

# Inseguridad en Smartphone Apps



**Simón Roses Femerling**

Fundador y CEO de Vulnex

**EL ABARATAMIENTO DE los smartphones** -potentes ordenadores de bolsillo permanentemente conectados a Internet- ha disparado el consumo de Apps entre los usuarios. IDC predice que en 2015 se venderán 982 millones de estos dispositivos y Morgan Stanley estima que en 2012 se venderán más *smartphones* que PC en todo el mundo.

Con este gran mercado potencial miles de desarrolladores, desde programadores en solitario hasta conocidas casas de desarrollo, se han lanzado a la publicación de aplicaciones móviles. Por ejemplo, en Google Play -antiguamente Google Market-, sólo en United Kingdom (UK) se lanzaron de media 701 Apps diarios durante todo 2011.

Desarrollar y publicar Apps en cualquiera de las tres plataformas líderes (iPhone, Android y Windows Phone 7) es muy sencillo y rápido y, por ello, todos estos programadores se centran en lanzar nuevas aplicaciones o actualizaciones de anteriores de forma constante, con el fin de obtener cuota de mercado y, por supuesto, ganar dinero. De hecho, medios especializados hablan de que la Web ha muerto y que hoy únicamente importa tener una buena App.

En la Figura 1 podemos apreciar la cantidad de Apps que tienen las tres plataformas principales. En cuanto a

número de descargas, en febrero de 2011 ascendió a 18 billones de Apps en iPhone y en diciembre 2011 se alcanzaban los 10 billones de Apps en Android.

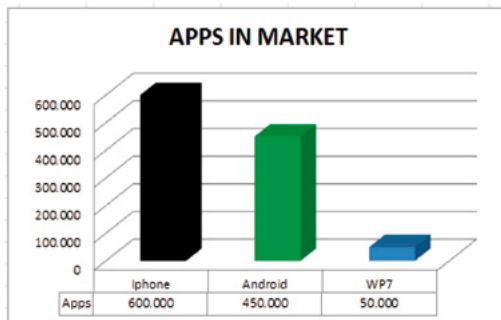


Figura 1. Número de Apps disponibles en sus respectivos mercados.

Por desgracia, en esta frenética actividad se tiende a sacrificar seguridad y privacidad: demasiadas de estas Apps, con millones de usuarios, son inseguras, llegando a comprometer la seguridad del dispositivo y los datos del propio usuario.

Desde Vulnex, empresa española altamente especializada en ciberseguridad, se han analizado más de 100 top Apps de iPhone y Android con el objetivo de determinar su postura de Seguridad, y cuyos resultados se resumen en este artículo. El lector podrá encontrar más información sobre la investigación en la web de la compañía ([www.vulnex.com](http://www.vulnex.com)).

### Mapa de vulnerabilidades en Apps

En el estudio citado, realizado en más de 100 top Apps, se identificaron diversas clases de vulnerabilidades, siendo algunas de éstas clasificadas graves, como por ejemplo, contraseñas en texto claro o canales inseguros.

Muchas de estas vulnerabilidades son ampliamente conocidas en las aplicaciones web y existe mucha literatura sobre cómo mitigarlas, por lo que no se entiende que se vuelvan a cometer los mismos errores en aplicaciones para *smartphones*.

En la Figura 2, se expone un mapa de las clases de vulnerabilidades identificadas en Apps. A pesar de que el título hace referencia a Android, también aplica a iPhone.

Algunas de estas vulnerabilidades son graves si tenemos en cuenta que, entre las Apps analizadas, se encuentran varias relacionadas con banca *online*, seguridad y comunicaciones. Y es que no podemos olvidar que los *smartphones* almacenan gran cantidad de información sensible e identificable de un usuario, que un atacante

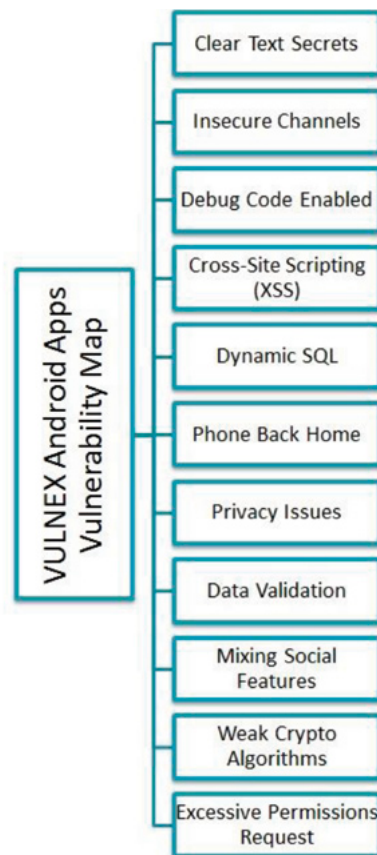


Figura 2. Clases de vulnerabilidades en aplicaciones móviles.

