Test Cases	Pre Conditions	Expected Result	Actual Result	Post Condition	Pass/Fail	Test Owner
To validate whether all the required mandatory fields are working as required.						
To validate that the mandatory fields are displayed on the screen differently than the non-mandatory fields.						
To validate whether the application works as per requirement whenever the application starts/stops.						
To validate whether the application goes into minimized mode whenever there is an incoming phone call.						
To validate whether the phone can store, process and receive SMS whenever the app runs.						
To validate that the device can perform required multitasking requirements whenever it is necessary to do so.						
To validate that the application allows necessary social network options such as sharing, posting, navigation, etc.						
To validate that the application supports any payment gateway transaction such as Visa, Mastercard, Paypal, etc, as required by the application.						
To validate that the page scrolling scenarios are being enabled in the application as necessary.						
To validate that the navigation between relevant modules in the application is as per the requirement.						
To validate that the truncation errors are absolute to an affordable limit.						
To validate that the user receives an appropriate error message like “Network error. Please try after some time” whenever there is any network error.						
To validate that the installed application enables other applications to perform satisfactorily and does not eat into the memory of the other applications.						
To validate that the application resumes at the last operation in case of a hard reboot or system crash.						
To validate whether the application installation can be done smoothly, provided the user has the necessary resources, it does not lead to any significant errors.						
To validate that the application performs auto start facility according to the requirements.						
To validate whether the application performs according to the requirement in all versions of Mobile, that is, 2g, 3g, and 4g.						
To perform Regression Testing to uncover new software bugs in existing areas of a system after changes have been made to them.						
To determine whether the application performs per the requirement under different load conditions.						
To determine whether the current network coverage can support the application at peak, average, and minimum user levels.						
To determine whether the existing client-server configuration setup provides the required optimum performance level.						
To identify the various application and infrastructure bottlenecks that prevent the application from performing at the required acceptability levels.						
To validate whether the response time of the application is as per the requirements.						
To evaluate product and/or hardware to determine if it can handle projected load volumes.						
To evaluate whether the battery life can support the application to perform under projected load volumes.						
To validate application performance when the network is changed to WIFI from 2G/3G or vice versa.						
To validate each of the required CPU cycles is optimization.						
To validate that the battery consumption, memory leaks, and resources like GPS, Camera performance is well within the required guidelines.						
To validate the application longevity whenever the user load is rigorous.						
To validate the network performance while moving around with the device.						
To validate the application performance when only intermittent phases of connectivity are required.						
To validate that the application can withstand any brute force attack.						
To validate whether an application is not permitting an attacker to access sensitive content or functionality without proper authentication.						
To validate that the application has a strong password protection system and it does not permit an attacker to obtain, change, or recover another user’s passwor						
To validate that the application does not suffer from insufficient session expiration.						
To identify the dynamic dependencies and take measures to prevent any attacker from accessing these vulnerabilities.						
To prevent SQL injection-related attacks.						
To identify and recover from any unmanaged code scenarios.						
To ensure whether the certificates are validated, does the application implement Certificate Pinning or not.						
To protect the application and the network from denial of service attacks.						
To analyze the data storage and data validation requirements.						
To enable the session management to prevent unauthorized users from accessing unsolicited information.						
To validate whether the business logic implementation is secured and not vulnerable to any attack from outside.						
To analyze file system interactions, determine any vulnerabilities, and correct these problems.						
To validate the protocol handlers, for example, trying to reconfigure the default landing page for the application using a malicious iframe.						
To protect against malicious client-side injections.						
To protect against malicious runtime injections.						
To investigate file caching and prevent any malicious possibilities from the same.						
To prevent insecure data storage in the keyboard cache of the applications.						
To investigate cookies and prevent any malicious deeds from the cookies.						
To provide regular audits for data protection analysis.						
Investigate custom-created files and prevent any malicious deeds from the custom-created files.						
To analyze different data streams and prevent any vulnerabilities from these.						
To ensure that the buttons are placed in the same section of the screen to avoid confusion for the end users.						
To ensure that the icons are natural and consistent with the application.						
To ensure that the buttons with the same function should also have the same color.						
To ensure the validation for the tapping, zoom-in, and zoom-out facilities should be enabled.						
To ensure that the keyboard input can be minimized appropriately.						
To ensure that the application provides a method for going back or undoing an action, on touching the wrong item, within an acceptable duration.						
To ensure that the text is kept simple and clear to be visible to the users.						
To ensure that the short sentences and paragraphs are readable to the end users.						
To ensure that the font size is big enough to be readable and not too big or too small.						
To validate, the application prompts the user whenever the user starts downloading a large amount of data which may not be conducive to the application's perf						
To validate that the closing of the application is performed from different states and verify if it re-opens in the same state.						

To ensure that all strings are converted into appropriate languages whenever a language translation facility is available.						
To ensure that the application items are always synchronized according to the user actions.						
To ensure that the end user is provided with a user manual that helps the end user to understand and operate the application who may be not familiar with the a						
To validate whether the application provides an available user guide for those unfamiliar with the app.						
To validate that the user Interface of the application is as per the screen size of the device, no text/control is partially invisible or inaccessible.						
To ensure that the text is readable for all users of the application.						
To ensure that the call/alarm functionality is enabled whenever the application runs.						