, check them
    if (isset($_POST["user"]) && isset($_POST["pass"]))
    {
        // if username and password are valid, log user in
        if ($_POST["user"] == USER && $_POST["pass"] == PASS)
        {
            // remember that user's logged in
            $_SESSION["authenticated"] = TRUE;

            // redirect user to home page, using absolute path, per
            // http://us2.php.net/manual/en/function.header.php
            $host = $_SERVER["HTTP_HOST"];
            $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
            header("Location: http://$host$path/home.php");
            exit;
        }
    }
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Log In</title>
  </head>
  <body>
    <? if (count($_POST) > 0) echo "INVALID LOGIN"; ?>
    <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
      <table>
```

```
        <tr>
          <td>Username:</td>
          <td><input name="user" type="text" value="<? echo $_POST["user"]; ?>" /></td>
        </tr>
        <tr>
          <td>Password:</td>
          <td><input name="pass" type="password" /></td>
        </tr>
        <tr>
          <td></td>
          <td><input type="submit" value="Log In" /></td>
        </tr>
      </table>
    </form>
  </body>
</html>
```

```
<?
    /**
     * login2.php
     *
     * A simple login module that pre-populates the username field
     * upon failed login, just in case user simply mistyped password.
     *
     * David J. Malan
     * Computer Science E-75
     * Harvard Extension School
     */

    // enable sessions
    session_start();

    // were this not a demo, these would be in some database
    define("USER", "jharvard");
    define("PASS", "crimson");

    // if username and password were submitted, check them
    if (isset($_POST["user"]) && isset($_POST["pass"]))
    {
        // if username and password are valid, log user in
        if ($_POST["user"] == USER && $_POST["pass"] == PASS)
        {
            // remember that user's logged in
            $_SESSION["authenticated"] = TRUE;

            // redirect user to home page, using absolute path, per
            // http://us2.php.net/manual/en/function.header.php
            $host = $_SERVER["HTTP_HOST"];
            $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
            header("Location: http://$host$path/home.php");
            exit;
        }
    }
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Log In</title>
  </head>
  <body>
    <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
      <table>
```

```
        <tr>
          <td>Username:</td>
          <td><input name="user" type="text" value="<? echo $_POST["user"]; ?>" /></td>
        </tr>
        <tr>
          <td>Password:</td>
          <td><input name="pass" type="password" /></td>
        </tr>
        <tr>
          <td></td>
          <td><input type="submit" value="Log In" /></td>
        </tr>
      </table>
    </form>
  </body>
</html>
```

```
<?
    /**
     * login3.php
     *
     * A simple login module that remembers username of most recently
     * authenticated user so that it can pre-populate the username
     * field next time.
     *
     * David J. Malan
     * Computer Science E-75
     * Harvard Extension School
     */

    // enable sessions
    session_start();

    // were this not a demo, these would be in some database
    define("USER", "jharvard");
    define("PASS", "crimson");

    // if username and password were submitted, check them
    if (isset($_POST["user"]) && isset($_POST["pass"]))
    {
        // if username and password are valid, log user in
        if ($_POST["user"] == USER && $_POST["pass"] == PASS)
        {
            // remember that user's logged in
            $_SESSION["authenticated"] = TRUE;

            // save username in cookie for a week
            setcookie("user", $_POST["user"], time() + 7 * 24 * 60 * 60);

            // redirect user to home page, using absolute path, per
            // http://us2.php.net/manual/en/function.header.php
            $host = $_SERVER["HTTP_HOST"];
            $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
            header("Location: http://$host$path/home.php");
            exit;
        }
    }
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Log In</title>
```

```
  </head>
  <body>
    <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
      <table>
        <tr>
          <td>Username:</td>
          <td><input name="user" type="text" value="<? echo ($_POST["user"]) ? $_POST["user"] : $_COOKIE["user"]; ?>" /></
td>
        </tr>
        <tr>
          <td>Password:</td>
          <td><input name="pass" type="password" /></td>
        </tr>
        <tr>
          <td></td>
          <td><input type="submit" value="Log In" /></td>
        </tr>
      </table>
    </form>
  </body>
</html>
```

