Android Reverse Engineering and Analysis

Tato Kutalia

tatocaster

Android Chapter Lead @ TBC

tatocaster.me

debuggerpodcast.ge

(debugger) -> {podcast}

Pocket Casts · Apple Podcasts · Spotify · Google Podcasts · iHeart RADIO

Plan

- Tools
- Static Analysis vs Dynamic
- What is Reverse Engineering (RE)
- Stats
- CTF

Tools

Static Analysis

- JADX - Decompiler
- ApkTool - Decompiler
- Dex2Jar - Dex decompiler to Jar
- JD-GUI - Java Decompiler

Dynamic analysis

- FRIDA

Disassembler

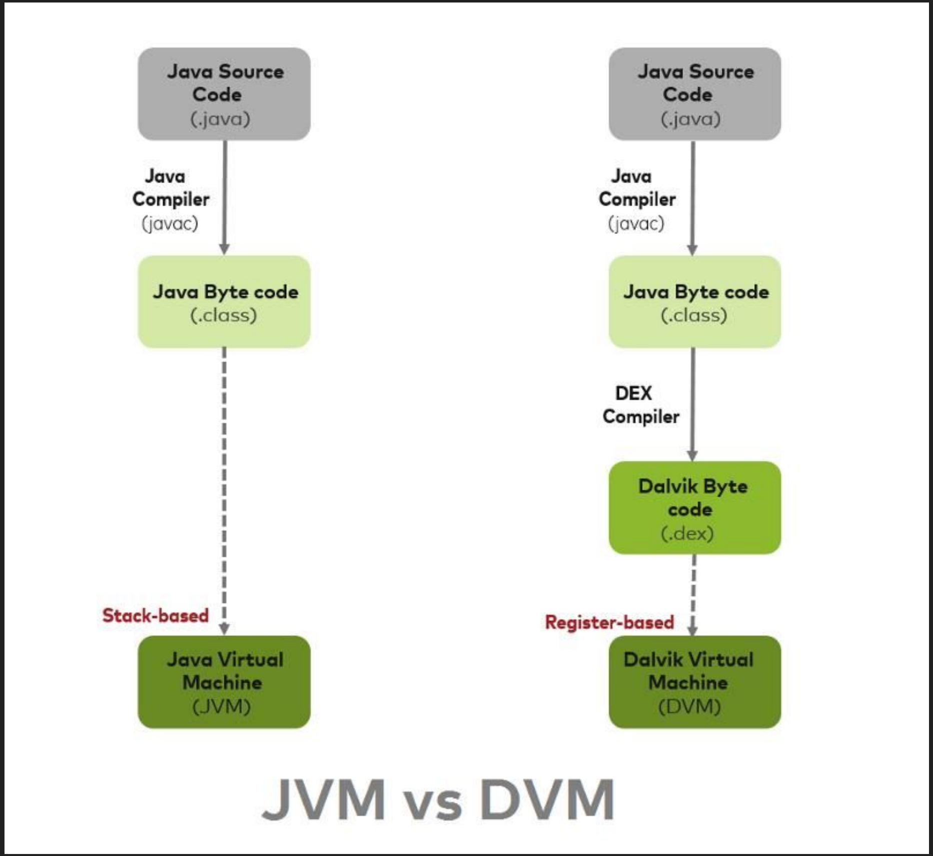
- GHIDRA
- IDA PRO

Application Structure

APK

- AndroidManifest.xml
- META-INF/ - java meta/signatures
- classes.dex - dalvik bytecode
- lib/ - native libs
- assets/ - other

