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

<?php
$studentname = getenv('STUDENTNAME');
if(!isset($_POST["poemtitle"]) || !isset($_FILES["poemfile"])) die('Invalid request');

$poemtitle = $_POST["poemtitle"];
$target_dir = "poems/" . $poemtitle . "/";
//$target_file = $target_dir . basename($_FILES["poemfile"]["name"]);
$target_file = $target_dir . basename($_FILES["poemfile"]["name"]);
$uploadOk = 1;
// Check titleiption format (max 30 chars, no spaces)
if(strlen($poemtitle) > 30 || strpos($poemtitle, ' ') !== false) die("Poem title is > 30 or has spaces.");

// Check file size
if ($_FILES["poemfile"]["size"] > 5000) die("Sorry, your peom is too long.");

// Allow only txt file formats
$poemFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
if($poemFileType != "txt" ) die("Sorry, only txt files are allowed.");

// try to upload file
if(!is_dir($target_dir) && !mkdir($target_dir, 0777, true)) die('Failed to create directories...');

move_uploaded_file($_FILES["poemfile"]["tmp_name"], $target_file) || die("Sorry, there was an error uploading your file.");

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

$conn = mysqli_connect($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 poems WHERE descr=?;";
$stmt = mysqli_prepare($conn, $query);
if(!$stmt) die('Invalid query prepare: ' . mysqli_error($conn));
mysqli_stmt_bind_param($stmt, "s", $poemtitle) || die('Invalid query bind param: ' . mysqli_error($conn));
mysqli_stmt_execute($stmt) || die('Invalid query execute: ' . mysqli_error($conn));
$queryres = mysqli_stmt_get_result($stmt);
if(!$queryres) die('Invalid query get result: ' . mysqli_error($conn));
#die("num_rows=" . $queryres->$num_rows);
if(mysqli_num_rows($queryres) === 0){
  // new poem, insert title into database:
  $query="INSERT INTO poems (descr) VALUES (?);";
```

```
49    $stmt = mysqli_prepare($conn, $query);
50    if(!$stmt) die('Invalid query prepare: ' . mysqli_error($conn));
51    mysqli_stmt_bind_param($stmt, "s", $poemtitle) || die('Invalid query bind param:
      ' . mysqli_error($conn));
52    mysqli_stmt_execute($stmt) || die('Invalid query execute: ' .
      mysqli_error($conn));
53  }
54
55  mysqli_close($conn);
56
57  if($studentname) echo "<i>(challenge assigned to " . $studentname . ")</i><br/>";
58
59  echo "The file ". htmlspecialchars( basename( $_FILES["poemfile"]["name"])). " has
    been uploaded. Thank you for uploading your literary work.";
60  ?>
61
62  <html>
63  <body>
64
65  <h1>The Dark Poetry Database</h1>
66  <img src="child_and_killers.jpg" alt="Street lights" width="500"><br/>
67
68  <h1>Return home</h1>
69  <a href="index.php">Click here</a>
70
71  <h1>See uploaded poems</h1>
72  <a href="poems.php">Click here</a>
73
74  <h1>If you are allowed to, see the flag</h1>
75  <a href="flag/flag.txt">Click here</a>
76
77  </body>
78  </html>
79
80
```