

Auditoria a aplicacion de Smartphone



Esteban Motyvay

Septiembre 27, 2017

Universidad Finis Terrae

Tabla de contenidos

- 1 Introducción
- 2 Aplicación escogida
- 3 Marco Teorico
- 4 Plan de Accion
- 5 Descompilacion
- 6 Pasos a seguir
- 7 Pruebas

Introducción

En el presente proyecto se realizara una auditoría de una aplicación Mobile, donde se deberá realizar una investigación de sus tipos de vulnerabilidades que se encuentran dentro de sus códigos, para luego realizar ataques éticos para ver que tan vulnerables es esta. Luego de haber documentado esta auditoría a la aplicación, se deberá reportar estos riesgos a la empresa que se le realizo la auditoría. Para que esta entidad pueda mitigar estos problemas de encontrados.

Introducción

En el presente proyecto se realizara una auditoría de una aplicación Mobile, donde se deberá realizar una investigación de sus tipos de vulnerabilidades que se encuentran dentro de sus códigos, para luego realizar ataques éticos para ver que tan vulnerables es esta. Luego de haber documentado esta auditoría a la aplicación, se deberá reportar estos riesgos a la empresa que se le realizo la auditoría. Para que esta entidad pueda mitigar estos problemas de encontrados.

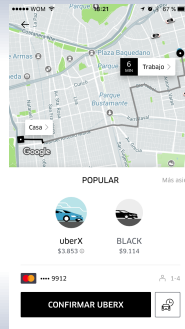
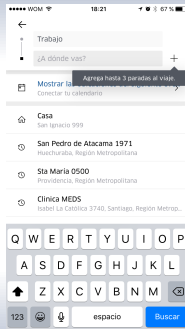
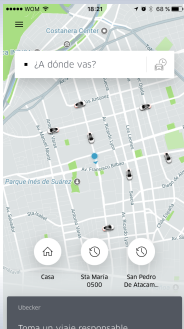
UBER

Uber es una compañía norteamericana que está transformando la manera en que las personas se mueven en las ciudades. Contactándose a través de una aplicación, de manera simple, a conductores con usuarios que requieren un servicio de traslado.



U B E R

Uso de aplicacion



Objetivos

Objetivo General

- Se deberá realizar una auditoria de seguridad haciendo distintos tipos de ataques éticos a la aplicación Uber, para detectar sus problemas y reportarlos.

Objetivos específicos

- Estudiar aplicación escogida
- Buscar puntos de vulnerabilidad
- Estudiar metodos de ataques a utilizar

Marco teorico

Tshark Es una herramienta multiplataforma con interfaz grafica para el analisis de red, producto de la evolución de Ethereum. Incluye la herramienta Tshark en modo consola para capturas, analisis de red, entre otras posibilidades.

GitHub Es una plataforma de desarrollo colaborativo para alojar proyectos utilizando el sistema de control de versiones Git. Utilizando el framework Ruby on rails por GitHub. El codigo se almacena de forma publica, aunque existe la opcion de almacenarlo de forma privada, pero para esto se debe crear una cuenta de pago.

Plan de Accion

Tshark Es una herramienta multiplataforma con interfaz grafica para el analisis de red, producto de la evolución de Ethereum. Incluye la herramienta Tshark en modo consola para capturas, analisis de red, entre otras posibilidades.

GitHub Es una plataforma de desarrollo colaborativo para alojar proyectos utilizando el sistema de control de versiones Git. Utilizando el framework Ruby on rails por GitHub. El codigo se almacena de forma publica, aunque existe la opcion de almacenarlo de forma privada, pero para esto se debe crear una cuenta de pago.

Plan de accion

Que es un plan de accion?

- Un plan de acción es una herramienta de planificación de gestión y control de tareas en un proyecto. Este se basa en objetivos planteados que van a ir de manera incremental por cada entrega que se realiza. El plan de acción sirve para coordinar y comprender En el presente trabajo el plan de de acción a seguir van a ser varios métodos de acción a realizar, donde a la aplicación se le realizara:

Actividades

- Modificar código fuente de apps en Smartphone
- Simulación de pago / Braintree
- Ataque de DDoS
- Inyección SQL mediante leveldb

Descompilacion

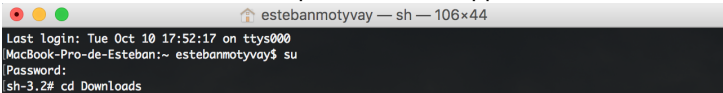
Para realizar la descompilacion de la APK y análisis de Uber, se debió realizar la instalación y actualización de algunos programas:

Programas:

- Java SDK y JRE
- Android SDK
- Apktool
- uber.apk

Paso a Paso

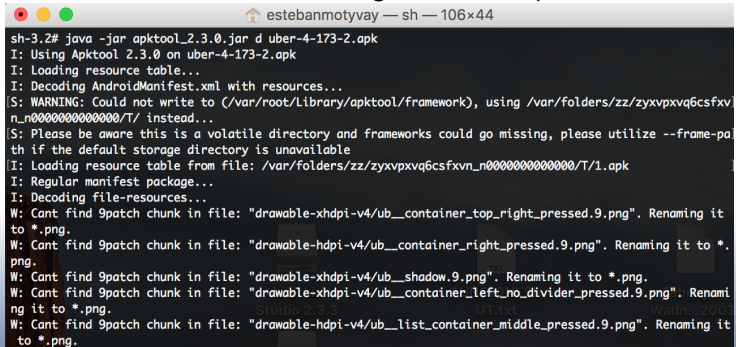
Luego de haber instalado todos los programas necesarios, se debe abrir la terminal, donde se debe iniciar el Super Usuario (su) y se debera ingresar la Pw correspondiente al super usuario. Luego se inicia todo el proceso de descompilacion de la Apps.



```
estebanmotyvay — sh — 106x44
Last login: Tue Oct 10 17:52:17 on ttys000
MacBook-Pro-de-Esteban:~ estebanmotyvay$ su
Password:
sh-3.2# cd Downloads
```

Paso a Paso

Luego de haber ejecutado el super usuario, se ejecuta la aplicacion Apktool.jar, este se busca por terminal y este se encuentra en descarga. Para poder ejecutarlo se ingresa el comando `java -jar d nombredelaapk.apk`. La d del comando significa descompilar.

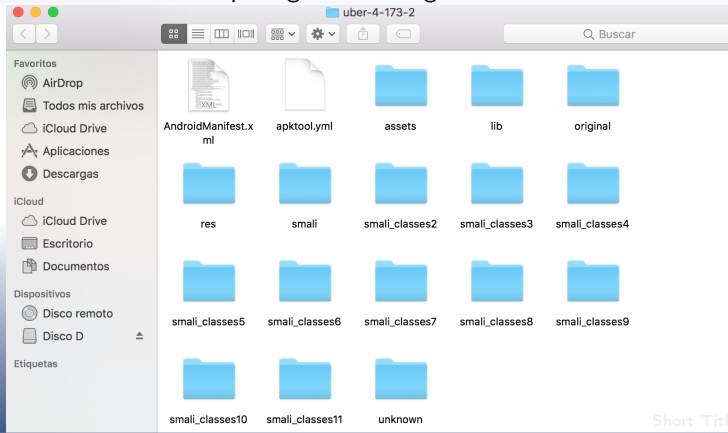


```

sh-3.2# java -jar apktool_2.3.0.jar d uber-4-173-2.apk
I: Using Apktool 2.3.0 on uber-4-173-2.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
[S: WARNING: Could not write to (/var/root/Library/apktool/framework), using /var/folders/zz/zyxvpxvq6csfxv
n_n0000000000000/T/ instead...
[S: Please be aware this is a volatile directory and frameworks could go missing, please utilize --frame-pa
th if the default storage directory is unavailable
[I: Loading resource table from file: /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/1.apk
I: Regular manifest package...
I: Decoding file-resources...
W: Cant find 9patch chunk in file: "drawable-xhdpi-v4/ub__container_top_right_pressed.9.png". Renaming it
to *.png.
W: Cant find 9patch chunk in file: "drawable-hdpi-v4/ub__container_right_pressed.9.png". Renaming it to *.
png.
W: Cant find 9patch chunk in file: "drawable-xhdpi-v4/ub__shadow.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "drawable-xhdpi-v4/ub__container_left_no_divider_pressed.9.png". Renami
ng it to *.png.
W: Cant find 9patch chunk in file: "drawable-hdpi-v4/ub__list_container_middle_pressed.9.png". Renaming it
to *.png.
  
```

Paso a Paso

Luego de descompilar la aplicación, este genera los archivos de la aplicación donde se encontrara el .XML que sera donde estara el código de la aplicación y otros archivos complementarios para la aplicación. La aplicación al descompilar genero los siguientes archivos:




Paso a Paso


Utilizando la aplicación Android Studio, se detecto que esta utilizaba el método de encriptacion de SHA1 y DSA


```
<!-- Signature Algorithms -->  
<Algorithm URI="http://www.w3.org/2000/09/xmlsig#dsa-sha1"  
  Description="Digital Signature Algorithm with SHA-1 message digest"  
  AlgorithmClass="Signature"  
  RequirementLevel="REQUIRED"  
  JCEName="SHA1withDSA"/>
```



BIN falso


Se realiza la generación de un bin falso dentro de una pagina web. En esto se realiza una investigación de los primeros 4 dígitos del bin que coincidan con un Banco y los siguientes 2 números con las sucursales.



