Automation Testing for SubExpert

Prepared for

Prof. Mukhtiar Zamin

Prepared by

Faizan (FA21-BSE-011)

Department of Computer Science

COMSATS University Islamabad, Lahore Campus

28 June 2024

Table of Contents

Introduction to the Module

Login and Authorization Module

The Login and Authorization module is a critical component of any application, providing a secure entry point for users to access their accounts. This module ensures that only authenticated users can log in and access authorized features based on their roles and permissions. The module typically includes functionality for user login, logout, password recovery, and session management. Effective testing of this module is essential to ensure the security and usability of the application.

Link for Video Presentation

https://drive.google.com/file/d/1L5_t86S9qwrzZEBHlOVYBHdtgHkpo31u/view?usp=drive_link

Test Cases for Login and Authorization Module

TC_ID	Name	Description	Input	Precondition	Expected Outcome
1	Valid Login	Test login with valid credentials	Username: validUser<br>Password: validPass	User is registered and active	User is logged in successfully
2	Invalid Login	Test login with invalid credentials	Username: validUser<br>Password: invalidPass	User is registered and active	Error message "Invalid credentials" is displayed
3	Blank Username	Test login with blank username	Username: ""<br>Password: validPass	-	Error message "Username is required" is displayed
4	Blank Password	Test login with blank password	Username: validUser<br>Password: ""	-	Error message "Password is required" is displayed
5	SQL Injection	Test login with SQL injection attempt	Username: ' OR '1'='1<br>Password: ' OR '1'='1	-	Error message "Invalid credentials" is displayed

6	Cross-Site Scripting (XSS)	Test login with XSS attack attempt	Username: <script>alert('xss')</script> Password: anyPass	-	Input is sanitized and error message "Invalid credentials" is displayed
7	Password Recovery	Test password recovery process	Email: registeredUserEmail	User has a registered email address	Password recovery email is sent to the registered email address
8	Logout	Test user logout functionality	-	User is logged in	User is logged out and redirected to the login page
9	Session Timeout	Test automatic session timeout after inactivity	-	User is logged in	User is logged out automatically after a period of inactivity
10	Role-Based Access	Test access control based on user roles	Username: adminUser Password: adminPass	User has admin role	User can access admin functionalities
11	Brute Force Protection	Test protection against brute force attacks	Multiple invalid login attempts with valid username	-	Account is locked after a certain number of failed attempts
12	Valid Signup	Test user registration with valid details	Username: newUser. Password: newPass, Email: newUser@example.com	-	User is registered successfully and can log in
13	Invalid Email Signup	Test signup with invalid email format	Username: newUser Password: newPass Email: invalidEmail	-	Error message "Invalid email format" is displayed
14	Blank Username Signup	Test signup with blank username	Username: "" Password: newPass Email: newUser@example.com	-	Error message “Username is required” is displayed

15	Blank Password Signup	Test signup with blank password	Username: newUser Password: "" Email: newUser@example.com	-	Error message "Password is required" is displayed
16	Duplicate Username Signup	Test signup with an already existing username	Username: existingUser Password: newPass Email: newUser@example.com	-	Error message "Username already exists" is displayed
	Duplicate Email Signup	Test signup with an already existing email	Username: newUser Password: newPass Email: existingUser@example.com	-	Error message "Email already exists" is displayed