**Bug Report:** Address Field Allows Input of Script Tag with Alert Message

**Report by:** Luciane Martins

**Severity:**  Critical  Major  Minor  Trivial

**Priority:**  High  Medium  Low

**Description:**

I identified a critical issue while testing the profile creation functionality on the website https://buggy.justtestit.org/. The bug allows users to input a script tag with an alert message, indicating a potential cross-site scripting (XSS) vulnerability.

**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. In the "Address" field, Enter a script tag with an alert message into the address field:
   1. <script>alert("XSS Vulnerability");</script>
5. Save the form clicking on “Save” button

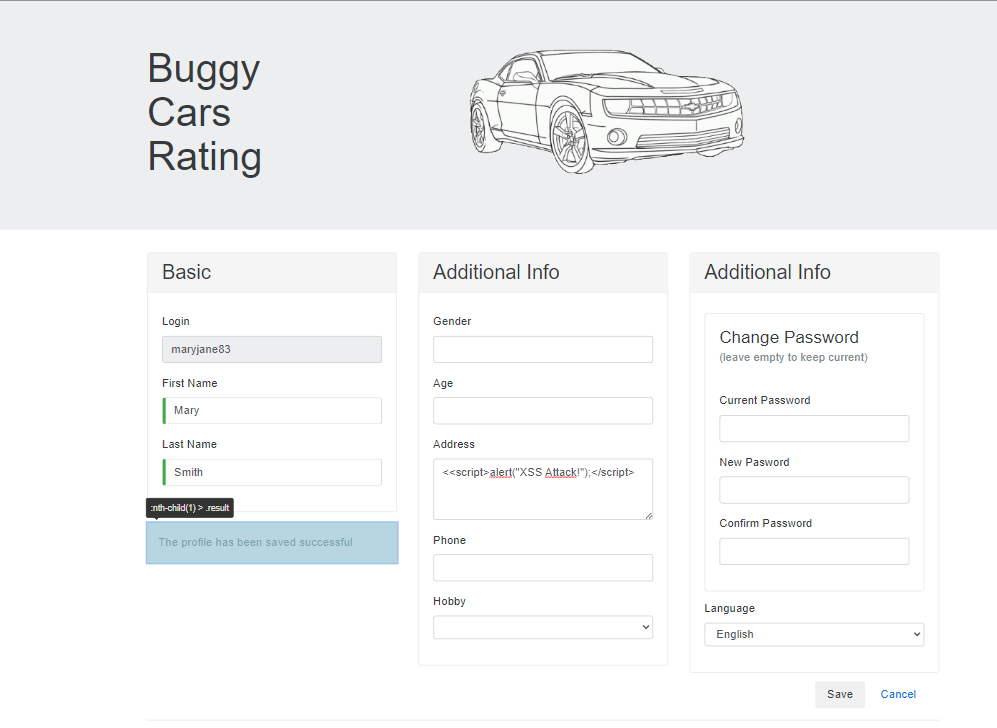
**Expected result:**

The address field should not allow the input of script tags or any HTML tags. The form submission should be prevented, and the input should be sanitized to prevent XSS attacks. No alerts or unexpected behaviour should occur on the output page.

**Actual result:**

Contrary to expectations, the form allows users to input a script tag with an alert message. Upon saving the profile, the system does not prevent the input, and the script is executed, resulting in a pop-up alert with the message "XSS Vulnerability."

**Screenshots:**



**Additional Notes:**

The security vulnerability poses a significant risk, as it exposes the application and its users to potential malicious attacks.

Implementing proper input validation and output encoding is essential to mitigate this vulnerability and prevent XSS attacks.