

INFORME DE PRUEBAS OFENSIVAS APP SIMA

Jorge Erick Cedillo

Offensive Security Experts

Febrero 10, 2022

Definiciones

Metodología de las pruebas

Mobile Application Security Verification Standard (MASVS)

El MASVS define dos niveles de verificación de seguridad (MASVS-L1 y MASVS-L2), así como un conjunto de requisitos de resistencia a la ingeniería inversa (MASVS-R). El nivel MASVS-L1 contiene requerimientos genéricos de seguridad recomendados para todas las aplicaciones móviles, mientras que MASVS-L2 debería aplicarse a aplicaciones que manejan datos altamente sensibles. MASVS-R cubre los controles de seguridad adicionales que se pueden aplicar si la prevención de las amenazas del lado del cliente es un objetivo de diseño.

El cumplimiento de los requerimientos de MASVS-L1 dará como resultado una aplicación segura que sigue las mejores prácticas de seguridad y no sufre de las vulnerabilidades más comunes. MASVS-L2 añade controles adicionales de defensa en profundidad, tales como SSL certificate pinning, haciendo la aplicación resistente a ataques más sofisticados, siempre y cuando los controles de seguridad del sistema operativo móvil estén intactos y que el usuario final no sea considerado como un potencial adversario. El cumplimiento de todos o de un subconjunto de los requerimientos de protección de software del nivel MASVS-R ayuda a prevenir amenazas específicas del lado del cliente cuando el usuario final es considerado malicioso y/o el sistema operativo móvil ha sido comprometido.



Alcance

Objetos evaluados y escenario de pruebas



2021-12-22

Se realizan pruebas ofensivas autenticadas (usuario valido) sobre la APP SIMA.

Resultados

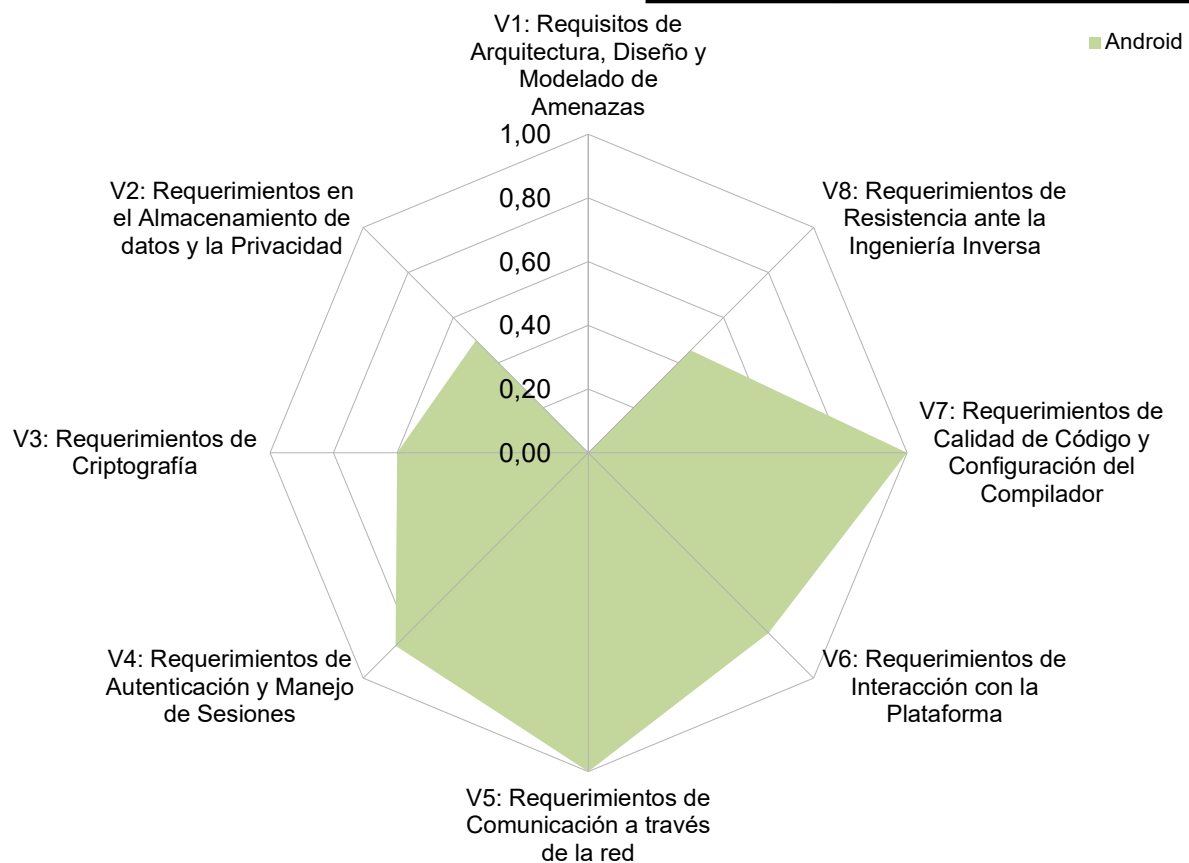
Resumen Ejecutivo

Resumen de resultados

Cumplimiento Estándar MASVS (/ 5)

3

MASVS Compliance Diagram - Android



	Android			
	P	F	NA	%
V1: Requisitos de Arquitectura, Diseño y Modelado de Amenazas	0	1	9	0,00%
V2: Requerimientos en el Almacenamiento de datos y la Privacidad	5	5	2	50,00%
V3: Requerimientos de Criptografía	3	2	1	60,00%
V4: Requerimientos de Autenticación y Manejo de Sesiones	6	1	4	85,71%
V5: Requerimientos de Comunicación a través de la red	6	0	0	100,00%
V6: Requerimientos de Interacción con la Plataforma	4	1	3	80,00%
V7: Requerimientos de Calidad de Código y Configuración del Compilador	6	0	3	100,00%
V8: Requerimientos de Resistencia ante la Ingeniería Inversa	5	6	1	45,45%

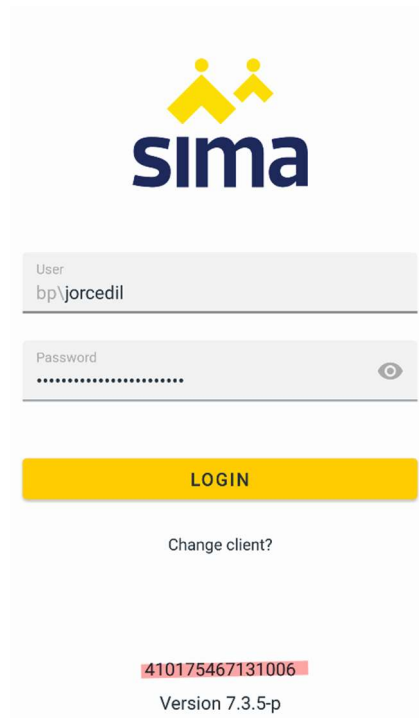
Símbolo	Definición
Pass	Requerimiento es aplicable a la Aplicación y se ha implementado de acuerdo con a las buenas prácticas
Fail	El requisito se aplicó a la aplicación, pero no ha sido satisfactorio.
N/A	El requisito no es aplicable a la aplicación móvil

Detalle Técnico

Evidencias

V1: Requisitos de Arquitectura, Diseño y Modelado de Amenazas

Se comprueba que la aplicación utiliza un control de seguridad IMEI a nivel de cliente, que se auto genera de por cada dispositivo móvil.