Java vs Android compilation



Java vs Smali

Java

```
private static void myMethod()
```

smali

```
.method private static myMethod()V
```

Java vs Smali

Java

```
public Boolean myStrMethod(byte mybyte, String str)
```

smali

```
.method public myStrMethod(B; Ljava/lang/String)Z –
```

http://pallergabor.uw.hu/androidblog/dalvik_opcodes.html

https://github.com/JesusFreke/smali/wiki

Entry point

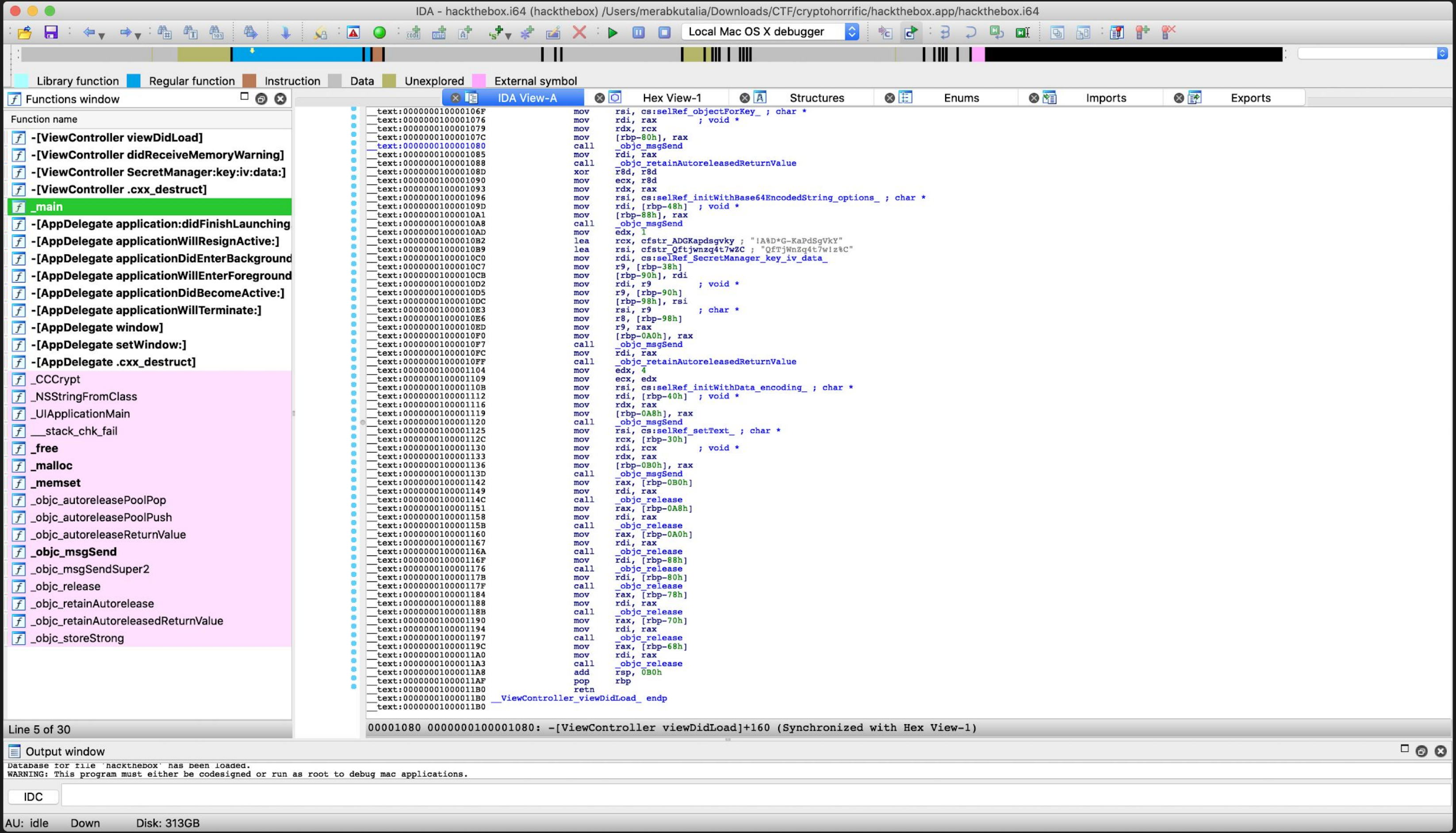
- Activity
- Services
- Receivers
- ContentProviders
- Application
- exported components!!

