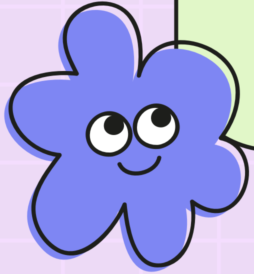
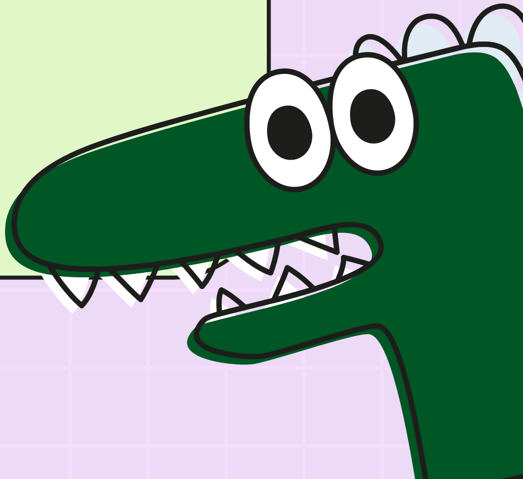
Mobile Pentest

-Introduction-





Summary

01

Emulation

02

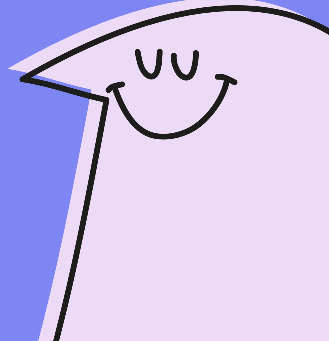
Static Analysis

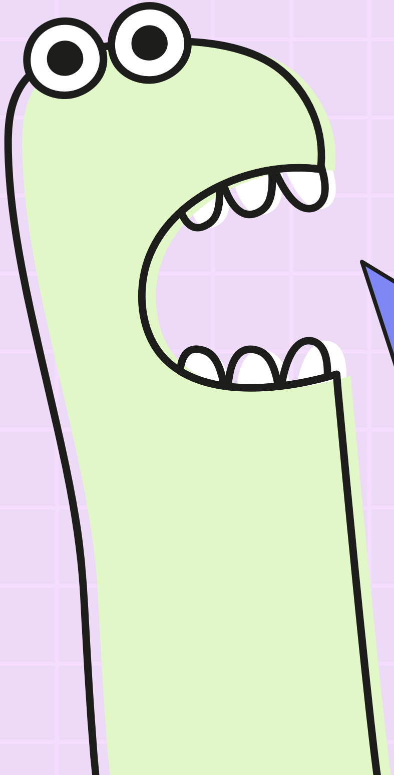
03

Dynamic Analysis

01

Emulation

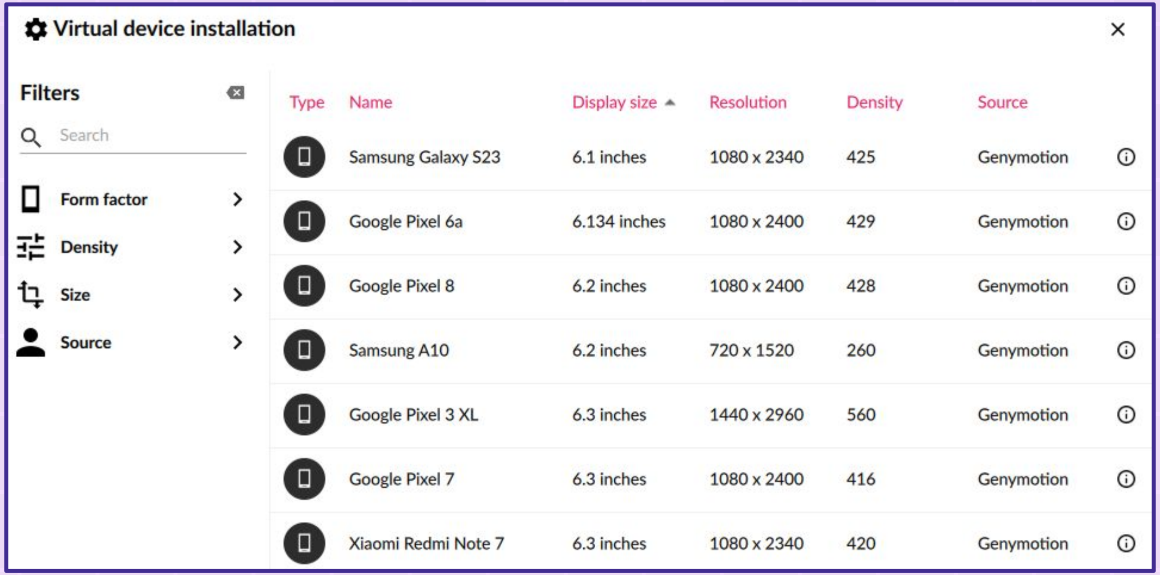




WHAT IS IT?

Emulation is the process of running mobile apps on non-mobile devices using software that simulates the Android/iOS operating system. This allows users and developers to test and use Android applications on computers.

How to ?



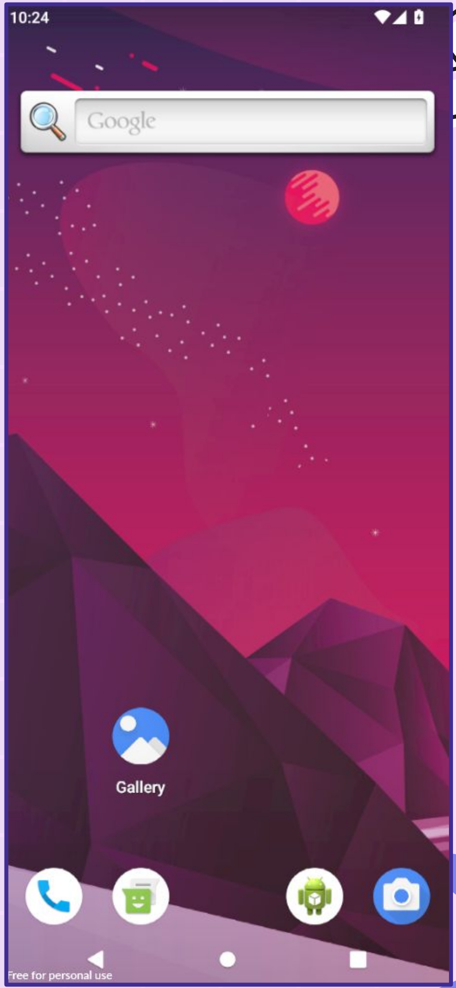
Virtual device installation ✕

Filters

Search

- Form factor >
- Density >
- Size >
- Source >

Type	Name	Display size ▲	Resolution	Density	Source	
▯	Samsung Galaxy S23	6.1 inches	1080 x 2340	425	Genymotion	ⓘ
▯	Google Pixel 6a	6.134 inches	1080 x 2400	429	Genymotion	ⓘ
▯	Google Pixel 8	6.2 inches	1080 x 2400	428	Genymotion	ⓘ
▯	Samsung A10	6.2 inches	720 x 1520	260	Genymotion	ⓘ
▯	Google Pixel 3 XL	6.3 inches	1440 x 2960	560	Genymotion	ⓘ
▯	Google Pixel 7	6.3 inches	1080 x 2400	416	Genymotion	ⓘ
▯	Xiaomi Redmi Note 7	6.3 inches	1080 x 2340	420	Genymotion	ⓘ



https://www.genymotion.com/

Get your APK

What is an APK ?

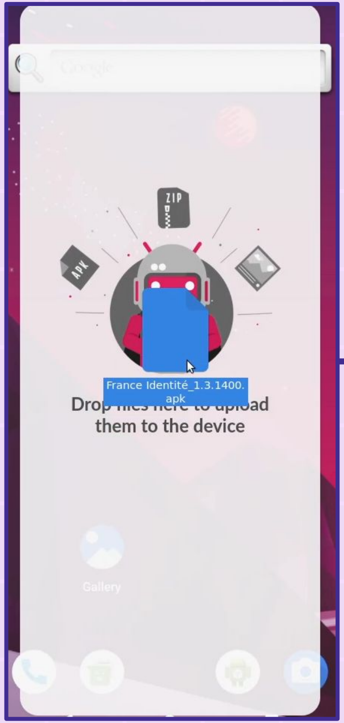
An **Android Package** file (**APK**) is a compressed archive containing all the data and resources needed to run an app on **Android devices**

How to get one ?

- **Pentest**
- **Bug Bounty**
- **Developer**
- **Malware Analysis**
- ...

Install the APK

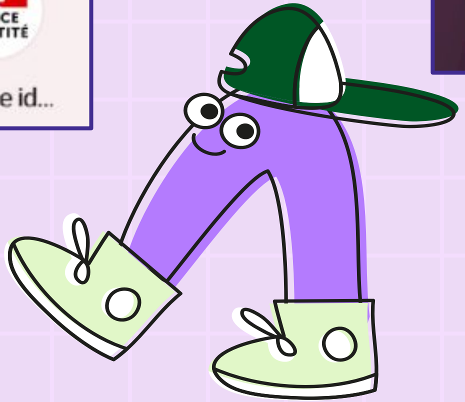
From APK File



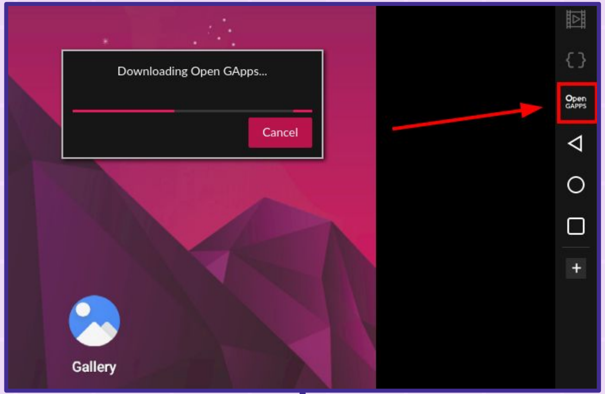
Google
ZIP
APK
France Identité_1.3.1400.apk
Drop files here to upload them to the device
Gallery

FRANCE IDENTITÉ

France id...