The login screen features the SIMA logo at the top, which consists of a yellow icon of two stylized figures above the word "sima" in blue. Below the logo are two input fields: "User" with the text "bp\jorcedil" and "Password" with masked characters. A yellow "LOGIN" button is positioned below the password field. Underneath the button is a link that says "Change client?". At the bottom of the screen, the IMEI number "410175467131006" is displayed in red, followed by the text "Version 7.3.5-p".



The home screen displays the SIMA logo at the top. Below the logo is a dark grey circular icon containing a white silhouette of a person. Underneath this icon, the text "Hello, jorcedil" is shown, followed by the IMEI number "373705350213704" in red. A button with a download icon and the text "EXPORT" is located below the IMEI number. At the very bottom of the screen, there is a link that says "Login with another account".

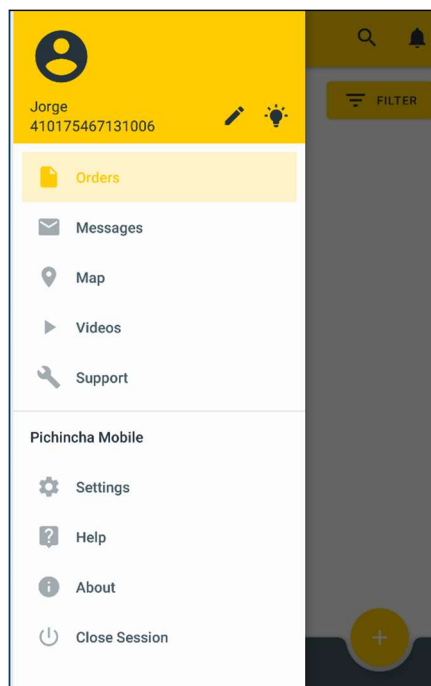
V2: Requerimientos en el Almacenamiento de datos y la Privacidad

Se detecta en la aplicación credenciales de acceso a APIs, que pueden ser usadas para poder acceder a los servicios que utiliza la aplicación como GoogleMaps, Zendesk.

🔑 POSSIBLE HARDCODED SECRETS

```
"api_key_zendesk_domain": "https://formiik.zendesk.com"
"api_key_zendesk_domain_no_http": "formiik.zendesk.com"
"api_key_zendesk_key": "fd5f7b032eb1c2d20e4105d26a2d70b3b34371d2f2972a5e"
"api_key_zendesk_sdk_key": "mobile_sdk_client_99b3955500ece315c7f7"
"direct_access_key": "6sjhedeGVK4/oAsQ/o1w1Rc5F2wAWkklmeyhvrmqj8pT9V8U5kWZK+uVAHkwNjbD01E6GPw9GQzMFQIUf/q1+w=="
"firebase_database_url": "https://formiik-android.firebaseio.com"
"google_api_key": "AlzaSyB0B_TbtqlgohXr_Jter3tJouygm-91Zs8"
"google_crash_reporting_api_key": "AlzaSyB0B_TbtqlgohXr_Jter3tJouygm-91Zs8"
"google_maps_android_api_key": "AlzaSyBZlrZEbueH6FvVq6N4LOUpdgB14Zjtwh"
"google_maps_key": "AlzaSyAgP2V1h0LSHlrPBfGeRBZ29x3BCk3Gc"
"google_maps_static_api_key": "AlzaSyASEJHXzviMYy9zc7F3ZaKyOjmnLYM5KjQ"
"google_maps_static_private_key_signature": "2T_4N6_qaKSnoq78jeOGokIvwqg="
"library_android_database_sqlcipher_authorWebsite": "https://www.zetetic.net/sqlcipher/"
"login_user": "Usuario"
"oauth": "Autenticaci3n"
"username": "Usuario"
"maps_API_OUTDATED_WARNING": "このアプリは古いバージョンのマップを使用しているため、正常に動作しない可能性があります。"
"mdtp_deleted_key": "%1$sを削除しました"
"direct_access_key": "6sjhedeGVK4/oAsQ/o1w1Rc5F2wAWkklmeyhvrmqj8pT9V8U5kWZK+uVAHkwNjbD01E6GPw9GQzMFQIUf/q1+w=="
"login_user": "User"
"oauth": "Auth"
"username": "User:"
"maps_API_OUTDATED_WARNING": "ငွေခံပေးနိုင်သောစီးထိရဲနဲ့ဘေးအန္တရာယ်ကင်းရှင်းတဲ့မြေပုံဆွဲယူတာလို့ပြောနေပါတယ်။"
"maps_API_OUTDATED_WARNING": "這個應用程式使用舊版的「地圖」，可能無法正常運作。"
```

La aplicación mantiene los datos activos y la sesión iniciada aun pasado a segundo plano.



V3: Requerimientos de Criptografía

Se detecta que la aplicación usa algoritmos de hash débil(md5) de 128 bits a nivel de librerías

```
01-31 10:47:40.208 11381 12903 D OkHttp : --> POST https://app.formiik.com:3034/SecurityPipeRest.svc/Login
01-31 10:47:40.208 11381 12903 D OkHttp : Content-Type: application/json
01-31 10:47:40.208 11381 12903 D OkHttp : Content-Length: 523
01-31 10:47:40.208 11381 12903 D OkHttp : Accept: text/json
01-31 10:47:40.208 11381 12903 D OkHttp : {"localDateTime": "2022-01-31 10:47:40", "password": "lXUN3-3et7i2-r7XNj3p-Mq_H4XpHePiPoZrI0mwo", "operatingSystemVersion": "11", "deviceModel": "sdk_gphone_x86", "pushDeviceId": "d12M2V0026r_kWTF9rP5v:APA91bGagKASfzPITV9yYR7kcuPvmaQ1kMU2HD3zps_sF5zW0jD8lwkMH8BVvHC6v10CT0lRtKFRdeUHuS20X3HtH0cWQ-nc0qly3VigAN7V3fA0UtpxPafsmU7xxx4a619", "pushDeviceType": "0.0", "deviceManufacturer": "Google", "operatingSystem": "Android", "version": "7.3.5-p", "username": "bp\\jorcedil", "deviceSerialNumber": "3373705350213704", "pushType": "FCM_v1"}
01-31 10:47:40.208 11381 12903 D OkHttp : --> END POST (523-byte body)
01-31 10:47:40.217 218 221 E android.system.suspend@1.0-service: Error opening kernel wakelock stats for: wakeup34: Permission denied
01-31 10:47:40.217 218 218 W Binder:218_2: type=1400 audit(0.0:618): avc: denied { read } for name="wakeup34" dev="sysfs" ino=18720 scontext=u:r:system_suspend:s0 tcontext=u:object_r:sysfs:s0 tclass=dir perm=ssive=0
01-31 10:47:40.220 218 221 E android.system.suspend@1.0-service: Error opening kernel wakelock stats for: wakeup35: Permission denied
01-31 10:47:40.217 218 218 W Binder:218_2: type=1400 audit(0.0:619): avc: denied { read } for name="wakeup35" dev="sysfs" ino=18783 scontext=u:r:system_suspend:s0 tcontext=u:object_r:sysfs:s0 tclass=dir perm=ssive=0
01-31 10:47:40.338 518 669 I system_server: oneway function results will be dropped but finished with status OK and parcel size 4
01-31 10:47:42.014 11381 12903 D OkHttp : <- 401 https://app.formiik.com:3034/SecurityPipeRest.svc/Login (1800ms)
01-31 10:47:42.014 11381 12903 D OkHttp : cache-control: no-cache; no-store; max-age=0
01-31 10:47:42.014 11381 12903 D OkHttp : content-type: application/json; charset=utf-8
01-31 10:47:42.014 11381 12903 D OkHttp : formikerrordescription: bp:Codigo: 4| Mensaje: Existe un inconveniente para ejecutar tu transacción. Por favor intenta más tarde. NO EXISTE EL IMEI ASIGNADO A UN USUARIO. Restan 2 intentos.
01-31 10:47:42.014 11381 12903 D OkHttp : request-context: appId=crId-v1:9c82b60c-b76c-4a09-ac7c-950892154369
01-31 10:47:42.014 11381 12903 D OkHttp : access-control-expose-headers: Request-Context
01-31 10:47:42.014 11381 12903 D OkHttp : x-frame-options: SAMEORIGIN
01-31 10:47:42.014 11381 12903 D OkHttp : x-xss-protection: 1; mode=block
01-31 10:47:42.014 11381 12903 D OkHttp : x-content-type-options: nosniff
01-31 10:47:42.014 11381 12903 D OkHttp : strict-transport-security: Strict-Transport-Security
01-31 10:47:42.014 11381 12903 D OkHttp : date: Mon, 31 Jan 2022 15:47:26 GMT
01-31 10:47:42.015 11381 12903 D OkHttp : content-length: 268
01-31 10:47:42.015 11381 12903 D OkHttp : {"Message": "bp:Codigo: 4| Mensaje: Existe un inconveniente para ejecutar tu transacción. Por favor intenta más tarde. NO EXISTE EL IMEI ASIGNADO A UN USUARIO. Restan 2 intentos.", "MinutesToLockScreen": null}
01-31 10:47:42.015 11381 12903 D OkHttp : <- END HTTP (268-byte body)
```