RE? Malware analysis? Pentest?

- list activities and exported components
- monitor api calls - Burp Suite + (bypass SSL pinning)?
- analyze decompiled code

RE: DEMO

What about .so files?

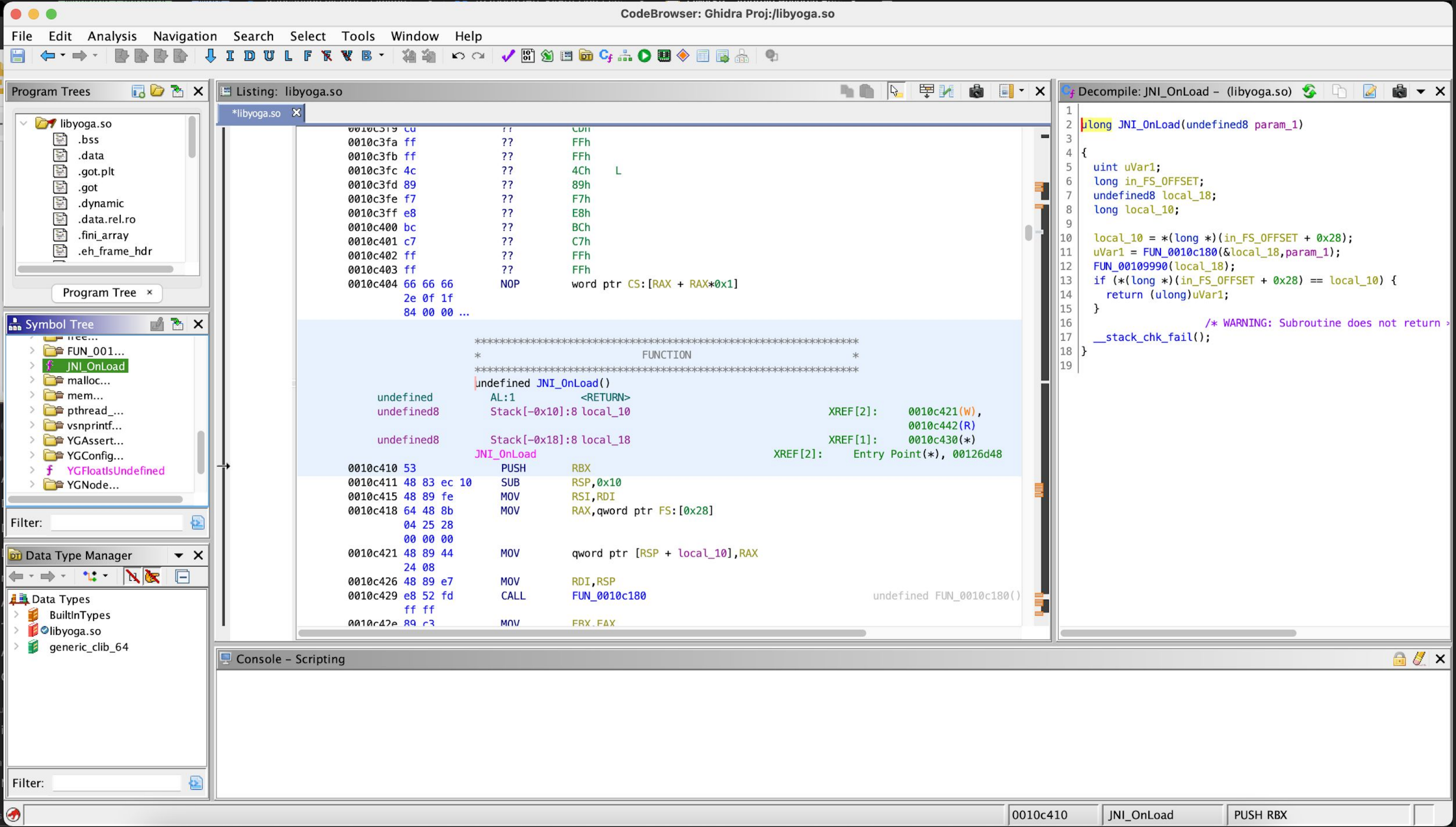


```
-[ViewController viewDidLoad]
-[ViewController didReceiveMemoryWarning]
-[ViewController SecretManager:key:iv:data:]
-[ViewController .cxx_destruct]
_main
-[AppDelegate application:didFinishLaunching
-[AppDelegate applicationWillResignActive:]
-[AppDelegate applicationDidEnterBackground
-[AppDelegate applicationWillEnterForeground
-[AppDelegate applicationDidBecomeActive:]
-[AppDelegate applicationWillTerminate:]
-[AppDelegate window]
-[AppDelegate setWindow:]
-[AppDelegate .cxx_destruct]
_CCCrypt
_NSStringFromClass
_UIApplicationMain
___stack_chk_fail
_free
_malloc
_memset
_objc_autoreleasePoolPop
_objc_autoreleasePoolPush
_objc_autoreleaseReturnValue
_objc_msgSend
_objc_msgSendSuper2
_objc_release
_objc_retainAutorelease
_objc_retainAutoreleasedReturnValue
_objc_storeStrong
```

```
__text:000000010000106F                 mov     rsi, cs:selRef_objectForKey_ ; char *
__text:0000000100001076                 mov     rdi, rax        ; void *
__text:0000000100001079                 mov     rdx, rcx
__text:000000010000107C                 mov     [rbp-80h], rax
__text:0000000100001080                 call    _objc_msgSend
__text:0000000100001085                 mov     rdi, rax
__text:0000000100001088                 call    _objc_retainAutoreleasedReturnValue
__text:000000010000108D                 xor     r8d, r8d
__text:0000000100001090                 mov     ecx, r8d
__text:0000000100001093                 mov     rdx, rax
__text:0000000100001096                 mov     rsi, cs:selRef_initWithBase64EncodedString_options_ ; char *
__text:000000010000109D                 mov     rdi, [rbp-48h]  ; void *
__text:00000001000010A1                 mov     [rbp-88h], rax
__text:00000001000010A8                 call    _objc_msgSend
__text:00000001000010AD                 mov     edx, 1
__text:00000001000010B2                 lea     rcx, cfstr_ADGKapdsgvky ; "!A%D*G-KaPdSgVkY"
__text:00000001000010B9                 lea     rsi, cfstr_Qftjwnzq4t7wZC ; "QfTjWnZq4t7w!z%C"
__text:00000001000010C0                 mov     rdi, cs:selRef_SecretManager_key_iv_data_
__text:00000001000010C7                 mov     r9, [rbp-38h]
__text:00000001000010CB                 mov     [rbp-90h], rdi
__text:00000001000010D2                 mov     rdi, r9         ; void *
__text:00000001000010D5                 mov     r9, [rbp-90h]
__text:00000001000010DC                 mov     [rbp-98h], rsi
__text:00000001000010E3                 mov     rsi, r9         ; char *
__text:00000001000010E6                 