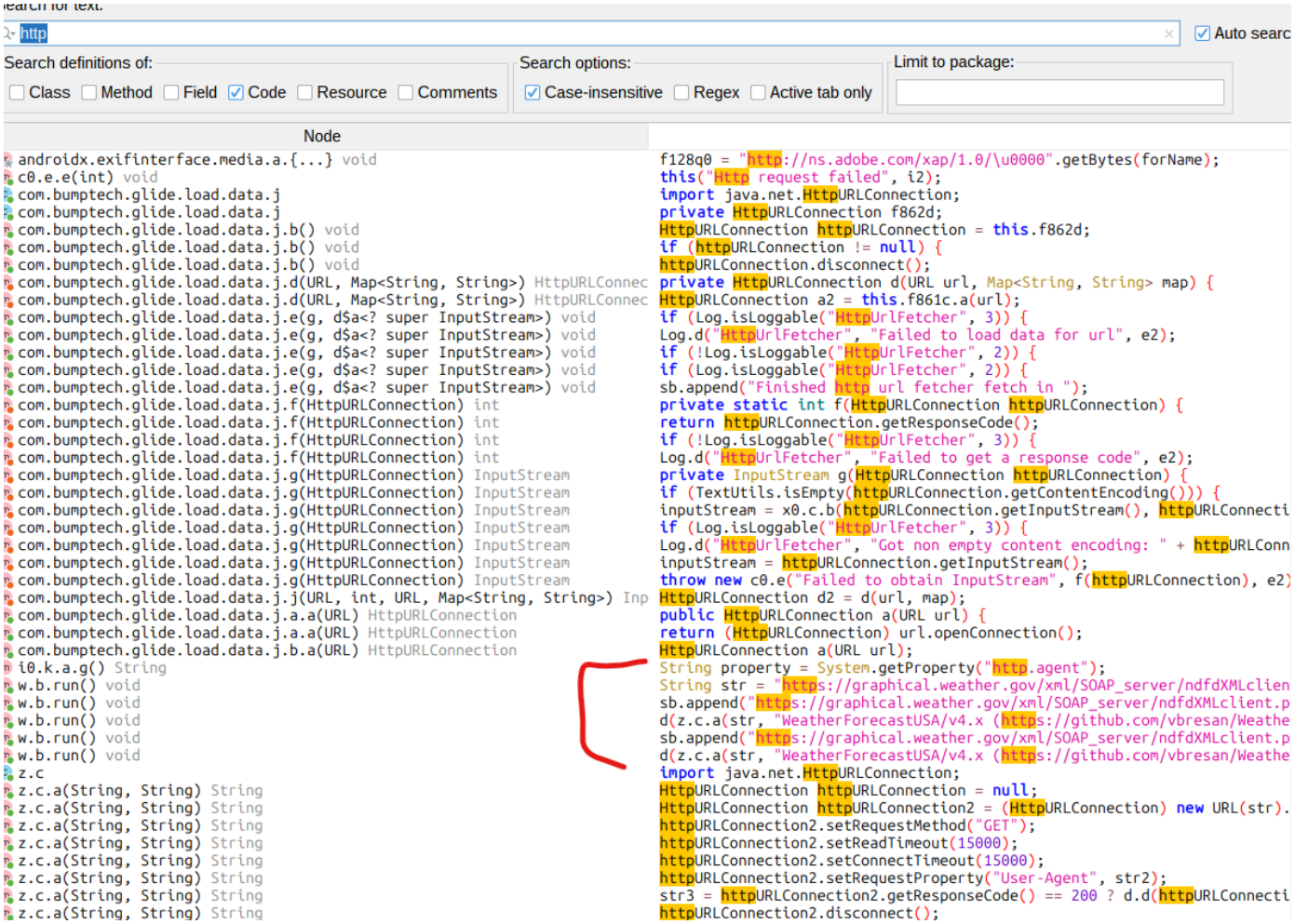
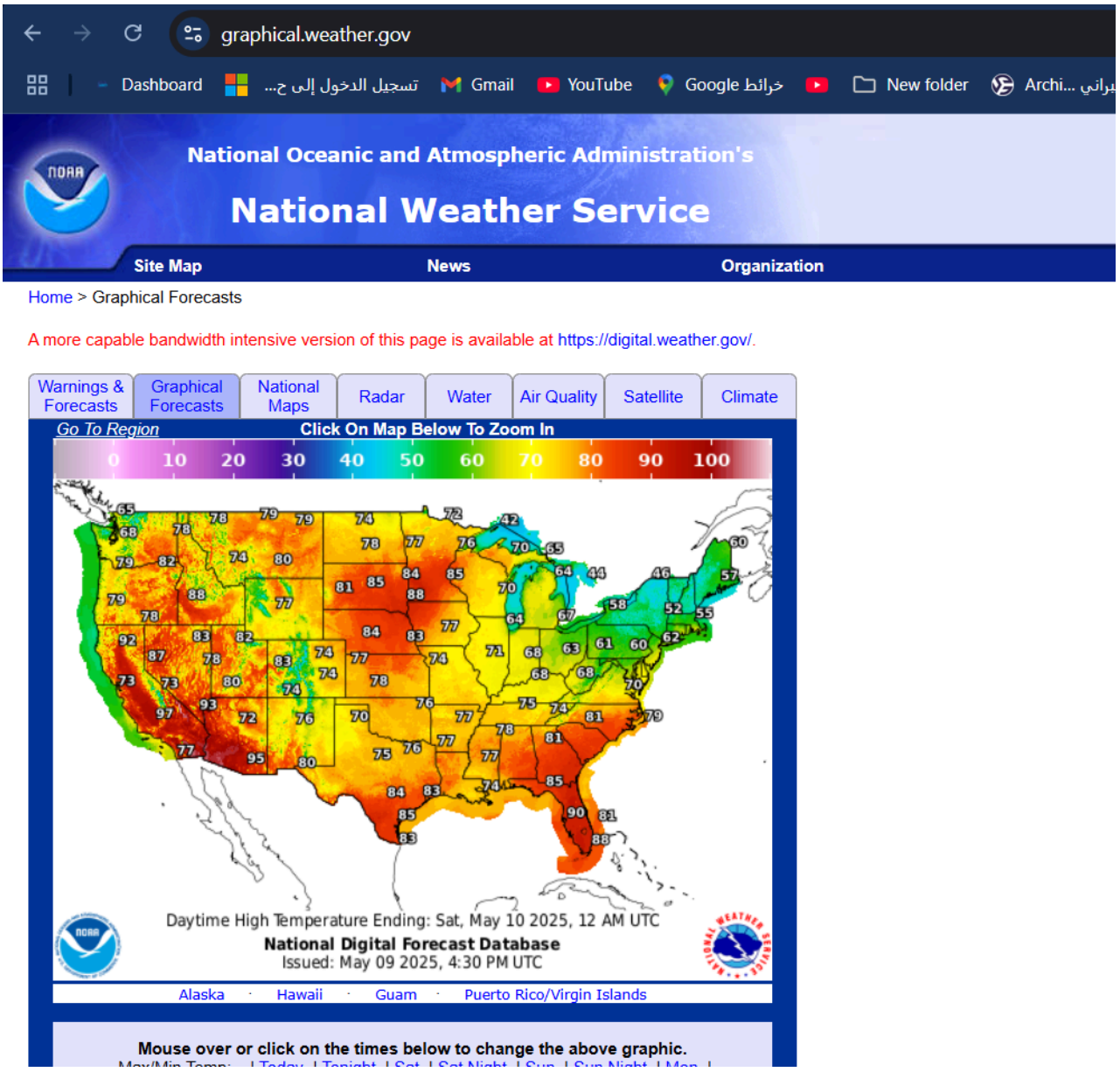
3-Reverse Engineering Android Apps

1- How to find API

لو عندك app وبيستخدم اي map يبقي ده بيعتمد علي API مثلا التطبيق ده فيه maps بيحدد الطقس يبقي كده هو بيستخدم API

فدلوقتي لو search for http : هنلاقيه فعلا بيستخدم API (SOAP API)


Search for text:
http
Auto searc
Search definitions of:
Class
Method
Field
Code
Resource
Comments
Search options:
Case-insensitive
Regex
Active tab only
Limit to package:
Node
androidx.exifinterface.media.a.{...} void
c0.e.e(int) void
com.bumptech.glide.load.data.j
com.bumptech.glide.load.data.j
com.bumptech.glide.load.data.j.b() void
com.bumptech.glide.load.data.j.b() void
com.bumptech.glide.load.data.j.b() void
com.bumptech.glide.load.data.j.d(URL, Map<String, String>) HttpURLConnec
com.bumptech.glide.load.data.j.d(URL, Map<String, String>) HttpURLConnec
com.bumptech.glide.load.data.j.e(g, d$a<? super InputStream>) void
com.bumptech.glide.load.data.j.e(g, d$a<? super InputStream>) void
com.bumptech.glide.load.data.j.e(g, d$a<? super InputStream>) void
com.bumptech.glide.load.data.j.e(g, d$a<? super InputStream>) void
com.bumptech.glide.load.data.j.e(g, d$a<? super InputStream>) void
com.bumptech.glide.load.data.j.f(HttpURLConnection) int
com.bumptech.glide.load.data.j.f(HttpURLConnection) int
com.bumptech.glide.load.data.j.f(HttpURLConnection) int
com.bumptech.glide.load.data.j.f(HttpURLConnection) int
com.bumptech.glide.load.data.j.g(HttpURLConnection) InputStream
com.bumptech.glide.load.data.j.g(HttpURLConnection) InputStream
com.bumptech.glide.load.data.j.g(HttpURLConnection) InputStream
com.bumptech.glide.load.data.j.g(HttpURLConnection) InputStream
com.bumptech.glide.load.data.j.g(HttpURLConnection) InputStream
com.bumptech.glide.load.data.j.g(HttpURLConnection) InputStream
com.bumptech.glide.load.data.j.g(HttpURLConnection) InputStream
com.bumptech.glide.load.data.j.j(URL, int, URL, Map<String, String>) Inp
com.bumptech.glide.load.data.j.a.a(URL) HttpURLConnection
com.bumptech.glide.load.data.j.a.a(URL) HttpURLConnection
com.bumptech.glide.load.data.j.b.a(URL) HttpURLConnection
i0.k.a.g() String
w.b.run() void
w.b.run() void
w.b.run() void
w.b.run() void
w.b.run() void
z.c
z.c.a(String, String) String
z.c.a(String, String) String
z.c.a(String, String) String
z.c.a(String, String) String
z.c.a(String, String) String
z.c.a(String, String) String
z.c.a(String, String) String
z.c.a(String, String) String
f128q0 = "http://ns.adobe.com/xap/1.0/\u0000".getBytes(forName);
this("Http request failed", i2);
import java.net.HttpURLConnection;
private HttpURLConnection f862d;
HttpURLConnection httpURLConnection = this.f862d;
if (httpURLConnection != null) {
httpURLConnection.disconnect();
private HttpURLConnection d(URL url, Map<String, String> map) {
HttpURLConnection a2 = this.f861c.a(url);
if (Log.isLoggable("HttpUrlFetcher", 3)) {
Log.d("HttpUrlFetcher", "Failed to load data for url", e2);
if (!Log.isLoggable("HttpUrlFetcher", 2)) {
if (Log.isLoggable("HttpUrlFetcher", 2)) {
sb.append("Finished http url fetcher fetch in ");
private static int f(HttpURLConnection httpURLConnection) {
return httpURLConnection.getResponseCode();
if (!Log.isLoggable("HttpUrlFetcher", 3)) {
Log.d("HttpUrlFetcher", "Failed to get a response code", e2);
private InputStream g(HttpURLConnection httpURLConnection) {
if (TextUtils.isEmpty(httpURLConnection.getContentEncoding())) {
inputStream = x0.c.b(httpURLConnection.getInputStream(), httpURLConnecti
if (Log.isLoggable("HttpUrlFetcher", 3)) {
Log.d("HttpUrlFetcher", "Got non empty content encoding: " + httpURLConn
inputStream = httpURLConnection.getInputStream();
throw new c0.e("Failed to obtain InputStream", f(httpURLConnection), e2)
HttpURLConnection d2 = d(url, map);
public HttpURLConnection a(URL url) {
return (HttpURLConnection) url.openConnection();
HttpURLConnection a(URL url);
String property = System.getProperty("http.agent");
String str = "https://graphical.weather.gov/xml/SOAP_server/ndfdXMLclien
sb.append("https://graphical.weather.gov/xml/SOAP_server/ndfdXMLclient.p
d(z.c.a(str, "WeatherForecastUSA/v4.x (https://github.com/vbresan/Weathe
sb.append("https://graphical.weather.gov/xml/SOAP_server/ndfdXMLclient.p
d(z.c.a(str, "WeatherForecastUSA/v4.x (https://github.com/vbresan/Weathe
import java.net.HttpURLConnection;
HttpURLConnection httpURLConnection = null;
HttpURLConnection httpURLConnection2 = (HttpURLConnection) new URL(str).
httpURLConnection2.setRequestMethod("GET");
httpURLConnection2.setReadTimeout(15000);
httpURLConnection2.setConnectTimeout(15000);
httpURLConnection2.setRequestProperty("User-Agent", str2);
str3 = httpURLConnection2.getResponseCode() == 200 ? d.d(httpURLConnecti
httpURLConnection2.disconnect();