MD5 is a weak hash known to have hash collisions.	warning	CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	l/o/a/c.java l/a/a/d/p/b.java l/i/a/a/d0/m.java l/i/a/a/c0/b.java l/i/a/a/c0/u.java
---	---------	---	---

```
ryLevel": "100", "EventDateTime": "2022/02/03 12:36:21.419", "NetworkDat
02-03 12:51:44.375 3955 3955 D WM-SystemJobService: onStartJob for 66356d5b-4399-4f0f-b930-374485f23c34
02-03 12:51:44.376 3955 4105 D WM-Processor: Work 66356d5b-4399-4f0f-b930-374485f23c34 is already enqueued for processing
02-03 12:51:44.380 3955 5879 D OkHttp : --> POST https://app.formiik.com:3034/MiddlewareRest.svc/SetOperatorEventComplex
02-03 12:51:44.380 3955 5879 D OkHttp : Content-Type: application/json; charset=UTF-8
02-03 12:51:44.380 3955 5879 D OkHttp : Content-Length: 836
02-03 12:51:44.380 3955 5879 D OkHttp : {"DeviceInfo": "H4sIAAAAAAAAA03YS2vjMBAA4L9SFk7S0d0a3Cw7Lguh7cG3pQRTi6xpagXHyW4o/e+VC4Vethe3\\nZMMOGB1nRg8+BjL18zmpjufzJP5AabcGgYWHf0lTCwruGMLGJcaBb1NMb1MrreH7tq33e+ue1\\nt6rf+Xh29TD4/rj0B7+JU04Qg4uD74aiHnzVPo1TCBDiCuInL7iYSzMXfkb400qNH36H/jHW1rno\\ndvsn38R60S0X0qaX4aEe2tATyZvsm3ESmc6U4Ba1+JgP3fq9gHEhZmAlohxngPzGb3+F7njXh0Pb1n+D6WZF3Th7aJ2cIf2gd/U78t8zqE9cZf7JrH1Xrs4ld/rFn9bFev10RiHhERIHh9NqEASIRgzh8N\\nyomQCInuvAkNAAIRtPKkginEUYGQYITCFEzIpxEKfHsvfB/IrQlyBHdgilRIFM6T1nmnGRCQxYZ\\nlbRWE+H57ULNkZ4Z1PDUhDq1E5kIT0xoQNLVeikHqNpmIMJTE1pAIIRCIjzh7zzIoTcmbJvlpVw\\n5kyBkFlmFo4VoGUGUNgSuy81VLGLoxUzD14RoENM/QZi83L8Ckvytgj0jAAA-\\n", "SecurityToken": "KQo7AeEpwgmBrgfn80unBewzpvXUcaRfx15d_L4DeatElUfLexKQLPmw-ZsjZ0pPSLx2t1GfuQ7g0lUe-tzknjKxDPIaDk5Sho0vuvvFWUMRDRAfG8UfGjGDzSwiSxpyLe5g4W9MsANbeyR1wxjKbK6s1jGt-uWRxUC38wsCAOdpmPpSL16V1q1CW160"}
```

```

1. package l.a.o.d.p;
2.
3. import java.math.BigInteger;
4. import java.security.MessageDigest;
5. import java.security.NoSuchAlgorithmException;
6. /* compiled from: Crypto.java */
7. /* loaded from: classes5.dex */
8. public class b {
9.     public static final char[] a = "0123456789ABCDEF".toCharArray();
10.
11.     public static String a(String str) {
12.         byte[] bytes = str.getBytes("UnicodeLittleUnmarked");
13.         try {
14.             MessageDigest instance = MessageDigest.getInstance("MD5");
15.             instance.reset();
16.             instance.update(bytes);
17.             byte[] digest = instance.digest();
18.             int length = digest.length;
19.             StringBuilder sb = new StringBuilder(length << 1);
20.             for (int i = 0; i < length; i++) {
21.                 sb.append(Character.forDigit((digest[i] & 240) >> 4, 16));
22.                 sb.append(Character.forDigit(digest[i] & 15, 16));
23.             }
24.             return sb.toString();
25.         } catch (NoSuchAlgorithmException unused) {
26.             return null;
27.         }
28.     }
29.
30.     public static int b(String str) {
31.         try {
32.             byte[] digest = MessageDigest.getInstance("MD5").digest(str.getBytes());
33.             char[] cArr = new char[digest.length * 2];