mov     r8, [rbp-98h]
__text:00000001000010ED                 mov     r9, rax
__text:00000001000010F0                 mov     [rbp-0A0h], rax
__text:00000001000010F7                 call    _objc_msgSend
__text:00000001000010FC                 mov     rdi, rax
__text:00000001000010FF                 call    _objc_retainAutoreleasedReturnValue
__text:0000000100001104                 mov     edx, 4
__text:0000000100001109                 mov     ecx, edx
__text:000000010000110B                 mov     rsi, cs:selRef_initWithData_encoding_ ; char *
__text:0000000100001112                 mov     rdi, [rbp-40h]  ; void *
__text:0000000100001116                 mov     rdx, rax
__text:0000000100001119                 mov     [rbp-0A8h], rax
__text:0000000100001120                 call    _objc_msgSend
__text:0000000100001125                 mov     rsi, cs:selRef_setText_ ; char *
__text:000000010000112C                 mov     rcx, [rbp-30h]
__text:0000000100001130                 mov     rdi, rcx        ; void *
__text:0000000100001133                 mov     rdx, rax
__text:0000000100001136                 mov     [rbp-0B0h], rax
__text:000000010000113D                 call    _objc_msgSend
__text:0000000100001142                 mov     rax, [rbp-0B0h]
__text:0000000100001149                 mov     rdi, rax
__text:000000010000114C                 call    _objc_release
__text:0000000100001151                 mov     rax, [rbp-0A8h]
__text:0000000100001158                 mov     rdi, rax
__text:000000010000115B                 call    _objc_release
__text:0000000100001160                 mov     rax, [rbp-0A0h]
__text:0000000100001167                 mov     rdi, rax
__text:000000010000116A                 call    _objc_release
__text:000000010000116F                 mov     rdi, [rbp-88h]
__text:0000000100001176                 call    _objc_release
__text:000000010000117B                 mov     rdi, [rbp-80h]
__text:000000010000117F                 call    _objc_release
__text:0000000100001184                 mov     rax, [rbp-78h]
__text:0000000100001188                 mov     rdi, rax
__text:000000010000118B                 call    _objc_release
__text:0000000100001190                 mov     rax, [rbp-70h]
__text:0000000100001194                 mov     rdi, rax
__text:0000000100001197                 call    _objc_release
__text:000000010000119C                 mov     rax, [rbp-68h]
__text:00000001000011A0                 mov     rdi, rax
__text:00000001000011A3                 call    _objc_release
__text:00000001000011A8                 add     rsp, 0B0h
__text:00000001000011AF                 pop     rbp
__text:00000001000011B0                 retn
__text:00000001000011B0 __ViewController_viewDidLoad_ endp
__text:00000001000011B0
```