Figura 3. Contraseña en texto claro.

```

C:\Users\conde\Downloads\android-sdk_r07-windows\android-sdk-windows\tools>adb s
hell
# cd /data/data/nartinicreations.passmanlite/
cd /data/data/nartinicreations.passmanlite/
# ls
ls
lib
databases
shared_prefs
# cd shared_prefs
cd shared_prefs
# ls
ls
Passman_prefs.xml
# cat Passman_prefs.xml
cat Passman_prefs.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <int name="CountDownValue" value="45" />
  <int name="PasswordLength" value="10" />
  <boolean name="EncryptDb" value="true" />
  <boolean name="AutoDestruction" value="false" />
  <boolean name="ListView" value="true" />
  <boolean name="ReadablePassword" value="true" />
  <int name="Order" value="0" />
  <boolean name="OnlyNumberPassword" value="false" />
  <boolean name="CountDown" value="true" />
  <boolean name="SecurePassword" value="false" />
  <boolean name="Inactivity" value="true" />
  <boolean name="startUpPassword" value="true" />
  <string name="Password">2222</string>
  <boolean name="InactivityTimeout" value="true" />
  <int name="InactivityValue" value="150" />
</map>
#
    
```

podría conseguir. Es mayor la preocupación cuando vemos que estos dispositivos, *smartphones* y tabletas, se están introduciendo rápidamente en el entorno corporativo y podrían ser utilizados como vector de ataque comprometiendo la seguridad de la organización.

En el análisis hemos encontrado vulnerabilidades ampliamente conocidas como contraseñas sin codificar, envío de información en texto claro sin ningún tipo de protección, *Cross-Site Scripting* (XSS) e inyección de SQL.

Otras vulnerabilidades hacen referencia a la capacidad que tienen las aplicaciones de recoger información del dispositivo (como lista de contactos, *bookmarks*, información de sistema operativo y *hardware*) y enviarla a un servidor remoto. Llama la atención la integración de redes sociales en Apps de banca *online*.

Es recomendable que los desarrolladores de este tipo de aplicaciones no abusen de la solicitud de permisos para su App, ya que podría provocar que los usuarios acepten sin revisar si los permisos son apropiados para la App en cuestión. Esto es importante ya que algunos permisos tienen un impacto económico.

En la Figura 3 tenemos un App de seguridad, CVE-2011-1840, que cifraba la contraseña maestra en texto claro y la almacenaba en un fichero XML de configuración. El desarrollador no protegió adecuadamente la contraseña porque confiaba en la seguridad de la plataforma, grave error. Un atacante o *malware* podría acceder a la contraseña almacenada en el dispositivo.

Sin duda, esta clase de vulnerabilidades puede ser grave y se han identificado algunas aplicaciones afectadas.

Otro ejemplo de vulnerabilidad es la capacidad de inyectar código malicioso mediante un ataque de MITM y que se ejecute en la App. En la Figura 4 se puede ver una demostración de una conocida App, con millones de usuarios, víctima de un ataque de *Cross-Site Scripting* (XSS).

Muchos usuarios utilizan sus dispositivos en lugares públicos como cafés, hoteles y aeropuertos y por eso este tipo de ataques pueden ser muy peligrosos.

El último ejemplo (ver Figura 5) es una conocida App para reproducir vídeos que tiene servidores web, Samba y FTP incluidos para subir ficheros directamente al dispositivo. Por desgracia, la aplicación no hace una correcta validación de datos, y un atacante puede enviar una sentencia maliciosa provocando un error en la App.

Este tipo de errores puede comprometer de forma muy grave la seguridad del dispositivo permitiendo a un atacante ejecutar código malicioso, lo que combinado con otras clases de vulnerabilidades -por ejemplo, de plataforma- podría ser devastador.

