**Manual Testing: Manual Test Scenarios for an App**

***QA Engineer Assessment***

**Compiled by: Tsotlhe Mabusela**

**Performance Testing Test Scenarios**

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Expected Result** | **Latest Result** | **Automated** |
| 1. Validate that the mobile application can be downloaded and installed for use. |  |  |  |
| 1. Verify that the mobile application can function as per the requirements under different load conditions. |  |  |  |
| 1. Check how the app functions under different internet networks (2G, 3FG, 4G, 5G networks). |  |  |  |
| 1. Verify that the client-server configuration setup provides the required performance level. |  |  |  |
| 1. Verify that the response time of the mobile application is per the set requirements. |  |  |  |
| 1. Evaluate whether the battery life can support the mobile application to perform under the expected load volumes. |  |  |  |
| 1. Verify that unavailable pages or an application crash redirect the user to the error page. |  |  |  |
| 1. Check the mobile application performance when the network is switched from 2G/3G/4G/5G to WIFI and from WIFI to 2G/3G/4G/5G. |  |  |  |
| 1. Check whether the mobile application works as anticipated when the mobile device receives an incoming call or SMS. |  |  |  |
| 1. Verify that the mobile application is compatible and adaptable to different mobile platforms or operating systems. |  |  |  |
| 1. Verify that the mobile application will function as intended after a successful update to the mobile application |  |  |  |
| 1. Verify that the mobile application does not drain the battery of the mobile device. |  |  |  |

**Usability & Compatibility Testing Test Scenarios**

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Expected Result** | **Latest Result** | **Automated** |
| 1. Verify that the mobile application’s user interface is adaptive to the screen size of any mobile device. |  |  |  |
| 1. Verify that all text is clear and readable across the mobile application for the user. |  |  |  |
| 1. Verify that text contrast is applied across the mobile application to facilitate readability for users. |  |  |  |
| 1. Verify that the buttons are visible and clickable on the mobile application. |  |  |  |
| 1. Verify that buttons and Icons are placed in the same section consistently across the application. |  |  |  |
| 1. Verify that all buttons with the same functionality use the same colour. |  |  |  |
| 1. Verify that the colours used to communicate actions are in line with the best practice methods. |  |  |  |
| 1. Verify that all fields on the page are aligned properly. |  |  |  |
| 1. Verify that all pages across the mobile application have a back button/method and or an undoing action with an acceptable time limit. |  |  |  |
| 1. Ensure that menus are not overloaded with content. |  |  |  |
| 1. Ensure that a user guide/manual is made available to the user to ensure that Users understand the application. |  |  |  |
| 1. Check that the application’s splash screens, and welcome screens start the application launch. |  |  |  |
| 1. . Ensure that all pages have a name. |  |  |  |
| 1. Ensure that to check all pages for broken links and images. |  |  |  |
| 1. Ensure to include confirmation messages when actions are completed. |  |  |  |

**Security Testing Test Cases**

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Expected Result** | **Latest Result** | **Automated** |
| 1. Validate that the password protection system of the mobile application is strong enough to withstand an attack. |  |  |  |
| 1. Validate that the mobile applications password protection system does not accept weak passwords. |  |  |  |
| 1. Validate that the password protection system has matrices to validate user password changes. |  |  |  |
| 1. Verify that the mobile application can withstand any brute force attack. |  |  |  |
| 1. Verify that the mobile application has a solid user authentication system. |  |  |  |
| 1. Verify that the mobile application properly implements session management, ensure that sessions expire |  |  |  |
| 1. Verify that the business logic of the mobile application is protected and secured to ensure that it will be vulnerable to an external attack. |  |  |  |
| 1. Verify that user data is adequately protected. |  |  |  |
| 1. Verify that the mobile application is protected from runtime injections. |  |  |  |
| 1. Verify that the mobile application is protected from client-side injections. |  |  |  |
| 1. Verify that the system is protected from SQL injections. |  |  |  |
| 1. Verify that cookie information is stored in an encrypted format only. |  |  |  |
| 1. Ensure that cookie sessions are terminated, and session management is applied to cookie sessions. |  |  |  |
| 1. Verify that the password field and banking information fields do not have an autocomplete feature |  |  |  |
| 1. Verify captcha functionality. |  |  |  |
| 1. Verify that privileges are implemented across the mobile application. |  |  |  |