```
00001080 0000000100001080: -[ViewController viewDidLoad]+160 (Synchronized with Hex View-1)
```

```
Database for file 'hackthebox' has been loaded.
WARNING: This program must either be codesigned or run as root to debug mac applications.
```



```
        0010c3f9 cd             ??         CDh
        0010c3fa ff             ??         FFh
        0010c3fb ff             ??         FFh
        0010c3fc 4c             ??         4Ch    L
        0010c3fd 89             ??         89h
        0010c3fe f7             ??         F7h
        0010c3ff e8             ??         E8h
        0010c400 bc             ??         BCh
        0010c401 c7             ??         C7h
        0010c402 ff             ??         FFh
        0010c403 ff             ??         FFh
        0010c404 66 66 66       NOP        word ptr CS:[RAX + RAX*0x1]
                 2e 0f 1f
                 84 00 00 ...

                            **************************************************************
                            *                          FUNCTION                          *
                            **************************************************************
                            undefined JNI_OnLoad()
              undefined         AL:1           <RETURN>
              undefined8        Stack[-0x10]:8 local_10                XREF[2]:     0010c421(W),
                                                                                    0010c442(R)
              undefined8        Stack[-0x18]:8 local_18                XREF[1]:     0010c430(*)
                            JNI_OnLoad                             XREF[2]:     Entry Point(*), 00126d48
        0010c410 53             PUSH       RBX
        0010c411 48 83 ec 10    SUB        RSP,0x10
        0010c415 48 89 fe       MOV        RSI,RDI
        0010c418 64 48 8b       MOV        RAX,qword ptr FS:[0x28]
                 04 25 28
                 00 00 00
        0010c421 48 89 44       MOV        qword ptr [RSP + local_10],RAX
                 24 08
        0010c426 48 89 e7       MOV        RDI,RSP
        0010c429 e8 52 fd       CALL       FUN_0010c180                          undefined FUN_0010c180()
                 ff ff
        0010c42e 89 c3          MOV        EBX,EAX
```

```c

ulong JNI_OnLoad(undefined8 param_1)

{
  uint uVar1;
  long in_FS_OFFSET;
  undefined8 local_18;
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  uVar1 = FUN_0010c180(&local_18,param_1);
  FUN_00109990(local_18);
  if (*(long *)(in_FS_OFFSET + 0x28) == local_10) {
    return (ulong)uVar1;
  }
                    /* WARNING: Subroutine does not return
  __stack_chk_fail();
}