Solving Challenge

1- install apk with adb

```
adb install io.hextree.reversingexample.apk
```

2- analyze app with jadx-gui and open AndroidMeniFast.xml

```
jadx-gui io.hextree.reversingexample.apk
```

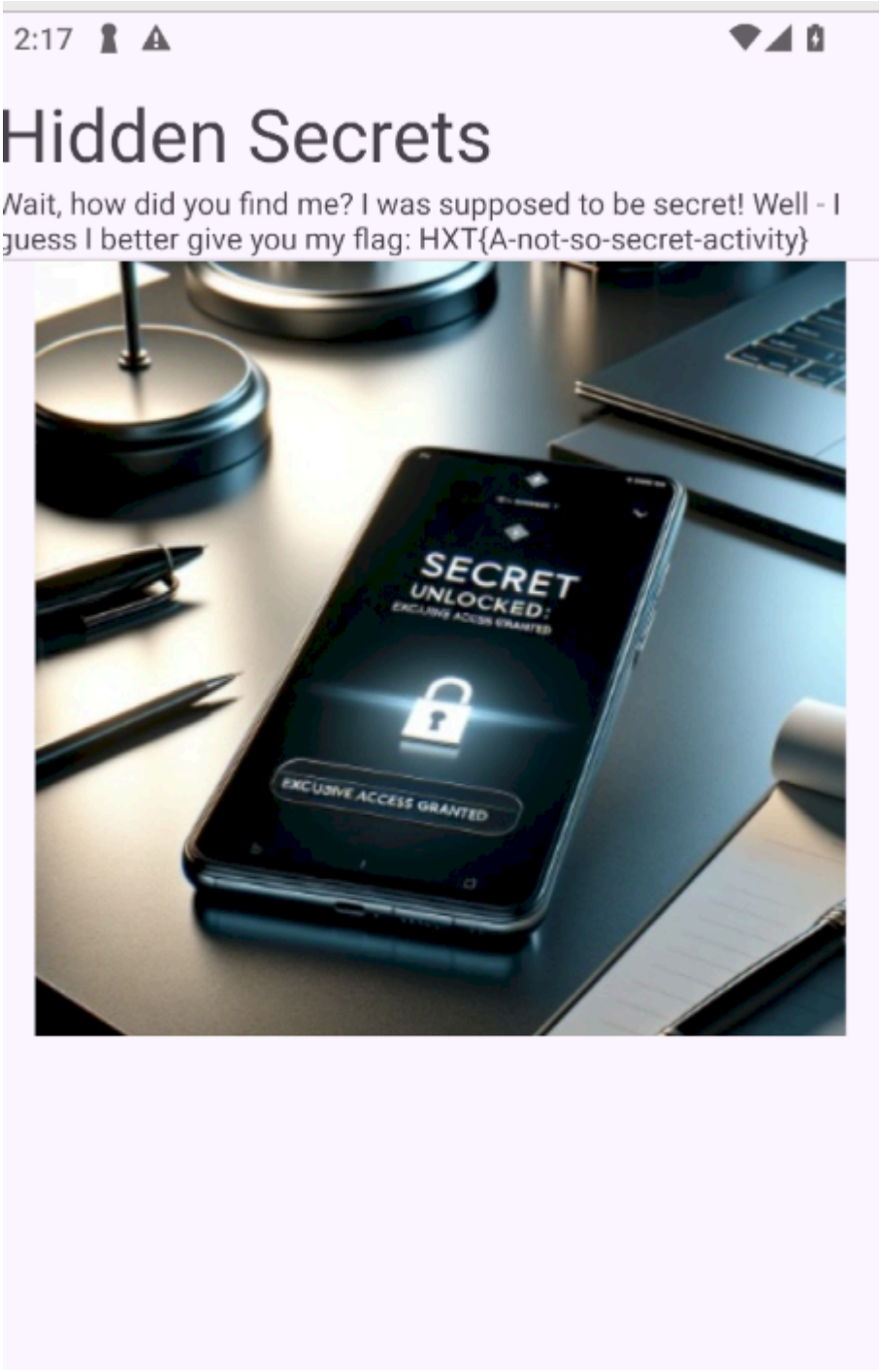
here this activity is exported

```
<activity
    android:name="io.hextree.reversingexample.SecretActivity"
    android:exported="true"/>
<activity
```

start activity

```
vbox86p:/ $ am start-activity -n
io.hextree.reversingexample/io.hextree.reversingexample.SecretActivity
Starting: Intent { cmp=io.hextree.reversingexample/.SecretActivity }
vbox86p:/ $
```

we get the flag **HXT{A-not-so-secret-activity}**



second flag

1- decompile app with apktool

```
apktool d io.hextree.reversingexample.apk
```

2- open AndroidMeniFast.xml file and change exported on all activity from false to true

before

```
    <activity
        android:theme="@style/Theme.ReversingExample"
        android:name="io.hextree.reversingexample.UnreachableActivity"
        android:exported="false"/>
    <activity
        android:name="io.hextree.reversingexample.ThirdPasswordActivity"
        android:exported="false"/>
    <activity
        android:name="io.hextree.reversingexample.SecondPasswordActivity"
        android:exported="false"/>
    <activity
        android:name="io.hextree.reversingexample.SecretActivity"
        android:exported="true"/>
    <activity
        android:name="io.hextree.reversingexample.LoggedInActivity"
        android:exported="false"/>
    <activity
        android:name="io.hextree.reversingexample.MainActivity"
        android:exported="true">
        <intent-filter>
            <action android:name="android.intent.action.MAIN"/>
            <category android:name="android.intent.category.LAUNCHER"/>
        </intent-filter>
```

after

```
        <activity android:exported="true" android:name="io.hextree.reversingexample.ThirdPasswordActivity"/>
        <activity android:exported="true" android:name="io.hextree.reversingexample.SecondPasswordActivity"/>
        <activity android:exported="true" android:name="io.hextree.reversingexample.SecretActivity"/>
        <activity android:exported="true" android:name="io.hextree.reversingexample.LoggedInActivity"/>
        <activity android:exported="true" android:name="io.hextree.reversingexample.MainActivity">
            <intent-filter>
```

3- build the app with apktool

```
➜  module3_reverse_enginerring apktool b io.hextree.reversingexample
I: Using Apktool 2.11.0 on io.hextree.reversingexample.apk with 4 threads
I: Checking whether sources have changed...
I: Smaling smali folder into classes.dex...
I: Checking whether sources have changed...
I: Smaling smali_classes2 folder into classes2.dex...
I: Checking whether sources have changed...
I: Smaling smali_classes3 folder into classes3.dex...
I: Checking whether resources have changed...
```

4- create key with keytool and set alias name

```
Enter keystore password:  %
➜  module3_reverse_enginerring keytool -genkey -v -keystore ~/android-app-hack.keystore -keysize 2048 -alias HexTree -keyalg RSA -validity 365
Enter keystore password:
```

```
Enter the distinguished name. Provide a single dot (.) to leave a sub-
component empty or press ENTER to use the default value in braces.
What is your first and last name?
  [Unknown]:
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
correct?
  [no]:  y

Generating 2048-bit RSA key pair and self-signed certificate (SHA384withRSA)
with a validity of 365 days
```