From Google PlayStore



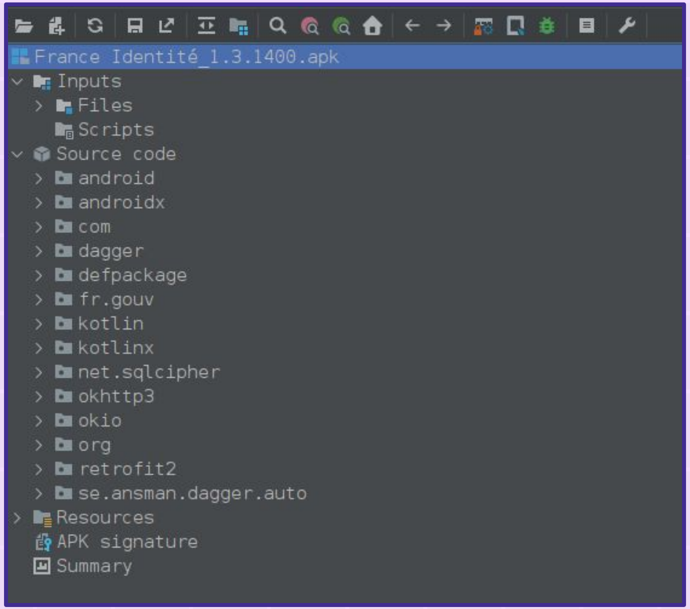
Downloading Open GApps...

Play Store ✓

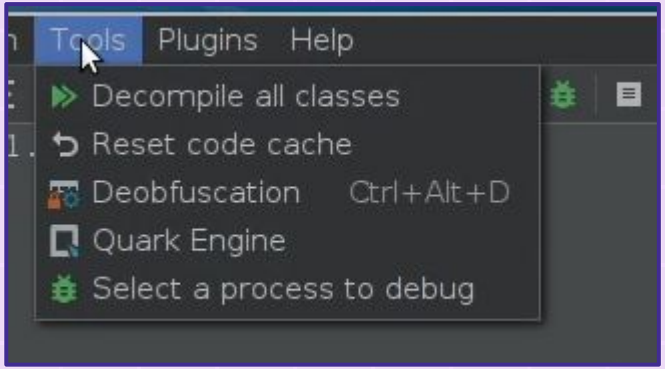
Static Analysis

02

Static Analysis - JADX



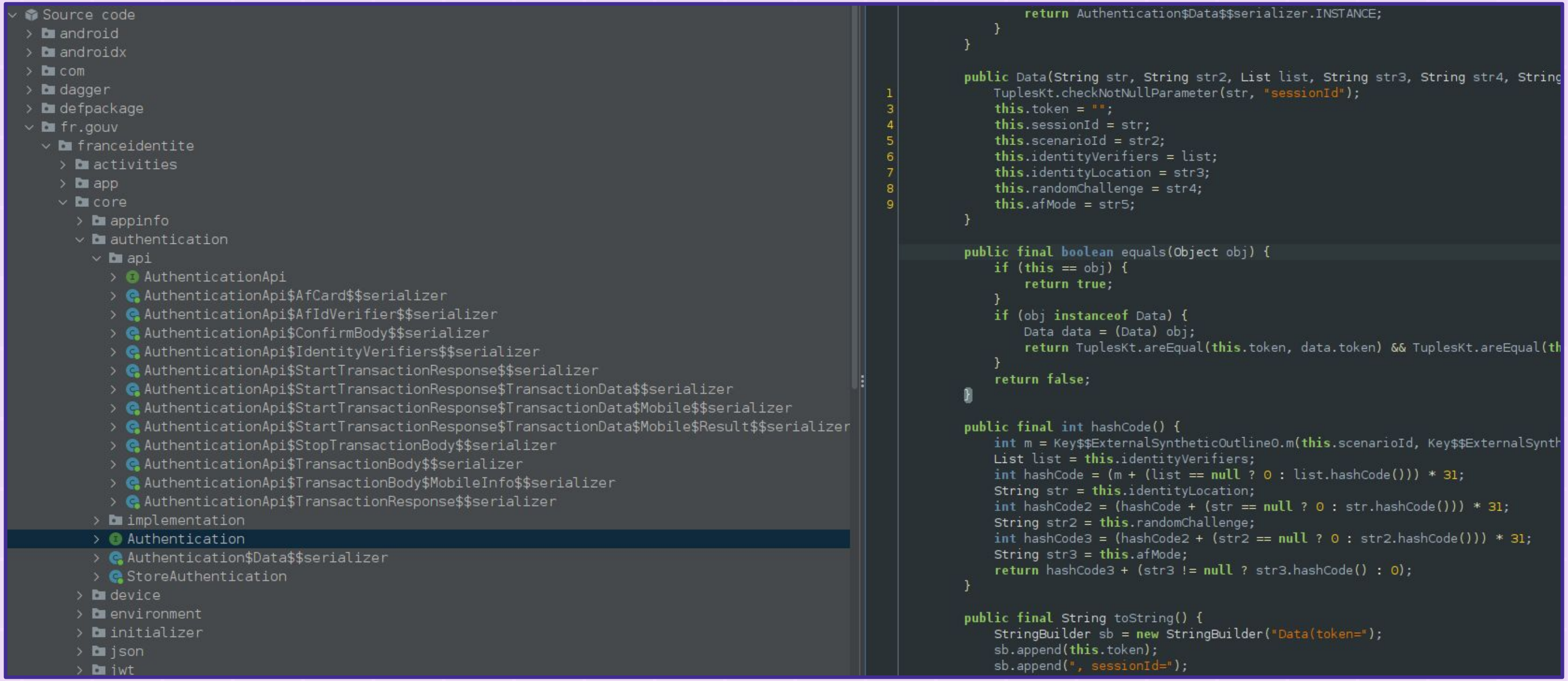
```
France Identité_1.3.1400.apk
  Inputs
    Files
    Scripts
  Source code
    android
    androidx
    com
    dagger
    defpackage
    fr.gouv
    kotlin
    kotlinx
    net.sqlcipher
    okhttp3
    okio
    org
    retrofit2
    se.ansman.dagger.auto
  Resources
  APK signature
  Summary
```



https://github.com/skylot/jadx

__JADX__ is a Command line and GUI tools for produce __Java__ source code from __Android Dex__ and __Apk files__

Static Analysis - JADX

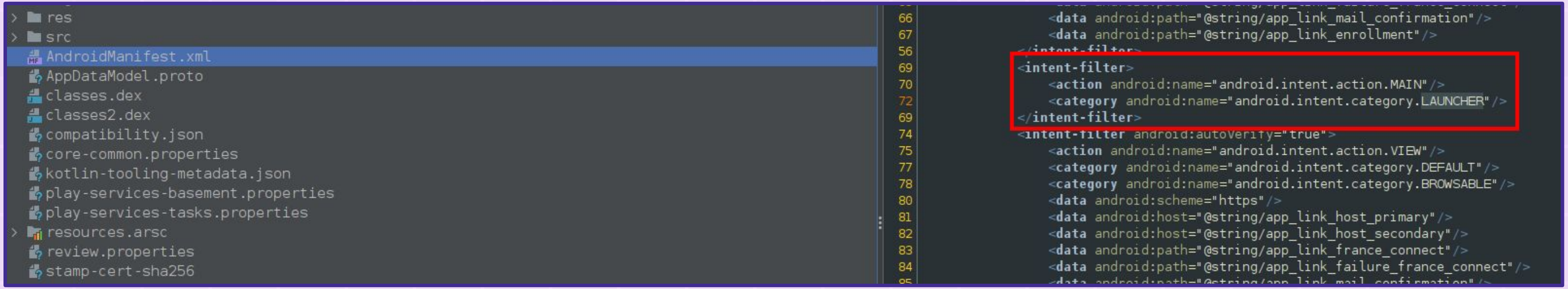


```
Source code
  android
  androidx
  com
  dagger
  defpackage
  fr.gouv
    franceidentite
      activities
      app
      core
        appinfo
        authentication
          api
            AuthenticationApi
            AuthenticationApi$AfCard$$serializer
            AuthenticationApi$AfIdVerifier$$serializer
            AuthenticationApi$ConfirmBody$$serializer
            AuthenticationApi$IdentityVerifiers$$serializer
            AuthenticationApi$StartTransactionResponse$$serializer
            AuthenticationApi$StartTransactionResponse$TransactionData$$serializer
            AuthenticationApi$StartTransactionResponse$TransactionData$Mobile$$serializer
            AuthenticationApi$StartTransactionResponse$TransactionData$Mobile$Result$$serializer
            AuthenticationApi$StopTransactionBody$$serializer
            AuthenticationApi$TransactionBody$$serializer
            AuthenticationApi$TransactionBody$MobileInfo$$serializer
            AuthenticationApi$TransactionResponse$$serializer
          implementation
          Authentication
          Authentication$Data$$serializer
          StoreAuthentication
        device
        environment
        initializer
        json
        jwt
```

```java
                return Authentication$Data$$serializer.INSTANCE;
            }
        }

        public Data(String str, String str2, List list, String str3, String str4, String
            TuplesKt.checkNotNullParameter(str, "sessionId");
            this.token = "";
            this.sessionId = str;
            this.scenarioId = str2;
            this.identityVerifiers = list;
            this.identityLocation = str3;
            this.randomChallenge = str4;
            this.afMode = str5;
        }

        public final boolean equals(Object obj) {
            if (this == obj) {
                return true;
            }
            if (obj instanceof Data) {
                Data data = (Data) obj;
                return TuplesKt.areEqual(this.token, data.token) && TuplesKt.areEqual(th
            }
            return false;
        }

        public final int hashCode() {
            int m = Key$$ExternalSyntheticOutline0.m(this.scenarioId, Key$$ExternalSynth
            List list = this.identityVerifiers;
            int hashCode = (m + (list == null ? 0 : list.hashCode())) * 31;
            String str = this.identityLocation;
            int hashCode2 = (hashCode + (str == null ? 0 : str.hashCode())) * 31;
            String str2 = this.randomChallenge;
            int hashCode3 = (hashCode2 + (str2 == null ? 0 : str2.hashCode())) * 31;
            String str3 = this.afMode;
            return hashCode3 + (str3 != null ? str3.hashCode() : 0);
        }

        public final String toString() {
            StringBuilder sb = new StringBuilder("Data(token=");
            sb.append(this.token);
            sb.append(", sessionId=");
```

