

Forum:[Hack Forums](#)

Thread: [How find vulnerability on the apk??](#)

selluk3 - February 26, 2023, 8:12 am

hu;

How find vulnerability on the apk??

i saw this program : Yaazhini

how use it and exploit the leaks for access admin

double-o-tuxedo - March 2, 2023, 11:23 am

1. Decompilation: APKs are compressed files, which can be decompiled using tools like Apktool, dex2jar, or JADX. Decompiling the APK can allow you to analyze its code and identify potential vulnerabilities.

2. Static Analysis: Once the APK is decompiled, you can perform a static analysis of the code. This can involve looking for potential vulnerabilities such as hard-coded passwords, sensitive data leaks, and code injection attacks.

3. Dynamic Analysis: Dynamic analysis involves running the APK on a virtual device or emulator, and using tools such as Burp Suite, Wireshark, or Frida to intercept and analyze network traffic. This can help you identify potential vulnerabilities such as insecure communication, session hijacking, and other network-based attacks.

4. Fuzzing: Fuzzing is a technique that involves sending large amounts of random data to an application to see how it responds. This can help identify potential vulnerabilities such as buffer overflows, input validation errors, and other software flaws.

5. Code Review: Finally, a thorough code review of the APK can help identify potential vulnerabilities that may have been missed during static or dynamic analysis.

selluk3 - March 3, 2023, 5:09 pm

(Mar 2, 2023 12:23 PM)double-o-tuxedo Wrote: [\[CITE\]](#) 1. Decompilation: APKs are compressed files, which can be decompiled using tools like Apktool, dex2jar, or JADX. Decompiling the APK can allow you to analyze its code and identify potential vulnerabilities.

2. Static Analysis: Once the APK is decompiled, you can perform a static analysis of the code. This can involve looking for potential vulnerabilities such as hard-coded passwords, sensitive data leaks, and code injection attacks.

3. Dynamic Analysis: Dynamic analysis involves running the APK on a virtual device or emulator, and using tools such as Burp Suite, Wireshark, or Frida to intercept and analyze network traffic. This can help you identify potential vulnerabilities such as insecure communication, session hijacking, and other network-based attacks.

4. Fuzzing: Fuzzing is a technique that involves sending large amounts of random data to an application to see how it responds. This can help identify potential vulnerabilities such as buffer overflows, input validation errors, and other software flaws.

5. Code Review: Finally, a thorough code review of the APK can help identify potential vulnerabilities that may have been missed during static or dynamic analysis.

thks very very much, i understand the method