EECS 2311 Take Home Assignment

Team: Salon AI

Section: [SectionName]

Student: Amit

March 24, 2025

End-to-End Manual Testing

User Story 1: Customer: Register and log in

Test Case 1: Registration Field Validation

1. Navigate to the homepage
2. Click on "Register"
3. Test each required field individually:
    - Submit with empty first name
    - Submit with empty last name
    - Submit with invalid email format
    - Submit with password less than 8 characters
    - Submit with mismatched password confirmation
    - Submit with invalid phone number format
4. Observe validation messages for each case

Expected Result: Appropriate validation error messages are displayed for each field.

Test Case 2: Login After Registration

1. Register a new account with valid information
2. Logout if automatically logged in
3. Navigate to login page
4. Enter the credentials of the newly registered account
5. Click "Login"
6. Verify successful login and access to customer features

Expected Result: New user can immediately login with their credentials and access customer features.

Test Case 3: Remember Me Functionality

1. Navigate to login page
2. Enter valid credentials
3. Check "Remember Me" option
4. Login successfully
5. Close the browser completely
6. Reopen browser and navigate to the salon website

Expected Result: User should remain logged in when returning to the site.

Test Case 4: Account Lockout After Failed Attempts

1. Navigate to login page
2. Enter a valid username but incorrect password
3. Attempt login multiple times (at least 5 attempts)
4. Observe if account gets locked
5. Try logging in with correct credentials

Expected Result: Account should be temporarily locked after multiple failed attempts.

Bug and Issue Reports

Bug 1: Registration Email Verification

Summary: Users can access full system functionality without verifying their email.
Steps to Reproduce:

1. Register a new account
2. Login immediately without clicking any verification link
3. Attempt to use all customer features

Expected Behavior: Certain features should be restricted until email verification.
Actual Behavior: All features are accessible without email verification.
Severity: Medium

Bug 2: Login Form XSS Vulnerability

Summary: Login form vulnerable to cross-site scripting attacks.
Steps to Reproduce:

1. Navigate to login page
2. Enter ‘¡script¿alert(”XSS”)¡/script¿‘ in the username field
3. Submit the form

Expected Behavior: Input should be properly sanitized with no script execution.
Actual Behavior: JavaScript alert executes, indicating XSS vulnerability.
Severity: Critical

Code Review

Code Smells Checked

- Security vulnerabilities
- Error handling
- Long parameter lists
- Shotgun surgery
- Inappropriate intimacy
- Global state
- Dead code

Code Smells Detected

1. **Inadequate Input Sanitization**

   User inputs are not properly sanitized before processing, creating security vulnerabilities.

   Recommendation: Implement proper input validation and sanitization, especially for user-generated content.

2. **Plain Text Password Transmission**

   Passwords appear to be transmitted to the server without encryption beyond HTTPS.

   Recommendation: Implement client-side hashing before transmission or use a secure authentication protocol.

3. **Global Authentication State**

   Authentication state is managed through global variables, making it difficult to track changes.

   Recommendation: Implement a proper state management solution like Context API or Redux.