5- check the key is created with keytool

```
keytool -list -keystore ~/android-app-hack.keystore
```

```
→ module3_reverse_enginerring keytool -list -keystore ~/android-app-hack.keystore
Enter keystore password:
Keystore type: PKCS12
Keystore provider: SUN

Your keystore contains 8 entries

alias_name, Mar 17, 2025, PrivateKeyEntry,
Certificate fingerprint (SHA-256): 06:3A:E7:6F:0F:2A:E3:02:A0:BA:59:04:B7:06:14:98:95:D8:87:E2:76:D7:3A:F8:0A:A0:BD
0:19:D7:01
hextree, May 9, 2025, PrivateKeyEntry,
Certificate fingerprint (SHA-256): E8:D3:03:18:39:10:02:3D:62:0B:5F:B6:98:AD:03:2D:45:68:C0:69:47:CA:11:E7:24:B6:9F
A:9E:CB:44
my_ass, Apr 12, 2025, PrivateKeyEntry,
Certificate fingerprint (SHA-256): 51:D6:DE:0D:63:5A:EA:DB:9D:17:C6:68:BF:5E:73:95:22:C2:BD:99:C3:6B:40:D1:5B:2D:1B
9:D3:20:12
my_key, Mar 18, 2025, PrivateKeyEntry,
Certificate fingerprint (SHA-256): 10:11:7A:C5:55:C1:24:1A:49:DA:36:66:51:51:0B:B5:8F:B5:4B:CF:48:EF:AB:4C:ED:5D:60
9:DC:48:CB
root_detection_key, Apr 21, 2025, PrivateKeyEntry,
Certificate fingerprint (SHA-256): F9:7A:6F:54:BE:61:15:18:31:2D:ED:40:45:AD:99:01:89:8A:FE:52:8D:45:8F:99:0D:60:2F
7:A4:AE:8C
smali_chellange, Apr 17, 2025, PrivateKeyEntry,
Certificate fingerprint (SHA-256): F4:F4:D4:B7:94:89:1C:26:7B:C3:7F:E3:16:9D:21:E6:37:59:36:18:BE:1F:44:CB:96:95:69
9:D7:1C:A9
smalie_challange_key, Apr 19, 2025, PrivateKeyEntry,
Certificate fingerprint (SHA-256): 09:AE:13:29:3D:2C:A5:7F:63:6E:8F:D4:F1:94:14:69:48:DD:0D:9F:3F:E4:C9:C4:0A:39:F9
C:AF:D2:FD
udemy, Mar 17, 2025, PrivateKeyEntry,
Certificate fingerprint (SHA-256): 88:4F:DB:C5:E5:AE:81:7D:FA:59:55:D3:36:0D:DA:DE:9E:1A:C3:7C:13:05:ED:78:E6:0E:9F
4:5B:C4:4D

Warning:
<alias_name> uses the SHA1withRSA signature algorithm which is considered a security risk.
<my_key> uses the SHA1withRSA signature algorithm which is considered a security risk.
<root_detection_key> uses the SHA1withRSA signature algorithm which is considered a security risk.
<udemy> uses the SHA1withRSA signature algorithm which is considered a security risk.
```

6- config lines with zipalign

```
→  dist zipalign -v 4 io.hextree.reversingexample.apk out.apk
```

7- sign key with apksigner

```
→  dist apksigner sign --ks-key-alias hextree -ks ~/android-app-hack.keystore out.apk
```

```
→ dist apksigner sign --ks-key-alias hextree -ks ~/android-app-hack.keystore out.apk
WARNING: A restricted method in java.lang.System has been called
WARNING: java.lang.System::loadLibrary has been called by org.conscrypt.NativeLibraryUtil in an unnamed module (file:/
me/ubuntu/Android/Sdk/build-tools/35.0.1/lib/apksigner.jar)
WARNING: Use --enable-native-access=ALL-UNNAMED to avoid a warning for callers in this module
WARNING: Restricted methods will be blocked in a future release unless native access is enabled

Keystore password for signer #1:
```

8- delete the old app from emulator

```
→  dist adb uninstall io.hextree.reversingexample
Success
```

9- install the new app

```
➜  dist adb install out.apk
Performing Incremental Install
Serving...
```

10- check all activities are changed : open jadx-gui out.apk

yes : all activities changed

AndroidManifest.xml

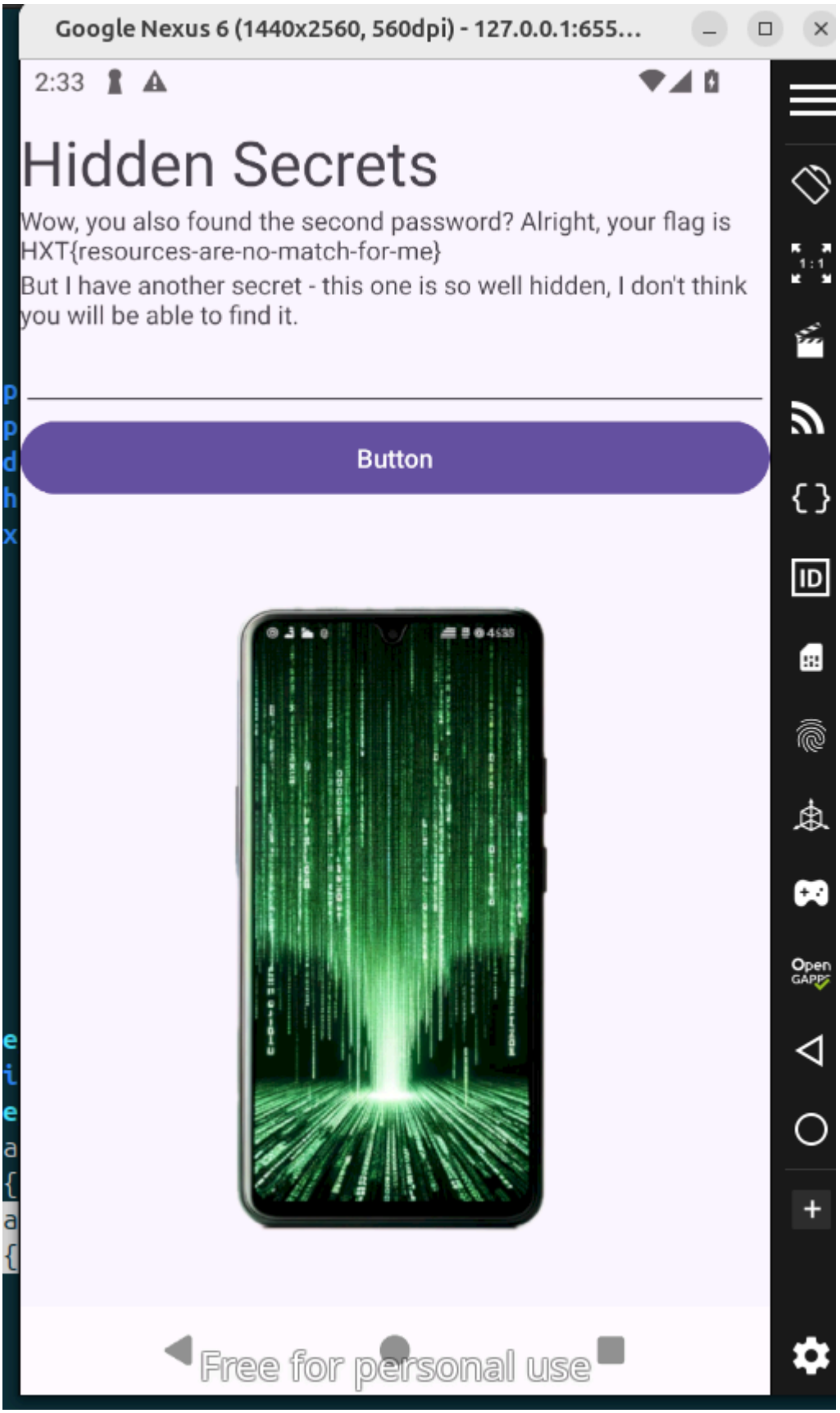
```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="1"
    android:versionName="1.0"
    android:compileSdkVersion="34"
    android:compileSdkVersionCodename="14"
    package="io.hextree.reversingexample"
    platformBuildVersionCode="34"
    platformBuildVersionName="14">
    <uses-sdk
        android:minSdkVersion="29"
        android:targetSdkVersion="34"/>
    <permission
        android:name="io.hextree.reversingexample.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION"
        android:protectionLevel="signature"/>
    <uses-permission android:name="io.hextree.reversingexample.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION"
    <application
        android:theme="@style/Theme.ReversingExample"
        android:label="Hidden Secrets"
        android:icon="@drawable/applogo"
        android:debuggable="true"
        android:allowBackup="true"
        android:supportsRtl="true"
        android:extractNativeLibs="false"
        android:fullBackupContent="@xml/backup_rules"
        android:roundIcon="@drawable/applogo"
        android:appComponentFactory="androidx.core.app.CoreComponentFactory"
        android:dataExtractionRules="@xml/data_extraction_rules">
        <activity
            android:theme="@style/Theme.ReversingExample"
            android:name="io.hextree.reversingexample.UnreachableActivity"
            android:exported="false"/>
        <activity
            android:name="io.hextree.reversingexample.ThirdPasswordActivity"
            android:exported="true"/>
        <activity
            android:name="io.hextree.reversingexample.SecondPasswordActivity"
            android:exported="true"/>
        <activity
            android:name="io.hextree.reversingexample.SecretActivity"
            android:exported="true"/>
        <activity
            android:name="io.hextree.reversingexample.LoggedInActivity"
            android:exported="true"/>
        <activity
            android:name="io.hextree.reversingexample.MainActivity"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
```

11- start activity for io.hextree.reversingexample.SecondPasswordActivity

```
vbox86p:/ $ am start-activity -n
io.hextree.reversingexample/io.hextree.reversingexample.SecondPasswordActivi
```

```
ty
Starting: Intent { cmp=io.hextree.reversingexample/.SecondPasswordActivity }
```

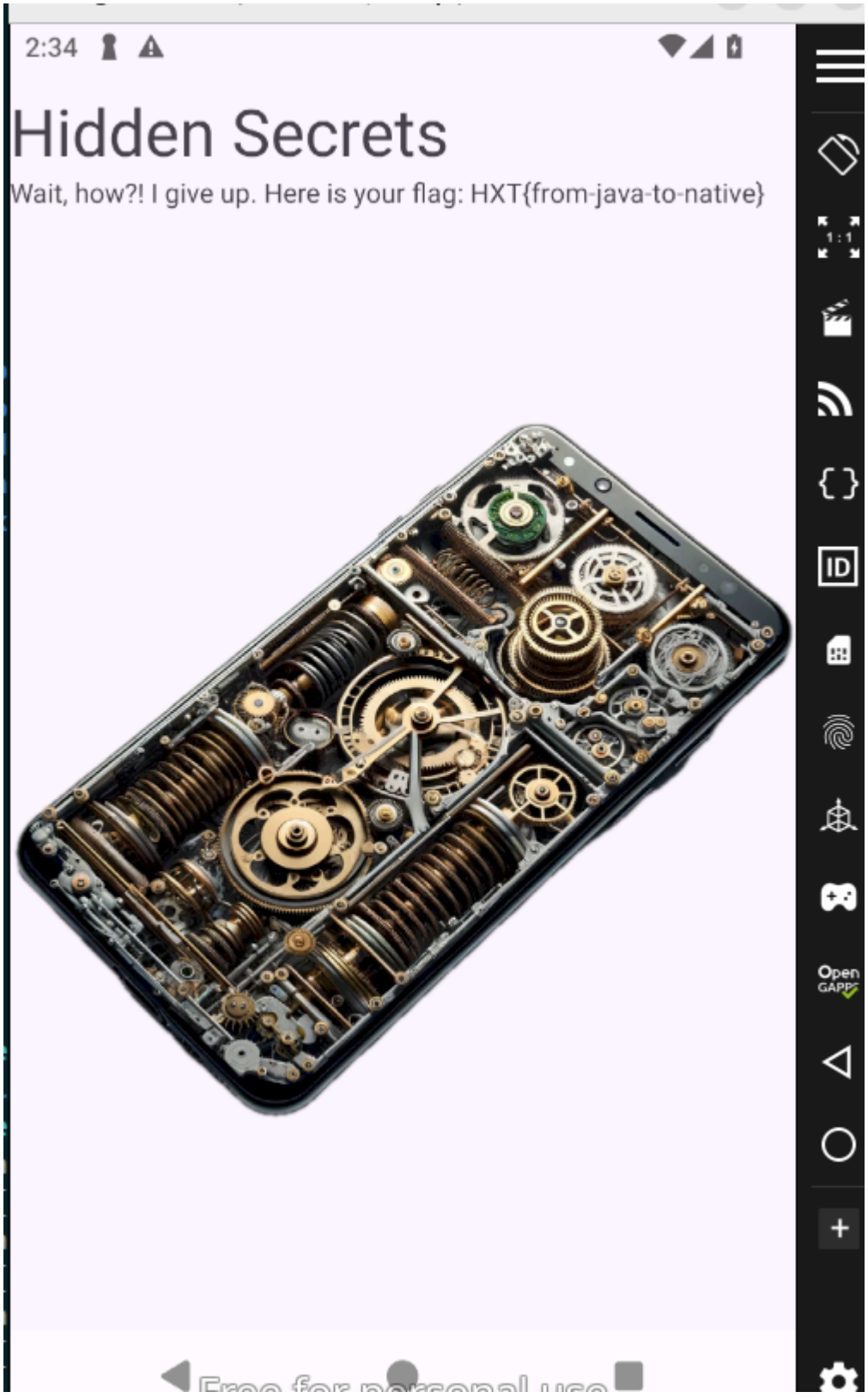
the flag is HXT{resources-are-no-match-for-me}



