

# Auditoria de Aplicación **Instagram**

## Seguridad Informática



UNIVERSIDAD  
**Finis Terrae**  
VINCE IN BONO MALUM

Camilo Zepeda Hoffmann

Prof. Maximiliano Vega

Octubre 25, 2017

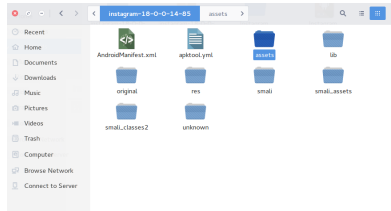
# Decompilación

## Uso de Apktool

Uso de herramienta **apktool**

apktool d Instagram.apk

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



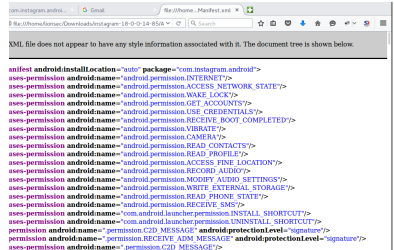
# Decompilación

## 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"/>

```

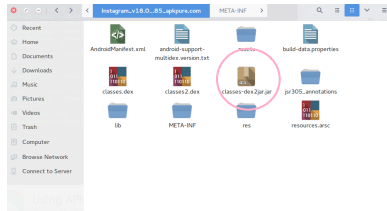
# Decompilación

## Obtención de Java

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

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

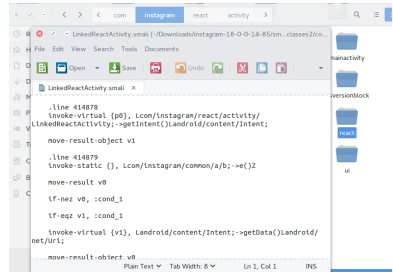
se utiliza el dex (Dalvik Executable) para obtener el comprimido del archivo APK. Lo que puede ser visto con un java decompiler, accediendo entonces a el archivo.



# 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.



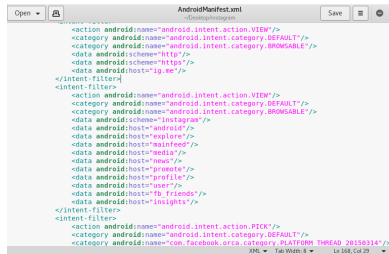


# Host de Browsers

## Hosts Encontrados en AndroidManifest.xml

Una vez conocida la url, se procede por medio de sqlmap a analizar el siguiente listado de host (Browsers) respectivos a la api:

- android
- explore
- mainfeed
- media
- news
- entre otros.





# Herramientas

## Uso de SQLMAP

Tras utilizar el comando:

```
sqlmap -u  
www.instagram.com/ Host Browsers
```

Realizando inyecciones dentro de la aplicación, de tal manera que se busquen fugas o posibles consultas.

