

Bug Title: Default Product List Not Displayed After Clearing Search Keyword

Description:

In the when a user searches for a keyword (e.g., "banana") and clears the search keyword, the default product list is not restored. Instead, the search results remain unchanged, which disrupts the expected behaviour of reverting to the default state.

Reproducible Steps:

- Open the web application.
- In the search bar, type "banana" and press Enter.
- Observe the search results.
- Clear the keyword from the search bar.
- Observe the product list.

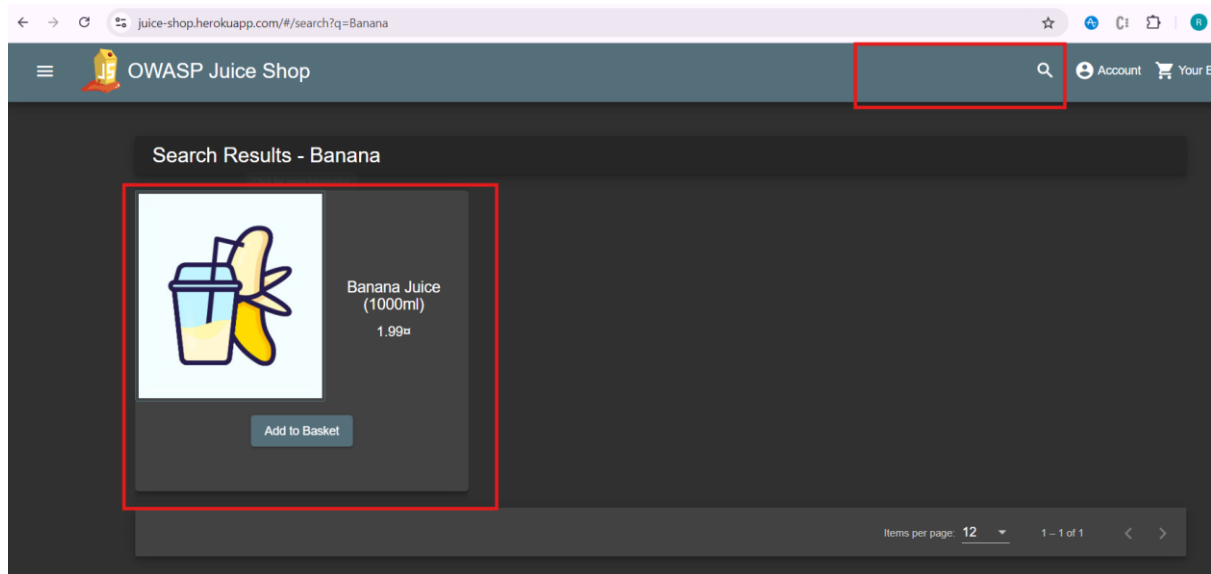
Actual Result:

After clearing the search keyword, the product list does not revert to the default state.

Expected Result:

Clearing the search keyword should restore the default product list, displaying all available products.

Screenshot:



Bug Title: 500 Error Encountered When Clicking on "Link Image" Without Entering a URL in Profile Section

Description:

In the web application, clicking on the Link Image button in the Profile section without entering a URL results in a 500 Internal Server Error.

Reproducible Steps:

- Log in to the web application.
- Navigate to the Profile section.
- Leave the URL input field empty.
- Click on the Link Image option.
- Observe the error message displayed.

