

Auditoria de Aplicación **Instagram**

Seguridad Informática



UNIVERSIDAD
Finis Terrae
VINCE IN BONO MALUM

Camilo Zepeda Hoffmann

Prof. Maximiliano Vega

Octubre 11, 2017



Licencias y Softwares Asociados

Los software y licencias asociadas a la aplicación son los siguientes:
AFNetworking, Appirater, Boost, CocoaLumberjack, Cocoawithlove, Flick-OAuth-iOS ,Google Breakpad entre muchos otros

De los cuales se hace una subdivisión por:

- Creación de Servicios (Android y iOS)
- Conexión a Servidores (Android y iOS)
- Aplicaciones Propias de dispositivos (Android y iOS)

Propuesta de Problemas

Además de las herramientas utilizadas se consideran realizar las siguientes pruebas:

- Validar la Seguridad de la Aplicación en Base a sus Herramientas/Software.
- Analizar el React Native de Instagram para Android y iOS.
- Realizar Pruebas Asociadas a la conexión Servidor Aplicación. haciendo uso de:
 - Man-in-the-middle.
 - DDoS.
- Decompilar la Aplicación (si es posible).
- Analizar ataque por medio de Restauración de Contraseña haciendo uso de Proxy Web. (ataque 2016).
- Posible Descompilación del Código.

Data de Problemas Relevantes

Vulnerabilidad en OAuth 2013



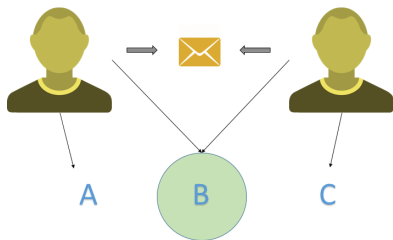
Luego de la compra de Facebook , se logra encontrar una falla de seguridad del software relacionada a la privacidad y confidencialidad de los datos, utilizando el protocolo OAuth. Dicho problema abrió paso a problemas como el acceso a la lista de amigos en Fb o filtración de imgenes.

Data de Problemas Relevantes

Cuentas Compartidas 2016

Consiste

en la compartición de cuentas por parte de un Sujeto 1 v's un Sujeto 2, donde ambos ya sea por motivos de asociación u otros comparten una cuenta en común B, dando paso a la notificación de cuentas fuera de su alcance. Lo que implica una filtración de información fuera del consentimiento de cada sujeto.



Data de Problemas Relevantes

Hackeo de Cuentas 2017

Hackeo masivo de cuentas, comprometiendo la seguridad de las cuentas en redes sociales. Llegando a circular datos de acceso a los perfiles a \$10 dolares cada cuenta. La información fue almacenada en la base de datos **Doxagram** en donde se realizó la venta.



Descarga de Aplicación

Obtención de Apk

apkpure  GAMES  APPS  TOPICS  PRODUCT

Home » Social » Instagram 



Instagram APK

 580    1  2.2K

★★★★★ 4.5/5 (475 Discussions)

Author:	Latest Version:	Publish Date:
Instagram	18.0.0.18.85	2017-10-10

[Download APK \(26.2 MB\)](#) 

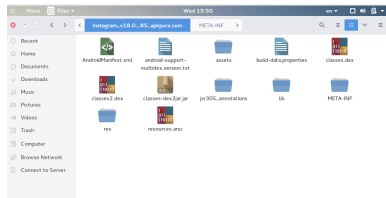
Using APKPure App to upgrade Instagram, fast, free and save your internet data.

Decompilación

Obtención de Archivos

Tras descargar el apk de instagram se utiliza la siguiente metodología:

- Convertir archivo a .ZIP, para obtener archivos.
- Obtención de XML, classes.dex, lib y Meta-inf.



En ésta carpeta es posible encontrar los métodos utilizados en la aplicación para la realización de encriptación y seguridad propiamente tal de los archivos dentro del desarrollo. Destacando entonces herramientas como:

- [illegible]

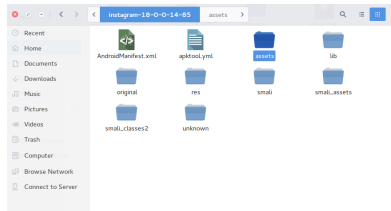
Decompilación

Uso de Apktool

Uso de herramienta **apktool**

apktool d Instagram.apk

se obtendrá archivos correspondientes a la aplicación además de los layouts, res y clases específicas del mismo.



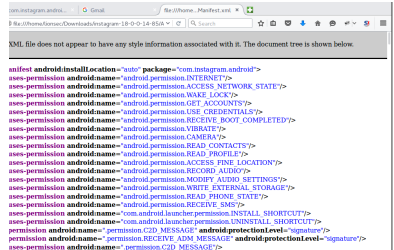
Decompilación

Obtención de XML

Por medio de la herramienta **apktool** y utilizando consola. se aplica comando

`apktool d Instagram.apk`

se obtendrá los xml y archivos correspondientes a la aplicación.



```

<manifest android:installLocation="auto" package="com.instagram.android">
  <uses-permission android:name="android.permission.INTERNET"/>
  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
  <uses-permission android:name="android.permission.WAKE_LOCK"/>
  <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
  <uses-permission android:name="android.permission.USE_CREDENTIALS"/>
  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
  <uses-permission android:name="android.permission.VIBRATE"/>
  <uses-permission android:name="android.permission.CAMERA"/>
  <uses-permission android:name="android.permission.READ_CONTACTS"/>
  <uses-permission android:name="android.permission.READ_PROFILE"/>
  <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
  <uses-permission android:name="android.permission.RECORD_AUDIO"/>
  <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
  <uses-permission android:name="android.permission.RECEIVE_SMS"/>
  <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
  <uses-permission android:name="com.android.launcher.permission.UNINSTALL_SHORTCUT"/>
  <permission android:name="permission.C2D_MESSAGE" android:protectionLevel="signature"/>
  <permission android:name="permission.RECEIVE_ADM_MESSAGE" android:protectionLevel="signature"/>
  <uses-permission android:name="permission.C2D_MESSAGE"/>

```

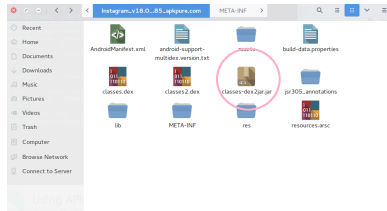
Decompilación

Obtención de Java

Por medio de la herramienta **dex2jar** y utilizando consola. se aplica comando

```
d2j-dex2jar classes.dex
```

se utiliza el dex (Dalvik Executable) para obtener el comprimido del archivo APK. Lo que puede ser visto con un java decompiler, accediendo entonces a el archivo.



Decompilación

Ver Archivos React

Se encuentran los archivos de react correspondiente las actividades, delegados o bien los archivos **.smali** correspondientes al assembly de lenguaje Java.

