```
<?php # script 10.2 - delete_user.php
//page for deleting a user form the database
//accessed through view_users.php

//$page_title = 'Delete a User';
//change page title to suit user to be edited as per Review and Pursue chapter 10
//changed again for ch13 Review and Pursue
//it is still really easy to hack this page as it stands even with the filter function or casting
//since the address bar info can easily be altered before the submit button is pressed.
if ($_SERVER['REQUEST_METHOD']=='GET'){
$fn = filter_var(trim($_GET['fn']), FILTER_SANITIZE_STRING);
$ln = filter_var(trim($_GET['ln']), FILTER_SANITIZE_STRING);
$page_title = 'Delete User: ' . $fn . ' ' . $ln;
//$page_title= 'Delete User: '. $_GET['fn'] . '  ' . $_GET['ln'];

}else{
$first_name      = filter_var(trim($_POST['first_name']), FILTER_SANITIZE_STRING);
$last_name = filter_var(trim($_POST['last_name']), FILTER_SANITIZE_STRING);
$page_title="Delete User: " . $first_name . ' ' . $last_name;
//$page_title = "Delete User; " . ($_POST['first_name']) . '  ' . ($_POST['last_name]);
}
include ('includes/header.html');
echo '<h1>Delete a User</h1>';

/*
//check for valid user ID, through GET or POST chapter 10
if ((isset($_GET['id'])) && (is_numeric($_GET['id']))){//this page accessed from view_user.php
        $id = $_GET['id'];
        $fn = $_GET['fn'];//needs this to pass to form
        $ln = $_GET['ln'];//needs this to pass to form
}elseif((isset($_POST['id'])) && (is_numeric($_POST['id']))){//submitted from this page and form
        $id = $_POST['id'];
        $fn = $_POST['first_name'];//from form from $_POST
        $ln = $_POST['last_name'];//from form from $_POST
}else{//no valid ID. end script
        echo '<p class="error">This page has been accessed in error.</p>';
        include ('includes/footer.html');
        exit();
}
*/


//check for valid user ID, through GET or POST chapter 13 review and pursue item 8
//and check for integer and clean string from input form
if ((isset($_GET['id'])) && (is_numeric($_GET['id']))){//this page accessed from view_user.php
        $id = filter_var(trim($_GET['id']),FILTER_VALIDATE_INT,array('min_range'=>1));
        $fn = filter_var(trim($_GET['fn']), FILTER_SANITIZE_STRING);//needs this to pass to form
        $ln = filter_var(trim($_GET['ln']), FILTER_SANITIZE_STRING);//needs this to pass to form
}elseif((isset($_POST['id'])) && (is_numeric($_POST['id']))){//submitted from this page and form
        $id = filter_var(trim($_POST['id']), FILTER_VALIDATE_INT,array('min_range'=>1));
        $fn = filter_var(trim($_POST['first_name']), FILTER_SANITIZE_STRING);//from form from $_POST
        $ln = filter_var(trim($_POST['last_name']), FILTER_SANITIZE_STRING);//from form from $_POST

}else{//no valid ID. end script
        echo '<p class="error">This page has been accessed in error.</p>';
        include ('includes/footer.html');
        exit();
}

require_once ('includes/mysqli_connect.php');//connect to the db

//has form been submitted
if ($_SERVER['REQUEST_METHOD']=='POST'){
```

```
	if ($_POST['sure']=='Yes'){//delete the record

		//make the query to delete
		$query = "DELETE FROM users WHERE user_id=$id LIMIT 1";
		$result = @mysqli_query($dbc, $query);
		if (mysqli_affected_rows($dbc) == 1){//query ran as expected

			//display message
			echo '<p>The user record has been deleted.</p>';

		}else{//went wahoonee shaped
			echo '<p class="error">The user record could not be deleted due to a system
error.</p>';
			//echo '<p>' . mysqli_error($dbc) . '<br />Query: ' . $query . '</p>';//debug message

		}//end affected rows system error

	}else{//no confirmation of deletion
		echo '<p>The user record has not been deleted.</p>';
	}//end of sure Yes

}else{//show the form with users details corresponding to user_id

	//retrieve user details
	$q = "SELECT CONCAT(last_name, ', ',first_name) FROM users WHERE user_id = $id";
	$r = @mysqli_query($dbc, $q);

	if (@mysqli_num_rows($r) == 1){//valid user_id

	//get the users info
	$row = mysqli_fetch_array($r, MYSQLI_NUM);

	//display the record to be deleted
	echo "<h3>Name: $row[0]</h3>
	Are you sure that you want to delete this user record?";

	//create the form
	echo '<form action="delete_user.php" method="post">
		<input type="radio" name="sure" value="Yes" />Yes
		<input type="radio" name="sure" value="No" checked="checked" />No
		<input type="submit" name="submit" value="Submit" />
		<input type="hidden" name="id" value =" ' . $id . '" />
		<input type="hidden" name="first_name" value =" ' . $fn . '" /><!--pass these hidden values
to $page_title-->
		<input type="hidden" name="last_name" value =" ' . $ln . '" />
		</form>';

	}else{//not a valid user ID
		echo '<p class="error">This page has been accessed in error.</p>';
	}

}//end main IF SERVER ... main conditional

mysqli_close($dbc);

include ('includes/footer.html');
?>
```