**Security Recommendations**

1. I chose minimum permission requirements. This is because our app request’s location and requires access to the internet to run.
2. Having the app only request access to location and the internet this prevent end-users from providing sensitive information, to mitigate damage if the app is used in some sort of cyber attack.
3. <https://github.com/OWASP/owasp-mastg/blob/master/Document/0x05h-Testing-Platform-Interaction.md#testing-app-permissions-mstg-platform-1>
4. The recommendation would have to be implemented when connecting the API. This is because the open weather API requires location to pull where the weather is being displayed from. Whenever someone displays the weather module of the app the app will have to gather location data from the phone. This means that requesting access to location data is required for the app operate. If data is not retrieved the app will still run but not display weather conditions. Furthermore, in order to access the API, it needs to connect to the internet. This again requires internet access, which can open the app up to new vulnerabilities however, using the app without internet access is still possible, it will just not display weather information.
5. Our app needs this because location access is potentially sensitive depending on where the user is positioned at (e.g., home address, workplace, etc.) However, since it is necessary to use location utilize the apps full functionality, we still need access to location data. Where we minimize the location data access, is giving the user options to turn off location tracking. As well, only using location data when the app is open. This prevents potential attacks on our software while the app is running in the background. Same with internet access the app only uses the internet while the user is using the app. This also prevent unwanted connections to the app and prevents excess internet/data usage for phones.
6. We can apply this recommendation by requesting the location data only when the user opens the weather page. If the user rejects the display that weather data will be unable to be accessed, and the allow the user to gracefully use other features of the app. Furthermore, disable location tracking once the user has exited the weather page this prevents leaving the location available to potentially malicious users. As well, stop grabbing information from the internet once the user as stop using the weather page. Once again this reduces the time that attackers can use the app as a vulnerability.
7. This should already be implemented as location tracking only turns on once the app is displaying the weather page. As well, the app only connects to internet while making a fetch call to the API. This means that internet connectivity is only used while fetching the API.