```

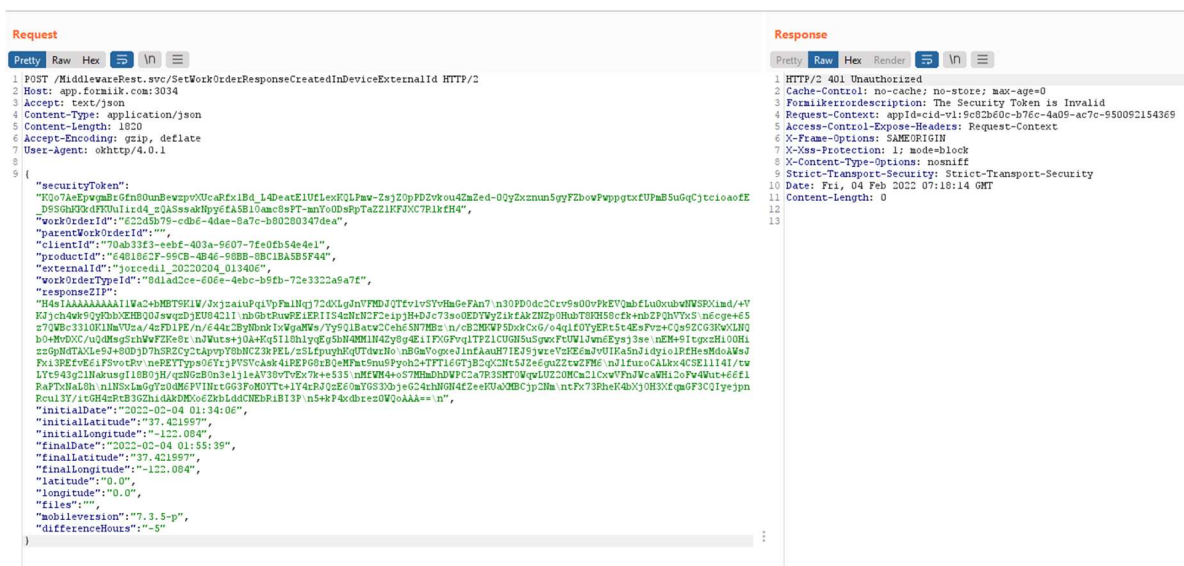
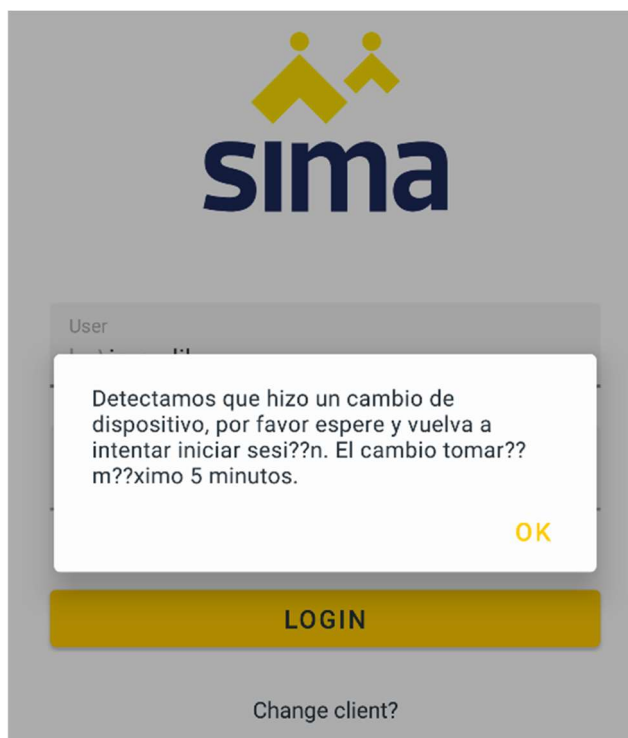
m.java

```

1. package l.i.a.o.d.b;
2.
3. import androidx.recyclerview.widget.RecyclerView;
4. import java.io.IOException;
5. import java.io.InputStream;
6. import java.io.OutputStream;
7. import java.io.UnsupportedEncodingException;
8. import java.net.URI;
9. import java.net.URLEncoder;
10. import java.net.URLDecoder;
11. import java.net.URLEncoder;
12. import java.security.MessageDigest;
13. import java.security.NoSuchAlgorithmException;
14. import java.text.SimpleDateFormat;
15. import java.util.Arrays;
16. import java.util.Date;
17. import java.util.List;
18. import java.util.Locale;
19. import java.util.TimeZone;
20. import java.util.concurrent.TimeUnit;
21. import javax.xml.parsers.SAXParserFactory;
22. import l.c.a.o.a;
23. import l.i.a.o.f;
24. import l.i.a.o.h;
25. import l.i.a.o.v;
26. import l.i.a.o.y;
27. /* compiled from: Utility.java */
28. /* loaded from: classes5.dex */
29. public final class m {
30.     public static final TimeZone a = TimeZone.getTimeZone("GMT");
31.     public static final TimeZone b = TimeZone.getTimeZone("UTC");
32.     public static final Locale c = Locale.US;
33.     public static final List<Integer> d = Arrays.asList(10000, 10001, 10002, 10003, 10004, 10005, 10006, 10007, 10008, 10009, 10010, 10011, 10012, 10013, 10014, 10015, 10016, 10017, 10018, 10019, 10020, 10021, 10022, 10023, 10024, 10025, 10026, 10027, 10028, 10029, 10030, 10031, 10032, 10033, 10034, 10035, 10036, 10037, 10038, 10039, 10040, 10041, 10042, 10043, 10044, 10045, 10046, 10047, 10048, 10049, 10050, 10051, 10052, 10053, 10054, 10055, 10056, 10057, 10058, 10059, 10060, 10061, 10062, 10063, 10064, 10065, 10066, 10067, 10068, 10069, 10070, 10071, 10072, 10073, 10074, 10075, 10076, 10077, 10078, 10079, 10080, 10081, 10082, 10083, 10084, 10085, 10086, 10087, 10088, 10089, 10090, 10091, 10092, 10093, 10094, 10095, 10096, 10097, 10098, 10099, 10100, 10101, 10102, 10103, 10104, 10105, 10106, 10107, 10108, 10109, 10110, 10111, 10112, 10113, 10114, 10115, 10116, 10117, 10118, 10119, 10120, 10121, 10122, 10123, 10124, 10125, 10126, 10127, 10128, 10129, 10130, 10131, 10132, 10133, 10134, 10135, 10136, 10137, 10138, 10139, 10140, 10141, 10142, 10143, 10144, 10145, 10146, 10147, 10148, 10149, 10150, 10151, 10152, 10153, 10154, 10155, 10156, 10157, 10158, 10159, 10160, 10161, 10162, 10163, 10164, 10165, 10166, 10167, 10168, 10169, 10170, 10171, 10172, 10173, 10174, 10175, 10176, 10177, 10178, 10179, 10180, 10181, 10182, 10183, 10184, 10185, 10186, 10187, 10188, 10189, 10190, 10191, 10192, 10193, 10194, 10195, 10196, 10197, 10198, 10199, 10200, 10201, 10202, 10203, 10204, 10205, 10206, 10207, 10208, 10209, 10210, 10211, 10212, 10213, 10214, 10215, 10216, 10217, 10218, 10219, 10220, 10221, 10222, 10223, 10224, 10225, 10226, 10227, 10228, 10229, 10230, 10231, 10232, 10233, 10234, 10235, 10236, 10237, 10238, 10239, 10240, 10241, 10242, 10243, 10244, 10245, 10246, 10247, 10248, 10249, 10250, 10251, 10252, 10253, 10254, 10255, 10256, 10257, 10258, 10259, 10260, 10261, 10262, 10263, 10264, 10265, 10266, 10267, 10268, 10269, 10270, 10271, 10272, 10273, 10274, 10275, 10276, 10277, 10278, 10279, 10280, 10281, 10282, 10283, 10284, 10285, 10286, 10287, 10288, 10289, 10290, 10291, 10292, 10293, 10294, 10295, 10296, 10297, 10298, 10299, 10300, 10301, 10302, 10303, 10304, 10305, 10306, 10307, 10308, 10309, 10310, 10311, 10312, 10313, 10314, 10315, 10316, 10317, 10318, 10319, 10320, 10321, 10322, 10323, 10324, 10325, 10326, 10327, 10328, 10329, 10330, 10331, 10332, 10333, 10334, 10335, 10336, 10337, 10338, 10339, 10340, 10341, 10342, 10343, 10344, 10345, 10346, 10347, 10348, 10349, 10350, 10351, 10352, 10353, 10354, 10355, 10356, 10357, 10358, 10359, 10360, 10361, 10362, 10363, 10364, 10365, 10366, 10367, 10368, 10369, 10370, 10371, 10372, 10373, 10374, 10375, 10376, 10377, 10378, 10379, 10380, 10381, 10382, 10383, 10384, 10385, 10386, 10387, 10388, 10389, 10390, 10391, 10392, 10393, 10394, 10395, 10396, 10397, 10398, 10399, 10400, 10401, 10402, 10403, 10404, 10405, 10406, 10407, 10408, 10409, 10410, 10411, 10412, 10413, 10414, 10415, 10416, 10417, 10418, 10419, 10420, 10421, 10422, 10423, 10424, 10425, 