Static Analysis - JADX

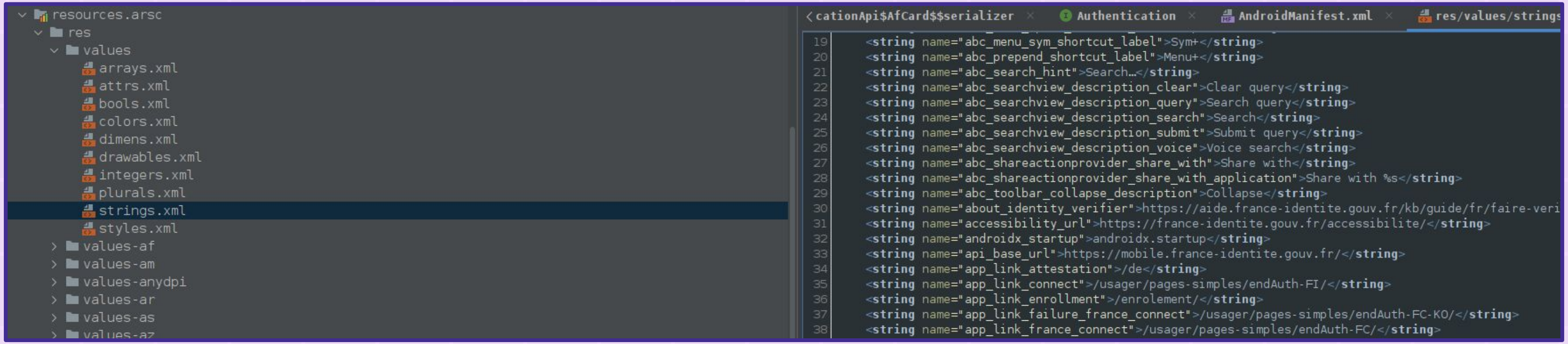
AndroidManifest.xml



```
> res
> src
  AndroidManifest.xml
  AppDataModel.proto
  classes.dex
  classes2.dex
  compatibility.json
  core-common.properties
  kotlin-tooling-metadata.json
  play-services-basement.properties
  play-services-tasks.properties
> resources.arsc
  review.properties
  stamp-cert-sha256
```

```xml
                <data android:path="@string/app_link_mail_confirmation"/>
                <data android:path="@string/app_link_enrollment"/>
            </intent-filter>
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
            <intent-filter android:autoVerify="true">
                <action android:name="android.intent.action.VIEW"/>
                <category android:name="android.intent.category.DEFAULT"/>
                <category android:name="android.intent.category.BROWSABLE"/>
                <data android:scheme="https"/>
                <data android:host="@string/app_link_host_primary"/>
                <data android:host="@string/app_link_host_secondary"/>
                <data android:path="@string/app_link_france_connect"/>
                <data android:path="@string/app_link_failure_france_connect"/>
```

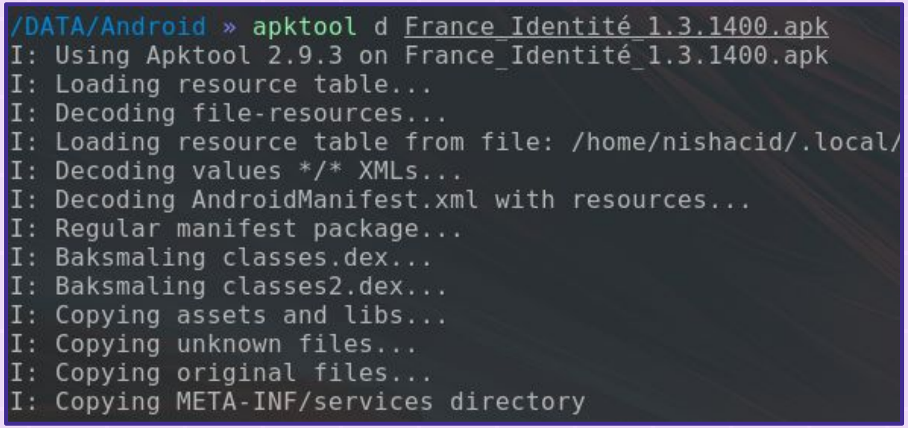
ressources / strings.xml



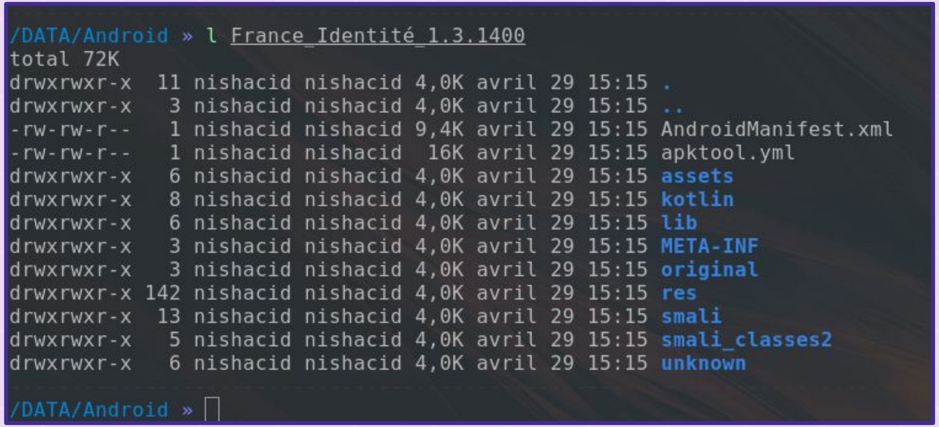
```
v resources.arsc
  v res
    v values
        arrays.xml
        attrs.xml
        bools.xml
        colors.xml
        dimens.xml
        drawables.xml
        integers.xml
        plurals.xml
        strings.xml
        styles.xml
    > values-af
    > values-am
    > values-anydpi
    > values-ar
    > values-as
```

```xml
    <string name="abc_menu_sym_shortcut_label">Sym+</string>
    <string name="abc_prepend_shortcut_label">Menu+</string>
    <string name="abc_search_hint">Search…</string>
    <string name="abc_searchview_description_clear">Clear query</string>
    <string name="abc_searchview_description_query">Search query</string>
    <string name="abc_searchview_description_search">Search</string>
    <string name="abc_searchview_description_submit">Submit query</string>
    <string name="abc_searchview_description_voice">Voice search</string>
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_toolbar_collapse_description">Collapse</string>
    <string name="about_identity_verifier">https://aide.france-identite.gouv.fr/kb/guide/fr/faire-veri
    <string name="accessibility_url">https://france-identite.gouv.fr/accessibilite/</string>
    <string name="androidx_startup">androidx.startup</string>
    <string name="api_base_url">https://mobile.france-identite.gouv.fr/</string>
    <string name="app_link_attestation">/de</string>
    <string name="app_link_connect">/usager/pages-simples/endAuth-FI/</string>
    <string name="app_link_enrollment">/enrolement/</string>
    <string name="app_link_failure_france_connect">/usager/pages-simples/endAuth-FC-KO/</string>
    <string name="app_link_france_connect">/usager/pages-simples/endAuth-FC/</string>
```

Static Analysis - ApkTool



```
/DATA/Android » apktool d France_Identité_1.3.1400.apk
I: Using Apktool 2.9.3 on France_Identité_1.3.1400.apk
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: /home/nishacid/.local/
I: Decoding values */* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory
```

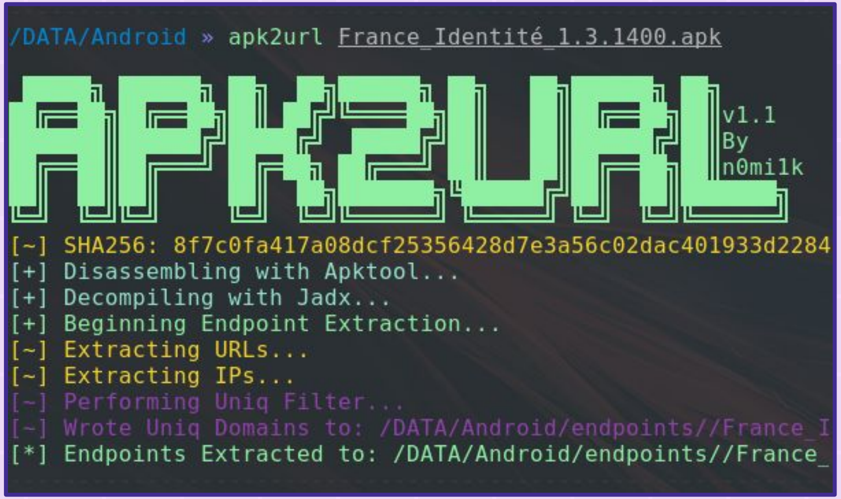


```
/DATA/Android » l France_Identité_1.3.1400
total 72K
drwxrwxr-x  11 nishacid nishacid 4,0K avril 29 15:15 .
drwxrwxr-x   3 nishacid nishacid 4,0K avril 29 15:15 ..
-rw-rw-r--   1 nishacid nishacid 9,4K avril 29 15:15 AndroidManifest.xml
-rw-rw-r--   1 nishacid nishacid  16K avril 29 15:15 apktool.yml
drwxrwxr-x   6 nishacid nishacid 4,0K avril 29 15:15 assets
drwxrwxr-x   8 nishacid nishacid 4,0K avril 29 15:15 kotlin
drwxrwxr-x   6 nishacid nishacid 4,0K avril 29 15:15 lib
drwxrwxr-x   3 nishacid nishacid 4,0K avril 29 15:15 META-INF
drwxrwxr-x   3 nishacid nishacid 4,0K avril 29 15:15 original
drwxrwxr-x 142 nishacid nishacid 4,0K avril 29 15:15 res
drwxrwxr-x  13 nishacid nishacid 4,0K avril 29 15:15 smali
drwxrwxr-x   5 nishacid nishacid 4,0K avril 29 15:15 smali_classes2
drwxrwxr-x   6 nishacid nishacid 4,0K avril 29 15:15 unknown

/DATA/Android »
```

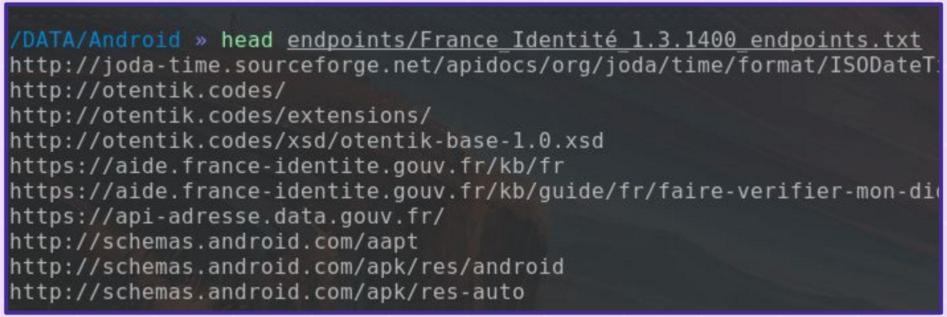
https://github.com/iBotPeaches/Apktool

***Apktool** is a tool for reverse engineering third-party, closed, binary, **Android** apps. It can decode resources to nearly original form and **rebuild** them after making some modifications*

