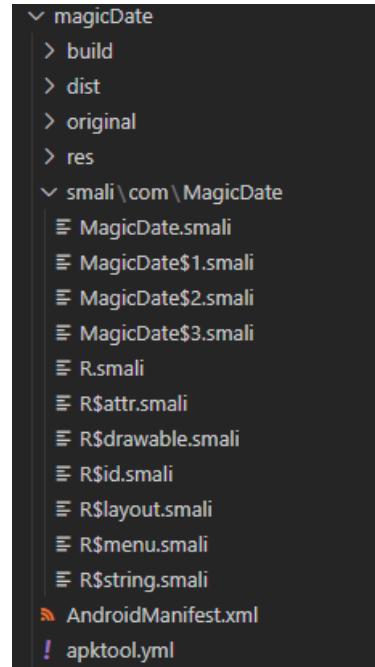


מעבדת התקפה – מטלת סיום

דביר אברהם – 207029364

תהליך הזרקת קוד זדוני לאפליקציה:

1. בתחילת פותחתי את קובץ האapk וקרויתי את מבנה האפליקציה.



2. הבנתי שהקוד החשוב שאלוי אני צריך להתייחס נמצא בקובץ MagicDate.smali המשכתי לחקור את הקוד שנמצא בו MagicDate.smali, ראיתי שלמחלוקת קוראים MagicDate והוא ירושת activity myIntent ומישמת את OnClickListener של View.OnClickListener. וראיתי שיש בה switch case על הceptors, בכפטור של getRandom רגע לפני שהפונקציה getRandom נקראת, הכנסתי לשם את הקוד/zdoni.

```
0     .line 137
1     .end local v0      # "tmpAnzahl":Ljava/lang/String;
2     :pswitch_1
3     invoke-direct {p0}, Lcom/MagicDate/MagicDate;->getInfo()V
4
5     invoke-direct {p0}, Lcom/MagicDate/MagicDate;->getRandom()V
6
7     goto :goto_0
8
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/zdoni כתבתי באפליקציה חדשה, שדיםתי כמה שיטור את האפליקציה שאלייה אני מכניס את הקוד, כלומר יצרתי MainActivity שירוש>MainActivity מימוש את OnClickListener, וקורא לפונקציה פרטית של המחלקה שם הקוד/zdoni נמצא.

4. בעזרת הקוד הזרוני גנבתי מידע על חומרת המכשיר, את אנשי הקשר במכשיר, את המשמש המחבר למכשיר ואת המיקום האחרון של המכשיר, לטובת זה השתמשתי בהרשאות מיקום והרשאות לאנשי הקשר. את המידע כתבתי לקובץ information.txt שנמצא בתיקייה של האפליקציה בatabase internal storage apktool.
5. בניתי apk חדש של האפליקציה הזרוני, פתחתה את apk בעזרת apktool וחיפשתי את הקוד הזרוני. ברגע שמצאתו אותו העתקתי אותו לזמין MagicDate.smali, עשית התאמות קטנות של שמות המחלקה וסגרתי בחזרה את התיקייה לapk חדש, חתמתי עלייו בעזרת jarsigner והתקנתו אותו על האימולטור ובדקתי שהוא תקין.
6. בסופו, נכנסתי לshell adb עם הרשאות root, הלכתי לתיקייה של האפליקציה בנתיב generic_x86:/data/user/0/com.MagicDate ושם היה הקובץ information.txt שכתבתי את המידע, נכנסי 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: 37.421998333333335, lon: -122.084
contacts:
    name: Dvir, phone number: 0500000000
    name: John Doe, phone number: 0522222222
generic_x86:/data/user/0/com.MagicDate #
```