10426, 10427, 10428, 10429, 10430, 10431, 10432, 10433, 10434, 10435, 10436, 10437, 10438, 10439, 10440, 10441, 10442, 10443, 10444, 10445, 10446, 10447, 10448, 10449, 10450, 10451, 10452, 10453, 10454, 10455, 10456, 10457, 10458, 10459, 10460, 10461, 10462, 10463, 10464, 10465, 10466, 10467, 10468, 10469, 10470, 10471, 10472, 10473, 10474, 10475, 10476, 10477, 10478, 10479, 10480, 10481, 10482, 10483, 10484, 10485, 10486, 10487, 10488, 10489, 10490, 10491, 10492, 10493, 10494, 10495, 10496, 10497, 10498, 10499, 10500, 10501, 10502, 10503, 10504, 10505, 10506, 10507, 10508, 10509, 10510, 10511, 10512, 10513, 10514, 10515, 10516, 10517, 10518, 10519, 10520, 10521, 10522, 10523, 10524, 10525, 10526, 10527, 10528, 10529, 10530, 10531, 10532, 10533, 10534, 10535, 10536, 10537, 10538, 10539, 10540, 10541, 10542, 10543, 10544, 10545, 10546, 10547, 10548, 10549, 10550, 10551, 10552, 10553, 10554, 10555, 10556, 10557, 10558, 10559, 10560, 10561, 10562, 10563, 10564, 10565, 10566, 10567, 10568, 10569, 10570, 10571, 10572, 10573, 10574, 10575, 10576, 10577, 10578, 10579, 10580, 10581, 10582, 10583, 10584, 10585, 10586, 10587, 10588, 10589, 10590, 10591, 10592, 10593, 10594, 10595, 10596, 10597, 10598, 10599, 10600, 10601, 10602, 10603, 10604, 10605, 10606, 10607, 10608, 10609, 10610, 10611, 10612, 10613, 10614, 10615, 10616, 10617, 10618, 10619, 10620, 10621, 10622, 10623, 10624, 10625, 10626, 10627, 10628, 10629, 10630, 10631, 10632, 10633, 10634, 10635, 10636, 10637, 10638, 10639, 10640, 10641, 10642, 10643, 10644, 10645, 10646, 10647, 10648, 10649, 10650, 10651, 10652, 10653, 10654, 10655, 10656, 10657, 10658, 10659, 10660, 10661, 10662, 10663, 10664, 10665, 10666, 10667, 10668, 10669, 10670, 10671, 10672, 10673, 10674, 10675, 10676, 10677, 10678, 10679, 10680, 10681, 10682, 10683, 10684, 10685, 10686, 10687, 10688, 10689, 10690, 10691, 10692, 10693, 10694, 10695, 10696, 10697, 10698, 10699, 10700, 10701, 10702, 10703, 10704, 10705, 10706, 10707, 10708, 10709, 10710, 10711, 10712, 10713, 10714, 10715, 10716, 10717, 10718, 10719, 10720, 10721, 10722, 10723, 10724, 10725, 10726, 10727, 10728, 10729, 10730, 10731, 10732, 10733, 10734, 10735, 10736, 10737, 10738, 10739, 10740, 10741, 10742, 10743, 10744, 10745, 10746, 10747, 10748, 10749, 10750, 10751, 10752, 10753, 10754, 10755, 10756, 10757, 10758, 10759, 10760, 10761, 10762, 10763, 10764, 10765, 10766, 10767, 10768, 10769, 10770, 10771, 10772, 10773, 10774, 10775, 10776, 10777, 10778, 10779, 10780, 10781, 10782, 10783, 10784, 10785, 10786, 10787, 10788, 10789, 10790, 10791, 10792, 10793, 10794, 10795, 10796, 10797, 10798, 10799, 10800, 10801, 10802, 10803, 10804, 10805, 10806, 10807, 10808, 10809, 10810, 10811, 10812, 10813, 10814, 10815, 10816, 10817, 10818, 10819, 10820, 10821, 10822, 10823, 10824, 10825, 10826, 10827, 10828, 10829, 10830, 10831, 10832, 10833, 10834, 10835, 10836, 10837, 10838, 10839, 10840, 10841, 10842, 10843, 10844, 10845, 10846, 10847, 10848, 10849, 10850, 10851, 10852, 10853, 10854, 10855, 10856, 10857, 10858, 10859, 10860, 10861, 10862, 10863, 10864, 10865, 10866, 10867, 10868, 10869, 10870, 10871, 10872, 10873, 10874, 10875, 10876, 10877, 10878, 10879, 10880, 10881, 10882, 10883, 10884, 10885, 10886, 10887, 10888, 10889, 10890, 10891, 10892, 10893, 10894, 10895, 10896, 10897, 10898, 10899, 10900, 10901, 10902, 10903, 10904, 10905, 10906, 10907, 10908, 10909, 10910, 10911, 10912, 10913, 10914, 10915, 10916, 10917, 10918, 10919, 10920, 10921, 10922, 10923, 10924, 10925, 10926, 10927, 10928, 10929, 10930, 10931, 10932, 10933, 10934, 10935, 10936, 10937, 10938, 10939, 10940, 10941, 10942, 10943, 10944, 10945, 10946, 10947, 10948, 10949, 10950, 10951, 10952, 10953, 10954, 10955, 10956, 10957, 10958, 10959, 10960, 10961, 10962, 10963, 10964, 10965, 10966, 10967, 10968, 10969, 10970, 10971, 10972, 10973, 10974, 10975, 10976, 10977, 10978, 10979, 10980, 10981, 10982, 10983, 10984, 10985, 10986, 10987, 10988, 10989, 10990, 10991, 10992, 10993, 10994, 10995, 10996, 10997, 10998, 10999, 11000, 11001, 11002, 11003, 11004, 11005, 11006, 11007, 11008, 11009, 11010, 11011, 11012, 11013, 11014, 11015, 11016, 11017, 11018, 11019, 11020, 11021, 11022, 11023, 11024, 11025, 11026, 11027, 11028, 11029, 11030, 11031, 