Static Analysis - Apk2URL



```
/DATA/Android » apk2url France_Identité_1.3.1400.apk
APK2URL v1.1
By
n0mi1k
[~] SHA256: 8f7c0fa417a08dcf25356428d7e3a56c02dac401933d2284
[+] Disassembling with Apktool...
[+] Decompiling with Jadx...
[+] Beginning Endpoint Extraction...
[~] Extracting URLs...
[~] Extracting IPs...
[~] Performing Uniq Filter...
[~] Wrote Uniq Domains to: /DATA/Android/endpoints//France_I
[*] Endpoints Extracted to: /DATA/Android/endpoints//France_
```

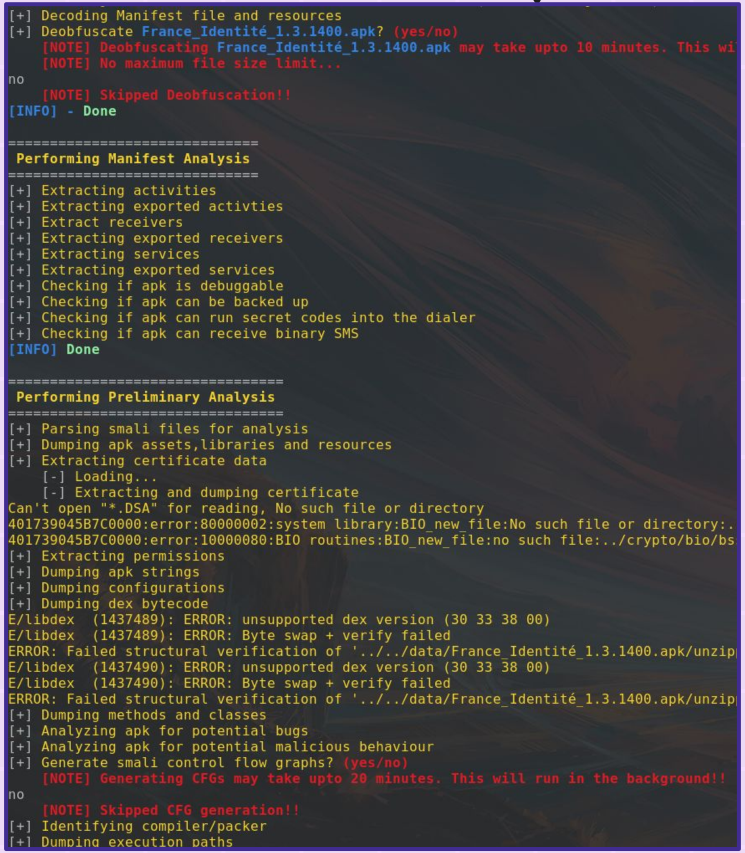


```
/DATA/Android » head endpoints/France_Identité_1.3.1400_endpoints.txt
http://joda-time.sourceforge.net/apidocs/org/joda/time/format/ISODateT
http://otentik.codes/
http://otentik.codes/extensions/
http://otentik.codes/xsd/otentik-base-1.0.xsd
https://aide.france-identite.gouv.fr/kb/fr
https://aide.france-identite.gouv.fr/kb/guide/fr/faire-verifier-mon-di
https://api-adresse.data.gouv.fr/
http://schemas.android.com/aapt
http://schemas.android.com/apk/res/android
http://schemas.android.com/apk/res-auto
```

https://github.com/n0mi1k/apk2url

Apk2URL** easily extracts **URL** and **IP endpoints** from an APK file and performs filtering into a **.txt output

Static Analysis – Mara Framework



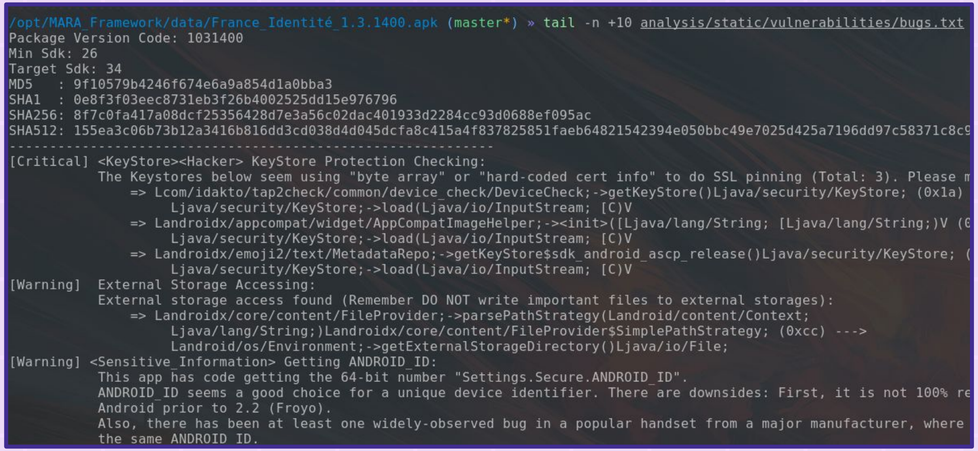
```
[+] Decoding Manifest file and resources
[+] Deobfuscate France_Identité_1.3.1400.apk? (yes/no)
    [NOTE] Deobfuscating France_Identité_1.3.1400.apk may take upto 10 minutes. This wi
    [NOTE] No maximum file size limit...
no
    [NOTE] Skipped Deobfuscation!!
[INFO] - Done

==============================
 Performing Manifest Analysis
==============================
[+] Extracting activities
[+] Extracting exported activties
[+] Extract receivers
[+] Extracting exported receivers
[+] Extracting services
[+] Extracting exported services
[+] Checking if apk is debuggable
[+] Checking if apk can be backed up
[+] Checking if apk can run secret codes into the dialer
[+] Checking if apk can receive binary SMS
[INFO] Done

=================================
 Performing Preliminary Analysis
=================================
[+] Parsing smali files for analysis
[+] Dumping apk assets,libraries and resources
[+] Extracting certificate data
    [-] Loading...
    [-] Extracting and dumping certificate
Can't open "*.DSA" for reading, No such file or directory
401739045B7C0000:error:80000002:system library:BIO_new_file:No such file or directory:.
401739045B7C0000:error:10000080:BIO routines:BIO_new_file:no such file:../crypto/bio/bs
[+] Extracting permissions
[+] Dumping apk strings
[+] Dumping configurations
[+] Dumping dex bytecode
E/libdex  (1437489): ERROR: unsupported dex version (30 33 38 00)
E/libdex  (1437489): ERROR: Byte swap + verify failed
ERROR: Failed structural verification of '../../data/France_Identité_1.3.1400.apk/unzip
E/libdex  (1437490): ERROR: unsupported dex version (30 33 38 00)
E/libdex  (1437490): ERROR: Byte swap + verify failed
ERROR: Failed structural verification of '../../data/France_Identité_1.3.1400.apk/unzip
[+] Dumping methods and classes
[+] Analyzing apk for potential bugs
[+] Analyzing apk for potential malicious behaviour
[+] Generate smali control flow graphs? (yes/no)
    [NOTE] Generating CFGs may take upto 20 minutes. This will run in the background!!
no
    [NOTE] Skipped CFG generation!!
[+] Identifying compiler/packer
[+] Dumping execution paths
```

https://github.com/xtiankisutsa/MARA_Framework

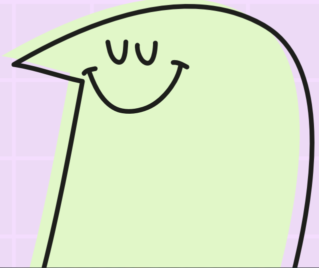
MARA is a tool that puts together commonly used mobile application **reverse engineering** and **analysis** tools, to assist in testing mobile applications against the **OWASP** mobile security threats.

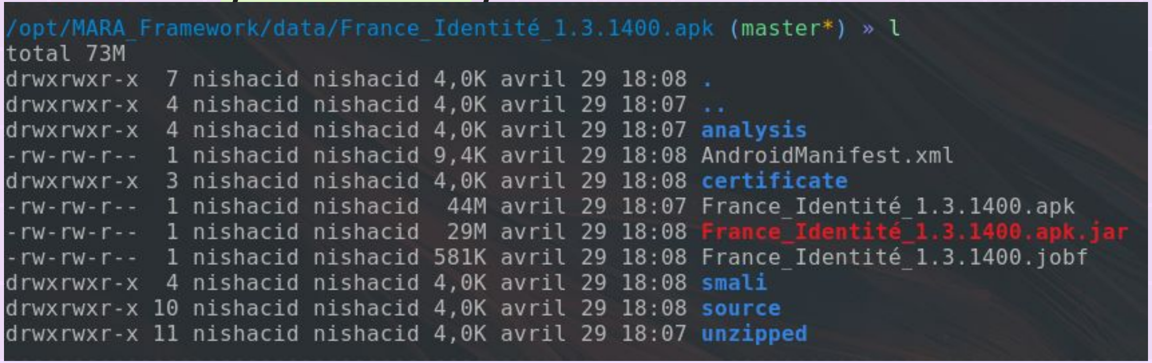
- **APK Analysis** (*Extract strings, URL, certificate..*)
- **APK Reverse Engineering** (*Disassembling, Decompiling...*)
- **APK Deobfuscation**
- **APK Manifest Analysis** (*Extract Intents, services..*)
- **Domain Analysis** (*SSL scan, website fingerprint...*)
- **Security Analysis** (*Code analysis OWASP...*)