```

Dynamic analysis

- change and examine app in runtime

FRIDA : DEMO

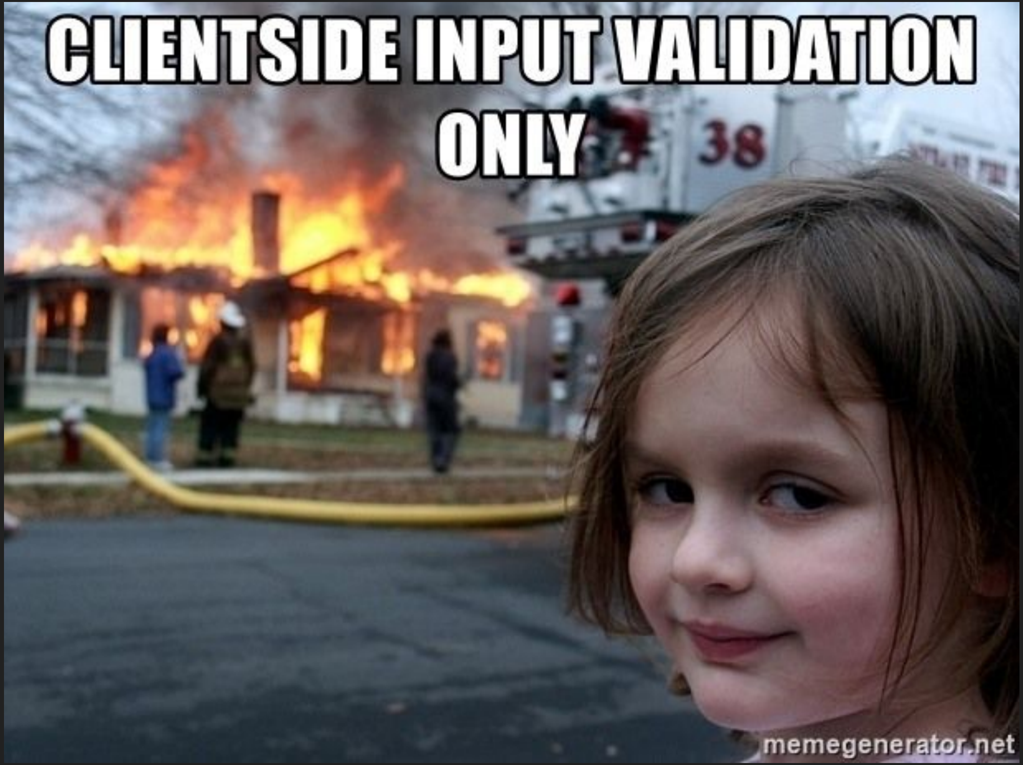
FRIDA Gadget vs FRIDA Server

```
// Gadget
 -   decompile APK
 -   add FRIDA native library to lib/
 -   inject into bytecode
 -   add permission
 -   repackage
 -   sign
 -   install
```

```
System.loadLibrary("frida-gadget")
```

```
const-string v0, "frida-gadget"
invoke-static {v0}, Ljava/lang/System;->loadLibrary(Ljava/lang/String;)V
```