```
do you want to try URI injections in the target URL itself? (Y/n/q) y
[16:40:19] [INFO] testing connection to the target URL
[16:40:20] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS: 200 OK
[16:40:31] [WARNING] reflective value(s) found and filtering out
[16:40:31] [INFO] testing if the target URL is blank
[16:40:34] [WARNING] URI parameter 'q' does not appear to be dynamic
[16:40:35] [WARNING] heuristic (basic) test shows that URI parameter 'q!' might not be injectable
[16:40:37] [INFO] testing for SQL injection on URI parameter 'q!'
[16:40:37] [INFO] testing AND boolean-based blind - WHERE or HAVING clause
[16:40:53] [INFO] testing MySQL = 5.0 boolean-based blind - Parameter replace
[16:40:56] [INFO] testing MySQL = 5.0 AND error-based - WHERE, HAVING, LIMIT BY or GROUP BY clause (FLOOR)
[16:40:58] [INFO] testing PostgreSQL AND error-based - WHERE or HAVING clause
[16:40:10] [INFO] testing Microsoft SQL Server/Oracle AND error-based - WHERE or HAVING clause (IN)
[16:40:22] [INFO] testing Oracle AND error-based - WHERE or HAVING clause (OR/Type)
[16:40:33] [INFO] testing MySQL = 5.0 error-based - Parameter replace (FLOOR)
[16:40:34] [INFO] testing MySQL inline queries
[16:40:35] [INFO] testing PostgreSQL inline queries
[16:40:36] [INFO] testing Microsoft SQL Server/Oracle inline queries
[16:40:38] [INFO] testing PostgreSQL = 0.1 stacked queries (comment)
[16:40:44] [INFO] testing Microsoft SQL Server/Oracle stacked queries (comment)
[16:40:51] [INFO] testing Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)
[16:40:58] [INFO] testing MySQL = 5.0.10 AND time-based blind
[16:50:09] [INFO] testing PostgreSQL = 0.1 AND time-based blind
[16:50:12] [INFO] testing Microsoft SQL Server/Oracle time-based blind (IF)
[16:50:25] [INFO] testing Oracle AND time-based blind
[16:50:36] [INFO] testing Oracle (XMLQuery, XMLError) - 1 to 10 columns
[16:50:36] [WARNING] using unoptimized version of the test because of zero knowledge of the back-end DBMS. You can try to explicitly set it with option '--dbms'
[16:50:52] [INFO] target URL appears to be UNION injectable with 8 columns
[16:50:53] [WARNING] applying generic concatenation (CONCAT)
[16:50:53] [WARNING] UNION-based SQL injection not detected. Do you want to try with a random integer value for option '--union-c
[16:52:30] [INFO] y
[16:52:30] [WARNING] if UNION-based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. --dbms=mysql)
```



# Herramientas

## Uso de SQLMAP

Encontrando  
el siguiente error, lo que implica que  
no se logró hacer ninguna inyección  
exitosa dentro de la aplicación.

```
Injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-  
char'? [Y/n] y  
[16:54:28] [WARNING] If UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.  
g. --ms=MySQL)  
[16:54:28] [WARNING] URI parameter '#1' does not seem to be injectable  
[16:54:28] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' value  
to perform more tests. Also, you can try to rerun by providing either a valid value for option '--string' (or  
"--rparam"). If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could  
retry with an option "--tamper" (e.g. "--tamper=space2comment")  
[*] shutting down at 16:54:28
```

# Herramientas

## Uso de NMAP

Tras utilizar el comando:

`nmap -O www.instagram.com`

Obteniendo los puertos  
abiertos dentro de la aplicación:

- Puerto 80/tcp
- Puerto 443/tcp

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-25 16:58 (EST)
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.9% done; ETC: 17:00 (0:01:16 remaining)
Nmap scan report for www.instagram.com (157.240.14.63)
Host is up (0.044s latency).
Other addresses for www.instagram.com (not scanned): 2a03:2080:f22c:1c4:face:b00c:0:43fe
rDNS record for 157.240.14.63: instagram-p3-shv-02-mia3.fcdn.net
Not shown: 995 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  tcpwrapped
443/tcp   open  tcpwrapped
|_ http-title: Instagram
|_ ssl-cert: Subject: commonName=*.instagram.com/organizationName=Facebook, Inc./stateOrProvinceName=California/countryName=US
|_ Subject Alternative Name: DNS:*.instagram.com, DNS:*.cdninstagram.com, DNS:*.igcdn.com, DNS:*.igsonar.com, DNS:cdninstagram.com, DNS:igcdn.com, DNS:igsonar.com, DNS:instagram.com
|_ Not valid before: 2016-12-18T00:00:00
|_ Not valid after: 2018-01-25T12:00:00
1728/tcp  open  tcpwrapped
2222/tcp  closed xmpo-client
Service type: general-purpose/bridge/VoIP phone
Running (JUST GUESSING): Linux 3.0.X(2.0.X (89%)), Oracle Virtualbox (86%), Cisco embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:1.0.9 cpe:/o:oracle:virtualbox cpe:/o:linux:linux_kernel:2.0.33 cpe:/h:cisco:inf-ig-phon-7912
Aggressive OS guesses: Linux 3.0.9 (89%), Oracle Virtualbox (86%), Linux 2.0.33 (85%), Cisco IP Phone 7912-seri
6 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  3.68 ms  10.0.2.2
2  3.77 ms  instagram-p3-shv-02-mia3.fcdn.net (157.240.14.63)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.23 seconds
```

# Herramientas

## Uso de Wireshark

Mediante el uso de wireshark, se realizan análisis de los paquetes captados en conjunto con la aplicación, de las cuales no se logra encontrar paquetes expuestos.

