Trabajo Final

Como trabajo final para aprobar el curso se entregará a los alumnos una aplicación Android. Esta aplicación contiene vulnerabilidades del tipo de las vistas en el curso. Se trata de un navegador que permite sincronizar el historial de un usuario registrado con un servidor externo. Además de la aplicación Android, van a tener los fuentes del servidor externo así lo pueden correr en sus redes utilizando python.

Se recomienda que instalen Santoku para realizar el trabajo final dado que cuenta con todas las herramientas necesarias para el mismo. De lo contrario por lo menos tendrán que instalar:

- Genymotion (o contar con un dispositivo)
- Android SDK
- Algún proxy del tipo ZAP, Burp, mitmproxy, etc.
- apktool, jadx o dex2jar y JD-GUI.

Para configurar la aplicación que utilice la IP en la cual se esté corriendo el servidor, se deberá escribir en la memoria externa (/mount/sdcard) del dispositivo bajo el archivo “server_address” con el formato IP_ADDRESS:8888.

La aplicación y el servidor pueden descargarse desde:
dc.exa.unrc.edu.ar/rio2015/cursos/android

El dispositivo Android que deberán crear para probar la aplicación será alguno con una versión 4.1.2. Si utilizan la VM provista del laboratorio ya hay un emulador creado bajo el nombre Testing. El mismo puede ser corrido utilizando el comando:

```
$ emulator @Testing -gpu on -noaudio
```

El objetivo del trabajo es que logren encontrar vulnerabilidades y clasificarlas, y encontrar la manera de explotar al menos una de ellas. Luego escribir un breve informe acerca de cuales fueron las vulnerabilidades encontradas en la aplicación. Para cada vulnerabilidad se debe incluir el vector de ataque, qué tipo de información puede ser obtenida o acción realizada. Es decir, si puede ser explotada remotamente, estando en la misma red, con una aplicación maliciosa, etc.

Se dará la siguiente taxonomía de las vulnerabilidades:

```
VULNERABILIDADES:
     |->  LOCAL
     |    |---------> DATOS MAL PROTEGIDOS
     |    |---------> COMPONENTES MAL EXPORTADOS
     |->  RED
     |    |---------> ACTIVO
     |    |---------> PASIVO
     |->  REMOTO
```

Se debe encontrar al menos una vulnerabilidad de cada uno de los tipos mencionados (una de datos mal protegidos, una de componentes mal exportados, una de red activo, etc) y por lo menos tener una prueba de concepto con un script funcionando de alguna de las vulnerabilidades encontradas del tipo LOCAL. Recomendamos que utilicen adb para ello.

El criterio de evaluación consiste en 70% de la nota en la cantidad de vulnerabilidades encontradas y 30% en la calidad del informe. Se formarán grupos de dos personas. La fecha límite de entrega del informe es el lunes 23/02/2015.

Cualquier duda, se puede consultar a los siguientes mails:
jrinaudo@fundacionsadosky.org.ar
jheguia@fundacionsadosky.org.ar