Static Analysis - Mara Framework

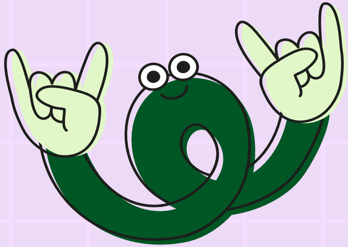


```
/opt/MARA_Framework/data/France_Identité_1.3.1400.apk (master*) » tail -n +10 analysis/static/vulnerabilities/bugs.txt
Package Version Code: 1031400
Min Sdk: 26
Target Sdk: 34
MD5   : 9f10579b4246f674e6a9a854d1a0bba3
SHA1  : 0e8f3f03eec8731eb3f26b4002525dd15e976796
SHA256: 8f7c0fa417a08dcf25356428d7e3a56c02dac401933d2284cc93d0688ef095ac
SHA512: 155ea3c06b73b12a3416b816dd3cd038d4d045dcfa8c415a4f837825851faeb64821542394e050bbc49e7025d425a7196dd97c58371c8c9
-------------------------------------------------------------
[Critical] <KeyStore><Hacker> KeyStore Protection Checking:
           The Keystores below seem using "byte array" or "hard-coded cert info" to do SSL pinning (Total: 3). Please m
               => Lcom/idakto/tap2check/common/device_check/DeviceCheck;->getKeyStore()Ljava/security/KeyStore; (0x1a)
                    Ljava/security/KeyStore;->load(Ljava/io/InputStream; [C)V
               => Landroidx/appcompat/widget/AppCompatImageHelper;-><init>([Ljava/lang/String; [Ljava/lang/String;)V (0
                    Ljava/security/KeyStore;->load(Ljava/io/InputStream; [C)V
               => Landroidx/emoji2/text/MetadataRepo;->getKeyStore$sdk_android_ascp_release()Ljava/security/KeyStore; (
                    Ljava/security/KeyStore;->load(Ljava/io/InputStream; [C)V
[Warning]  External Storage Accessing:
           External storage access found (Remember DO NOT write important files to external storages):
               => Landroidx/core/content/FileProvider;->parsePathStrategy(Landroid/content/Context;
                    Ljava/lang/String;)Landroidx/core/content/FileProvider$SimplePathStrategy; (0xcc) --->
                    Landroid/os/Environment;->getExternalStorageDirectory()Ljava/io/File;
[Warning] <Sensitive_Information> Getting ANDROID_ID:
           This app has code getting the 64-bit number "Settings.Secure.ANDROID_ID".
           ANDROID_ID seems a good choice for a unique device identifier. There are downsides: First, it is not 100% re
           Android prior to 2.2 (Froyo).
           Also, there has been at least one widely-observed bug in a popular handset from a major manufacturer, where
           the same ANDROID_ID.
```

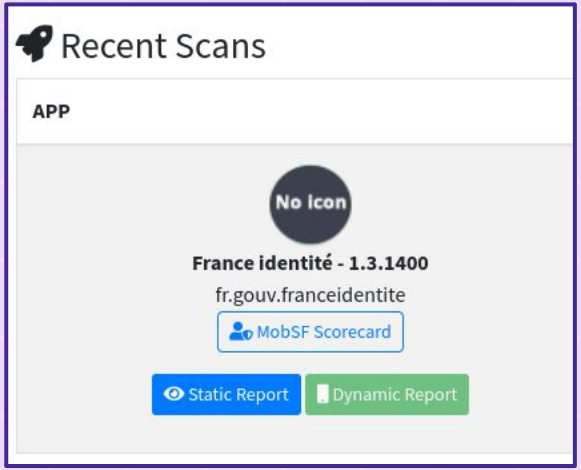




```
/opt/MARA_Framework/data/France_Identité_1.3.1400.apk (master*) » l
total 73M
drwxrwxr-x  7 nishacid nishacid 4,0K avril 29 18:08 .
drwxrwxr-x  4 nishacid nishacid 4,0K avril 29 18:07 ..
drwxrwxr-x  4 nishacid nishacid 4,0K avril 29 18:07 analysis
-rw-rw-r--  1 nishacid nishacid 9,4K avril 29 18:08 AndroidManifest.xml
drwxrwxr-x  3 nishacid nishacid 4,0K avril 29 18:08 certificate
-rw-rw-r--  1 nishacid nishacid  44M avril 29 18:07 France_Identité_1.3.1400.apk
-rw-rw-r--  1 nishacid nishacid  29M avril 29 18:08 France_Identité_1.3.1400.apk.jar
-rw-rw-r--  1 nishacid nishacid 581K avril 29 18:08 France_Identité_1.3.1400.jobf
drwxrwxr-x  4 nishacid nishacid 4,0K avril 29 18:08 smali
drwxrwxr-x 10 nishacid nishacid 4,0K avril 29 18:08 source
drwxrwxr-x 11 nishacid nishacid 4,0K avril 29 18:07 unzipped
```



"Static" Analysis - MOBSF



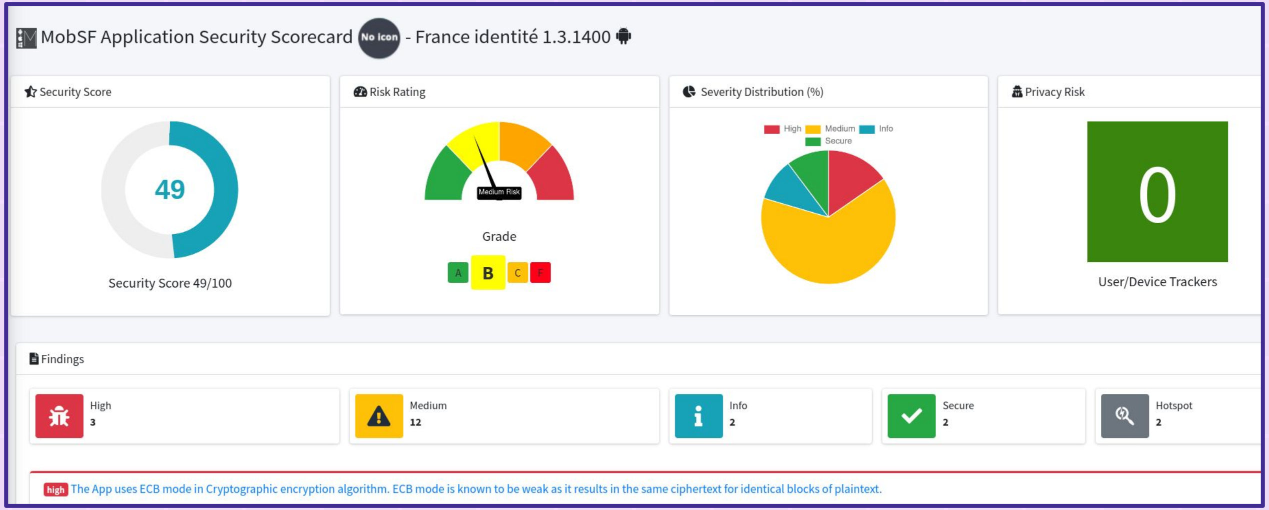
Recent Scans

APP

No Icon

France identité - 1.3.1400

fr.gouv.franceidentite



MobSF Application Security Scorecard No Icon - France identité 1.3.1400

Security Score

49

Security Score 49/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)

Privacy Risk

0

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
3	12	2	2	2

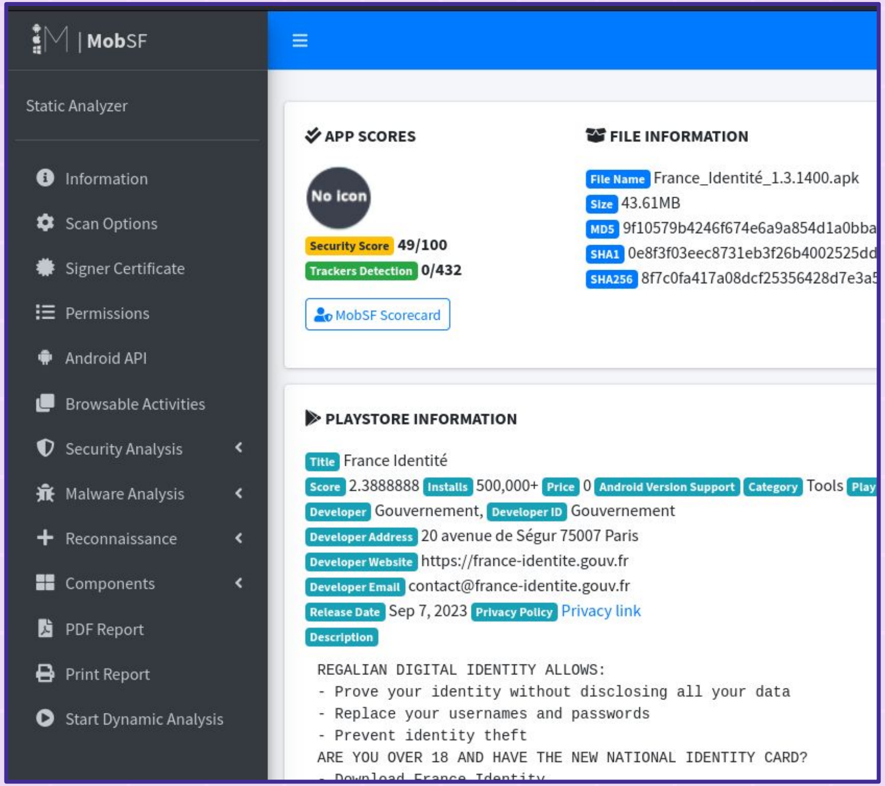
high The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.

https://github.com/MobSF/Mobile-Security-Framework-MobSF

MobSF is a web security research platform for mobile applications in **Android, iOS** and **Windows Mobile**.

