Ex140

Joshua Main-Smith

2020-12-08

Contents

Technical Report **2**
Finding: Sensitive Data Exfiltrated 2
Risk Assessment 2
Vulnerability Description 2
Mitigation or Resolution Strategy 2

Attack Narrative **2**
Downloading and Analyzing F4rmC0rp.apk 2

Technical Report

Finding: Sensitive Data Exfiltrated

Risk Assessment

User credentials were exfiltrated by doing a simple string search for key information.The consequence of this is an attacker can gain access to the user account after recovering credentials.

Vulnerability Description

After decompiling the application an attacker was easily able to see the functionality of the app by viewing the source code, as it was not obfuscated. An attacker can view sensitive information as the data was not properly handled.

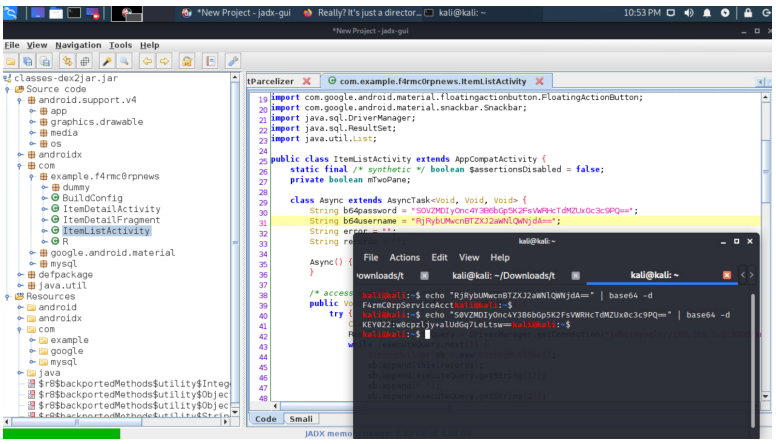
Mitigation or Resolution Strategy

Follow the OWASP Mobile Application Security Verification Standard to implement Resiliency Against Reverse Engineering and Tampering (MASVS-R).

Attack Narrative

Downloading and Analyzing F4rmC0rp.apk

We began by downloading F4rmC0rp's new application located at the web address **www.f4rmc0rp.com/apps/f4rmc0rp.apk**. We were able to open and decompile the a application by converting the apk file to a jar file with **d2j-dex2jar -d f4rmc0rp.apk**. We were then able to open the jar file in a **jadx** GUI by calling **jadx-gui** then opening the newly created .jar file.



We tested the application against reverse engineering and code modification resilience by searching for key strings. Specifically, we found that we were able to find service credentials by simply searching for a username or password in the jadx GUI (enabling string searches in the code).

These credentials were located under **com/example.f4rmc0rpnews/ItemListActivity** and were encrypted using base64, which were decrypted giving us user credentials.