מטלת סיכום – מעבדת התקפה

מגישים- יניר כהן - 318658812 שלמה פרל – 314676362

לא הוספנו הרשאות חדשות

התהליך:

1) יצרנו אפליקציה משלנו בה כתבנו את כל הפונקציות שמביאות מידע על המכשיר ורושמות אותו לקובץ. את הקובץ מצאנו בתוך ה device file explorer.
כל הפונקציות שלנו היו בנפרד בתוך הclass ופונקציה אחת מרכזית הפעילה את כולן שלחצו על כפתור ששמנו כדי לדמות למה שצריך שיקרה באפליקציה magicDate. ווידאנו שהכל עובד כמו שצריך.

2) לאחר מכן יצרנו מהאפליקציה שלנו קובץ apk והעברנו אותו ל smali כדי שנוכל להעתיק משם את דברים הרלוונטיים.

3) העברנו את קובץ ה apk של האפלקציה magicDate ל smali . שם ראינו שיש 2 פונקציות בשם calc , getRandom. לפי המובן מהכפתורים שיש באפליקציה – random, calculate יכולנו להבין איזה פונקציה מופעלת שלוחצים על כפתור הrandom .
חיפשנו איפה הפונקציה getRandom מופיעה וזיהינו את המקום בו קוראים לה והוספנו שם שורה שתפעיל בנוסף גם את הפונקציה המרכזית שלנו שהיא כבר יודעת לקרוא לכל שאר הפונקציות ולכתוב את כל המידע שהשגנו בעזרתן בקובץ.
במקום בקובץ בו זיהינו שמופיעות כל הפונקציות של האפליקציה הוספנו כל הפונקציות שלנו

4) עברנו על כל ההוספות שלנו ועשינו את ההחלפות המתאימות כדי שהפונקציות שלנו יהיו זהות מבחינת שם האפליקציה (במקום attack – שלנו החלפנו ל- magicDate).

5) לאחר מכן עשינו את התהליך של ההחזרה לקובץ apk עם השינויים וחתמנו אותו התקנו את האפליקציה על המכשיר הפעלנו ורק כאשר לוחצים על כפתור הrandom הקובץ נוצר.

* בהתחלה שניסינו לגשת לתיקייה של האפליקציה magicDate הופיעה שם הכיתוב " no debuggable " ולא יכולנו להיכנס לתיקייה ואז הוספנו לקובץ הAndroid Manifest תחת application את "android:debuggable=true" לאחר מכן חזרנו על תהליך החתימה וכל הנדרש ויכולנו לראות את הקובץ שנוצר לאחר הלחיצה על כפתור הrandom.