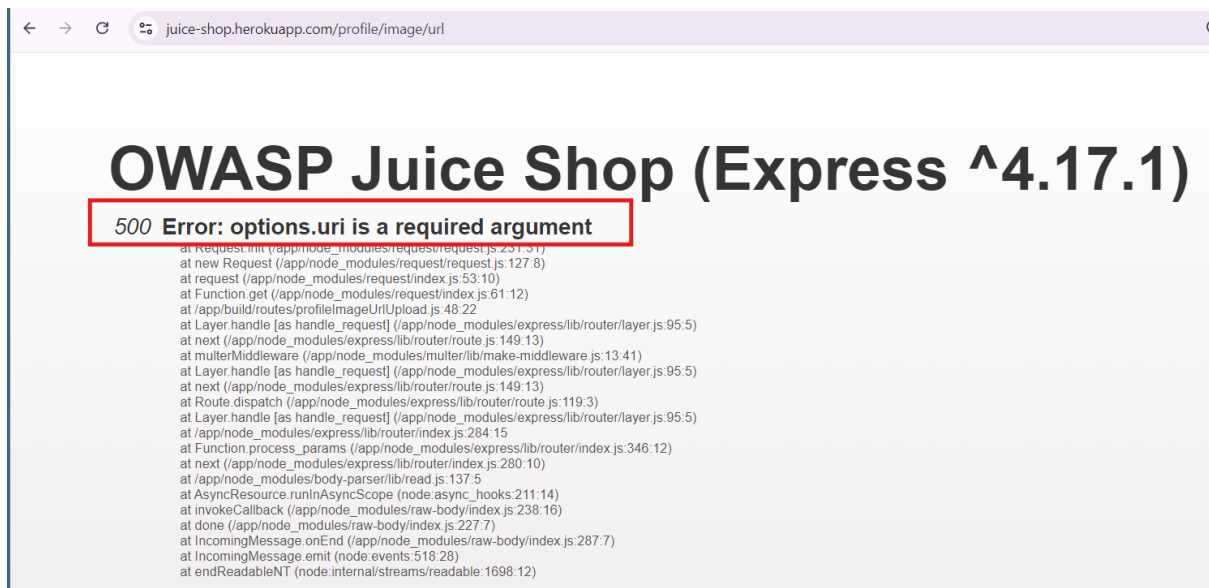
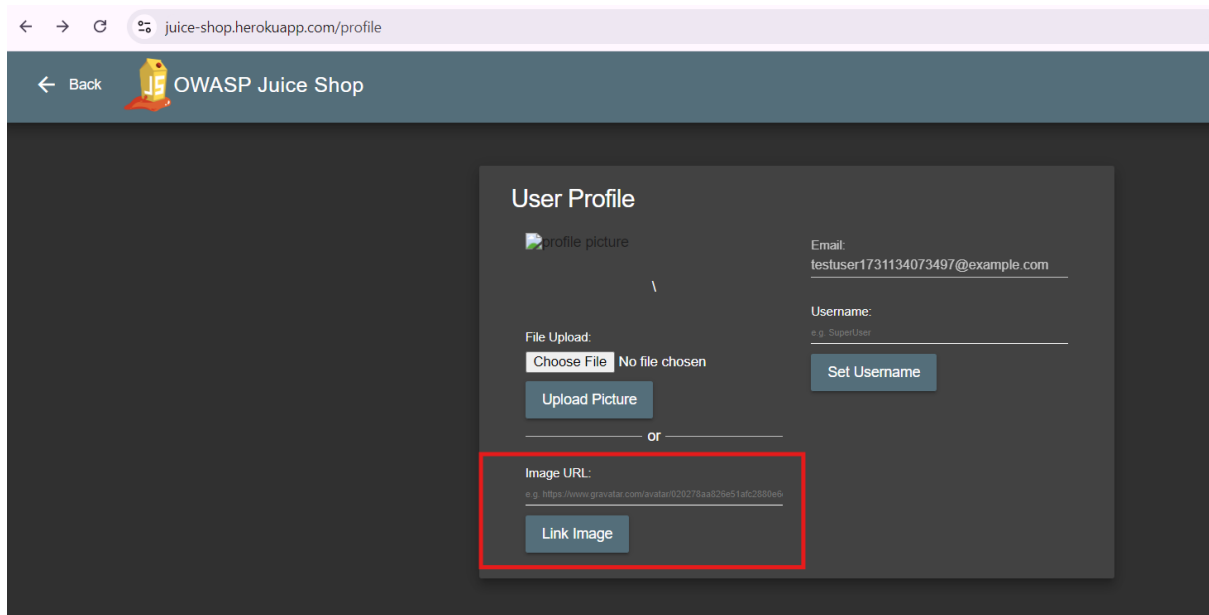
Actual Result:

A 500 Internal Server Error is displayed, and the action fails.

Expected Result:

The system should display a validation error message, such as "Please enter a valid URL," and prevent the submission without causing a server error.

Screenshot:



Bug Title: Broken Image Displayed After Uploading Profile Image**Description:**

In the web application, after uploading a profile image, the image appears broken, indicating that it failed to load properly. This issue prevents users from viewing their uploaded profile picture.

Reproducible Steps:

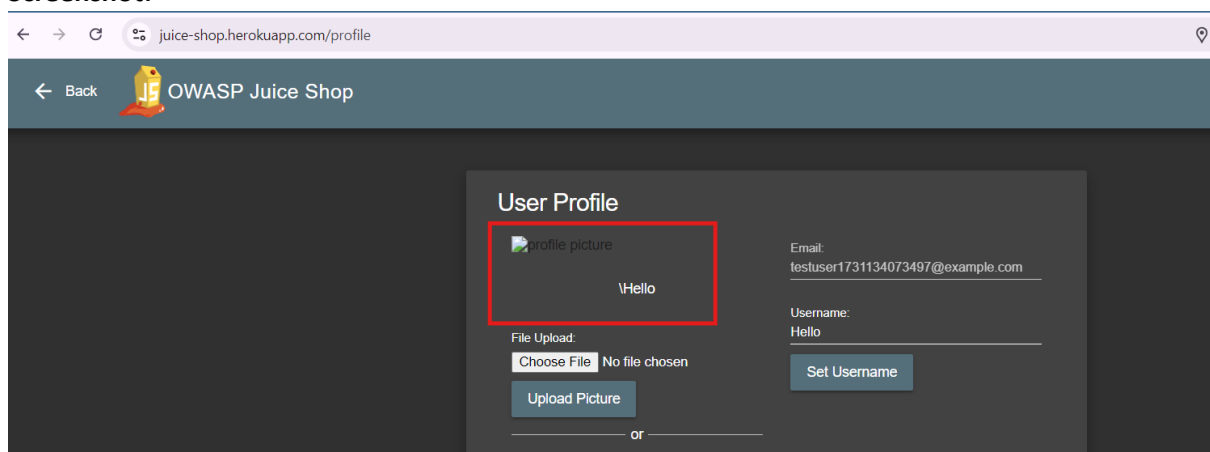
- Log in to the web application.
- Navigate to the Profile section.
- Click on the Upload Image option.
- Select and upload a valid image file.
- Observe the profile image display after the upload is complete.

Actual Result:

A broken image icon is displayed instead of the uploaded profile image.

Expected Result:

The uploaded profile image should be displayed correctly without any errors.

Screenshot:**Bug Title:** Missing Email Validation for "Test@ccc" During Registration Process**Description:**

During the registration process, the email address "Test@ccc" is accepted without proper validation. This email lacks a valid top-level domain (TLD), making it an invalid format. However, the system allows this incorrect email format to be submitted, which should not be the case.

Reproducible Steps:

- Navigate to the registration page of the application.
- In the email input field, enter "Test@ccc".
- Complete the other required fields
- Submit the registration form.
- Observe whether the form is submitted successfully or if there is an error message.

Actual Result:

The email "Test@ccc" is accepted and the registration process is completed without showing any validation errors.

Expected Result:

The registration process should display an error message such as "Please enter a valid email address" or "Invalid email format" and prevent submission if the email address lacks a valid TLD.

Screenshot:

The top screenshot shows the 'User Registration' form on the OWASP Juice Shop application. The email field contains 'Test@ccc' and is highlighted with a red box. The password field is empty, and the repeat password field is also empty. The password advice section shows a list of requirements: contains at least one lower character (checked), contains at least one upper character (unchecked), contains at least one digit (unchecked), contains at least one special character (unchecked), and contains at least 8 characters (unchecked). The security question is 'Mother's birth date? (MM/DD/YY)' and the answer is 'Test'.

The bottom screenshot shows the 'Login' form on the OWASP Juice Shop application. The email field contains 'Test@ccc' and is highlighted with a red box. The password field is empty. A 'Save password?' dialog box is overlaid on the right side of the form, also containing the email 'Test@ccc' and highlighted with a red box. The dialog box has 'Save' and 'Never' buttons. Below the dialog box, there is a message: 'You can use saved passwords on any device. They're saved to Google Password Manager for rajesh@give.do.'

Bug Title: Password Criteria Not Enforced Correctly During Registration**Description:**

During the registration process, the password criteria (such as minimum length, special characters, uppercase letters, etc.) are not being enforced correctly, even though the registration is successful. Users can create accounts with passwords that do not meet the defined criteria, which compromises security.

Reproducible Steps:

- Navigate to the registration page of the application.
- In the Password field, enter a password that does not meet the specified criteria (e.g., too short, lacks special characters, or has no uppercase letters).
- Example: prime
- Complete the rest of the registration form (e.g., email, username).
- Submit the registration form.
- Observe whether the registration is successful or if a password validation error is shown.

Actual Result:

The registration process is successfully completed even if the password does not meet the required criteria.

Expected Result:

The system should enforce the password criteria, displaying an error message (e.g., "Password must be at least 8 characters long and contain an uppercase letter, a number, and a special character.") and prevent submission if the password does not match the required pattern.

Screenshot:

juice-shop.herokuapp.com/#/register

User Registration

Email *
Test1223@yopmail.com

Password *
.....
1 Password must be 5-40 characters long. 5/20


Repeat Password *
.....
5/40

☒ Show password advice

- ✓ contains at least one lower character
- ! contains at least one upper character
- ! contains at least one digit
- ! contains at least one special character
- ! contains at least 8 characters

Security Question *
Mother's maiden name? ▾
1 This cannot be changed later!

Answer *
Test

 Register

Already a customer?

juice-shop.herokuapp.com/#/login

OWASP Juice Shop


You successfully solved a challenge. Admin Section (Access the administration section of the store.)

Login

Email *


Password *

Forgot your password?

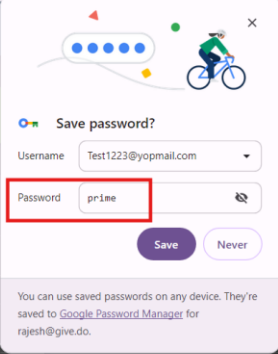
 Log in

☐ Remember me

or

 Log in with Google



Not yet a customer?



Save password?

Username: Test1223@yopmail.com

Password: prime

 Save  Never

You can use saved passwords on any device. They're saved to [Google Password Manager](#) for rajesh@give.do.