

Práctica Vulnerabilidades en APKs

1. Tomar una apk y decompilarla con apktool d nombreapk.apk. Esto se puede realizar tomando la apk del dispositivo con adb shell como se vio en la clase (recomendado) o descargando una apk (no recomendado). También se puede realizar la actividad con APKparser en Android - Genymotion - unzip - jadx.
2. Buscar ejemplos de configuraciones vistas en clase, ya sea configuraciones mal implementadas, o bien implementadas en caso de no encontrar malas prácticas. Pueden basarse en:
 - a. debug
 - b. backup
 - c. strings.xml
 - d. network security config
 - e. webviews
 - f. activities - intent filters - extra params
 - g. permisos
 - h. deeplinks
3. Documentar los hallazgos y subir un archivo PDF, detallando los pasos realizados, comandos, herramientas utilizadas, detallar el problema, cuál es la recomendación para aplicar la corrección, y agregar capturas de pantalla de ser necesario.

Fuente utilizada mayormente durante el desarrollo → [Developer Guides](#)

Resolución

Primero conectamos por USB al dispositivo móvil a la computadora con el modo debugging activado, también conocido como modo de depuración.

```
C:\adb>adb devices
List of devices attached
ZY322RM5R2      device
```

Listamos los dispositivos conectados. En este caso realice la actividad con un **Motorola Moto G6 Plus**

```
C:\adb>adb shell pm list packages
package:com.android.internal.display.cutout.emulation.noCutout
package:com.android.cts.priv.ctsshim
package:com.google.android.youtube
package:com.android.internal.display.cutout.emulation.corner
package:com.google.android.ext.services
package:com.motorola.motocare
package:com.android.internal.display.cutout.emulation.double
package:com.android.providers.telephony
package:com.google.android.googlequicksearchbox
package:com.android.providers.calendar
package:com.google.android.apps.googleassistant
package:org.telegram.messenger
package:com.android.providers.media
package:com.google.android.apps.docs.editors.docs
package:com.qti.service.colorservice
package:com.google.android.onetimeinitializer
package:com.google.android.ext.shared
package:com.motorola.brapps
package:com.motorola.bug2go
package:com.motorola.mya.fmwkwrapper
package:com.android.wallpapercropper
package:com.quicinc.cne.CNEService
package:com.mercadopago.wallet
package:com.motorola.ccc.devicemanagement
package:com.motorola.android.fmradio
package:com.motorola.faceunlocktrustagent
package:com.marsvard.stickermakerforwhatsapp
package:com.android.documentsui
package:com.motorola.android.settings.modemdebug
package:com.android.externalstorage
package:com.motorola.omadm.service
package:com.motorola.voiceauthtrustagent
package:com.android.htmlviewer
package:com.whatsapp
package:com.qualcomm.qti.uceShimService
package:com.android.companiondevicemanager
package:com.android.mms.service
package:com.google.android.apps.docs.editors.sheets
package:com.google.android.apps.docs.editors.slides
package:com.android.providers.downloads
package:com.motorola.coresettingstext
```

Listamos todos los **paquetes** que existen en el dispositivo y copiamos el nombre del que sea de nuestro interés.

```
package:com.google.android.apps.messaging
package:com.motorola.android.settings.diag_mdlog
package:com.roaming.android.gsimcontentprovider
package:com.motorola.att.phone.extensions
package:com.motorola.ccc.checkin
package:com.motorola.programmenu
package:com.qualcomm.qti.telephonyservice
package:com.motorola.timezonedata
package:com.motorola.ccc.mainplm
package:com.google.android.configupdater
package:com.motorola.camera2
package:com.motorola.ccc.ota
package:com.motorola.ccc.notification
package:com.android.defcontainer
package:com.cidi.cba
package:com.android.timezone.updater
package:com.google.ar.core
package:com.android.providers.downloads.ui
package:com.android.vending
package:com.android.pacprocessor
package:com.android.simappdialog
package:com.motorola.pgmsystem2
package:com.dolby.daxservice
package:com.motorola.faceunlock
package:com.motorola.demo.env
package:com.motorola.ptt.prip
package:com.banconacion.bnamas
package:com.android.internal.display.cutout.emulation.tall
package:ar.com.personal
package:com.android.certinstaller
package:com.android.carrierconfig
package:com.google.android.marvin.talkback
package:com.google.android.apps.work.oobconfig
package:com.qti.qualcomm.datastatusnotification
package:android
package:com.android.hotwordenrollment.xgoogle
package:com.motorola.android.provisioning
package:ar.com.bancar.uala
package:com.motorola.imagertuning_evert
package:com.lenovo.FileBrowser2
package:com.android.egg
package:com.android.mtp
```

```
package:com.android.nfc
package:com.android.stk
package:com.motorola.photoeditor
package:com.android.backupconfirm
package:com.instagram.android
package:com.motorola.timeweatherwidget
package:com.google.android.deskclock
package:org.codeaurora.ims
package:com.android.statementservice
package:com.motorola.motokeysystem
package:com.republicwireless.tel
package:com.google.android.gm
package:com.google.android.apps.tachyon
package:com.motorola.motocit
package:com.motorola.motokey
package:com.moodle.moodlemobile
package:com.android.settings.intelligence
package:com.android.systemui.theme.dark
package:com.microsoft.office.outlook
package:com.google.android.setupwizard
package:com.qualcomm.qcrilmsgtunnel
package:com.android.providers.settings
package:com.android.sharedstoragebackup
package:com.google.android.music
package:com.android.printspooler
package:com.android.hotwordenrollment.okgoogle
package:com.motorola.colorprofiles
package:com.dolby.dax2appUI
package:com.android.dreams.basic
package:com.lenovo.lsf.user
package:com.android.se
package:com.android.inputdevices
package:com.motorola.android.nativedropboxagent
package:com.google.android.dialer
package:com.motorola.mya
package:com.motorola.nfc
package:com.android.hotwordenrollment.tgoogle
package:com.motorola.audiomonitor
package:com.android.bips
package:android.oem.overlay
package:com.motorola.android.jvtcmd
package:com.motorola.frameworks.singlehand
```

```
package:com.disney.starplus
package:com.motorola.motosignature.app
package:com.google.android.apps.cloudprint
package:com.twitter.android
package:com.google.android.apps.docs
package:com.google.android.apps.maps
package:com.android.cellbroadcastreceiver
package:com.motorola.invisiblenet
package:com.google.android.webview
package:com.amazon.appmanager
package:com.google.android.contacts
package:com.motorola.contacts.preloadcontacts
package:com.android.server.telecom
package:com.google.android.syncadapters.contacts
package:com.motorola.android.providers.settings
package:com.android.keychain
package:com.google.android.calculator
package:com.android.chrome
package:com.google.android.packageinstaller
package:com.google.android.gms
package:com.google.android.gsf
package:com.google.android.ims
package:com.google.android.tts
package:com.android.calllogbackup
package:com.google.android.partnersetup
package:com.motorola.genie
package:com.motorola.setup
package:com.google.android.videos
package:com.android.carrierdefaultapp
package:com.pedidosya
package:com.motorola.appdirectedsmsproxy
package:com.android.proxyhandler
package:com.netflix.mediaclient
package:com.google.android.feedback
package:com.google.android.printservice.recommendation
package:com.google.android.apps.photos
package:com.google.android.calendar
package:com.android.managedprovisioning
package:com.motorola.launcherconfig
package:com.spotify.music
package:com.mercadolibre
package:com.twa_cbaciudad.app
```