```
<?
    /**
     * login4.php
     *
     * A simple login module that lets a user stay logged in
     * by saving username and, ack, password in cookies.
     *
     * David J. Malan
     * Computer Science E-75
     * Harvard Extension School
     */

    // enable sessions
    session_start();

    // were this not a demo, these would be in some database
    define("USER", "jharvard");
    define("PASS", "crimson");

    // if username and password were saved in cookie, check them
    if (isset($_COOKIE["user"]) && isset($_COOKIE["pass"]))
    {
        // if username and password are valid, log user back in
        if ($_COOKIE["user"] == USER && $_COOKIE["pass"] == PASS)
        {
            // remember that user's logged in
            $_SESSION["authenticated"] = TRUE;

            // re-save username and, ack, password in cookies for another week
            setcookie("user", $_COOKIE["user"], time() + 7 * 24 * 60 * 60);
            setcookie("pass", $_COOKIE["pass"], time() + 7 * 24 * 60 * 60);

            // redirect user to home page, using absolute path, per
            // http://us2.php.net/manual/en/function.header.php
            $host = $_SERVER["HTTP_HOST"];
            $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
            header("Location: http://$host$path/home.php");
            exit;
        }
    }

    // else if username and password were submitted, grab them instead
    else if (isset($_POST["user"]) && isset($_POST["pass"]))
    {
        // if username and password are valid, log user in
        if ($_POST["user"] == USER && $_POST["pass"] == PASS)
        {
```

```
            // remember that user's logged in
            $_SESSION["authenticated"] = TRUE;

            // save username in cookie for a week
            setcookie("user", $_POST["user"], time() + 7 * 24 * 60 * 60);

            // save password in, ack, cookie for a week if requested
            if ($_POST["keep"])
                setcookie("pass", $_POST["pass"], time() + 7 * 24 * 60 * 60);

            // redirect user to home page, using absolute path, per
            // http://us2.php.net/manual/en/function.header.php
            $host = $_SERVER['HTTP_HOST'];
            $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
            header("Location: http://$host$path/home.php");
            exit;
        }
    }
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Log In</title>
  </head>
  <body>
    <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
      <table>
        <tr>
          <td>Username:</td>
          <td><input name="user" type="text" value="<? echo ($_POST["user"]) ? $_POST["user"] : $_COOKIE["user"]; ?>" /></
td>
        </tr>
        <tr>
          <td>Password:</td>
          <td><input name="pass" type="password" /></td>
        </tr>
        <tr>
          <td></td>
          <td><input name="keep" type="checkbox" />   keep me logged in until I click <b>log out</b></td>
        </tr>
        <tr>
          <td></td>
          <td><input type="submit" value="Log In" /></td>
        </tr>
      </table>
```

```
    </form>
  </body>
</html>
```

```
<?
    /**
     * login5.php
     *
     * A simple login module that checks a username and password
     * against a MySQL table with no encryption.
     *
     * David J. Malan
     * Computer Science E-75
     * Harvard Extension School
     */

    // enable sessions
    session_start();

    // connect to database
    if (($connection = mysql_connect("", "", "")) === FALSE)
        die("Could not connect to database");

    // select database
    if (mysql_select_db("", $connection) === FALSE)
        die("Could not select database");

    // if username and password were submitted, check them
    if (isset($_POST["user"]) && isset($_POST["pass"]))
    {
        // prepare SQL
        $sql = sprintf("SELECT * FROM users WHERE user='%s'",
                       mysql_real_escape_string($_POST["user"]));

        // execute query
        $result = mysql_query($sql);
        if ($result === FALSE)
            die("Could not query database");

        // check whether we found a row
        if (mysql_num_rows($result) == 1)
        {
            // fetch row
            $row = mysql_fetch_assoc($result);

            // check password
            if ($row["pass"] == $_POST["pass"])
            {
                // remember that user's logged in
                $_SESSION["authenticated"] = TRUE;
```

