

```
1 <!-- index.php -->
2 <!DOCTYPE html>
3
4 <?php
5 $dbhost="localhost";
6 $dbuser = "root";
7 $dbpass = null;
8 $dbname = "highfashion";
9
10 $conn = mysqli_connect($dbhost, $dbuser, $dbpass);
11 if(!$conn) die("Connection failed: " . mysqli_connect_error());
12
13 mysqli_select_db($conn, $dbname) || die('Corrupted database: ' .
    mysqli_error($conn));
14
15 $query="SELECT * FROM poses;";
16 $queryres = mysqli_query($conn, $query);
17 if(!$queryres) die('Invalid query: ' . mysqli_error($conn));
18 mysqli_close($conn);
19
20 if(isset($_POST["setfavpose"]))
21     setcookie("favposeid", $_POST["setfavpose"], time() + (86400 *
        30), "/");
22 ?>
23
24 <html>
25 <body>
26
27 <h1>High Fashion Poses!!!</h1>
28 
29
30 <h2>Look for a pose</h2>
31 <ul>
32 <?php
33 //iterate over poses
34 while ($row = mysqli_fetch_assoc($queryres)) {
35     $poseid = $row["id"];
36     $posename = $row["name"];
37     echo "<li>" . $posename . ": <a href=\"viewpose.php?id=" . $poseid
        . "\">see this pose and astonish!</a></li>\n";
38 }
39 ?>
40
41 <h1>View your favourite pose (if any)</h1>
42 <a href="viewfav.php">Click here</a>
43
```

```
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
```

```
1 <!-- viewpose.php -->
2 <!DOCTYPE html>
3
4 <?php
5 if(!isset($_GET["id"])) die('Invalid request');
6 $poseid = $_GET["id"];
7
8 switch($poseid){
9     case "magnum":
10         $descr_path = "descr/magnum.txt";
11         break;
12     case "bluesteel":
13         $descr_path = "descr/bluesteel.txt";
14         break;
15     case "ferrari":
16         $descr_path = "descr/ferrari.txt";
17         break;
18     case "letigre":
19         $descr_path = "descr/letigre.txt";
20         break;
21     case "hansellook":
22         $descr_path = "descr/hansellook.txt";
23         break;
24     default:
25         die('Invalid request');
26 }
27
28 $dbhost="localhost";
29 $dbuser = "root";
30 $dbpass = null;
31 $dbname = "highfashion";
32
33 $conn = mysqli_connect($dbhost, $dbuser, $dbpass);
34 if(!$conn) die("Connection failed: " . mysqli_connect_error());
35
36 mysqli_select_db($conn, $dbname) || die('Corrupted database: ' .
    mysqli_error($conn));
37
38 $query="SELECT * FROM poses WHERE id='" . $poseid . "'";
39 $queryres = mysqli_query($conn, $query);
40 if(!$queryres) die('Invalid query: ' . mysqli_error($conn));
41
42 $row = mysqli_fetch_assoc($queryres);
43 if(!$row) die('Unknown pose.');
```

```
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 " 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
```

```
1 <!-- viewfav.php -->
2 <!DOCTYPE html>
3
4 <?php
5 if(!isset($_COOKIE["favposeid"])) die('Invalid request');
6
7 $poseid = $_COOKIE["favposeid"];
8 $descr_path = "descr/" . $poseid . ".txt";
9
10 $dbhost="localhost";
11 $dbuser = "root";
12 $dbpass = null;
13 $dbname = "highfashion";
14
15 $conn = mysqli_connect($dbhost, $dbuser, $dbpass);
16 if(!$conn) die("Connection failed: " . mysqli_connect_error());
17
18 mysqli_select_db($conn, $dbname) || die('Corrupted database: ' .
    mysqli_error($conn));
19
20 $query="SELECT * FROM poses WHERE id='" .
    mysqli_real_escape_string($conn, $poseid) . "'";
21 $queryres = mysqli_query($conn, $query);
22 if(!$queryres) die('Invalid query: ' . mysqli_error($conn));
23
24 $row = mysqli_fetch_assoc($queryres);
25 if(!$row){
26     $posename = "(unknown pose)";
27     $posepicturepath = "derek_and_hansel.jpg";
28 }
29 else{
30     $posename = $row["name"];
31     $posepicturepath = $row["picturepath"];
32     if(!$posename || !$posepicturepath) die('Corrupted database: ' .
        mysqli_error($conn));
33 }
34
35 mysqli_close($conn);
36
37 $posedescr = file_get_contents($descr_path);
38 if(!$posedescr) die('Error in file_get_content');
39 ?>
40
41 <html>
42 <body>
43
```

```
44 <h1>High Fashion Poses!</h1>
45 <p>This is... <?php echo $posename; ?></p>
46 " 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
```