The Kings CCGEN
Generador de Tarjetas de Credito
CCV2 CCV1 CCV0 CCV3


 BIN



 Incluir


Fechas
 
 CCV
 
 Banco



 Cantidad


 Formato

CHECKER


 CCV2


 Mes


 Año

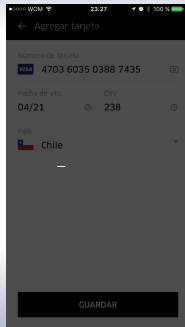
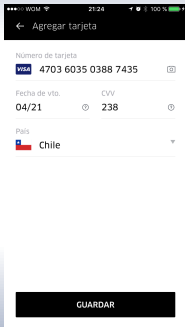
```

4703603503887435104120211238
4703607546600366104120221120
4703605842747758112120201576
470360482226727102120231537
4703602347072311106120231508
4703604246830666109120221864
4703607842016317102120211658
4703608782207361104120211510
4703601316178034110120211688
4703606651573301107120201924

```


Ingresando bin

Se realiza la prueba de ingresar el Bin generado a la plataforma de Uber.



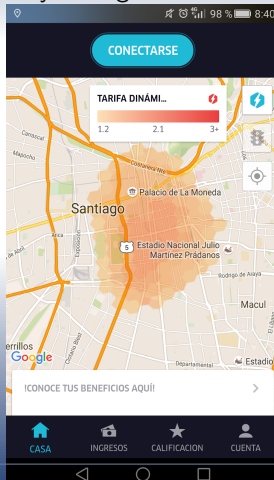
Ubicación actual

En Uber existe la aplicación Uber Drive que es la aplicación de los choferes de uber, esta trabaja con un mapa, donde este dice el lugar donde se encuentran mas demanda y a la vez si se encuentra con tarifa dinamica. Se realizo la instalacion de Cydia al equipo iphone y se instalo un FakeGps para modificar la ubicación actual del telefono.



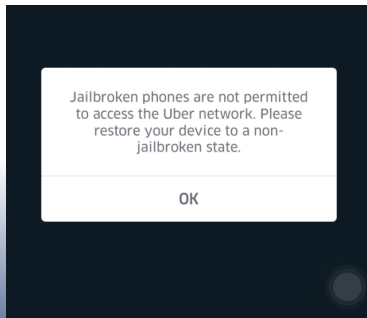
Ubicación Actual

Se realiza la generación de un bin falso dentro de una plataforma web. En esto se realiza una investigación de los primeros 4 dígitos del bin que coincidan con un Banco y los siguientes 2 números con las sucursal.



Resultado Ubicación actual

Luego de ciertos problemas que esta tuvo con sus conductores que realizaban esa actividad para generar mas ingresos. La empresa decidió en que en su aplicación no pueda ser ejecutada si es que el equipo móvil se encontraba alterado, esto transformo a Uber en una de las aplicaciones mas seguras que se encuentran en el mercado.



Análisis de puertos

Se realiza un análisis de puertos a Uber, donde para esto se reviso AndroidManifest.xml buscando la direccion hacia el servidor de la aplicacion Uber.

```
<action android:name="android.intent.action.VIEW"/>
<category android:name="android.intent.category.DEFAULT"/>
<category android:name="android.intent.category.BROWSABLE"/>
<data android:host="m.uber.com" android:pathPrefix="/ul/" android:scheme="http"/>
<data android:host="m.uber.com" android:pathPrefix="/ul/" android:scheme="https"/>
```

NMAP

Una vez obtenido la dirección del servidor de Uber, se le realiza un análisis de puerto.

```
Nmap scan report for m.uber.com (104.36.194.160)
Host is up (0.24s latency).
Other addresses for m.uber.com (not scanned): 104.36.194.232 104.36.194.134 104.36.194.159 104.36.194.190 1
04.36.194.234 104.36.194.231 104.36.194.191
Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
```

Vulnerabilidad de Puertos

Puerto 21 - ftp: Buffer Overflow Denegacion de Servicio (DoS) Ataque de Fuerza Bruta Punto de Acceso

Puerto 80 http: Ataque CGI Buffer Oveflow Denegación de Servicio (DoS) Recogida de Información Punto de Acceso Posibilidad de sniffer.