```
                // redirect user to home page, using absolute path, per
                // http://us2.php.net/manual/en/function.header.php
                $host = $_SERVER["HTTP_HOST"];
                $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
                header("Location: http://$host$path/home.php");
                exit;
            }
        }
    }
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Log In</title>
  </head>
  <body>
    <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
      <table>
        <tr>
          <td>Username:</td>
          <td>
            <input name="user" type="text" /></td>
        </tr>
        <tr>
          <td>Password:</td>
          <td><input name="pass" type="password" /></td>
        </tr>
        <tr>
          <td></td>
          <td><input type="submit" value="Log In" /></td>
        </tr>
      </table>
    </form>
  </body>
</html>
```

```
<?
    /**
     * login6.php
     *
     * A simple login module that checks a username and password
     * against a MySQL table with no encryption by asking for a binary answer.
     *
     * David J. Malan
     * Computer Science E-75
     * Harvard Extension School
     */

    // enable sessions
    session_start();

    // connect to database
    if (($connection = mysql_connect("", "", "")) === FALSE)
        die("Could not connect to database");

    // select database
    if (mysql_select_db("", $connection) === FALSE)
        die("Could not select database");

    // if username and password were submitted, check them
    if (isset($_POST["user"]) && isset($_POST["pass"]))
    {
        // prepare SQL
        $sql = sprintf("SELECT 1 FROM users WHERE user='%s' AND pass='%s'",
                       mysql_real_escape_string($_POST["user"]),
                       mysql_real_escape_string($_POST["pass"]));

        // execute query
        $result = mysql_query($sql);
        if ($result === FALSE)
            die("Could not query database");

        // check whether we found a row
        if (mysql_num_rows($result) == 1)
        {
            // remember that user's logged in
            $_SESSION["authenticated"] = TRUE;

            // redirect user to home page, using absolute path, per
            // http://us2.php.net/manual/en/function.header.php
            $host = $_SERVER["HTTP_HOST"];
            $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
            header("Location: http://$host$path/home.php");
```

```
            exit;
        }
    }
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Log In</title>
  </head>
  <body>
    <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
      <table>
        <tr>
          <td>Username:</td>
          <td>
            <input name="user" type="text" /></td>
        </tr>
        <tr>
          <td>Password:</td>
          <td><input name="pass" type="password" /></td>
        </tr>
        <tr>
          <td></td>
          <td><input type="submit" value="Log In" /></td>
        </tr>
      </table>
    </form>
  </body>
</html>
```

```
<?
    /**
     * login7.php
     *
     * A simple login module that checks a username and password
     * against a MySQL table with weak encryption (well, a weak hash).
     *
     * David J. Malan
     * Computer Science E-75
     * Harvard Extension School
     */

    // enable sessions
    session_start();

    // connect to database
    if (($connection = mysql_connect("", "", "")) === FALSE)
        die("Could not connect to database");

    // select database
    if (mysql_select_db("", $connection) === FALSE)
        die("Could not select database");

    // if username and password were submitted, check them
    if (isset($_POST["user"]) && isset($_POST["pass"]))
    {
        // prepare SQL
        $sql = sprintf("SELECT 1 FROM users WHERE user='%s' AND pass=PASSWORD('%s')",
                       mysql_real_escape_string($_POST["user"]),
                       mysql_real_escape_string($_POST["pass"]));

        // execute query
        $result = mysql_query($sql);
        if ($result === FALSE)
            die("Could not query database");

        // check whether we found a row
        if (mysql_num_rows($result) == 1)
        {
            // remember that user's logged in
            $_SESSION["authenticated"] = TRUE;

            // redirect user to home page, using absolute path, per
            // http://us2.php.net/manual/en/function.header.php
            $host = $_SERVER["HTTP_HOST"];
            $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
            header("Location: http://$host$path/home.php");
```

```
            exit;
        }
    }
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Log In</title>
  </head>
  <body>
    <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
      <table>
        <tr>
          <td>Username:</td>
          <td>
            <input name="user" type="text" /></td>
        </tr>
        <tr>
          <td>Password:</td>
          <td><input name="pass" type="password" /></td>
        </tr>
        <tr>
          <td></td>
          <td><input type="submit" value="Log In" /></td>
        </tr>
      </table>
    </form>
  </body>
</html>
```

