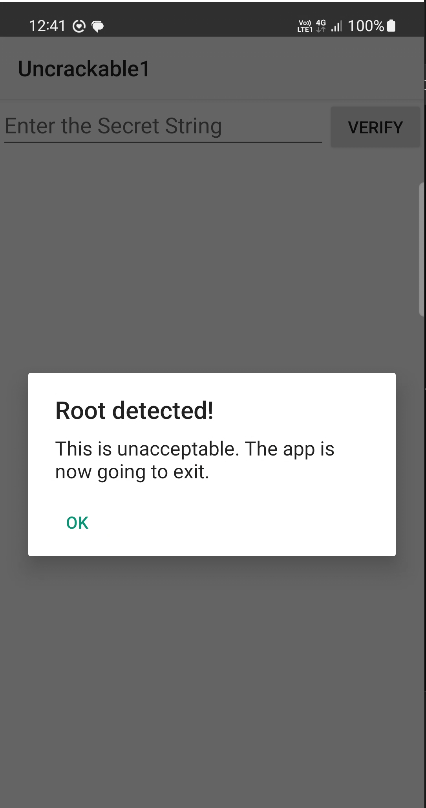
תרגיל Uncrackable1

בתרגיל זה ניישם טכניקות של ניתוח סטטי ודינמי כדי לפתור את האתגר Uncrackable1.apk.

מטרה: עליכם להבין מה האפליקציה עושה ולמצוא את הקוד הסודי.

# פתרון:

1. ניתוח התנהגות: הריצו את האפליקציה:



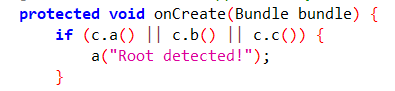
2. קודם כל צריך לנטרל את בדיקת ה root. אפשר לדלג על שלב זה ולחפש דרך להגיע לסוד ישירות, אבל מומלץ לתרגל תרחיש זה.

# 2.1 ניטרול בדיקת root:

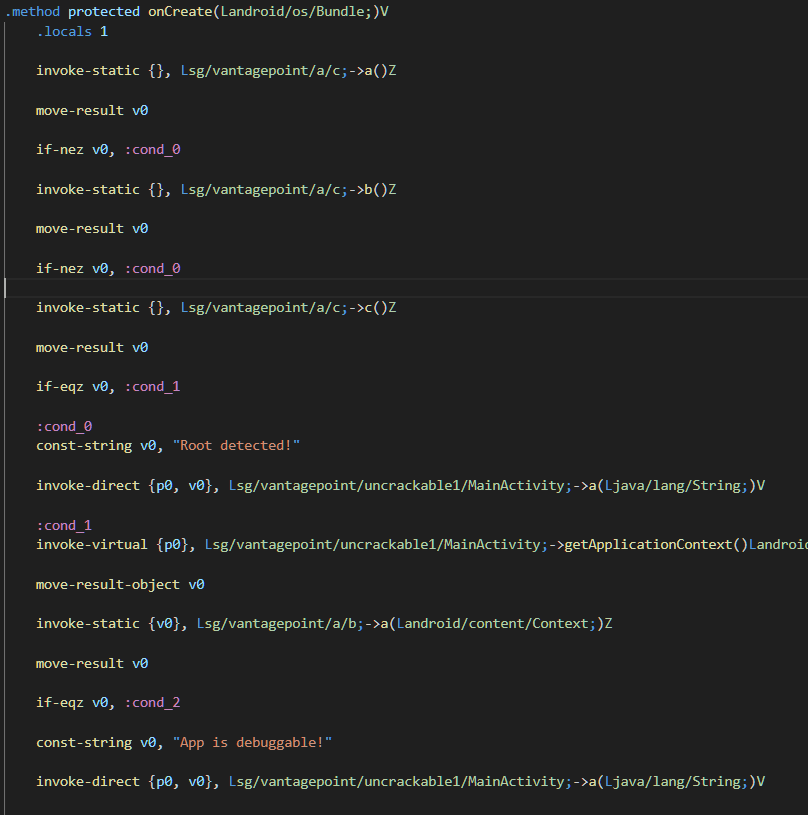
* נבצע ניתוח סטטי כדי למצוא את הבדיקה.
  + פתחו את ה apk ב jadx-gui
  + נגלה ב mainfest שיש activity אחד:



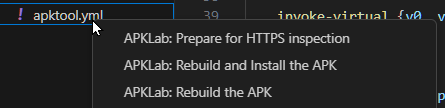
* + הקוד הרלוונטי נמצא כאן:



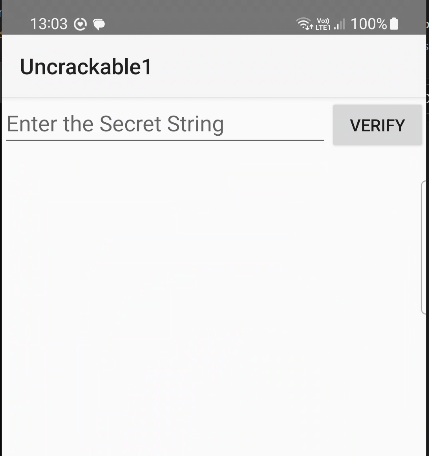
* צריך לשנות את התנאי כך שיחזיר False או לבטל אותו.
* אפשר לעשות patching ל apk או לשנות דינמית עם פרידה.
  + **אפשרות 1**: patching:
    - פתחו את ה apk עם apklab. כל הקוד smali להלן מבצע את הבדיקות, אפשר להסיר אותו (שורות 55 עד 93 כולל(:



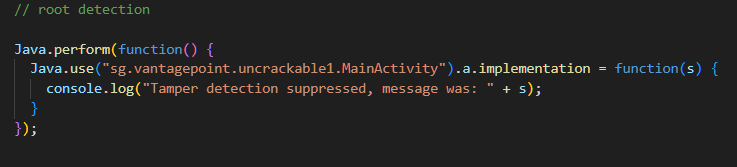
* + - בנו מחדש את ה apk:



* + - הריצו מחדש את ה apk שבניתם:
* \UnCrackable-Level11\dist\UnCrackable-Level1.apk
  + - בדיקת ה root בוטלה:



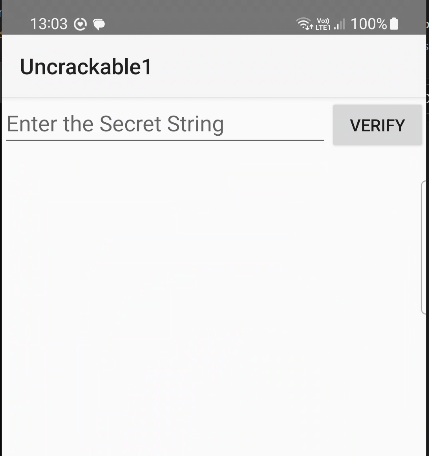
* + **אפשרות 2**: frida
    - וודאו ש frida-server רץ על המכשיר:
    - 
    - כתבו את הסקריט הבא בתוך uncrackable1.js:



* + - הריצו את פרידה עם הסקריפט:

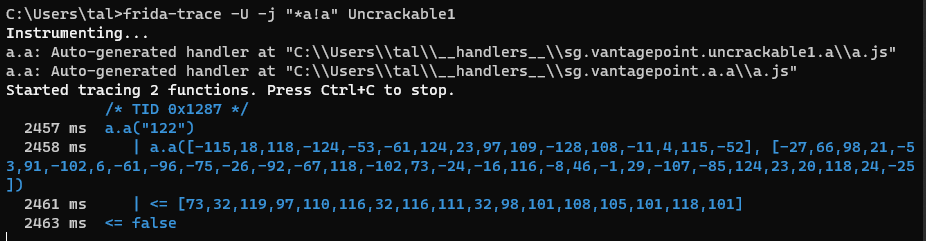


* + - וודאו שהאפליקציה נפתחת בלי בדיקת root:



# 2.2 שליפת הסוד:

* + - הריצו trace על הפונקציה aשמחזירה את הסוד מפוענח מהצפנה:
    - frida-trace -U -j "\*a!a" Uncrackable1



* + - תרגמו את ה ascii לתווים וקבלו את הסוד:

