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

SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";

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

--
-- Table structure for table ‘customers‘
--

CREATE TABLE ‘customers‘ (
  ‘id‘ int(10) unsigned NOT NULL auto_increment,
  ‘name‘ varchar(255) NOT NULL,
  ‘street‘ varchar(255) NOT NULL,
  ‘city‘ varchar(255) NOT NULL,
  ‘state‘ varchar(255) NOT NULL,
  ‘zip‘ varchar(10) NOT NULL,
  ‘lastmod‘ timestamp NOT NULL default CURRENT_TIMESTAMP on update CURRENT_TIMESTAMP,
  PRIMARY KEY  (‘id‘),
  KEY ‘name‘ (‘name‘)
) ENGINE=MyISAM  DEFAULT CHARSET=latin1 AUTO_INCREMENT=3 ;
```

```
<?
    /**
     * login9.php
     *
     * A simple login module that lets a user stay logged in by saving
     * username and (in theory) a randomly generated token in a MySQL table.
     *
     * 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");

    // check for token
    if (isset($_COOKIE["user"]) && isset($_COOKIE["token"]))
    {
        // prepare SQL
        $sql = sprintf("SELECT 1 FROM tokens WHERE user='%s' AND token='%s'",
                       mysql_real_escape_string($_COOKIE["user"]),
                       mysql_real_escape_string($_COOKIE["token"]));

        // 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;
    }
}

// else if username and password were submitted, check them
else 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;

        // remember user if requested
        if ($_POST["keep"])
        {
            // (pretend to) generate a token
            $token = "123456789";

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

            // prepare SQL
            $sql = sprintf("INSERT INTO tokens (user, token) VALUES('%s', '%s') " .
                           "ON DUPLICATE KEY UPDATE token=VALUES(token)",
                           mysql_real_escape_string($_POST["user"]), $token);

            // remember token
            if (mysql_query($sql) === FALSE)
                die("Could not insert into database");
        }

        // 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 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>
```