### Conclusiones

A lo largo de este artículo hemos expuesto algunas clases de vulnerabilidades que afectan a aplicaciones que utilizan con millones de personas, lo que supone un asunto muy serio sobre seguridad y privacidad de las Apps.

```

2012-03-01 22:14:54.742 431:3031 I
2012-03-01 22:14:54.744 431:3031 I
2012-03-01 22:14:54.746 431:3031 I
2012-03-01 22:14:54.750 431:3031 I
2012-03-01 22:14:54.752 431:3031 I
2012-03-01 22:14:54.754 431:3031 I
2012-03-01 22:14:54.756 431:3031 I
2012-03-01 22:14:54.758 431:3031 I
2012-03-01 22:14:54.760 431:3031 I
2012-03-01 22:14:54.762 431:3031 I
2012-03-01 22:14:54.764 431:3031 I
2012-03-01 22:14:54.766 431:3031 I
2012-03-01 22:14:54.768 431:3031 I
2012-03-01 22:14:54.770 431:3031 I
2012-03-01 22:14:54.772 431:3031 I
2012-03-01 22:14:54.774 431:3031 I
2012-03-01 22:14:54.776 431:3031 I
2012-03-01 22:14:54.778 431:3031 I
2012-03-01 22:14:54.780 431:3031 I
2012-03-01 22:14:54.782 431:3031 I
2012-03-01 22:14:54.784 431:3031 I
2012-03-01 22:14:54.786 431:3031 I
2012-03-01 22:14:54.788 431:3031 I
2012-03-01 22:14:54.790 431:3031 I
2012-03-01 22:14:54.792 431:3031 I
2012-03-01 22:14:54.794 431:3031 I
2012-03-01 22:14:54.796 431:3031 I
2012-03-01 22:14:54.798 431:3031 I
2012-03-01 22:14:54.800 431:3031 I
2012-03-01 22:14:54.802 431:3031 I
2012-03-01 22:14:54.804 431:3031 I
2012-03-01 22:14:54.806 431:3031 I
2012-03-01 22:14:54.808 431:3031 I
2012-03-01 22:14:54.810 431:3031 I
2012-03-01 22:14:54.812 431:3031 I
2012-03-01 22:14:54.814 431:3031 I
2012-03-01 22:14:54.816 431:3031 I
2012-03-01 22:14:54.818 431:3031 I
2012-03-01 22:14:54.820 431:3031 I
2012-03-01 22:14:54.822 431:3031 I
2012-03-01 22:14:54.824 431:3031 I
2012-03-01 22:14:54.826 431:3031 I
2012-03-01 22:14:54.828 431:3031 I
2012-03-01 22:14:54.830 431:3031 I
2012-03-01 22:14:54.832 431:3031 I
2012-03-01 22:14:54.834 431:3031 I
2012-03-01 22:14:54.836 431:3031 I
2012-03-01 22:14:54.838 431:3031 I
2012-03-01 22:14:54.840 431:3031 I
2012-03-01 22:14:54.842 431:3031 I
2012-03-01 22:14:54.844 431:3031 I
2012-03-01 22:14:54.846 431:3031 I
2012-03-01 22:14:54.848 431:3031 I
2012-03-01 22:14:54.850 431:3031 I
2012-03-01 22:14:54.852 431:3031 I
2012-03-01 22:14:54.854 431:3031 I
2012-03-01 22:14:54.856 431:3031 I
2012-03-01 22:14:54.858 431:3031 I
2012-03-01 22:14:54.860 431:3031 I
2012-03-01 22:14:54.862 431:3031 I
2012-03-01 22:14:54.864 431:3031 I
2012-03-01 22:14:54.866 431:3031 I
2012-03-01 22:14:54.868 431:3031 I
2012-03-01 22:14:54.870 431:3031 I
2012-03-01 22:14:54.872 431:3031 I
2012-03-01 22:14:54.874 431:3031 I
2012-03-01 22:14:54.876 431:3031 I
2012-03-01 22:14:54.878 431:3031 I
2012-03-01 22:14:54.880 431:3031 I
2012-03-01 22:14:54.882 431:3031 I
2012-03-01 22:14:54.884 431:3031 I
2012-03-01 22:14:54.886 431:3031 I
2012-03-01 22:14:54.888 431:3031 I
2012-03-01 22:14:54.890 431:3031 I
2012-03-01 22:14:54.892 431:3031 I
2012-03-01 22:14:54.894 431:3031 I
2012-03-01 22:14:54.896 431:3031 I
2012-03-01 22:14:54.898 431:3031 I
2012-03-01 22:14:54.900 431:3031 I
2012-03-01 22:14:54.902 431:3031 I
2012-03-01 22:14:54.904 431:3031 I
2012-03-01 22:14:54.906 431:3031 I
2012-03-01 22:14:54.908 431:3031 I
2012-03-01 22:14:54.910 431:3031 I
2012-03-01 22:14:54.912 431:3031 I
2012-03-01 22:14:54.914 431:3031 I
2012-03-01 22:14:54.916 431:3031 I
2012-03-01 22:14:54.918 431:3031 I
2012-03-01 22:14:54.920 431:3031 I
2012-03-01 22:14:54.922 431:3031 I
2012-03-01 22:14:54.924 431:3031 I
2012-03-01 22:14:54.926 431:3031 I
2012-03-01 22:14:54.928 431:3031 I
2012-03-01 22:14:54.930 431:3031 I
2012-03-01 22:14:54.932 431:3031 I
2012-03-01 22:14:54.934 431:3031 I
2012-03-01 22:14:54.936 431:3031 I
2012-03-01 22:14:54.938 431:3031 I
2012-03-01 22:14:54.940 431:3031 I
2012-03-01 22:14:54.942 431:3031 I
2012-03-01 22:14:54.944 431:3031 I
2012-03-01 22:14:54.946 431:3031 I
2012-03-01 22:14:54.948 431:3031 I
2012-03-01 22:14:54.950 431:3031 I
2012-03-01 22:14:54.952 431:3031 I
2012-03-01 22:14:54.954 431:3031 I
2012-03-01 22:14:54.956 431:3031 I
2012-03-01 22:14:54.958 431:3031 I
2012-03-01 22:14:54.960 431:3031 I
2012-03-01 22:14:54.962 431:3031 I
2012-03-01 22:14:54.964 431:3031 I
2012-03-01 22:14:54.966 431:3031 I
2012-03-01 22:14:54.968 431:3031 I
2012-03-01 22:14:54.970 431:3031 I
2012-03-01 22:14:54.972 431:3031 I
2012-03-01 22:14:54.974 431:3031 I
2012-03-01 22:14:54.976 431:3031 I
2012-03-01 22:14:54.978 431:3031 I
2012-03-01 22:14:54.980 431:3031 I
2012-03-01 22:14:54.982 431:3031 I
2012-03-01 22:14:54.984 431:3031 I
2012-03-01 22:14:54.986 431:3031 I
2012-03-01 22:14:54.988 431:3031 I
2012-03-01 22:14:54.990 431:3031 I
2012-03-01 22:14:54.992 431:3031 I
2012-03-01 22:14:54.994 431:3031 I
2012-03-01 22:14:54.996 431:3031 I
2012-03-01 22:14:54.998 431:3031 I
2012-03-01 22:14:55.000 431:3031 I
    
```

