

Final project for Manual Testing

***Test and report for specified website***

Fanka Shundovska

Skopje, December 2023

* As a final assignment, we will use this website: https://qatest-dev.indvp.com/ and test Create an Account, Login Functionality. **Write at least 10 test cases** based on the techniques, heuristics and all the knowledge you have gained. All the test cases and defects should be written in word or excel and attached to the assignment.

Based on a specific requirements and functionality of the system under test, the test cases cover a range of scenarios for testing the Create an Account and Login Functionality of the website:

Login name: [marija.mariovska@msn.com](mailto:marija.mariovska@msn.com)

/ Password: Marijamariovska@@@

* Create Account:

1. Verify that a user can successfully create a new account by filling in all the required fields and clicking on the "Sign Up" button.

2. Verify that all the required fields are marked with an asterisk (\*) and cannot be left blank during the account creation process.

3. Verify that a user cannot create an account with an invalid email address.

4. Verify that a user cannot create an account with a password that does not meet the specified criteria (e.g., minimum length, special characters).

5. Verify that a user cannot create an account if the password and confirm password fields do not match.

6. Verify that a user cannot create an account if the username/email is already registered in the system.

1. Test Case: Successful account creation
   * Steps:
     1. Navigate to the website.
     2. Click on the "Create Account" button.
     3. Fill in all the mandatory fields with valid data.
     4. Submit the form.
   * Expected Result: Account is created successfully.
   * Defect: If the account is not created or an error message is displayed, it indicates a defect.
2. Test Case: Invalid email format
   * Steps:
     1. Navigate to the website.
     2. Click on the "Create Account" button.
     3. Enter an invalid email address.
     4. Fill in other mandatory fields.
     5. Submit the form.
   * Expected Result: An appropriate error message is displayed for the invalid email format.
   * Defect: If the invalid email is accepted or no error message is displayed, it indicates a defect.
3. Test Case: Password strength validation
   * Steps:
     1. Navigate to the website.
     2. Click on the "Create Account" button.
     3. Enter a weak password (e.g., less than 6 characters).
     4. Fill in other mandatory fields.
     5. Submit the form.
   * Expected Result: An appropriate error message is displayed for weak password strength.
   * Defect: If a weak password is accepted or no error message is displayed, it indicates a defect.
4. Test Case: Existing email address
   * Steps:
     1. Navigate to the website.
     2. Click on the "Create Account" button.
     3. Enter an email address that is already associated with an existing account.
     4. Fill in other mandatory fields.
     5. Submit the form.
   * Expected Result: An appropriate error message is displayed for an existing email address.
   * Defect: If the existing email address is accepted or no error message is displayed, it indicates a defect.

* Login Functionality:

1. Verify that a registered user can successfully login using valid credentials.

2. Verify that the login process fails if the user enters an invalid username/email.

3. Verify that the login process fails if the user enters an incorrect password.

4. Verify that the login process fails if the user leaves the username/email field blank.

5. Verify that the login process fails if the user leaves the password field blank.

6. Verify that the login page contains a "Forgot Password" link and it redirects the user to a password reset page.

1. Test Case: Successful login
   * Steps:
     1. Navigate to the website.
     2. Click on the "Login" button.
     3. Enter valid credentials for an existing account.
     4. Submit the form.
   * Expected Result: User is logged in successfully to their account.
   * Defect: If login fails or an error message is displayed, it indicates a defect.
2. Test Case: Invalid login credentials
   * Steps:
     1. Navigate to the website.
     2. Click on the "Login" button.
     3. Enter invalid credentials (e.g., wrong email/password combination).
     4. Submit the form.
   * Expected Result: An appropriate error message is displayed for invalid login credentials.
   * Defect: If invalid login credentials are accepted or no error message is displayed, it indicates a defect.
3. Test Case: Password recovery functionality
   * Steps:
     1. Navigate to the website.
     2. Click on the "Forgot password?" link.
     3. Enter a valid registered email address.
     4. Submit the form.
   * Expected Result: User receives an email with instructions on password recovery.
   * Defect: If no email is received or an error occurs during password recovery, it indicates a defect.
4. Test Case: Logout functionality
   * Steps:
     1. Navigate to the website.
     2. Login to the account.
     3. Click on the "Logout" button.
   * Expected Result: User is successfully logged out.
   * Defect: If the user remains logged in or experiences any error during logout, it indicates a defect.
5. Test Case: Session timeout functionality
   * Steps:
     1. Navigate to the website.
     2. Login to the account.
     3. Wait for a session timeout duration.
     4. Perform any action (e.g., clicking a link or submitting a form).
   * Expected Result: User is redirected to the login page with an appropriate session expired message.
   * Defect: If the session does not expire or the user is not redirected, it indicates a defect.
6. Test Case: Account activation via email
   * Steps:
     1. Navigate to the website.
     2. Complete the registration process by entering valid data.
     3. Check the registered email inbox for an activation email.
     4. Follow the activation link from the email.
   * Expected Result: Account is successfully activated and login becomes possible.
   * Defect: If the email is not received or the activation link does not work, it indicates a defect.

* Cross-browser Testing:

1. Verify login and account creation tests on multiple browsers (e.g., Chrome, Firefox, Safari) to ensure compatibility and consistent behaviour.

2. Verify that the design and functionality of the website are consistent across different browsers.

* Performance Testing:

1. Verify the response time of the account creation and login process with a high number of concurrent users to determine if it can handle the expected load and provide acceptable performance.

* Security Testing:

1. Verify that password fields are properly masked to prevent the leakage of sensitive information.

2. Verify any potential security vulnerabilities during the login and account creation processes.

* Usability Testing:

1. Verify evaluation of the user interface and experience of the account creation and login pages to ensure they are intuitive, user-friendly, and accessible.

2. Verify if error messages are displayed clearly and provide meaningful information to users when they encounter issues during account creation or login.

* Localization Testing:

1. Verify that the account creation and login processes work accurately when different languages and locales are selected.

2. Verify if translated text and labels are displayed correctly without any distortion or truncation.

* Password Recovery:

1. Verify the password recovery feature by entering a valid registered email address and verifying if the user receives an email with password reset instructions.

2. Verify attempt password recovery with an invalid or unregistered email address to check if an appropriate error message is displayed.

* Social Login Integration (if applicable):

1. Verify that users can use their social media accounts (e.g., Google, Facebook, Twitter / X, Pinterest) to create an account or log in.

2. Verify if the necessary permissions are granted and information is correctly fetched from the social media platform.

* Session Management:

1. Verify that the user session remains active after successful login and accessing multiple pages of the website.

2. Verify if the session is properly invalidated after logging out, and the user cannot access restricted pages without re-logging in.