12-start activity for io.hextree.reversingexample.ThirdPasswordActivity

```
vbox86p:/ $ am start-activity -n
io.hextree.reversingexample/io.hextree.reversingexample.ThirdPasswordActivit
y
Starting: Intent { cmp=io.hextree.reversingexample/.ThirdPasswordActivity }
vbox86p:/ $
```

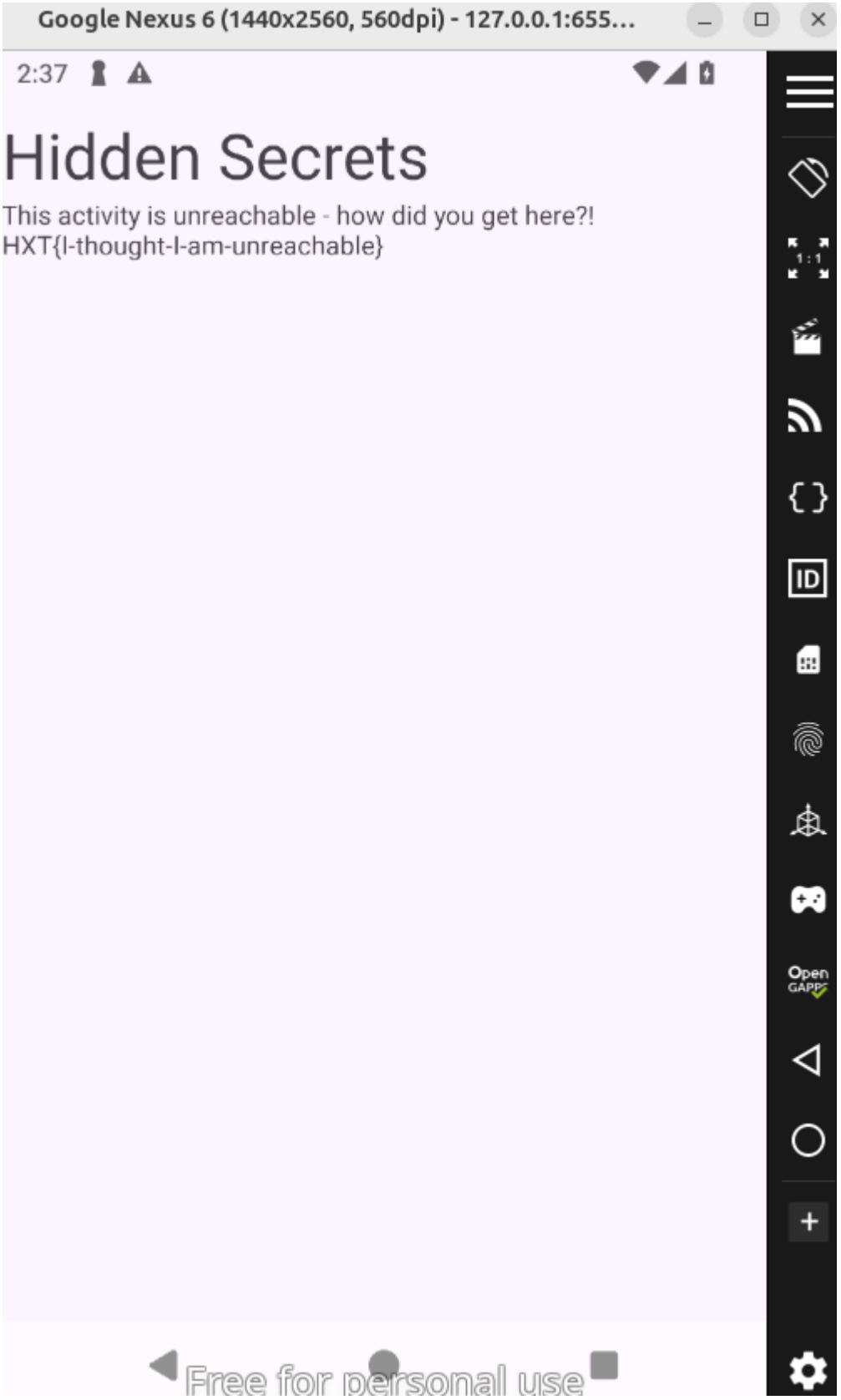
the flag is HXT{from-java-to-native}



13-start activity for io.hextree.reversingexample.UnreachableActivity

```
vbox86p:/ $ am start-activity -n
io.hextree.reversingexample/io.hextree.reversingexample.UnreachableActivity
Starting: Intent { cmp=io.hextree.reversingexample/.UnreachableActivity }
```

the flag is **HXT{I-thought-I-am-unreachable}**



3 flag

open MainActivity on app

here code java for MainActivity

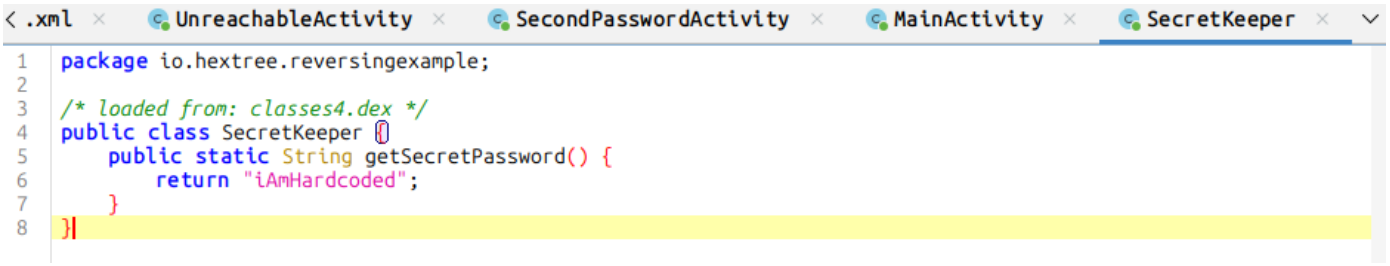
st.xml | UnreachableActivity | SecondPasswordActivity | MainActivity | SecretKeepe

```
import android.os.Bundle;
import android.util.Log;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import androidx.activity.EdgeToEdge;
import androidx.appcompat.app.AppCompatActivity;
import androidx.core.graphics.Insets;
import androidx.core.view.OnApplyWindowInsetsListener;
import androidx.core.view.ViewCompat;
import androidx.core.view.WindowInsetsCompat;

/* loaded from: classes4.dex */
public class MainActivity extends AppCompatActivity {
    static String TAG = "MainActivity";
    private Button checkPasswordButton;
    private EditText password;

    @Override // androidx.fragment.app.FragmentActivity, androidx.activity.ComponentActivity, androidx.co
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        EdgeToEdge.enable(this);
        setContentView(R.layout.activity_main);
        ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), new OnApplyWindowInsetsListene
            @Override // androidx.core.view.OnApplyWindowInsetsListener
            public final WindowInsetsCompat onApplyWindowInsets(View view, WindowInsetsCompat windowInse
                return MainActivity.lambda$onCreate$0(view, windowInsetsCompat);
            }
        });
        this.password = (EditText) findViewById(R.id.password_text);
        this.checkPasswordButton = (Button) findViewById(R.id.check_password_button);
        this.checkPasswordButton.setOnClickListener(new View.OnClickListener() { // from class: io.hextr
            @Override // android.view.View.OnClickListener
            public void onClick(View view) {
                String passwordText = MainActivity.this.password.getText().toString();
                Log.v(MainActivity.TAG, "check password clicked:" + passwordText);
                if (passwordText.equals(SecretKeeper.getSecretPassword())) {
                    Log.v(MainActivity.TAG, "Password correct!");
                    Intent intent = new Intent(MainActivity.this.getBaseContext(), (Class<?>) LoggedInAct
                    MainActivity.this.startActivity(intent);
                }
            }
        });
    }

    static /* synthetic */ WindowInsetsCompat lambda$onCreate$0(View v, WindowInsetsCompat insets) {
        Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
        v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
        return insets;
    }
}
```

in this condition he compare the password use enter with **SecretKeeper.getSecretPassword()**