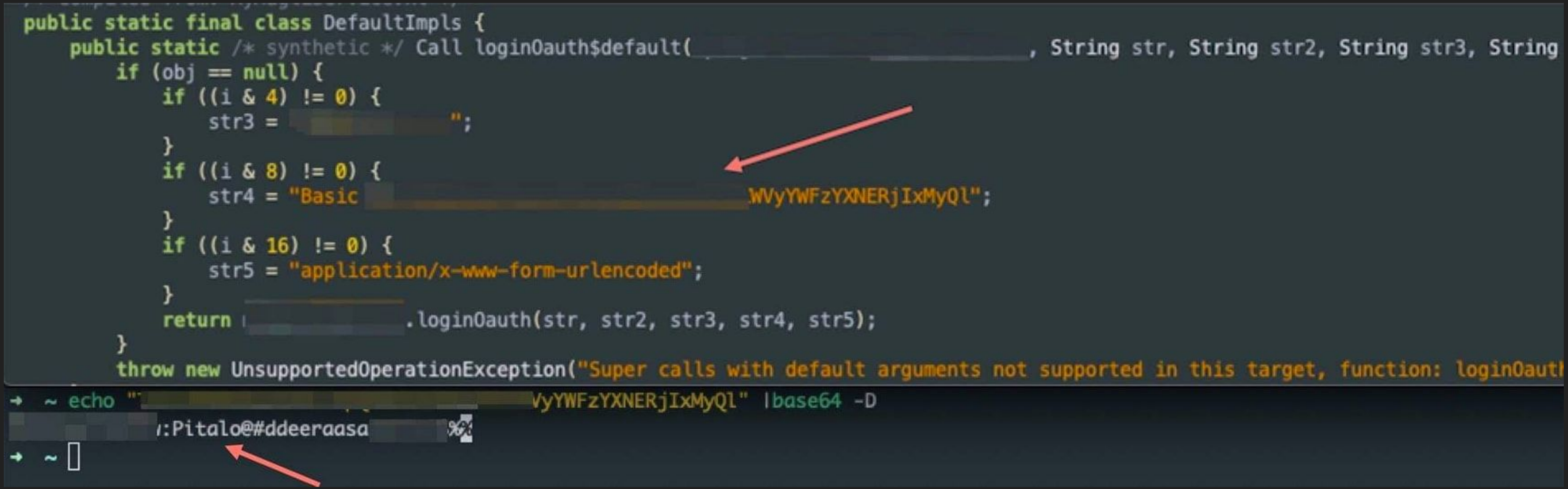
Scanned Apps



Scanned Apps

- bypass otp/pin - client side check only
- SQL injection
- base64 decoding leading to app crash
- mobile number / otp / pin / email enumeration
- exposed client secrets
- save sessionId in preferences
- password reset does not kill the current session
- leaking Google API keys
- leaking test url and users in prod
- leaking test features in production app

Scanned Apps

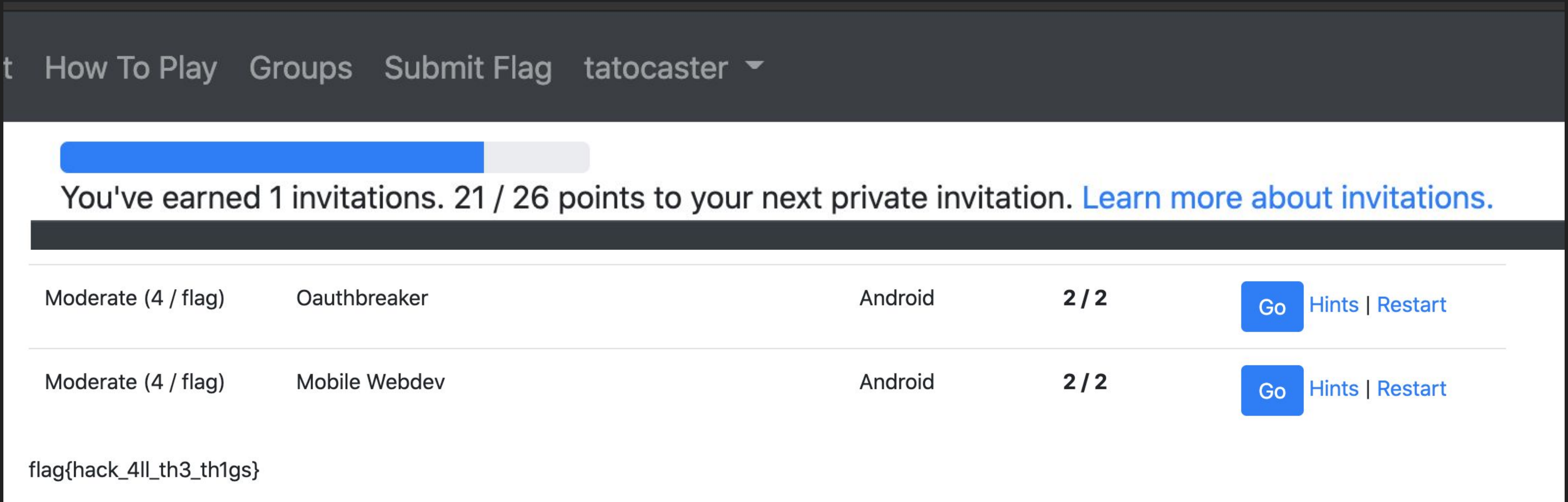


```
public static final class DefaultImpls {
    public static /* synthetic */ Call loginOauth$default([redacted], String str, String str2, String str3, String
        if (obj == null) {
            if ((i & 4) != 0) {
                str3 = [redacted]";
            }
            if ((i & 8) != 0) {
                str4 = "Basic [redacted]WVyYWFzYXNERjIxMyQl";
            }
            if ((i & 16) != 0) {
                str5 = "application/x-www-form-urlencoded";
            }
            return [redacted].loginOauth(str, str2, str3, str4, str5);
        }
        throw new UnsupportedOperationException("Super calls with default arguments not supported in this target, function: loginOauth
```

```
→ ~ echo "[redacted]VyYWFzYXNERjIxMyQl" |base64 -D
[redacted]:Pitalo@#ddeeraasa[redacted]%
→ ~
```

