Entrega № 1 Proyecto Seguridad Informática

Definición de Aplicación a Auditar
con Listado de Entregables

Camilo Zepeda Hoffmann

Profesor Maximiliano Vega

27 de Septiembre 2017

1. Resumen

La realización de auditorías tanto de sistemas como aplicaciones es una conducta regular en áreas informáticas o de desarrollo, de las cuales se desprenden secciones completamente dedicadas al tema, incluso haciendo uso de recompensas para individuos que encuentren e informen fallas en los sistemas pertinente. Entonces el conocimiento de los posibles errores o bien aperturas dentro del sistema dan al ente (empresa, desarrollador o benefactor) la oportunidad de mitigar dichos problemas, generando medidas apropiadas y actualizaciones que en el mejor de los casos eliminen la falla o ayuden a la detección de las mismas, efectuando así, una mayor seguridad y encapsulamiento de la aplicación. Es por ésta razón que se solicita a los alumnos del curso de Seguridad Informática la búsqueda de una aplicación móvil popular que se encuentre dentro de las tiendas, disponible para sistema operativos iOs y Android. De tal manera que se tenga una comprensión de las licencias y software involucrados en la aplicación, generando así, planes de acción frente a las posibles fallas y pruebas asociadas que rectifiquen un desempeño óptimo.

2. Propuesta

Frente a la problemática descrita se escoge como aplicación popular **Instagram**, la que es descrita como una Red Social desarrollada por Kevin Systrom y Mike Krieger el año 2010 que permite compartir imágenes y vídeos, aplicando efectos fotográficos del tipo : filtros, marcos, retro, vintage, entre otros, los cuales pueden ser vistos tanto en la aplicación como en otros entornos (Facebook, Twitter, Flickr, etc). Entre los sistemas compatibles a la aplicación se destaca Android y iOs, destacando por su popularidad y uso.

Actualmente los desarrolladores designados a la empresa son Facebook, dando paso a funcionalidades similares, como lo son direct (inbox) y etiquetados de usuarios en las fotos compartidas (entre las destacadas). Ahora bien entre las licencias asociadas a la empresa se describe y nombra el siguiente listado:

1. **AFNetworking**: framework utilizado para enviar y recibir datos de un servidor desde una aplicación iOS, permitiendo la comunicación entre dispositivos del mismo sistema.

2. **Apache Thrift**: herramienta que permite la creación de servicios web, generando respuestas acorde a los valores indicados o métodos pertinentes.

3. **Appirater**: es una clase que puede ser implementada en cualquier app de iphone o Android, que ayuda en recordar a los usuarios a revisar la aplicación en la Tienda según corresponda el dispositivo.

4. **Apple Reachability**: funcion de iOS que da acceso a los usuarios al resto de las aplicaciones haciendo uso de sólo una mano o doble click sobre el Home, aplicado para dispositivos Iphone 6 y Iphone 6 plus a causa del tamaño de sus pantallas.

5. **Boost**: licencia de software libre del tipo BBSD y MIT que hace uso de bibliotecas boost, lo que implica un desarrollo de código abierto escrito en C++.

6. **CocoaLumberjack**: propiedad de biblioteca Cocoa utilizada para entornos de iOS particularmente Objective-C, swift que provee un formato y manejo ambientado al a un ambiente especifico de desarrollo.

7. **Cocoawithlove-Base64**: utilizado en plataformas Unix haciendo uso de bibliotecas criptograficas (Biblioteca OpenSSL) e integrado con tipos de datos usados en Objetive-C (como NSdata y NSString) con disponibilidad para Iphone. Realizando codificación y decodificación en base64 con OpenSSl.

8. **Curl**: software que provee bibliotecas y herramientas por líneas de comando para la transferencia d información haciendo uso diversos protocolos.

Si bien se describen algunos de los software utilizados por la aplicación existe un número superior de las mismas, de las que se nombran : Google Breakpad, Google-glog, ios5-cookbook, JSONKit, LXReorderableCollectionViewFlowLayout, MBProgressHUD, MyOpenAL-Support, NSNotifications and Background Threads, NSString+XMLEntitites, oauthconsumer, ohhttpstubs, protobuf, QSUtilities, SocketRocket, scifihifi-iphone y UICKeyChainStore. Se espera generar un informe descrito a fondo de las mismas, con tal de tener un mayor entendimiento y comprensión de las tecnologías que afectan la aplicación, complementando así, la auditoría a realizar en conjunto con los posibles ataques y pruebas a realizar.

En segundo plano y en concordancia con lo descrito, se definen los siguientes puntos a probar como objetivos de la auditoría para la aplicación Instagram.

- 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.
- Descompilar la Aplicación (si es posible).
- Analizar ataque por medio de Restauración de Contraseña haciendo uso de Proxy Web. (ataque 2016).
- Posible Des compilación del Código.

Posterior a los objetivos descritos se espera que en futuras entregas se complemente en forma más exacta cada objetivo, y relacionado a lo aprendido en el curso de Seguridad Informática de la mano con una investigación independiente de manera exhaustiva y coherente.

Referencias

[1] .ᴬFNetworking: un gran framework de comunicaciones para iPhone/iPad", Blog de Miguel Gutiérrez, 2017. [Online]. Available: https://miguelgutierrezmoreno.wordpress.com/2012/11/26/afnetworking-un-extraordinario-framework-para-iphoneipad/. [Accessed: 27- Sep- 2017] "Guía de referencia de Nmap (Página de manual)", Nmap.org, 2017. [Online]. Available: https://nmap.org/man/es/index.html. [Accessed: 24- Aug- 2017].

[2] "Peticiones a un servidor desde iOS con AFNetworking", AxiaCore, 2017. [Online]. Available: https://axiacore.com/blog/2012/08/peticiones-a-un-servidor-desde-ios-con-afnetworking/. [Accessed: 27- Sep- 2017]

[3] 2017. [Online]. Available: http://www.elconspirador.com/2015/01/20/que-es-apache-thrift-server/. [Accessed: 27- Sep- 2017]

[4] https://www.buzztouch.com/forum/thread.php?tid=B60C6EE41CD7D289048B0F4

[5] https://github.com/arashpayan/appirater

[6] https://iphoneros.com/44273/asi-es-el-modo-reachability-para-poder-utilizar-el-iphone-6-plus-con-una-sola-mano-video

[7] https://curl.haxx.se/docs/history.html