בשלב הראשון במשימה חיפשתי את הפונקציה שנקראת OnClick בלחיצה על כפתור ה Random באפליקציית magic date

על מנת לעשות זאת השתמשתי ב apktool על מנת לחלץ את קבצי הSMALI והXMLים של התכנים של האפליקציה וחיפשתי את הטקסט "Random" שמופיע על הכפתור במסך האפליקציה.

בקובץ strings.xml מצאתי את הרפרנס ל string של Random תחת השם 'zufall'

לאחר מכן השתמשתי ב dex2jar על מנת לנסות לבצע decompilation לאפליקציה ולנסות לקבל מקובץ הDEX source code . בחיפוש של zufall בקובץ הJAR שנוצר , מצאתי רפרנס אליו בפונקציית onClick שבתוכה היה switch case שמזהה את ה ID של הכפתורים השונים במסך הראשי של האפליקציה שאותו כפתור RANDOM הוא אחד מהם.

כאשר הCASE של כפתור ה RANDOM נלחץ, ישנה קריאה לפונקצייה פנימית הנקראית getRandom() ואחריה הCASE מסתיים.

המטרה שלי בשלב זה היה להכניס את הקוד הזדוני בתוך אותו SWITCH CASE שמתבצע בעת לחיצה על כפתור RANDOM , לאחר הקריאה ל getRadom() .

בקוד MagicDate.smali שנוצר מהרצת apktool מצאתי את ה SWITCH CASE המדובר

```
.line 137
.end local v0    # "tmpAnzahl":Ljava/lang/String;
:pswitch_1
invoke-direct {p0}, Lcom/MagicDate/MagicDate;->getRandom()V

## getRandom() function here
invoke-direct {p0, p0}, Lcom/MagicDate/MagicDate;->blabla(Landroid/content/Context;)V

## end changed code

goto :goto_0
```

הפונקציה blabla() שנקראת לאחר ההערה שהכנסתי היא הקריאה לפונקציה הזדונית שכתבתי והזרקתי לתוך האפליקציה ומבצעת את איסוף המידע שנשמר בסופו של דבר לקובץ ה information.txt

לאחר זיהוי המקום בקוד בו עלי להכניס את הקוד הזדוני, ניסיתי לבצע בדיקה קטנה של כתיבה לקובץ LOG כדי לראות שאכן הקוד נקרא כמתוכנן והאפליקציה לא קורסת.

משלב זה ואילך העבודה שלי התמקדה בכתיבת הקוד שיאסוף את המידע באפליקציה שיצרתי ב android studio , קימפלו לקוד SMALI , העתקתו לקובץ ה MagicDate.smali , אריזתו מחדש עם apk tool , לאחר מכן חתימתו עם מפתחות DEBUG של אנרואיד, ולבסוף התקנת והרצת האפליקציה עם הקוד הזדוני ובדיקה שאכן הקובץ information נוצר כמתוכנן עם המידע שרציתי לאסוף לאחר לחיצה על כפתור ה RANDOM באפליקציה.

המידע שאספתי כולל כתובת

IP , USER AGENT , ROUTER/AP IP, OS VERSION, DEVICE MODEL AND OTHER DETIALS, ARCHITECTURE, USERNAME, HOSTNAME, ANDROID VERSION, HARDWARE VERSION, PHONE CONTACTS AND PHONE CALL RECORDS

את כל אלו אספתי בעזרת שימוש ב3 הרשאות בלבד שהתווספו לאפליקציה לאחר הזרקת הקוד הזדוני.