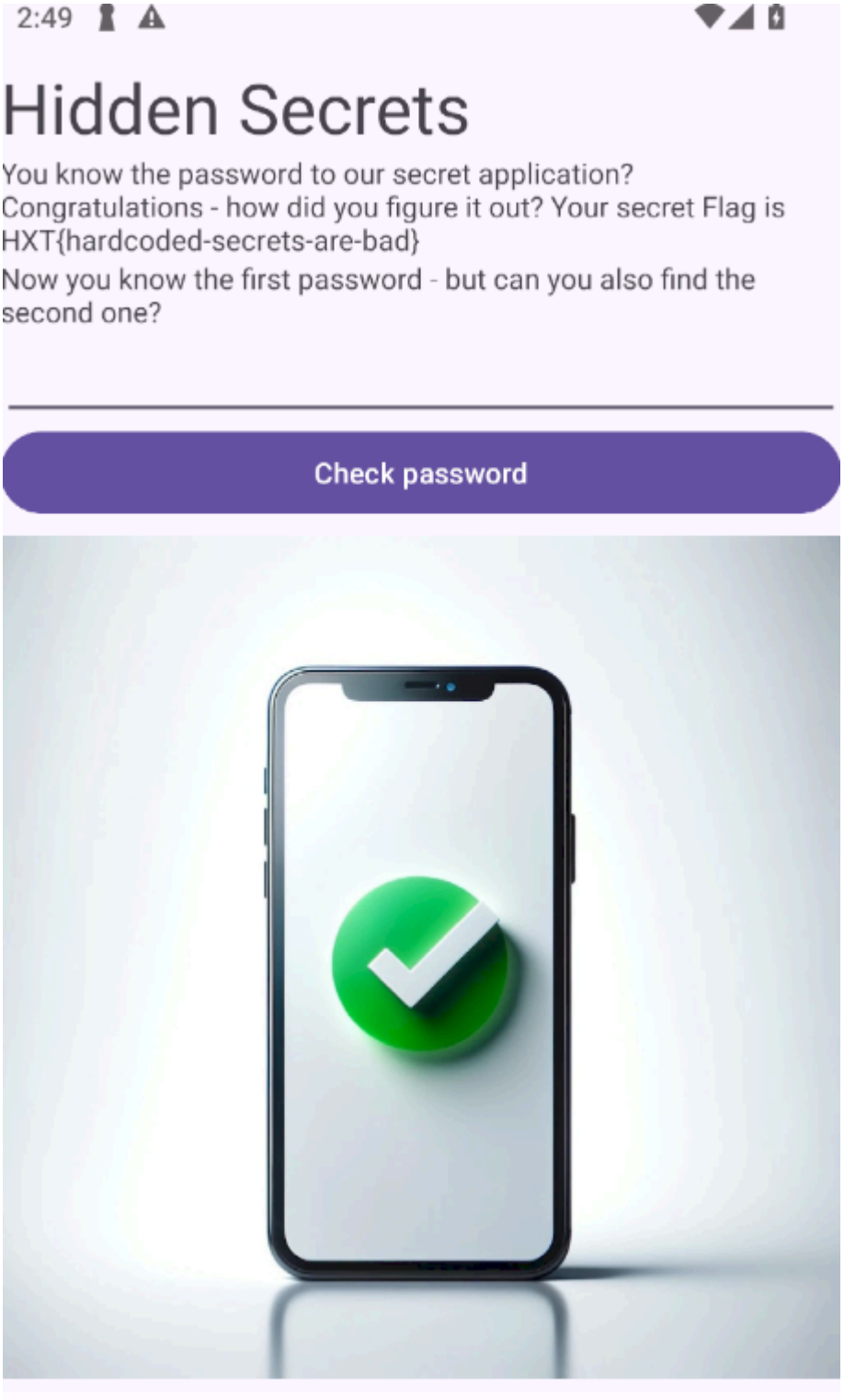
```
    if (passwordText.equals(SecretKeeper.getSecretPassword())) {
        Log.v(MainActivity.TAG, "Password correct!");
        Intent intent = new Intent(MainActivity.this.getBaseContext(), (Class
        MainActivity.this.startActivity(intent);
    }
}
```

if we click on this SecretKeeper.getSecretPassword() we will find the password : **iAmHardcoded**



check the password on app

the flag is **HXT{hardcoded-secrets-are-bad}**



4 flag

open LoggedInActivity java file and analyze it

```
ctivity × SecondPasswordActivity × MainActivity × SecretKeeper × LoggedInActivity ×
```

```java
package io.hextree.reversingexample;

import android.content.Intent;
import android.os.Bundle;
import android.util.Log;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import androidx.activity.EdgeToEdge;
import androidx.appcompat.app.AppCompatActivity;
import androidx.core.graphics.Insets;
import androidx.core.view.OnApplyWindowInsetsListener;
import androidx.core.view.ViewCompat;
import androidx.core.view.WindowInsetsCompat;

/* loaded from: classes4.dex */
public class LoggedInActivity extends AppCompatActivity {
    static String TAG = "LoggedInActivity";
    private Button checkPasswordButton;
    private EditText password;

    @Override // androidx.fragment.app.FragmentActivity, androidx.activity.ComponentActivity, androidx.core.a
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        EdgeToEdge.enable(this);
        setContentView(R.layout.activity_logged_in);
        ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), new OnApplyWindowInsetsListener()
            @Override // androidx.core.view.OnApplyWindowInsetsListener
            public final WindowInsetsCompat onApplyWindowInsets(View view, WindowInsetsCompat windowInsetsCo
                return LoggedInActivity.lambda$onCreate$0(view, windowInsetsCompat);
            }
        });
        this.password = (EditText) findViewById(R.id.second_password);
        this.checkPasswordButton = (Button) findViewById(R.id.check_password2_button);
        this.checkPasswordButton.setOnClickListener(new View.OnClickListener() { // from class: io.hextree.re
            @Override // android.view.View.OnClickListener
            public void onClick(View view) {
                String passwordText = LoggedInActivity.this.password.getText().toString();
                Log.v(LoggedInActivity.TAG, "check password clicked:" + passwordText);
                if (passwordText.equals(LoggedInActivity.this.getString(R.string.secret2))) {
                    Log.v(LoggedInActivity.TAG, "Password correct!");
                    Intent intent = new Intent(LoggedInActivity.this.getBaseContext(), (Class<?>) SecondPassw
                    LoggedInActivity.this.startActivity(intent);
                }
            }
        });
    }

    static /* synthetic */ WindowInsetsCompat lambda$onCreate$0(View v, WindowInsetsCompat insets) {
        Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
        v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
```

he contain this condition : he compare the password with R.string.secret2

```java
if (passwordText.equals(LoggedInActivity.this.getString(R.string.secret2))) {
    Log.v(LoggedInActivity.TAG, "Password correct!");
    Intent intent = new Intent(LoggedInActivity.this.getBaseContext(), (Class<?>) SecondPassw
    LoggedInActivity.this.startActivity(intent);
}
```

R.string.secret2 --> this is variable is exist after decompile the app on
/io.hextree.reversingexample/res/values/strings.xml

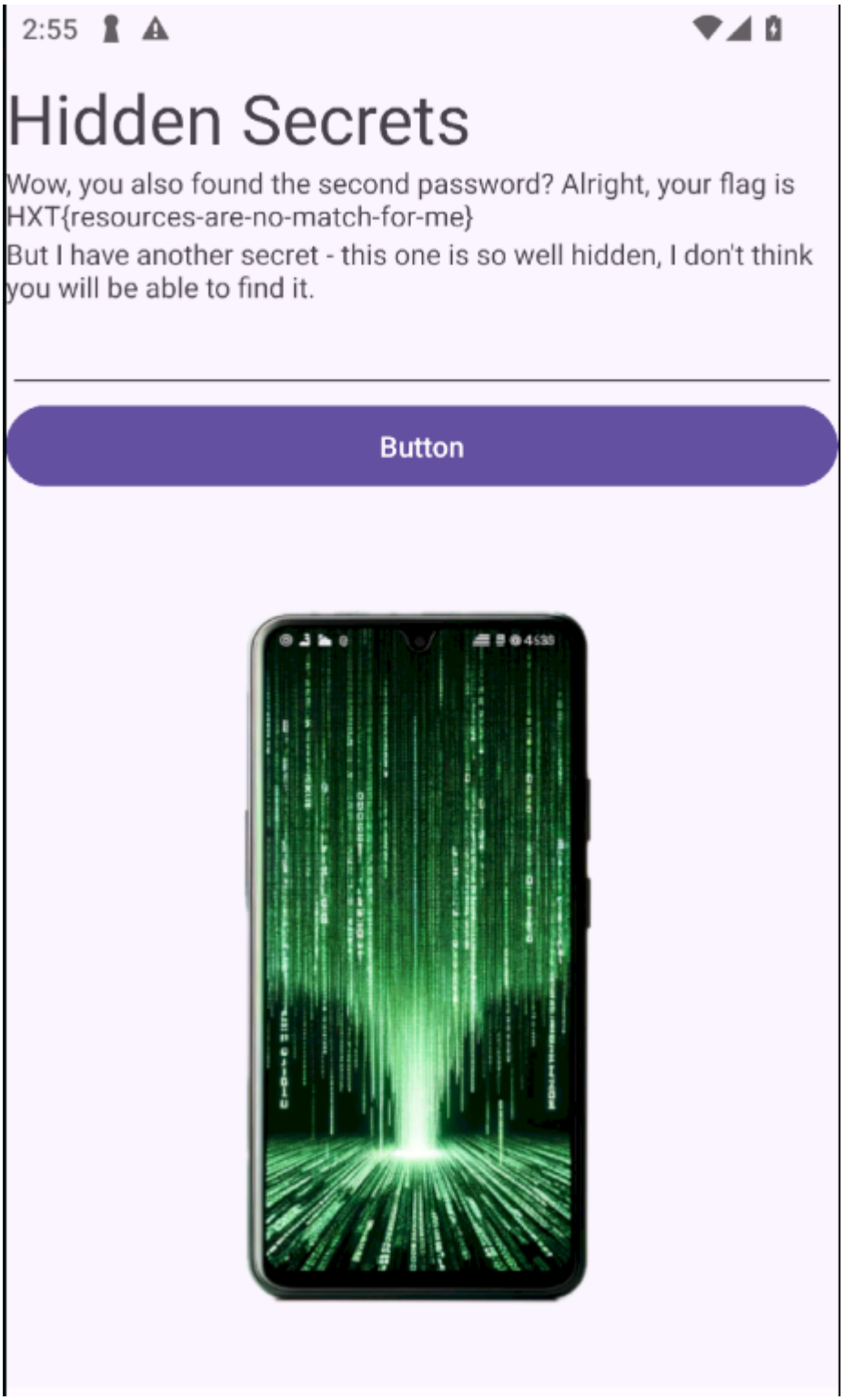
open file and get the password of secret2

the password is VeryResourcefulSecret

```
→ values pwd
/home/ubuntu/apps/Hexatree/module3_reverse_enginerring/io.hextree.reversingexample/res/values
→ values cat strings.xml |grep secret2
    <string name="secret2">VeryResourcefulSecret</string>
→ values
```

