Mobile CTF Challenge Questions

21PC35 - Smrithi P
21PC37 - Tharageshwaran S

Challenge 1: Understanding Log Output Behavior

Description:
An APK is provided where an interaction within the app appears to trigger background processes. Upon closer inspection of the app's main entry point, you observe certain functions writing runtime data to system outputs.

Question:
How can you use in-app behavior and system outputs to detect critical debug information related to the challenge?

Challenge 2: Hidden Data in Resources

Description:
In this challenge, the static contents of the application reveal embedded data. Navigating through configuration and resource files leads to a format that conceals readable information using a common encoding scheme.

Question:
What are the steps to identify and interpret obfuscated values stored in resource files of an Android application?

Challenge 3: Game Engine Reverse Engineering

Description:
This application is developed using a game engine that differs from standard Android apps. This makes traditional approaches less effective. However, there are still ways to uncover hidden content by understanding the underlying structure.

Question:
What strategies would you apply when analyzing Android applications built with non-native game development platforms?

Challenge 4: Repackaging and Deployment Testing

Description:
The challenge involves modifying the behavior of an app, then rebuilding and reinstalling it for observation. The app needs to be restructured carefully and made deployable again after the changes.

Question:
What general steps must be followed to repackage, align, and sign a modified Android application for installation?

Challenge 5: Exported Components and Backup Exploits

Description:
An app with a login feature reveals potential issues in its configuration. Investigation shows the possibility of bypassing certain screens and accessing core data through backup techniques or exported functionality.

Question:
What approach can be taken to access internal app data and functionalities when the app has misconfigured component permissions and backup settings?