- **Static Analysis** (*Android / iOS*)
- **Dynamic Analysis** (*Android / iOS*)
- **Web API Viewer**
- **CI/CD**

“Static” Analysis - MOBSF



APP SCORES

No Icon

Security Score 49/100

Trackers Detection 0/432

MobSF Scorecard

FILE INFORMATION

File Name France_Identité_1.3.1400.apk

Size 43.61MB

MD5 9f10579b4246f674e6a9a854d1a0bba

SHA1 0e8f3f03eec8731eb3f26b4002525dd

SHA256 8f7c0fa417a08dcf25356428d7e3a5

PLAYSTORE INFORMATION

Title France Identité

Score 2.3888888 Installs 500,000+ Price 0 Android Version Support Category Tools Play

Developer Gouvernement, Developer ID Gouvernement

Developer Address 20 avenue de Ségur 75007 Paris

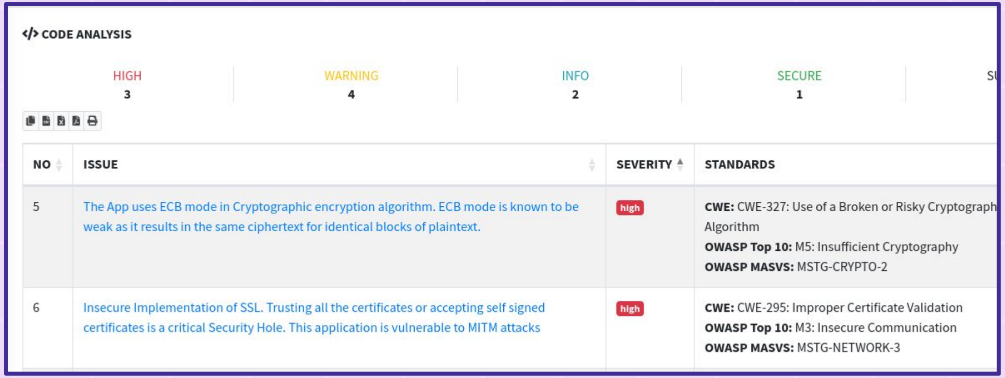
Developer Website https://france-identite.gouv.fr

Developer Email contact@france-identite.gouv.fr

Release Date Sep 7, 2023 Privacy Policy Privacy link

Description

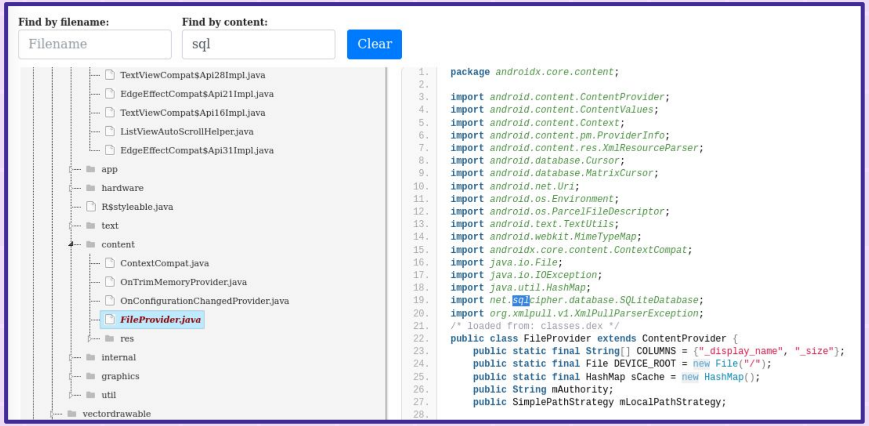
```
REGALIAN DIGITAL IDENTITY ALLOWS:
- Prove your identity without disclosing all your data
- Replace your usernames and passwords
- Prevent identity theft
ARE YOU OVER 18 AND HAVE THE NEW NATIONAL IDENTITY CARD?
- Download France Identity
```



CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SU
3	4	2	1	

NO	ISSUE	SEVERITY	STANDARDS
5	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	**CWE:** CWE-327: Use of a Broken or Risky Cryptograph Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-2
6	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	**CWE:** CWE-295: Improper Certificate Validation **OWASP Top 10:** M3: Insecure Communication **OWASP MASVS:** MSTG-NETWORK-3



Find by filename: Filename

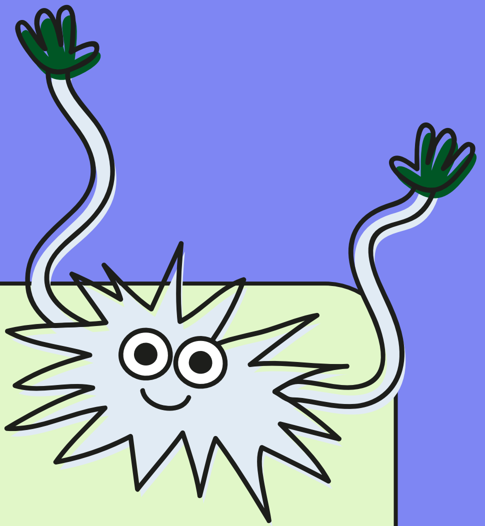
Find by content: sql

Clear
TextViewCompat$Api28Impl.java
EdgeEffectCompat$Api21Impl.java
TextViewCompat$Api16Impl.java
ListViewAutoScrollHelper.java
EdgeEffectCompat$Api31Impl.java
app
hardware
R$styleable.java
text
content
ContextCompat.java
OnTrimMemoryProvider.java
OnConfigurationChangedProvider.java
FileProvider.java
res
internal
graphics
util
vectordrawable

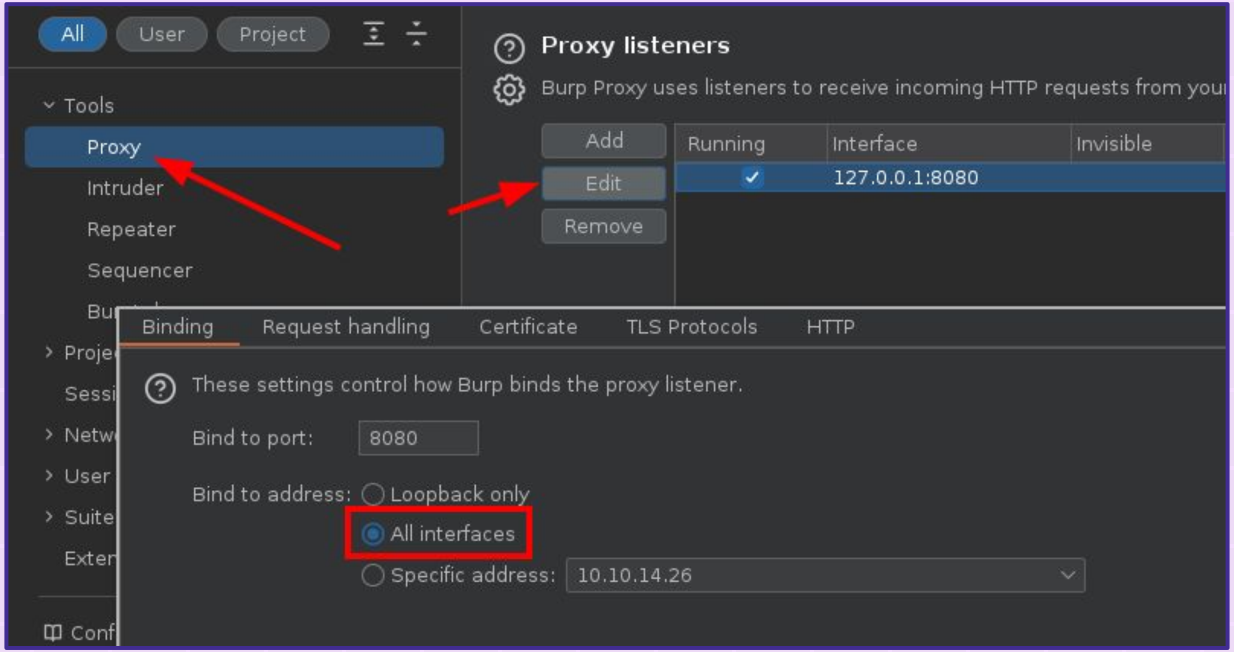
```java
package androidx.core.content;

import android.content.ContentProvider;
import android.content.ContentValues;
import android.content.Context;
import android.content.pm.ProviderInfo;
import android.content.res.XmlResourceParser;
import android.database.Cursor;
import android.database.MatrixCursor;
import android.net.Uri;
import android.os.Environment;
import android.os.ParcelFileDescriptor;
import android.text.TextUtils;
import android.webkit.MimeTypeMap;
import androidx.core.content.ContextCompat;
import java.io.File;
import java.io.IOException;
import java.util.HashMap;
import net.sqlcipher.database.SQLiteDatabase;
import org.xmlpull.v1.XmlPullParserException;
/* loaded from: classes.dex */
public class FileProvider extends ContentProvider {
    public static final String[] COLUMNS = {"_display_name", "_size"};
    public static final File DEVICE_ROOT = new File("/");
    public static final HashMap sCache = new HashMap();
    public String mAuthority;
    public SimplePathStrategy mLocalPathStrategy;

```

03

Dynamic Analysis



Dynamic Analysis - BurpSuite



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from you

Running	Interface	Invisible
✓	127.0.0.1:8080	

These settings control how Burp binds the proxy listener.

Bind to port: 8080

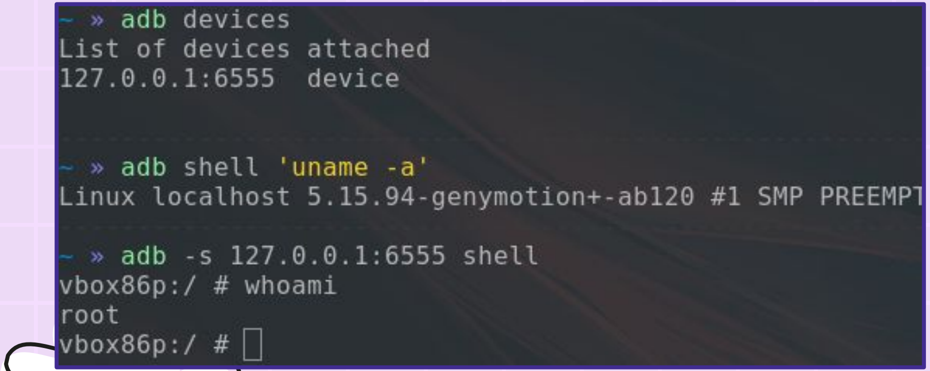
Bind to address: ○ Loopback only

● All interfaces

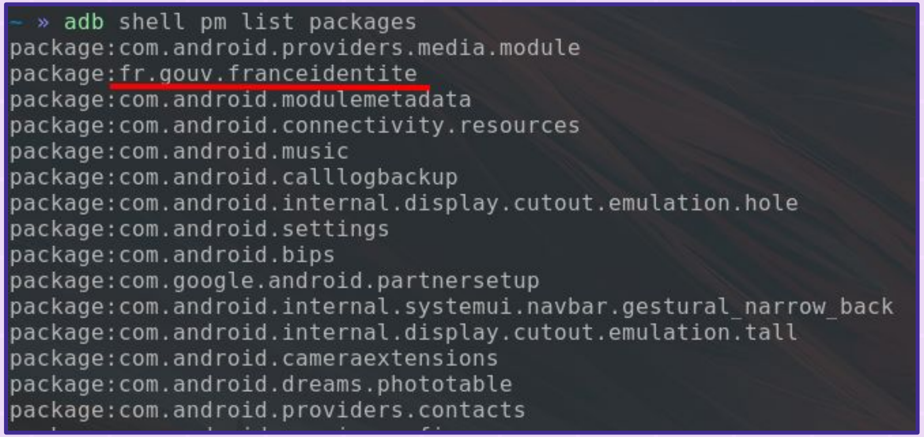
○ Specific address: 10.10.14.26

https://portswigger.net/burp/documentation/desktop/mobile/config-android-device

Dynamic Analysis - ADB



```
~ » adb devices
List of devices attached
127.0.0.1:6555  device


~ » adb shell 'uname -a'
Linux localhost 5.15.94-genymotion+-ab120 #1 SMP PREEMPT

~ » adb -s 127.0.0.1:6555 shell
vbox86p:/ # whoami
root
vbox86p:/ #
```

