1) If you are performing the demo of the attack:

inside the "main.php" file the form action field file name has to be "sec_page.php"

2) For prevention:

2.1) For sanitized input only:

open "sec_page.php" file and uncomment the username, password pair with mysqli_real_escape_string and comment the one without, so as to accept only validated user input.

2.2) For parameterized query with phpDataObject:

From the "main.php" change form action to file name "pdoeg.php".