Internship Report on Cybersecurity Tasks

Submitted by: Deepak Yadav

Internship Provider: NULLCLASS

Date: 04-10-2024 to 04-11-2024

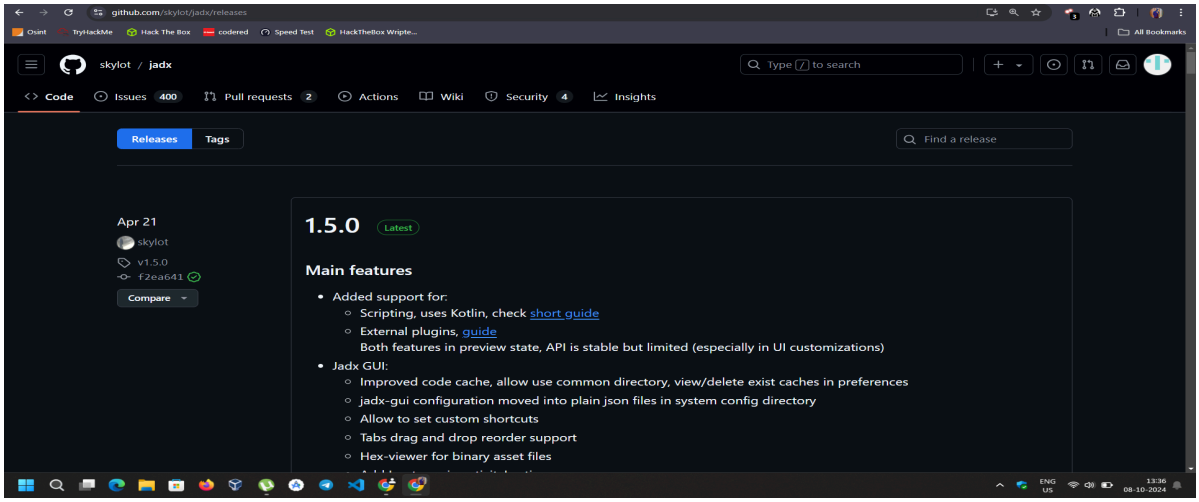
Overview

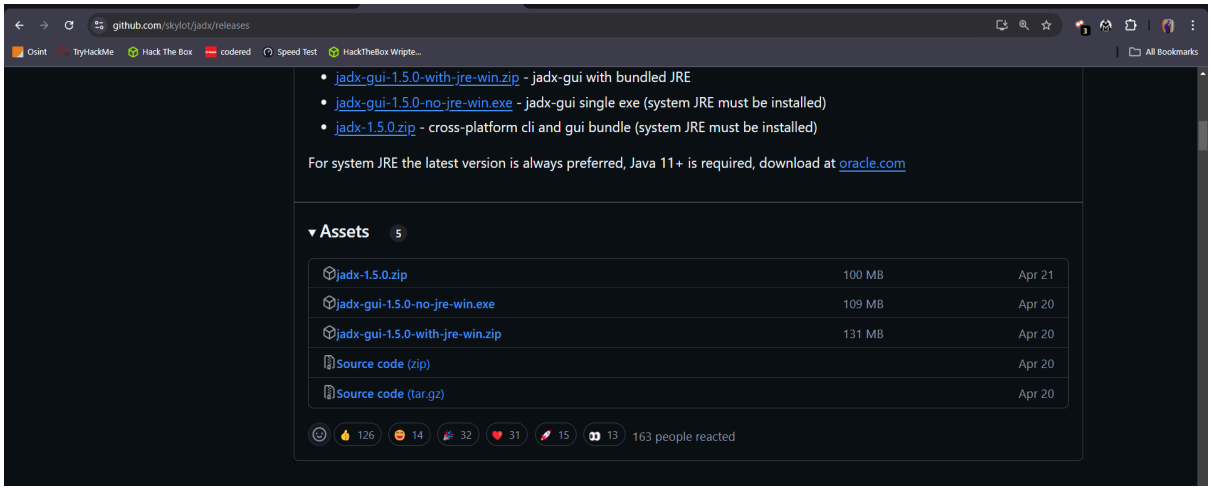
During my internship with NULLCLASS, I was tasked with completing three key assignments that involved hands-on technical implementation and documentation. These assignments not only enhanced my understanding of critical cybersecurity concepts but also honed my practical skills in Android OS penetration, Mobile Device Management (MDM), and APK file analysis. Below is a detailed report on the assigned tasks, showcasing both the methodology and proof of concept (POC) for each.

Task 3: Decompiling an APK File Using JADX

Overview:

In this task, I will demonstrate how to decompile an Android APK file using two popular tools, **JADX**, to extract its source code and resources. This process is essential for reverse engineering Android applications to analyze their structure and understand their functionalities for research or security pur