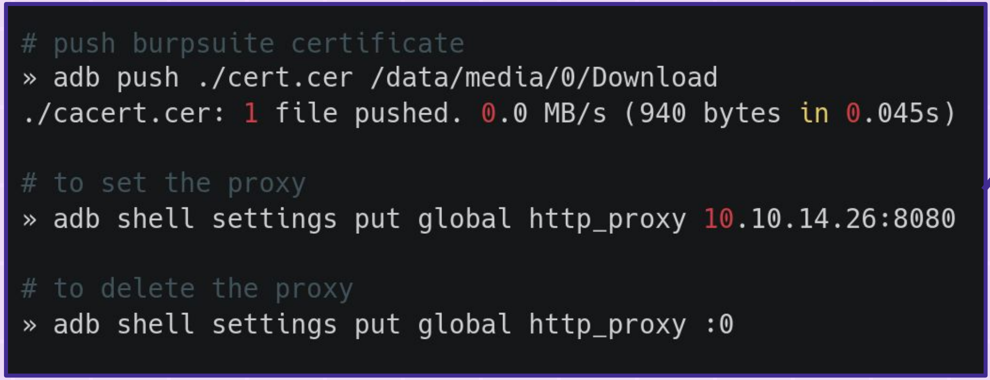


```
~ » adb shell pm list packages
package:com.android.providers.media.module
package:fr.gouv.franceidentite
package:com.android.modulemetadata
package:com.android.connectivity.resources
package:com.android.music
package:com.android.calllogbackup
package:com.android.internal.display.cutout.emulation.hole
package:com.android.settings
package:com.android.bips
package:com.google.android.partnersetup
package:com.android.internal.systemui.navbar.gestural_narrow_back
package:com.android.internal.display.cutout.emulation.tall
package:com.android.cameraextensions
package:com.android.dreams.phototable
package:com.android.providers.contacts
```

https://developer.android.com/tools/adb

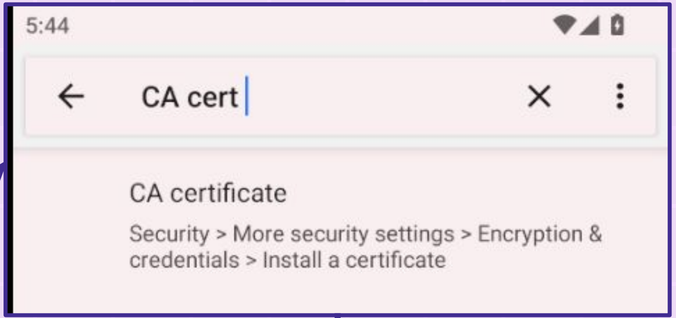
Dynamic Analysis - Proxy Certificate

1



```
# push burpsuite certificate
» adb push ./cert.cer /data/media/0/Download
./cacert.cer: 1 file pushed. 0.0 MB/s (940 bytes in 0.045s)

# to set the proxy
» adb shell settings put global http_proxy 10.10.14.26:8080

# to delete the proxy
» adb shell settings put global http_proxy :0
```

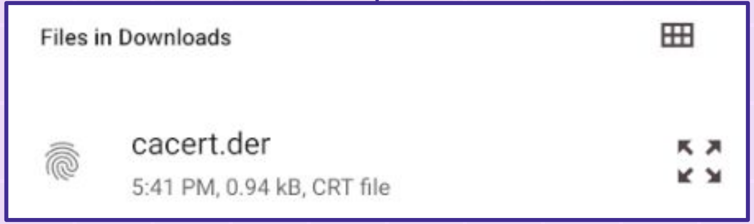
2



CA certificate

Security > More security settings > Encryption & credentials > Install a certificate

3

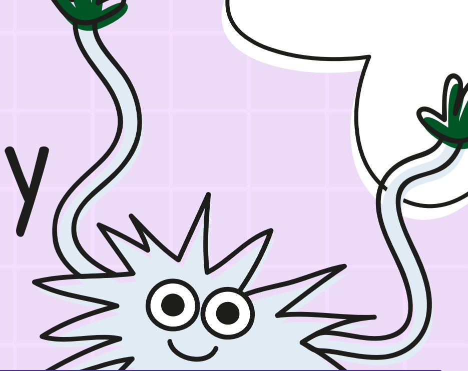


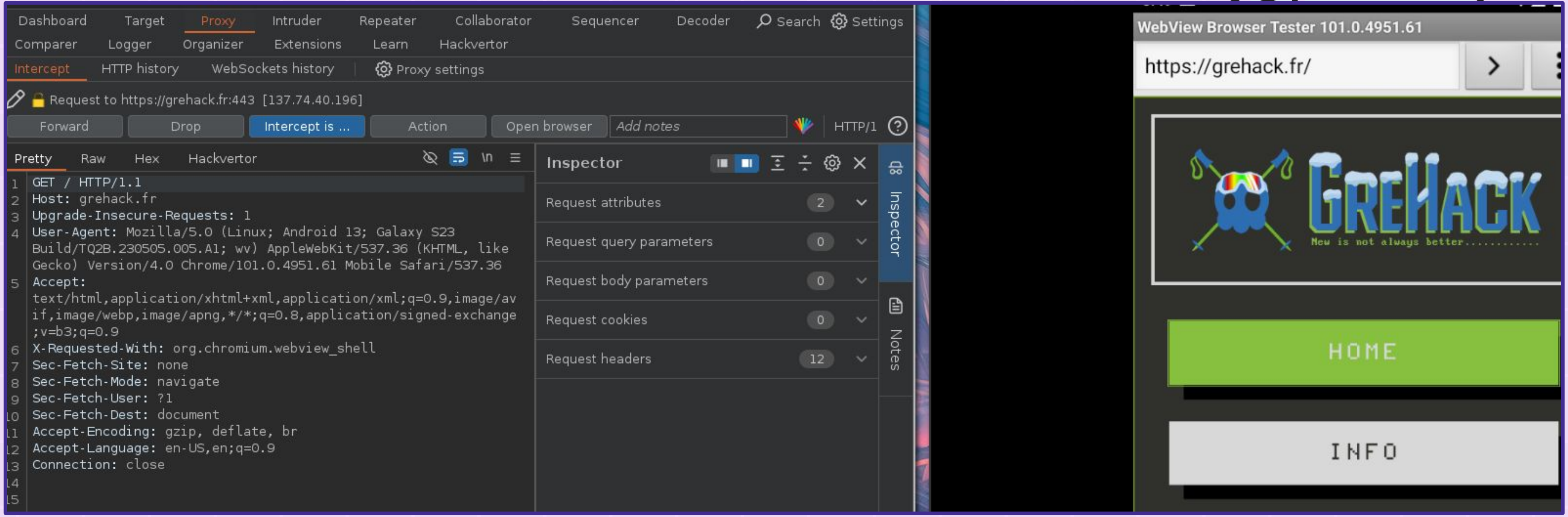
Files in Downloads

cacert.der

5:41 PM, 0.94 kB, CRT file

Dynamic Analysis – Proxy





Request to https://grehack.fr:443 [137.74.40.196]

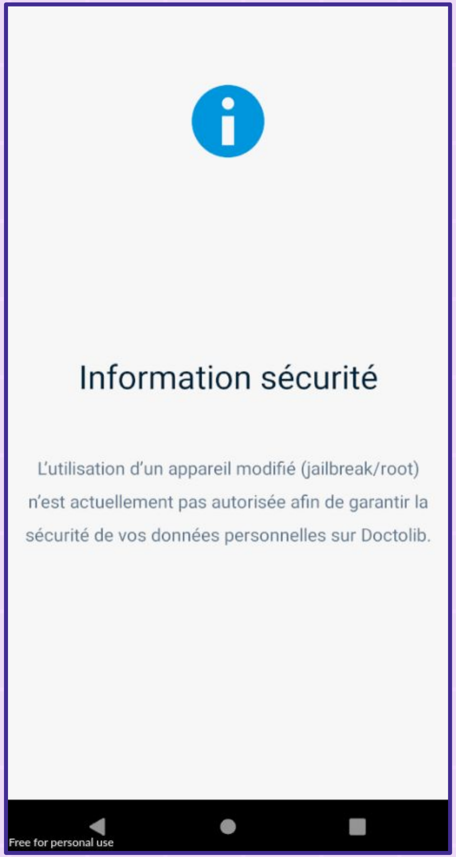
```
GET / HTTP/1.1
Host: grehack.fr
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 13; Galaxy S23
Build/TQ2B.230505.005.A1; wv) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/101.0.4951.61 Mobile Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.9
X-Requested-With: org.chromium.webview_shell
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```

Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 12

WebView Browser Tester 101.0.4951.61

https://grehack.fr/

Dynamic Analysis - Bypass root protection



Information sécurité

L'utilisation d'un appareil modifié (jailbreak/root) n'est actuellement pas autorisée afin de garantir la sécurité de vos données personnelles sur Doctolib.

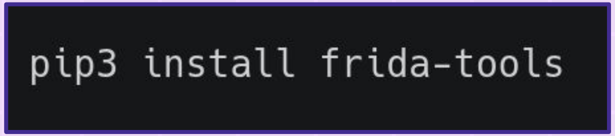
Root protection refers to security measures used to detect if a device is **rooted**. Rooting grants full control over the OS, potentially exposing it to security risks.

SSL pinning involves verifying that the server's certificate matches a known good copy stored within the app. This prevents attacks involving **forged certificates**, enhancing security by ensuring the app communicates only with the **authentic server**.

Dynamic Analysis – Frida

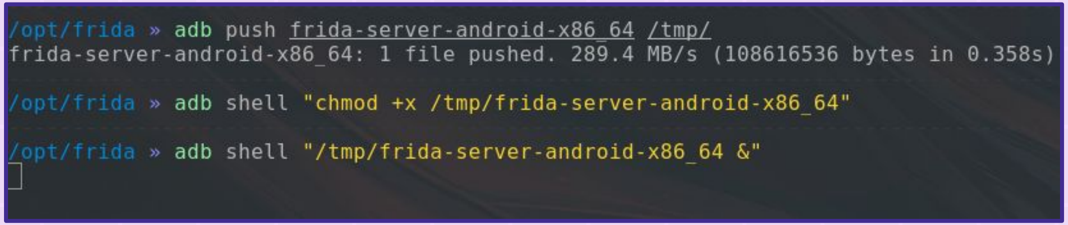
Frida is a free **dynamic instrumentation toolkit** that can be used for many things on various platforms.

- **Read app memory** (Full memory access)
- **Call methods / functions**
- **Hook methods / functions**

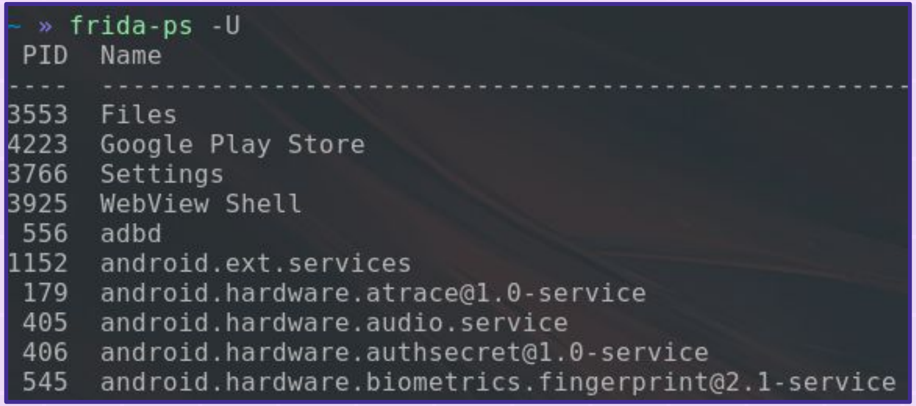