Figura 5. Atacando el servicio FTP de la App.

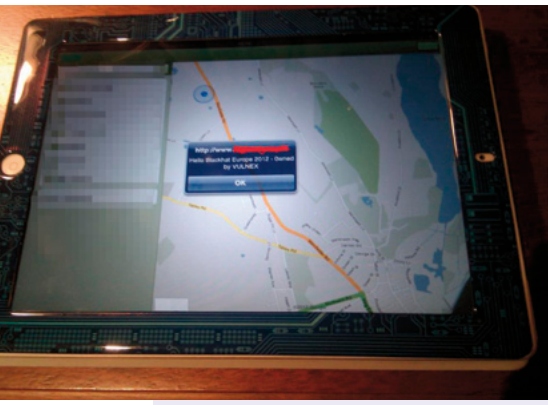


Figura 4. Ataque de Cross-Site Scripting (XSS).

Las Apps son un mercado imparable y, por ello, deberían seguir un ciclo de desarrollo seguro.

Afortunadamente existen diversos recursos como OWASP Mobile Project ([https://www.owasp.org/index.php/OWASP\\_Mobile\\_Security\\_Project](https://www.owasp.org/index.php/OWASP_Mobile_Security_Project)), así como las webs de los respectivos fabricantes con información para desarrollar Apps de forma segura. ■