CSCI 445 - Homework #3: Getting started with Android application analysis*

Assigned Feb 29th; due 11:59pm on March 19th

Prof. Adwait Nadkarni

1 Assignment Description {50 points}

In this assignment, you will learn the basics of analyzing Android applications. You will manually analyze a simple Android application (obtained from the Blackboard site for this assignment) for vulnerabilities, after disassembling it using apktool.

1.1 Setup Instructions

Setup apktool according to the instructions on the website, and *disassemble* the application. The disassembled code is fairly readable, however, here is another (optional) guide to help you understand the output of apktool: Reverse Engineering android: Disassembling Hello World.

For this analysis, you will be looking at two objects: (1) the AndroidManifest.xml, and (2) the activity classes (i.e., the .smali files for them).

1.2 Analysis Requirements and Results

Most of this analysis will be manual, i.e., you will manually inspect the disassembled code to find signs of specific vulnerabilities, and report the culprit lines.

You will look for signs of the following two vulnerabilities:

1. *Unprotected components, 10 points*, i.e., application components that may be accessible to other applications.
2. *SSL vulnerabilities, 40 points*, i.e., instances of SSL misuse resulting from overriding safe defaults, as discussed in class. There is one such SSL flaw.

*Last revised on February 29, 2024.

Your assignment is to write an analysis report that will contain instances of both the cases. That is, you will analyze the given app, and for both these cases, **you will report the line numbers and lines themselves** as your solution.

1.3 Extra Credit

1 bonus point *on the course grade* if you successfully recommend how to resolve *all* of the flaws in the application.

2 Submission Instructions

Submit your solution as a single PDF named **lastname-hw3.pdf** to Blackboard. To upload your assignment, navigate to the "CSCI 445: Mobile Application Security (Spring 2024)" course. Use the "Homework 3" assignment. **Please note that if LaTeX is not used for this assignment, you will receive zero points.**

Please post questions (especially requests for clarification) about this homework to Piazza.