Bug Bounty

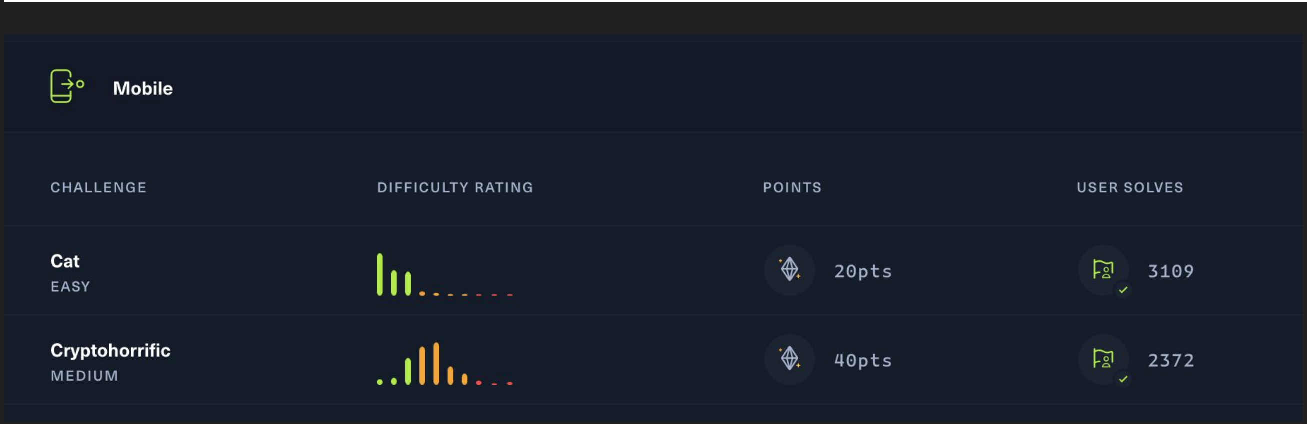
Catch the Flags



You've earned 1 invitations. 21 / 26 points to your next private invitation. Learn more about invitations.

Moderate (4 / flag)	Oauthbreaker	Android	**2 / 2**	Go Hints | Restart
Moderate (4 / flag)	Mobile Webdev	Android	**2 / 2**	Go Hints | Restart

flag{hack_4ll_th3_th1gs}



Mobile

CHALLENGE	DIFFICULTY RATING	POINTS	USER SOLVES
Cat EASY		20pts	3109
Cryptohorrific MEDIUM		40pts	2372

Questions