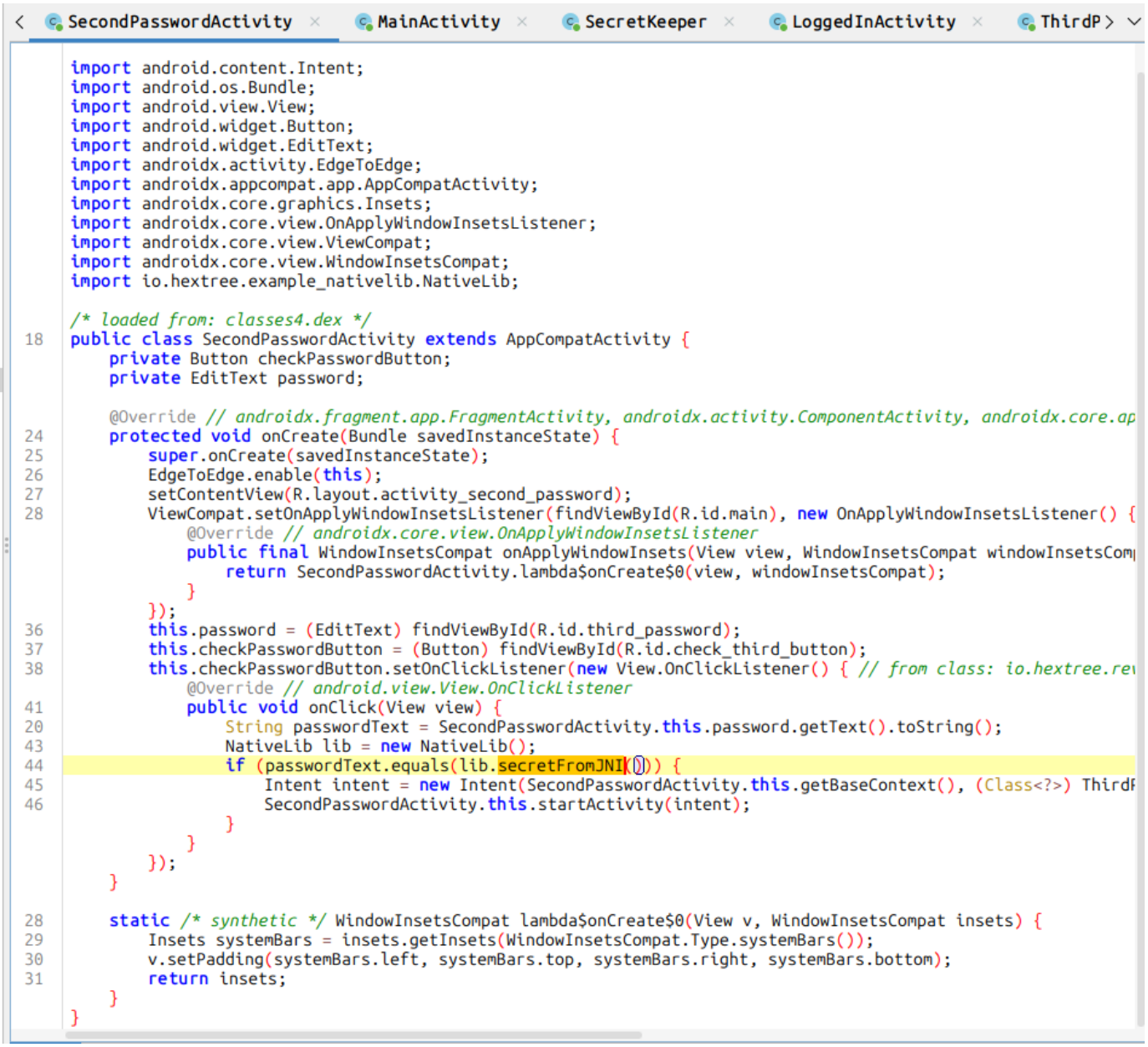
check the password :

flag is **HXT{resources-are-no-match-for-me}**

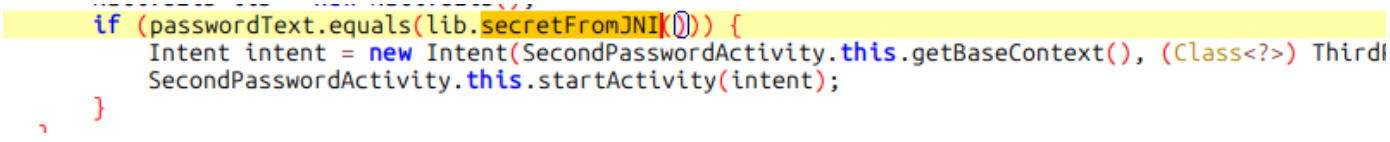


5- flag we got it when change the vale of exported to true on SecondPasswordActivity

analyze the SecondPasswordActivity java



in if condition he compare the password with lib.secretFromJNI



if we click on lib.secretFromJNI

he load example_nativelib

this library is exist on /io.hextree.reversingexample/lib/arm64-v8a/libexample_nativelib.so

to open this library we want to ghidra tool and after open with ghidra we will see the password

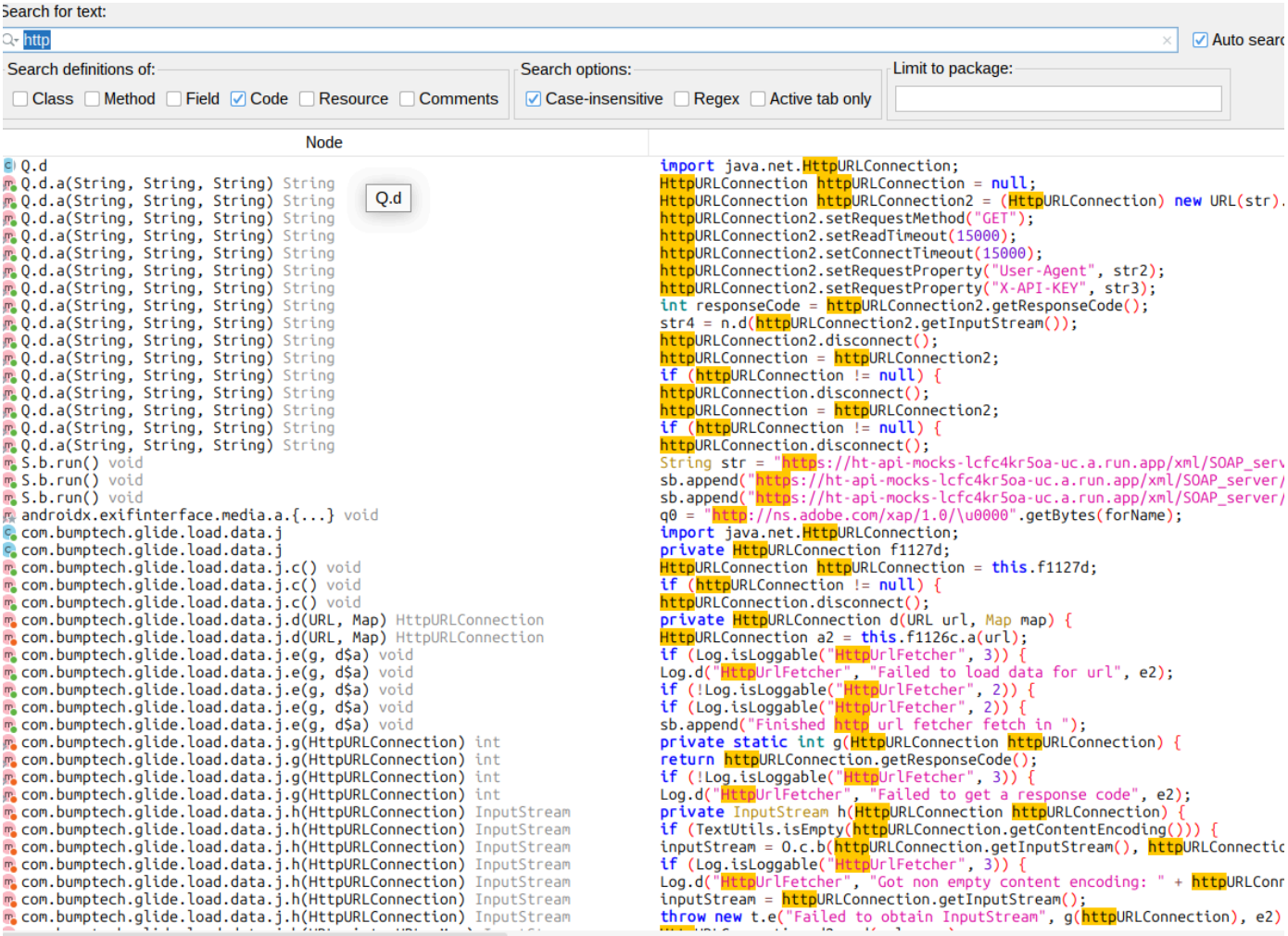
---

API Flag Chellagne

1- install app on emulator

2- app contain map so it contain API

3- search for http on app after open with jadx-gui



we will find he contain SOAP API

```
String str = "https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_serv
sb.append("https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/
sb.append("https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/
q0 = "http://ns.adobe.com/xap/1.0/\u0000".getBytes(forName);
import java.net.HttpURLConnection;
```

Click on this link and open file contain this link

AndroidManifest.xml | b

```
16          stringBuffer.append(str);
23          stringBuffer.append(c());
26          return stringBuffer.toString();
        }

        private StringBuffer c() {
3           StringBuffer stringBuffer = new StringBuffer();
8           stringBuffer.append("&product=time-series&begin=");
            try {
28              stringBuffer.append(URLEncoder.encode(f449d.format(new Date()), "UTF-8"));
            } catch (UnsupportedEncodingException unused) {
            }
33          stringBuffer.append("&maxt=maxt");
38          stringBuffer.append("&mint=mint");
43          stringBuffer.append("&dew=dew");
48          stringBuffer.append("&appt=appt");
53          stringBuffer.append("&wx=wx");
58          stringBuffer.append("&icons=icons");
63          stringBuffer.append("&wwa=wwa");
68          stringBuffer.append("&Submit=Submit");
195         return stringBuffer;
        }

        protected abstract void d(String str);

        @Override // java.lang.Thread, java.lang.Runnable
        public void run() {
            StringBuilder sb;
            String b2;
3           String str = "https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php";
5           if (this.f450a == null) {
31              if (this.f451b != null) {
35                  sb = new StringBuilder();
38                  sb.append("https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php")
43                  b2 = b(this.f451b);
                }
63              d(d.a(str, "HextreeForecastUSA/v4.x", this.f452c.getString(R.string.ApiKey)));
            }
9           sb = new StringBuilder();
12          sb.append("https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php");
17          b2 = a(this.f450a);
21          sb.append(b2);
24          str = sb.toString();
63          d(d.a(str, "HextreeForecastUSA/v4.x", this.f452c.getString(R.string.ApiKey)));
        }

1       public b(String str, Context context) {
            this.f451b = str;
            this.f452c = context;
        }
```

he contain variable **R.string.ApiKey** and this on **/app_name_after_decompile/res/values/string.xml** get the api