11032, 11033, 11034, 11035, 11036, 11037, 11038, 11039, 11040, 11041, 11042, 11043, 11044, 11045, 11046, 11047, 11048, 11049, 11050, 11051, 11052, 11053, 11054, 11055, 11056, 11057, 11058, 11059, 11060, 11061, 11062, 11063, 11064, 11065, 11066, 11067, 11068, 11069, 11070, 11071, 11072, 11073, 11074, 11075, 11076, 11077, 11078, 11079, 11080, 11081, 11082, 11083, 11084, 11085, 11086, 11087, 11088, 11089, 11090, 11091, 11092, 11093, 11094, 11095, 11096, 11097, 11098, 11099, 11100, 11101, 11102, 11103, 11104, 11105, 11106, 11107, 11108, 11109, 11110, 11111, 11112, 11113, 11114, 11115, 11116, 11117, 11118, 11119, 11120, 11121, 11122, 11123, 11124, 11125, 11126, 11127, 11128, 11129, 11130, 11131, 11132, 11133, 11134, 11135, 11136, 11137, 11138, 11139, 11140, 11141, 11142, 11143, 11144, 11145, 11146, 11147, 11148, 11149, 11150, 11151, 11152, 11153, 11154, 11155, 11156, 11157, 11158, 11159, 11160, 11161, 11162, 11163, 11164, 11165, 11166, 11167, 11168, 11169, 11170, 11171, 11172, 11173, 11174, 11175, 11176, 11177, 11178, 11179, 11180, 11181, 11182, 11183, 11184, 11185, 11186, 11187, 11188, 11189, 11190, 11191, 11192, 11193, 11194, 11195, 11196, 11197, 11198, 11199, 11200, 11201, 11202, 11203, 11204, 11205, 11206, 11207, 11208, 11209, 11210, 11211, 11212, 11213, 11214, 11215, 11216, 11217, 11218, 11219, 11220, 11221, 11222, 11223, 11224, 11225, 11226, 11227, 11228, 11229, 11230, 11231, 11232, 11233, 11234, 11235, 11236, 11237, 11238, 11239, 11240, 11241, 11242, 11243, 11244, 11245, 11246, 11247, 11248, 11249, 11250, 11251, 11252, 11253, 11254, 11255, 11256, 11257, 11258, 11259, 11260, 11261, 11262, 11263, 11264, 11265, 11266, 11267, 11268, 11269, 11270, 11271, 11272, 11273, 11274, 11275, 11276, 11277, 11278, 11279, 11280, 11281, 11282, 11283, 11284, 11285, 11286, 11287, 11288, 11289, 11290, 11291, 11292, 11293, 11294, 11295, 11296, 11297, 11298, 11299, 11300, 11301, 11302, 11303, 11304, 11305, 11306, 11307, 11308, 11309, 11310, 11311, 11312, 11313, 11314, 11315, 11316, 11317, 11318, 11319, 11320, 11321, 11322, 11323, 11324, 11325, 11326, 11327, 11328, 11329, 11330, 11331, 11332, 11333, 11334, 11335, 11336, 11337, 11338, 11339, 11340, 11341, 11342, 11343, 11344, 11345, 11346, 11347, 11348, 11349, 11350, 11351, 11352, 11353, 11354, 11355, 11356, 11357, 11358, 11359, 11360, 11361, 11362, 11363, 11364, 11365, 11366, 11367, 11368, 11369, 11370, 11371, 11372, 11373, 11374, 11375, 11376, 11377, 11378, 11379, 11380, 11381, 11382, 11383, 11384, 11385, 11386, 11387, 11388, 11389, 11390, 11391, 11392, 11393, 11394, 11395, 11396, 11397, 11398, 11399, 11400, 11401, 11402, 11403, 11404, 11405, 11406, 11407, 11408, 11409, 11410, 11411, 11412, 11413, 11414, 11415, 11416, 11417, 11418, 11419, 11420, 11421, 11422, 11423, 11424, 11425, 11426, 11427, 11428, 11429, 11430, 11431, 11432, 11433, 11434, 11435, 11436, 11437, 11438, 11439, 11440, 11441, 11442, 11443, 11444, 11445, 11446, 11447, 11448, 11449, 11450, 11451, 11452, 11453, 11454, 11455, 11456, 11457, 11458, 11459, 11460, 11461, 11462, 11463, 11464, 11465, 11466, 11467, 11468, 11469, 11470, 11471, 11472, 11473, 11474, 11475, 11476, 11477, 11478, 11479, 11480, 11481, 11482, 11483, 11484, 11485, 11486, 11487, 11488, 11489, 11490, 11491, 11492, 11493, 11494, 11495, 11496, 11497, 11498, 11499, 11500, 11501, 11502, 11503, 11504, 11505, 11506, 11507, 11508, 11509, 11510, 11511, 11512, 11513, 11514, 11515, 11516, 11517, 11518, 11519, 11520, 11521, 11522, 11523, 11524, 11525, 11526, 11527, 11528, 11529, 11530, 11531, 11532, 11533, 11534, 11535, 11536, 11537, 11538, 11539, 11540, 11541, 11542, 11543, 11544, 11545, 11546, 11547, 11548, 11549, 11550, 11551, 11552, 11553, 11554, 11555, 11556, 11557, 11558, 11559, 11560, 11561, 11562, 11563, 11564, 11565, 11566, 11567, 11568, 11569, 11570, 11571, 11572, 11573, 11574, 11575, 11576, 11577, 11578, 11579, 11580, 11581, 11582, 11583, 11584, 11585, 11586, 11587, 11588, 11589, 11590, 11591, 11592, 11593, 11594, 11595, 11596, 11597, 11598, 11599, 11600, 11601, 11602, 11603, 11604, 11605, 11606, 11607, 11608, 11609, 11610, 11611, 11612, 11613, 11614, 11615, 11616, 11617, 11618, 11619, 11620, 11621, 11622, 11623, 11624, 11625, 11626, 11627, 11628, 11629, 11630, 11631, 11632, 11633, 11634, 11635, 11636, 11637
```