Setting Up the Tools

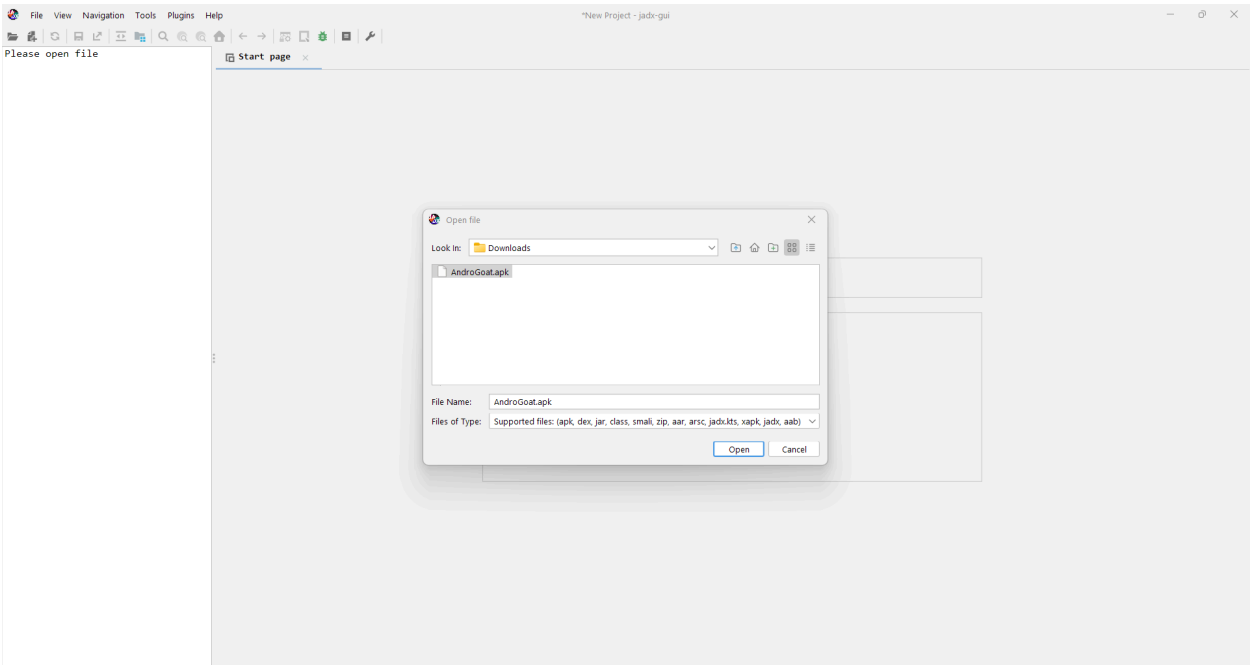
Download JADX:

- **Go to the official GitHub page of JADX.**
- **Download the latest version of JADX (jadx-gui-1.5.0-no-jre-win.exe) and extract it to a folder of your choice.**
- **Run .exe file**

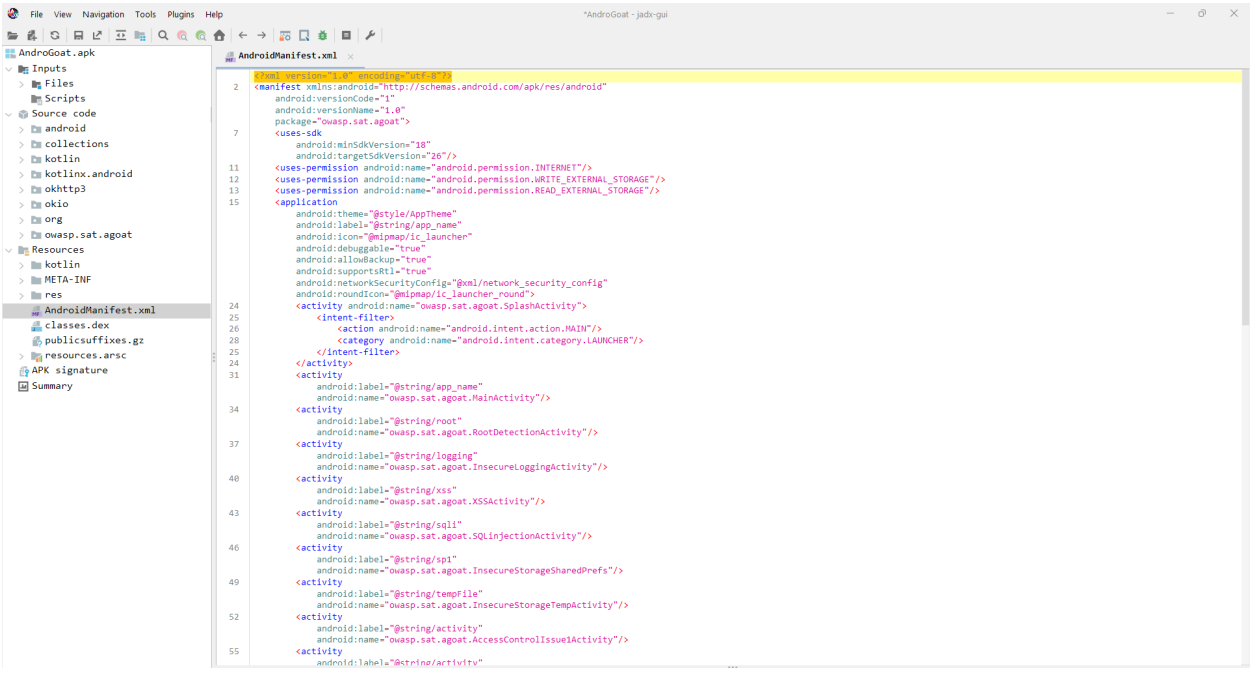
Then the dashboard page is open after that perform step given below

```
:open file

:select your .apk file

:then click open
```

`Your file is successful decompile now you can see the source code and resource`



In the given below you can see the android resource file which says which permission required to run app and other things



Impact:

Decompiling APK files with tools like JADX and APKTool is invaluable for app security auditing, bug fixing, and understanding third-party software. It aids in identifying security vulnerabilities, ensuring compliance with security standards, and analyzing the inner workings of mobile applications. By reverse engineering apps, security professionals can detect malicious behavior, intellectual property violations, or even optimize app performance, leading to better overall application security and user trust.

Conclusion:

Decompiling an APK file allows you to reverse engineer an Android app to analyze its behavior, security flaws, or UI components. Both JADX and APKTool are powerful tools in this process, with JADX providing Java-readable source code and APKTool focusing more on resources and smali code. This makes these tools essential for security researchers and developers who wish to understand the inner workings of Android applications.