the flag is **HXT{android-api-key-b1872g}**

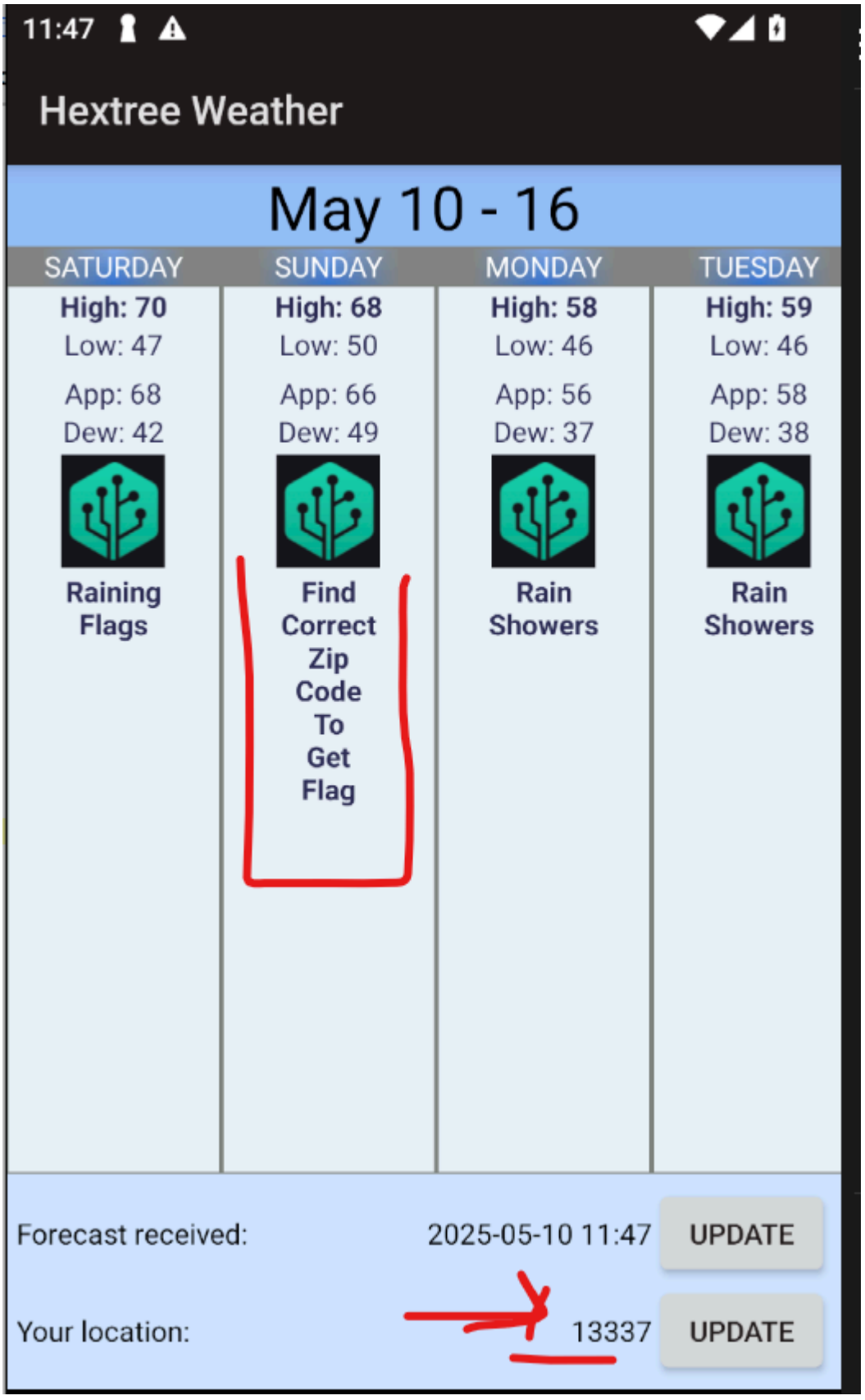
```
➜  values pwd
/home/ubuntu/apps/Hexatree/module3_reverse_enginerring/io.hextree.weatherusa/res
/values
➜  values cat strings.xml |grep -i api
    <string name="ApiKey">HXT{android-api-key-b1872g}</string>
➜  values
```

6- find the flag for hextree weather api 1

هنا هو عاوز flag اللي لو روحنا وشوفنا في MainActivity هو بيشوف ان لازم zip =13337 or 42

```
        p(false);
        boolean location = Preferences.setLocation(this);
        String zip = Preferences.getZip(this);
        if (!zip.equals("13337") && !zip.equals("42")) {
            Toast.makeText(this, "Weather Updates Disabled", 0).show();
            return;
        }
        if (location) {
            this.f1276b.i(this.f1275a.b());
        } else if (zip.length() == 5) {
            this.f1276b.j(zip);
        }
    }
```

بس احنا لو دخلنا 13337 مش هيبقي هنا flag بس هيبقي في 42 بس هو بيتأكد ان لازم length =5 فكده ان مش هنعرف نجيب flag



الو روحنا بقي شوفنا هنلاقي ان هو بيستدعي اصلا API في S.b Class هنا اهو هو بيطلب API اللي هو url بس بيبعت معاها API key

```java
@Override // java.lang.Thread, java.lang.Runnable
public void run() {
    StringBuilder sb;
    String b2;
    String str = "https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php";
    if (this.f450a == null) {
        if (this.f451b != null) {
            sb = new StringBuilder();
            sb.append("https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php");
            b2 = b(this.f451b);
        }
        d(d.a(str, "HextreeForecastUSA/v4.x", this.f452c.getString(R.string.ApiKey)));
    }
    sb = new StringBuilder();
    sb.append("https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php");
    b2 = a(this.f450a);
    sb.append(b2);
    str = sb.toString();
    d(d.a(str, "HextreeForecastUSA/v4.x", this.f452c.getString(R.string.ApiKey)));
}

public b(String str, Context context) {
    this.f451b = str;
    this.f452c = context;
}
```

لو عاوزين نبعت من غير API key بس هيجيب Missing API Key

```
→ ~ curl https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php
Missing API Key%
```

دلوقتي بقي هنجيب قيمة المتغير اللي هو R.string.ApiKey من app/res/values/strings.xml

```
→ dist ls
io.hextree.weatherusa.apk  out.apk  out.apk.idsig
→ dist cd ../res/values
→ values cat strings.xml|grep -i apikey
    <string name="ApiKey">HXT{android-api-key-b1872g}</string>
→ values
```

هنبعت request نشوف هو فعلا ولا لا

```
→ ~ curl  "https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php" -H "X-Api-Key:HXT{android-ap
i-key-b1872g}"
Unauthorized User-Agent%
→ ~
```

بس هنا لازم نغير User-Agent ل HextreeForecastUSA/v4.x

```java
    d(d.a(str, "HextreeForecastUSA/v4.x", this.f452c.getString(R.string.ApiKey)));
}
```

بس هيجيب wrong client

```
→ ~ curl  "https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php" -H "X-Api-Key:HXT{android-ap
i-key-b1872g}" -H "User-Agent:HextreeForecastUSA/v4.x"
Wrong client%
→ ~
```

بس لو روحنا ل this.f450a هلناقي هناك قيمة client

```
        sb = new StringBuilder();
        sb.append("https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php");
        b2 = a(this.f450a);
        sb.append(b2);
        str = sb.toString();
        d(d.a(str, "HextreeForecastUSA/v4.x", this.f452c.getString(R.string.ApiKey)));
    }

    public b(String str, Context context) {
```

client --> ?whichClient=NDFDgen

```
private String a(Location location) {
    StringBuffer stringBuffer = new StringBuffer();
    stringBuffer.append("?whichClient=NDFDgen");
    stringBuffer.append("&lat=");
    stringBuffer.append(location.getLatitude());
    stringBuffer.append("&lon=");
    stringBuffer.append(location.getLongitude());
    stringBuffer.append(c());
    return stringBuffer.toString();
}

private String b(String str) {
    StringBuffer stringBuffer = new StringBuffer();
    stringBuffer.append("?whichClient=NDFDgen");
    stringBuffer.append("&zipCodeList=");
    stringBuffer.append(str);
    stringBuffer.append(c());
    return stringBuffer.toString();
}
```

لو بعتنا بقي request هقول Wrong Product ا

```
→  ~ curl  "https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php?whichClient=NDFDgen" -H "X-Api-Key:HXT{android-api-key-b1872g}" -H "User-Agent:HextreeForecastUSA/v4.x"
Wrong product%
```

بس لو روحنا ل this.f450a هلناقي هناك قيمة product اللي فيه محتاج قيمة ZipCode اللي هو 42

```
private StringBuffer c() {
    StringBuffer stringBuffer = new StringBuffer();
    stringBuffer.append("&product=time-series&begin=");
    try {
```

هبعت request بس هيقول Required maxt

```
→  ~ curl  "https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php?whichClient=NDFDgen&product=time-series&begin=42" -H "X-Api-Key:HXT{android-api-key-b1872g}" -H "User-Agent:HextreeForecastUSA/v4.x"
Required maxt%
→  ~
```

بس لو روحنا ل this.f450a هلناقي هناك قيمة maxt اللي هي maxt=maxt&

```
    } catch (UnsupportedEncodingException unused) {
    }
    stringBuffer.append("&maxt=maxt");
    stringBuffer.append("&mint=mint");
    stringBuffer.append("&dew=dew");
    stringBuffer.append("&appt=appt");
    stringBuffer.append("&wx=wx");
    stringBuffer.append("&icons=icons");
    stringBuffer.append("&wwa=wwa");
    stringBuffer.append("&Submit=Submit");
    return stringBuffer;
}
```

وهكذ هيعقد يقول require ونضيفله القيمة اللي هو عايزها وهيبقي كده URL في الاخر او request اللي هنبعته

```
➜  ~ curl  "https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php?whichClient=NDFDgen&product=time-series&begin=2025-05-10T13:15&maxt=maxt&mint=mint&dew=dew&appt=appt&wx=wx&icons=icons&wwa=wwa&Submit=Submit&zipCodeList=42" -H "X-Api-Key:HXT{android-api-key-b1872g}" -H "User-Agent:HextreeForecastUSA/v4.x"
```

```
    <value coverage="chance" intensity="light" weather-type="rain showers" qualifier="none">
      <visibility units="statute miles">5</visibility>
    </value>
  </weather-conditions>
  <weather-conditions>
    <value coverage="chance" intensity="light" weather-type="HXT{android-api-h192gsa0}" qualifier="none">
      <visibility units="statute miles">5</visibility>
    </value>
  </weather-conditions>
  <weather-conditions>
```

Flag is **HXT{android-api-h192gsa0}**

6- find the flag for hextree weather api 2

هنا ديه زي flag اللي فات بس هنا هو مش موجود api-key اللي هنحتاجه في الكود : هو موجود في native-library هنا اهو مش موجود ولكن لو روحنا للملف InternetUtil

