**Bug Report:** Profile Option Allows to update with a previously Breached Passwords

**Report by:** Luciane Martins

**Severity:**  Critical  Major  Minor  Trivial

**Priority:**  High  Medium  Low

**Description:**

The profile option on the website is currently allowing users to create an account using a password that has been breached before. This security vulnerability compromises user account integrity and exposes the system to potential unauthorized access.

**Environment:**

Cypress Version: 12.17.4

Browser: Google Chrome 116.0.5845.97

Operating System: Windows 10

**Steps to Reproduce:**

1. Navigate to the website: <https://buggy.justtestit.org/>.
2. Login with username “maryjane83” and password “Password1!”
3. Click on the "Profile" button to access the form.
4. Enter a new password that has been breached before (e.g., a password from a well-known data breach - <https://haveibeenpwned.com/Passwords> ) that meets the password criteria.
5. Complete the registration process and create an account successfully.

**Expected result:**

The profile option should enforce password security measures, preventing users from using passwords that have been compromised in previous data breaches.

The system should detect breached passwords and display an error message or warning, advising users to choose a stronger and more secure password.

**Actual result:**

The profile option allows users to create a new password that have been breached before without any warning.

There is no indication that the system is checking for breached passwords during the process.

**Screenshots:**