V4: Requerimientos de Autenticación y Manejo de Sesiones

Se observa una buena práctica en la gestión de caducidad de las sesiones después de cerrar la aplicación, uso de controles de bloquea por intentos fallidos de inicio de sesión evidenciando una suspensión temporal de 15 minutos por usuario, y mensajes de informativos en cambios de dispositivo.



V6: Requerimientos de Interacción con la Plataforma

Permisos de Aplicación

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

Showing 11 to 20 of 32 entries

Previous 1 2 3 4 Next

V8: Requerimientos de Resistencia ante la Ingeniería Inversa

La aplicación no posee aún ningún control que dificulte procesos de ingeniería inversa, lo que permite conocer, enumerar, modificar archivos e inyectar código malicioso.

```
(root@Pentesting)~# python3 frida_lief_injection.py
[+] Enter the path of your APK: /home/jcedillo/Documents/Tools/Mobil/7.3.5-p.release.build.77.apk
[+] Unzip the /home/jcedillo/Documents/Tools/Mobil/7.3.5-p.release.build.77.apk in /tmp/tmpavd_dkqn_lief_frida
[+] Select the architecture of your system:
If you don't know run: adb shell getprop ro.product.cpu.abi
1) x86
2) armeabi-v7a
3) x86_64
4) arm64-v8a
5) I don't know. Inject frida-gadget for all architectures (slower)
> 4

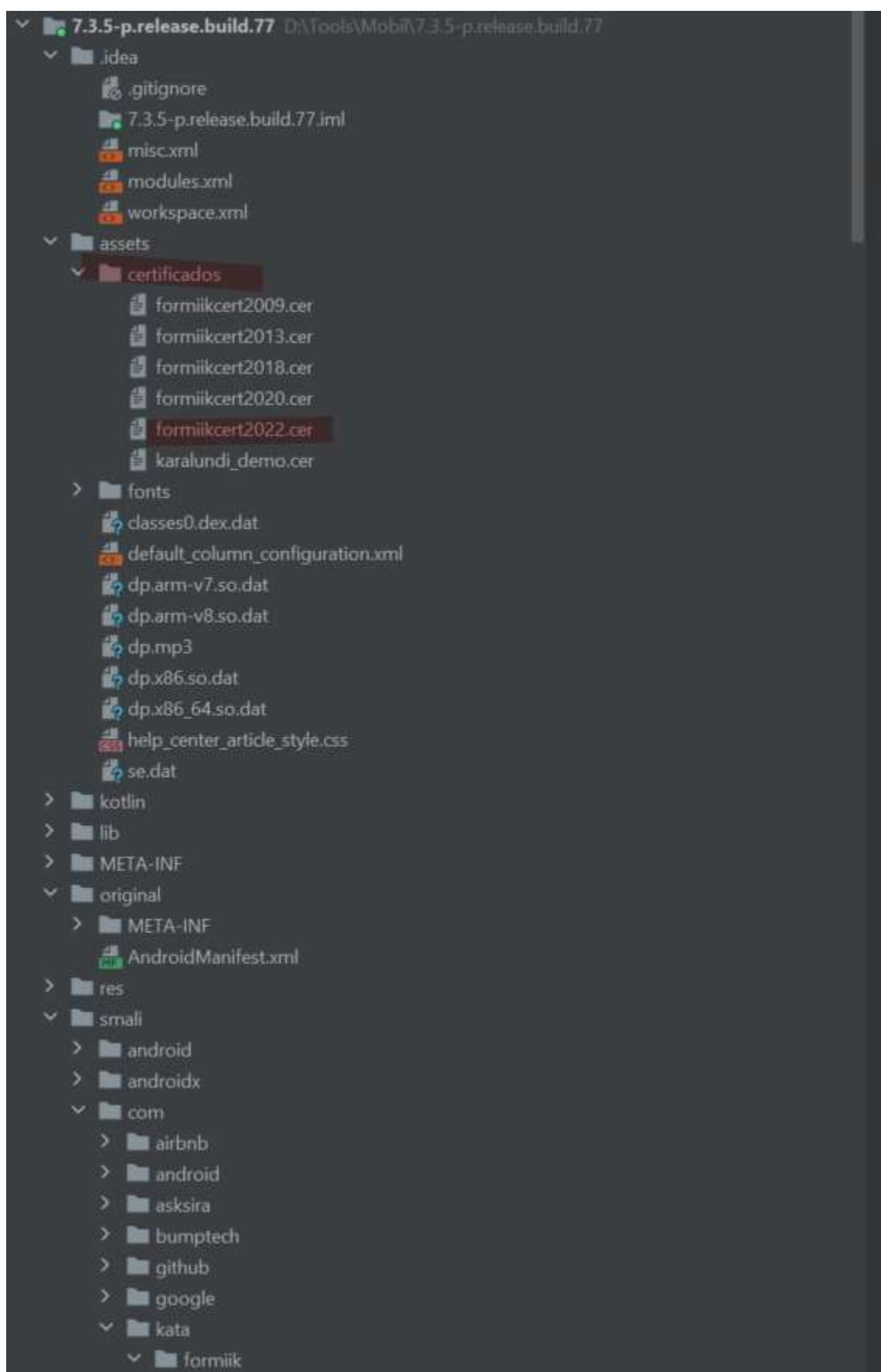
[+] In with library do you want to inject?:
1) libzbarjni.so
2) libsqlcipher.so
3) libiconv.so
4) libFormiikNative.so
5) libopencv_java3.so
6) libtool-checker.so
7) libgmm-jni.so

[+] Enter the number of the desired library:
> 4
[+] Downloading and extracting frida gadget for: arm64-v8a
[+] Injecting libgdt.so into arm64-v8a/libFormiikNative.so

[*] Removing old signature
[+] APK Building...
[+] SUCCESS!! Your new apk is : my_app.apk. Now you should sign it.

(root@Pentesting)~#
```

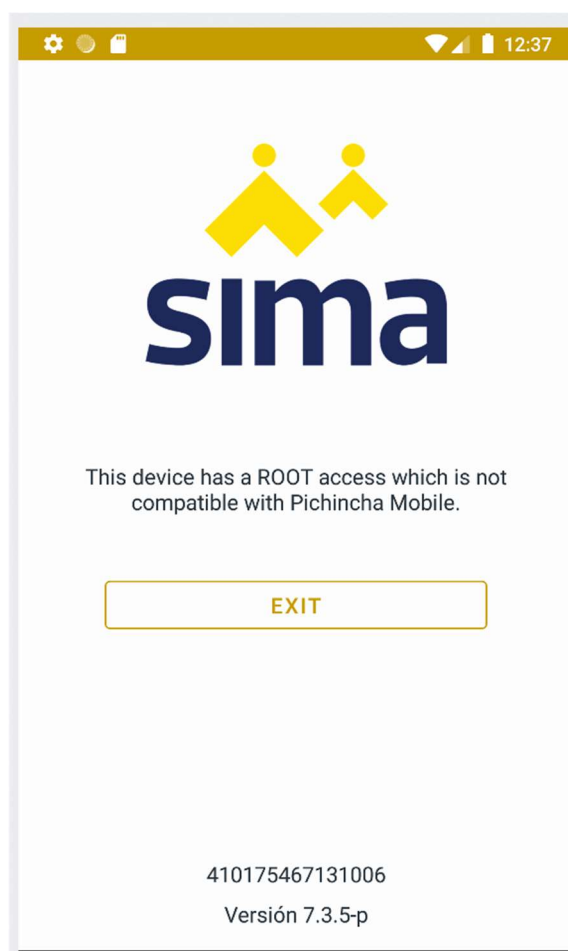
```
D:\Tools\Mobil>apktool d 7.3.5-p.release.build.77.apk
I: Using Apktool 2.4.1 on 7.3.5-p.release.build.77.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\Erick Moreno\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Baksmaling classes4.dex...
I: Baksmaling classes5.dex...
I: Baksmaling classes6.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory
D:\Tools\Mobil>
```



7.3.5-p.release.build.77 > assets > certificados					Search certificados
Name	Date modified	Type	Size		
 formiikcert2009.cer	2/2/2022 23:13	Security Certificate	2 KB		
 formiikcert2013.cer	2/2/2022 23:13	Security Certificate	3 KB		
 formiikcert2018.cer	2/2/2022 23:13	Security Certificate	3 KB		
 formiikcert2020.cer	2/2/2022 23:13	Security Certificate	3 KB		
 formiikcert2022.cer	2/2/2022 23:13	Security Certificate	3 KB		
 karalundi_demo.cer	2/2/2022 23:13	Security Certificate	2 KB		

ROOT Detection

La aplicación detecta y responde a la presencia de un dispositivo rooteado, alertando al usuario y no permite la ejecución de la aplicación.