```
pip3 install frida-tools
```

https://github.com/frida/frida/releases/

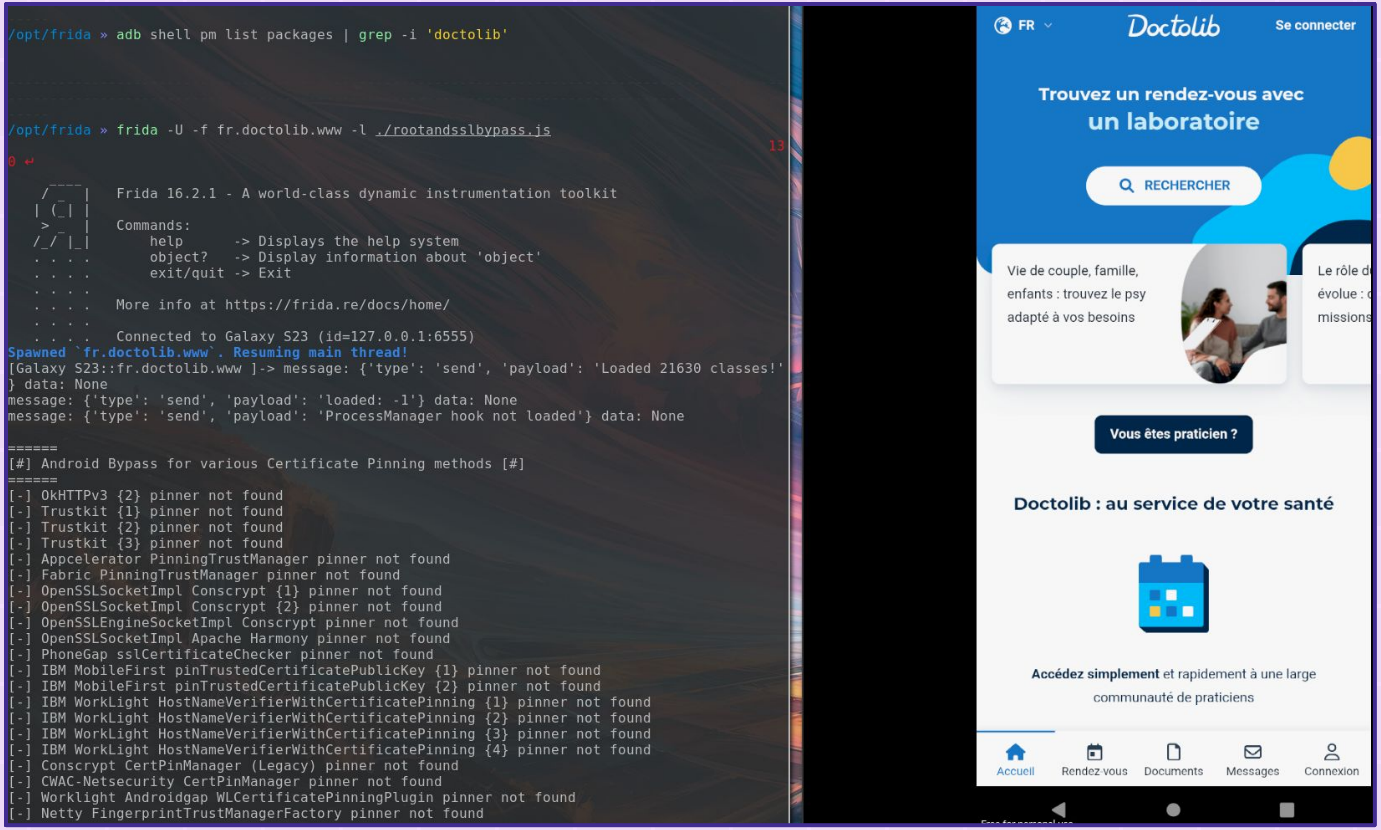


```
/opt/frida » adb push frida-server-android-x86_64 /tmp/
frida-server-android-x86_64: 1 file pushed. 289.4 MB/s (108616536 bytes in 0.358s)

/opt/frida » adb shell "chmod +x /tmp/frida-server-android-x86_64"

/opt/frida » adb shell "/tmp/frida-server-android-x86_64 &"
```



```
~ » frida-ps -U
 PID  Name
----  --------------------------------------------------------
3553  Files
4223  Google Play Store
3766  Settings
3925  WebView Shell
 556  adbd
1152  android.ext.services
 179  android.hardware.atrace@1.0-service
 405  android.hardware.audio.service
 406  android.hardware.authsecret@1.0-service
 545  android.hardware.biometrics.fingerprint@2.1-service
```

Dynamic Analysis – Bypass root protection



```
/opt/frida » adb shell pm list packages | grep -i 'doctolib'


/opt/frida » frida -U -f fr.doctolib.www -l ./rootandsslbypass.js                    13
0 ↵
     ____
    / _  |   Frida 16.2.1 - 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 Galaxy S23 (id=127.0.0.1:6555)
Spawned `fr.doctolib.www`. Resuming main thread!
[Galaxy S23::fr.doctolib.www ]-> message: {'type': 'send', 'payload': 'Loaded 21630 classes!'
} data: None
message: {'type': 'send', 'payload': 'loaded: -1'} data: None
message: {'type': 'send', 'payload': 'ProcessManager hook not loaded'} data: None

======
[#] Android Bypass for various Certificate Pinning methods [#]
======
[-] OkHTTPv3 {2} pinner not found
[-] Trustkit {1} pinner not found
[-] Trustkit {2} pinner not found
[-] Trustkit {3} pinner not found
[-] Appcelerator PinningTrustManager pinner not found
[-] Fabric PinningTrustManager pinner not found
[-] OpenSSLSocketImpl Conscrypt {1} pinner not found
[-] OpenSSLSocketImpl Conscrypt {2} pinner not found
[-] OpenSSLEngineSocketImpl Conscrypt pinner not found
[-] OpenSSLSocketImpl Apache Harmony pinner not found
[-] PhoneGap sslCertificateChecker pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey {1} pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey {2} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {1} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {2} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {3} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {4} pinner not found
[-] Conscrypt CertPinManager (Legacy) pinner not found
[-] CWAC-Netsecurity CertPinManager pinner not found
[-] Worklight Androidgap WLCertificatePinningPlugin pinner not found
[-] Netty FingerprintTrustManagerFactory pinner not found
```

Trouvez un rendez-vous avec
un laboratoire

Vie de couple, famille, enfants : trouvez le psy adapté à vos besoins

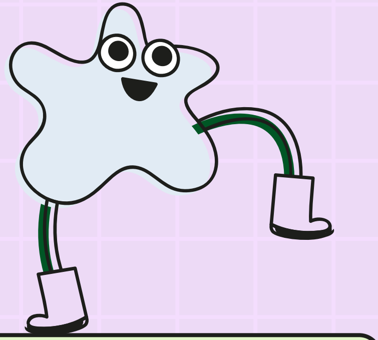
Le rôle d
évolue : c
missions

Doctolib : au service de votre santé

Accédez simplement et rapidement à une large communauté de praticiens

Collection of **Frida scripts** :

https://codeshare.frida.re/



https://codeshare.frida.re/@KaiserBloo/ssl-and-root-bypass/

Others technos

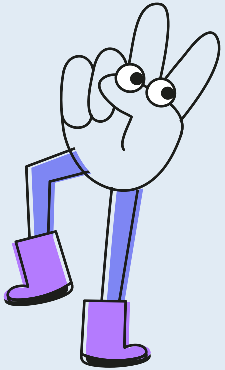
you are here

Catch them all

- **Java** - Original language for Android, versatile.
- **Kotlin** - Modernizes and simplifies Android code.
- **Flutter** - Creates cross-platform apps with Dart.
- **Unity** - Ideal for games, uses C#.
- **React Native** - Cross-platform development in JavaScript.
- **Xamarin** - Shares C# code between Android and iOS.
- **Cordova** - Converts web applications to mobile.

RESOURCES

- Big thanks to @pwnwithlove
- Getting Started with Frida
- HackTricks - Frida Tutorial
- @Cyxo - Reverse Engineering d'applications Android
- Awesome Android Reverse Engineering
- Configuring an Android device to work with Burp Suite
- BurpSuite Mobile testing
- SSL Pinning in Android
- Bypassing Root Detection the Universal Way
- How to use Ghidra to Reverse Engineer Mobile Application



THANKS!

DO YOU HAVE ANY QUESTIONS?

@Nishacid