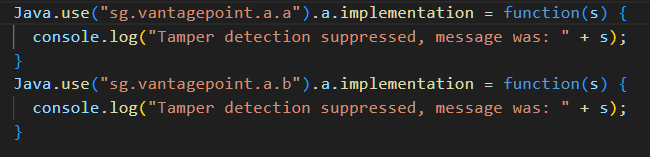
תרגיל uncrackable 2

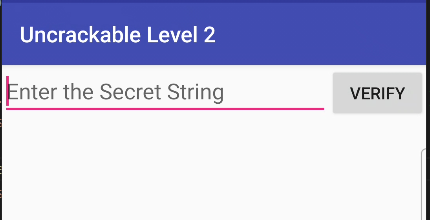
עליכם לגלות את הקוד הסודי באפליקציה UnCrackable-Level2.

פתרון:

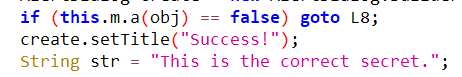
1. מההתנהגות יש הגנת root ו-debuggable. נטרלו את ההגנות כפי שלמדנו בתרגיל הקודם עם פרידה:



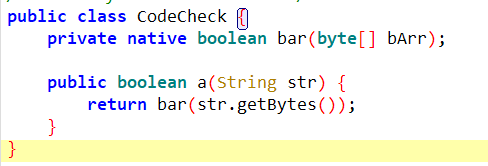
צריך לגלות את הקוד הסודי:



נסתכל בקוד:

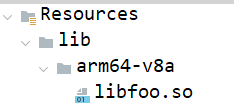






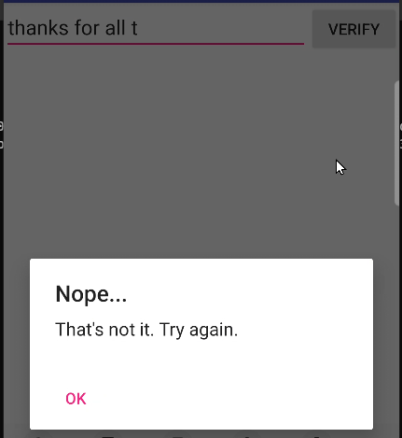
כלומר הפונקציה שבודקת את הקוד היא native.

זאת הספרייה:



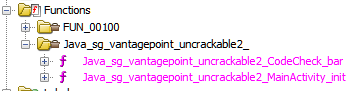
אם נבצע strings נמצא משהו חשוד אבל לא עובד:



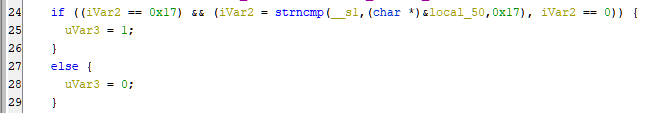


נבצע disassembly עם ghidra

נמצא את הפונקציה bar:



נראה שיש strncmp שמקבל את המשתנה עם הסוד:



יש שלושה משתנים לוקליים שמכילים את המחרוזות של הסוד:



נתרגם ל ASCII:



נחבר:



כמעט הגענו:



