PenTest Lab Exercise Ex140 – Mobile App Test

Goal

Use mobile application penetration testing techniques to see if a mobile app is exposing sensitive data.

Tasks

1. Art's Tailor Shoppe is developing an Android mobile application to provide all their customers with fresh content. Find the app and see if you can identify any serious problems with it. You will likely want to use `jadx-gui` (which is installed on `Kali`) to accomplish this task. It would be very difficult to decompile the `classes.dex` file contained with the apk from scratch.

2. An apk file for version 0.01 of the application is available from `http://www.artstailor.com/apps/ArtsTailorNews.apk`.

3. Examine the app and see what you can find. The kinds of things you might look for are those covered by the MASVS. New developers are likely to exfiltrate sensitive data without realizing it. Try to identify strings that can be extracted from the program, what their purpose is, and how they are transmitted. If you use a tool that exposes developer variable names, you might want to look for variables names that might be associated with credential exchange.

4. If you find credentials and references to a database server, try to use those credentials to get access to the server. Two final exam leeway points are available for those who are able to exfiltrate critical PCI data. If you are able do this, make sure to obfuscate your reported data in such a way that Art and Otto will still know you were able to exfiltrate it.

5. Write a partial penetration test report about what you discover. Make sure to include Mitre ATT&CK TTPs and CVSS scores as appropriate.