

Multimedia im Netz, Assignment 1 Solution, Task 1

by Julian Pömp

```
<!DOCTYPE html>
<html>
<head lang="en">
  <meta charset="UTF-8">
  <title>What's wrong here?</title>
</head>
<body>
<?php
function loginUser($email, $password)
{
  /* 1. Passwords shouldn't be visible in code as plain text. It might be right
    that in PHP only developers see this password, but in a real life project
    you have to encrypt the passwords. That's why I hashed the password with
    sha1 and compare this with the hash of the (input).

    2. The combination of email and password must be checked. Before you could
    use any email address with the right password. That was a security issue
    because the password was the only information a hacker needed to log in.

    */
  if (
    $email === "max@mustermann.de"
    && sha1($password) === '515aa587ef74010ef87086c523e04e69787719df'
  ) {
    echo '<p>You are now logged in.</p>';
  } else {
    // The user should get only the information that something is wrong to make
    // it harder to hack.
    echo '<p>Wrong password or email address</p>';
  }
}
if ($_POST['submit']) {
  // 3. The credentials must not be submitted via GET, because they are shown in
  // the URL.
  loginUser($_POST['email'], $_POST['password']);
} else {
  ?>
  <form method="post">
    <label>
      Email: <input type="email" name="email"/>
    </label>
    <label>
      Password: <input type="password" name="password"/>
    </label>
    <!--
    4. In your task description you have forgotten to set the type to "submit"
    -->
    <input name="submit" type="submit"/>
  </form>
<?php } ?>
</body>
</html>
```