```php
<!-- index.php -->
<!DOCTYPE html>

<?php
$dbhost="localhost";
$dbuser = "root";
$dbpass = null;
$dbname = "highfashion";

$conn = mysqli_connect($dbhost, $dbuser, $dbpass);
if(!$conn) die("Connection failed: " . mysqli_connect_error());

mysqli_select_db($conn, $dbname) || die('Corrupted database: ' .
mysqli_error($conn));

$query="SELECT * FROM poses;";
$queryres = mysqli_query($conn, $query);
if(!$queryres) die('Invalid query: ' . mysqli_error($conn));
mysqli_close($conn);

if(isset($_POST["setfavpose"]))
    setcookie("favposeid", $_POST["setfavpose"], time() + (86400 *
    30), "/");
?>

<html>
<body>

<h1>High Fashion Poses!!!</h1>
<img src="derek_and_hansel.jpg" alt="Derek and Hansel" width="400">

<h2>Look for a pose</h2>
<ul>
<?php
//iterate over poses
while ($row = mysqli_fetch_assoc($queryres)) {
    $poseid = $row["id"];
    $posename = $row["name"];
    echo "<li>" . $posename . ": <a href=\"viewpose.php?id=" . $poseid
    . "\">see this pose and astonish!</a></li>\n";
}
?>

<h1>View your favourite pose (if any)</h1>
<a href="viewfav.php">Click here</a>

```

```
44 <h2>If you are allowed to, see the flag</h2>
45 <a href="flag/flag.txt">Click here</a>
46
47 </body>
48 </html>
49
50
```

```php
<!-- viewpose.php -->
<!DOCTYPE html>

<?php
if(!isset($_GET["id"])) die('Invalid request');
$poseid = $_GET["id"];

switch($poseid){
    case "magnum":
        $descr_path = "descr/magnum.txt";
    break;
    case "bluesteel":
        $descr_path = "descr/bluesteel.txt";
    break;
    case "ferrari":
        $descr_path = "descr/ferrari.txt";
    break;
    case "letigre":
        $descr_path = "descr/letigre.txt";
    break;
    case "hansellook":
        $descr_path = "descr/hansellook.txt";
    break;
    default:
        die('Invalid request');
}

$dbhost="localhost";
$dbuser = "root";
$dbpass = null;
$dbname = "highfashion";

$conn = mysqli_connect($dbhost, $dbuser, $dbpass);
if(!$conn) die("Connection failed: " . mysqli_connect_error());

mysqli_select_db($conn, $dbname) || die('Corrupted database: ' .
mysqli_error($conn));

$query="SELECT * FROM poses WHERE id='" . $poseid . "';";
$queryres = mysqli_query($conn, $query);
if(!$queryres) die('Invalid query: ' . mysqli_error($conn));

$row = mysqli_fetch_assoc($queryres);
if(!$row) die('Unknown pose.');
$posename = $row["name"];
$posepicturepath = $row["picturepath"];
```

```
46 if(!$posename || !$posepicturepath) die('Corrupted database: ' .
   mysqli_error($conn));
47
48 mysqli_close($conn);
49
50 $posedescr = file_get_contents($descr_path);
51 if(!$posedescr) die('Error in file_get_content');
52 ?>
53
54 <html>
55 <body>
56
57 <h1>High Fashion Poses!</h1>
58 <p>This is... <?php echo $posename; ?></p>
59 <img src="<?php echo $posepicturepath;?>" alt="<?php echo
   $posename;?>" width="500"><br/>
60 <p><?php echo $posedescr;?></p>
61
62 <form action="index.php" method="post">
63 <input type="submit" value="Set it as favourite and return to pose
   list"/>
64 <input type="hidden" name="setfavpose" value="<?php echo $poseid;
   ?>"/>
65 </form>
66
67 <h1>Return to the pose list</h1>
68 <a href="index.php">Click here</a>
69
70 <h1>If you are allowed to, see the flag</h1>
71 <a href="flag/flag.txt">Click here</a>
72
73 </body>
74 </html>
75
76
```

```php
<!-- viewfav.php -->
<!DOCTYPE html>

<?php
if(!isset($_COOKIE["favposeid"])) die('Invalid request');

$poseid = $_COOKIE["favposeid"];
$descr_path = "descr/" . $poseid . ".txt";

$dbhost="localhost";
$dbuser = "root";
$dbpass = null;
$dbname = "highfashion";

$conn = mysqli_connect($dbhost, $dbuser, $dbpass);
if(!$conn) die("Connection failed: " . mysqli_connect_error());

mysqli_select_db($conn, $dbname) || die('Corrupted database: ' .
mysqli_error($conn));

$query="SELECT * FROM poses WHERE id='" .
mysqli_real_escape_string($conn, $poseid) . "';";
$queryres = mysqli_query($conn, $query);
if(!$queryres) die('Invalid query: ' . mysqli_error($conn));

$row = mysqli_fetch_assoc($queryres);
if(!$row){
    $posename = "(unknown pose)";
    $posepicturepath = "derek_and_hansel.jpg";
}
else{
    $posename = $row["name"];
    $posepicturepath = $row["picturepath"];
    if(!$posename || !$posepicturepath) die('Corrupted database: ' .
    mysqli_error($conn));
}

mysqli_close($conn);

$posedescr = file_get_contents($descr_path);
if(!$posedescr) die('Error in file_get_content');
?>

<html>
<body>

```

```
44 <h1>High Fashion Poses!</h1>
45 <p>This is... <?php echo $posename; ?></p>
46 <img src="<?php echo $posepicturepath;?>" alt="<?php echo
   $posename;?>" width="500"><br/>
47 <p><?php echo $posedescr;?></p>
48
49 <h1>Return to the pose list</h1>
50 <a href="index.php">Click here</a>
51
52 <h1>If you are allowed to, see the flag</h1>
53 <a href="flag/flag.txt">Click here</a>
54
55 </body>
56 </html>
57
```