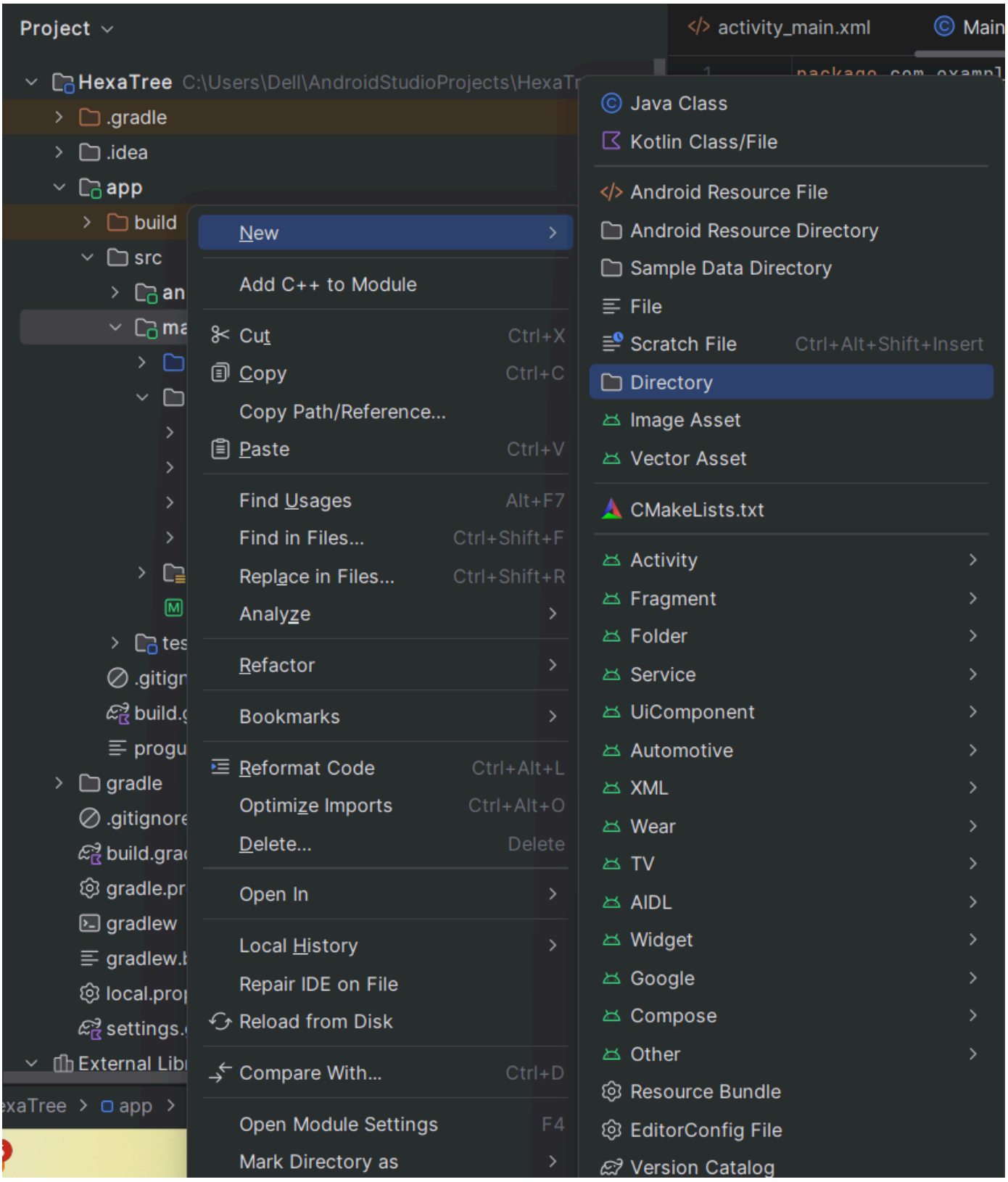
```
    protected abstract void d(String str);

    @Override // java.lang.Thread, java.lang.Runnable
    public void run() {
        StringBuilder sb;
        String b2;
        String str = "https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php";
        if (this.f450a == null) {
            if (this.f451b != null) {
                sb = new StringBuilder();
                sb.append("https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php");
                b2 = b(this.f451b);
            }
            d(InternetUtil.a(str, "HextreeForecastUSA/v4.x"));
        }
        sb = new StringBuilder();
        sb.append("https://ht-api-mocks-lcfc4kr5oa-uc.a.run.app/xml/SOAP_server/ndfdXMLclient.php");
        b2 = a(this.f450a);
        sb.append(b2);
        str = sb.toString();
        d(InternetUtil.a(str, "HextreeForecastUSA/v4.x"));
    }

    public b(String str, Context context) {
        this.f451b = str;
        this.f452c = context;
    }
}
```

```
/* loaded from: classes.dex */
public abstract class InternetUtil {
    public static String a(String str, String str2) {
        System.loadLibrary("native-lib");
        String str3 = "";
        HttpURLConnection httpURLConnection = null;
        try {
            try {
                HttpURLConnection httpURLConnection2 = (HttpURLConnection) new URL(str).openConnection();
                try {
                    httpURLConnection2.setRequestMethod("GET");
                    httpURLConnection2.setReadTimeout(15000);
                    httpURLConnection2.setConnectTimeout(15000);
                    if (!TextUtils.isEmpty(str2)) {
                        httpURLConnection2.setRequestProperty("User-Agent", str2);
                    }
                    httpURLConnection2.setRequestProperty("X-API-KEY", getKey("moiba1cybar8smart4sheriff4secur
                    int responseCode = httpURLConnection2.getResponseCode();
                    if (responseCode == 200) {
                        str3 = m.d(httpURLConnection2.getInputStream());
                    } else {
                        Log.e("HXT", "API Error: " + responseCode);
                    }
                    httpURLConnection2.disconnect();
                } catch (IOException e2) {
                    e = e2;
                    httpURLConnection = httpURLConnection2;
                    Log.e("HXT", "API Error", e);
                    if (httpURLConnection != null) {
                        httpURLConnection.disconnect();
                    }
                    return str3;
                } catch (Throwable th) {
                    th = th;
                    httpURLConnection = httpURLConnection2;
                    if (httpURLConnection != null) {
                        httpURLConnection.disconnect();
                    }
                    throw th;
                }
            } catch (Throwable th2) {
```

هنا اهو هو بيستدعي variable ده moiba1cybar8smart4sheriff4securi اللي في native-lib احنا ممكن بقي نعمل كده من خلال ناخد الكود ده و run on android studio ونستدعي المكتبة برده ونعرف ايه هوApiKey

احنا دلوقتي بقي هناخج المكتبات دي ونحطها علي visual studio ونحاول نعرض flag

1-create new folder and copy all library to the folder



2- copy these files to folder

3- create java class for file and set name

```
io.hextree.weatherusa.InternetUtil
```

4- write code for get api key for moiba1cybar8smart4sheriff4securi

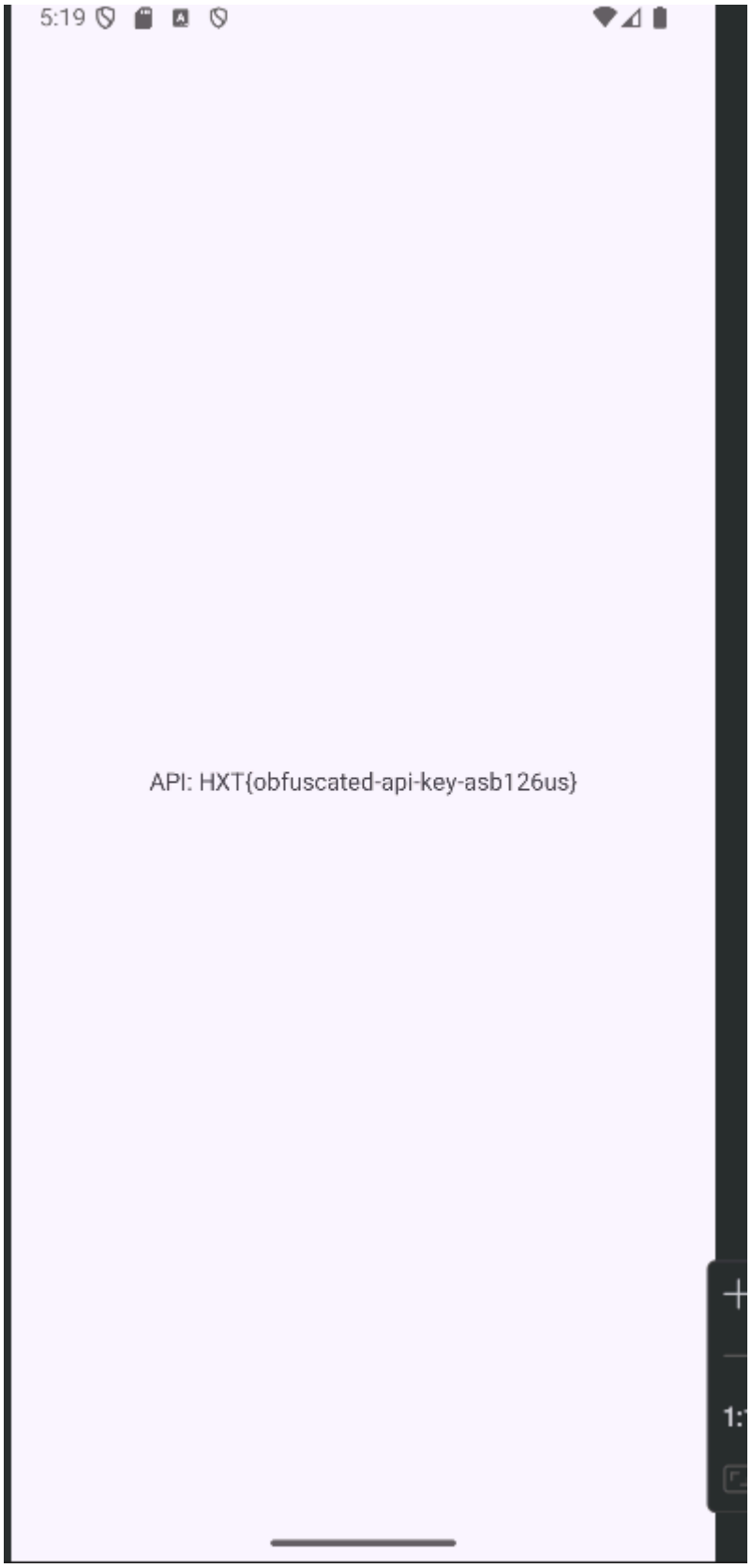
```
package io.hextree.weatherusa;

no usages
public class InternetUtil {
    1 usage
    private static native String getKey(String str);
    no usages
    public static String solve(){
        System.loadLibrary( libname: "native-lib");
        return getKey( str: "moiba1cybar8smart4sheriff4securi");
    }
}
```

5- MainActivity

```java
package com.example.hexatree;
import io.hextree.weatherusa.InternetUtil;
import android.os.Bundle;
import android.widget.TextView;

import androidx.activity.EdgeToEdge;
import androidx.appcompat.app.AppCompatActivity;
import androidx.core.graphics.Insets;
import androidx.core.view.ViewCompat;
import androidx.core.view.WindowInsetsCompat;

public class MainActivity extends AppCompatActivity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        EdgeToEdge.enable( $this$enableEdgeToEdge: this);
        setContentView(R.layout.activity_main);
        ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), (v, insets) -> {
            Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
            v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
            return insets;
        });
        TextView homeText=findViewById(R.id.home_text);
        homeText.setText("API: "+ InternetUtil.solve());
    }
}
```

6- run app and get flag

flag is **HXT{obfuscated-api-key-asb126us}**


5:19
API: HXT{obfuscated-api-key-asb126us}