```
<?
    /**
     * login8.php
     *
     * A simple login module that checks a username and password
     * against a MySQL table with strong encryption (but insecure secret).
     *
     * David J. Malan
     * Computer Science E-75
     * Harvard Extension School
     */

    // enable sessions
    session_start();

    // connect to database
    if (($connection = mysql_connect("", "", "")) === FALSE)
        die("Could not connect to database");

    // select database
    if (mysql_select_db("", $connection) === FALSE)
        die("Could not select database");

    // if username and password were submitted, check them
    if (isset($_POST["user"]) && isset($_POST["pass"]))
    {
        // prepare SQL
        $sql = sprintf("SELECT 1 FROM users WHERE user='%s' AND pass=AES_ENCRYPT('%s', 'secret')",
                       mysql_real_escape_string($_POST["user"]),
                       mysql_real_escape_string($_POST["pass"]));

        // execute query
        $result = mysql_query($sql);
        if ($result === FALSE)
            die("Could not query database");

        // check whether we found a row
        if (mysql_num_rows($result) == 1)
        {
            // remember that user's logged in
            $_SESSION["authenticated"] = TRUE;

            // redirect user to home page, using absolute path, per
            // http://us2.php.net/manual/en/function.header.php
            $host = $_SERVER["HTTP_HOST"];
            $path = rtrim(dirname($_SERVER["PHP_SELF"]), "/\\");
            header("Location: http://$host$path/home.php");
```

```
            exit;
        }
    }
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Log In</title>
  </head>
  <body>
    <form action="<? echo $_SERVER["PHP_SELF"]; ?>" method="post">
      <table>
        <tr>
          <td>Username:</td>
          <td>
            <input name="user" type="text" /></td>
        </tr>
        <tr>
          <td>Password:</td>
          <td><input name="pass" type="password" /></td>
        </tr>
        <tr>
          <td></td>
          <td><input type="submit" value="Log In" /></td>
        </tr>
      </table>
    </form>
  </body>
</html>
```

```
<?
    /**
     * logout.php
     *
     * A simple logout module for all of our login modules.
     *
     * David J. Malan
     * Computer Science E-75
     * Harvard Extension School
     */

    // enable sessions
    session_start();

    // delete cookies, if any
    setcookie("user", "", time() - 3600);
    setcookie("pass", "", time() - 3600);

    // log user out
    setcookie(session_name(), "", time() - 3600);
    session_destroy();
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Log Out</title>
  </head>
  <body>
    <h1>You are logged out!</h1>
    <h3><a href="home.php">home</a></h3>
  </body>
</html>
```

```
-- phpMyAdmin SQL Dump
-- http://www.phpmyadmin.net

SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";

-- --------------------------------------------------------

--
-- Table structure for table ‘users‘
--

CREATE TABLE ‘users‘ (
  ‘user‘ varchar(8) NOT NULL,
  ‘password‘ varchar(8) NOT NULL,
  PRIMARY KEY  (‘user‘)
) ENGINE=MyISAM DEFAULT CHARSET=latin1;

--
-- Dumping data for table ‘users‘
--

INSERT INTO ‘users‘ VALUES(’jharvard’, ’crimson’);
INSERT INTO ‘users‘ VALUES(’jane’, ’crimson’);
```

```
-- phpMyAdmin SQL Dump
-- http://www.phpmyadmin.net

SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";

-- --------------------------------------------------------

--
-- Table structure for table ‘users‘
--

CREATE TABLE ‘users‘ (
  ‘user‘ varchar(8) NOT NULL,
  ‘pass‘ varchar(255) NOT NULL,
  PRIMARY KEY  (‘user‘)
) ENGINE=MyISAM DEFAULT CHARSET=latin1;

--
-- Dumping data for table ‘users‘
--

INSERT INTO ‘users‘ VALUES(’jharvard’, ’*02A501BC718BBD7927FC5805D858811E3C3F1825’);
```