Del listado anterior (no es exhaustivo), seleccionamos *com.cidi.cba* correspondiente a la app de **Ciudadano Digital**

```
C:\adb>adb shell pm path com.cidi.cba
package:/data/app/com.cidi.cba-PEy_M6Ei-Qi6TwymQnt29Q==/base.apk
package:/data/app/com.cidi.cba-PEy_M6Ei-Qi6TwymQnt29Q==/split_config.arm64_v8a.apk
package:/data/app/com.cidi.cba-PEy_M6Ei-Qi6TwymQnt29Q==/split_config.en.apk
package:/data/app/com.cidi.cba-PEy_M6Ei-Qi6TwymQnt29Q==/split_config.es.apk
package:/data/app/com.cidi.cba-PEy_M6Ei-Qi6TwymQnt29Q==/split_config.xxhdpi.apk
```

De esta forma obtenemos las rutas donde se encuentra ese paquete

```
C:\adb\pentest>adb pull /data/app/com.cidi.cba-PEy_M6Ei-Qi6TwymQnt29Q==/base.apk
/data/app/com.cidi.cba-PEy_M6Ei-Qi6TwymQnt29Q==/base.apk: ...le pulled, 0 skipped.
30.3 MB/s (11244617 bytes in 0.354s)
```

Con el comando anterior nos hacemos un pull de la apk desde el dispositivo android hasta la carpeta *pentest*

Ahora utilizando la herramienta **apktool** lo que haremos es decompilar la APK

```
C:\adb\pentest>apktool d base.apk
I: Using Apktool 2.6.1 on base.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\Agustin\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

equipo > Disco local (C:) > adb > pentest > base				
Nombre	Fecha de modificación	Tipo	Tamaño	
assets	23/10/2022 16:33	Carpeta de archivos		
original	23/10/2022 16:33	Carpeta de archivos		
res	23/10/2022 16:33	Carpeta de archivos		
smali	23/10/2022 16:33	Carpeta de archivos		
unknown	23/10/2022 16:33	Carpeta de archivos		
AndroidManifest.xml	23/10/2022 16:33	Documento XML	9 KB	
apktool.yml	23/10/2022 16:33	Archivo YML	4 KB	

Podemos observar que la apk de la app fue decompilada correctamente

Análisis de configuraciones de seguridad

AndroidManifest.xml

- El atributo *android:protectionLevel* no está establecido en **signature**, ni siquiera está declarado.
- El atributo *android:allowBackup* está establecido en **false**, es una configuración acertada

```
<application android:allowBackup="false" android:appComponentFactory="androidx.core.app.CoreComponentFactory"
  <meta-data android:name="com.google.firebase.messaging.default_notification_icon" android:resource="@draw
  <activity android:configChanges="keyboard|keyboardHidden|locale|orientation|screenLayout|screenSize|small
    <intent-filter>
      <action android:name="android.intent.action.MAIN"/>
      <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
    <meta-data android:name="android.app.shortcuts" android:resource="@xml/shortcuts"/>
    <intent-filter>
      <action android:name="android.intent.action.VIEW"/>
      <category android:name="android.intent.category.DEFAULT"/>
      <category android:name="android.intent.category.BROWSABLE"/>
      <data android:scheme="@string/custom_url_scheme"/>
    </intent-filter>
```

- El atributo *android:debuggable* no está establecido en **false**, ni siquiera está declarado.
- El atributo *android:autoVerify* no está establecido en **true**, ni siquiera está declarado.
- El atributo *android:usesCleartextTraffic* no está establecido en **false**

```
android:usesCleartextTraffic="true">
```

- No encontré el archivo denominado *network_security_config.xml*
- No encontré malas configuraciones dentro del archivo *strings.xml*

- Observación: se definió el atributo *android:scheme* como un custom string (un string personalizado) el cual debe coincidir siempre con **com.cidi.cba** para lo cual deben realizarse validaciones donde corresponda. No obstante, no encontré otros sitios donde se use este string dentro del apk.

```
<data android:scheme="@string/custom_url_scheme"/>
```

→ AndroidManifest.xml

```
<string name="custom_url_scheme">com.cidi.cba</string>
```

→ res/values/strings.xml