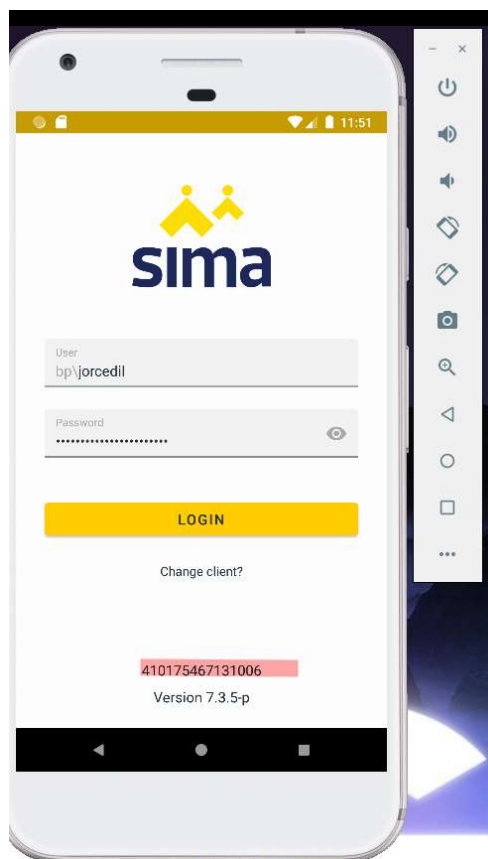
ROOT Detection Bypass

Fue posible ejecutar técnicas ofensivas avanzadas en la aplicación que permitieron evadir este control, permitiendo ejecutar la aplicación con IMEI 410175467131006 sobre un dispositivo rootado y en un entorno emulado.

```

Command Prompt - frida -l root_bypass.js -U -f com.kata.formiik --no-pause
message: {'type': 'send', 'payload': 'Bypass native fopen >> /su/bin/su'} data: None
message: {'type': 'send', 'payload': 'Bypass native fopen >> /system/bin/su'} data: None
message: {'type': 'send', 'payload': 'Bypass native fopen >> /system/bin/.ext/su'} data: None
message: {'type': 'send', 'payload': 'Bypass native fopen >> /system/bin/failsafe/su'} data: None
message: {'type': 'send', 'payload': 'Bypass native fopen >> /system/sd/xbinsu'} data: None
message: {'type': 'send', 'payload': 'Bypass native fopen >> /system/usr/we-need-root/su'} data: None
message: {'type': 'send', 'payload': 'Bypass native fopen >> /system/xbinsu'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: magisk'} data: None
Android Emulator 5554::com.kata.formiik]-> %resume

```



SSL Pinning

La aplicación posee un control de SSL Pinning o fijación de certificado SSL, lo cual la protege contra ataques de hombre en medio cuando se insertan certificados SSL sin firmar o firmados por una entidad en la cual la aplicación no confía.

SSL Pinning Bypass

Fue posible ejecutar técnicas ofensivas avanzadas en la aplicación que permitieron evadir este control, permitiendo inyectar en tiempo de ejecución librerías maliciosas y certificados SSL falsos que otorgaron visibilidad total del tráfico de red.

The screenshot shows a Windows Terminal window titled "Windows PowerShell". The command prompt displays the following sequence of events:

```
PS C:\Users\Erick Moreno\Desktop> objection --gadget com.kata.formiik explore -s "android sslpinning disable"
Using USB device 'Android Emulator 5554'
Agent injected and responds ok!
Running a startup command... android sslpinning disable
(agent) Custom TrustManager ready, overriding SSLContext.init()
(agent) Found com.android.org.conscrypt.TrustManagerImpl, overriding TrustManagerImpl.verifyChain()
(agent) Found com.android.org.conscrypt.TrustManagerImpl, overriding TrustManagerImpl.checkTrustedRecursive()
(agent) Registering job 756215. Type: android-sslpinning-disable
```

A green ASCII art logo follows, representing the word "injection":

```

 _ _ | _ | _ _ _ _ _ | _ | _ _ _ _ _
| . | . | | - | - | | . | | 
|_ _ _ _ _ | _ _ _ _ _ | _ _ _ _ _ |
    |___|(object)inject(ion) v1.11.0

```

Below the logo, it says "Runtime Mobile Exploration by: @leonjza from @sensepost".

Pressing [tab] triggers command suggestions, showing several instances of the command being executed:

```
[agent] com.kata.formiik on (google: 8.1.0) [756215] Called SSLContext.init(), overriding TrustManager with empty one.
[agent] [756215] Called SSLContext.init(), overriding TrustManager with empty one.
[agent] [756215] Called SSLContext.init(), overriding TrustManager with empty one.
[agent] [756215] Called SSLContext.init(), overriding TrustManager with empty one.
com.kata.formiik on (google: 8.1.0) [usb] #
```

Es posible entonces conocer todo el tráfico que genera la aplicación y conocer la estructura y consumo completo de los servicios que usa en la nube para conectar con los servidores de formiik.

```
Request to https://app.formiik.com:3034 [70.37.48.30]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
1 POST /SecurityPipeRest.svc/Login HTTP/2
2 Host: app.formiik.com:3034
3 Accept: text/json
4 Content-Type: application/json
5 Content-Length: 537
6 Accept-Encoding: gzip, deflate
7 User-Agent: okhttp/4.0.1
8
9 {
10   "localDateTime": "2022-02-04 00:01:39",
11   "password": "RKID-BuX0vcr-VzEhg8rGKjmbSUoG_CyD4pL-MFjC1k,",
12   "operatingSystemVersion": "8.1.0",
13   "deviceModel": "Android SDK built for x86",
14   "pushDeviceId": "cR5q74ng0guSFvpveY03bE:APA91hEggtKxniA0PBCKyJ4qps6EYxhucgavZWoc3k0sCGORST1Uz1S_HceyaUsgD0eY8EzaUfctPj7r7J9nq1mi2PkjDclKAPR0tQEz6-b1Yf4pKA4vCgeQHuc2f7oojMNRjMdfJMSv",
15   "pushDeviceType": 0.0,
16   "deviceManufacturer": "Google",
17   "operatingSystem": "Android",
18   "version": "T.3.5-p",
19   "username": "bp\\jorcedil",
20   "deviceSerialNumber": "373705350213704",
21   "pushType": "FCM_v1"
22 }
```

```
POST https://app.formiik.com:3034/SecurityPipeRest.svc/Login Send 401 Unauthorized 2.18 s 177 B 2 Minutes Ago
JSON Auth Query Header Docs Preview Header Cookie Timeline
1 {
2   "localDateTime": "2022-02-03 11:59:12",
3   "password": "54z1bxSDIj068Mq2nhFA11duzrMRdbf7jKDYMEj0FY,",
4   "operatingSystemVersion": "8.1.0",
5   "deviceModel": "Android SDK built for x86",
6   "pushDeviceId": "cR5q74ng0guSFvpveY03bE:APA91hEggtKxniA0PBCKyJ4qps6EYxhucgavZWoc3k0sCGORST1Uz1S_HceyaUsgD0eY8EzaUfctPj7r7J9nq1mi2PkjDclKAPR0tQEz6-b1Yf4pKA4vCgeQHuc2f7oojMNRjMdfJMSv",
7   "pushDeviceType": 0,
8   "deviceManufacturer": "Google",
9   "operatingSystem": "Android",
10  "version": "T.3.5-p",
11  "username": "bp\\jorcedil",
12  "deviceSerialNumber": "373705350213704",
13  "pushType": "FCM_v1"
14 }
```

IMEI Bypass

Es posible manipular el campo 'deviceSerialNumber' de la trama del inicio de sesión, alterando el IMEI no autorizado por un IMEI de un dispositivo autorizado, evadiendo el control de integridad IMEI.





User
bp\jorcedil

Password
.....

LOGIN

Change client?

410175467131006

Version 7.3.5-p

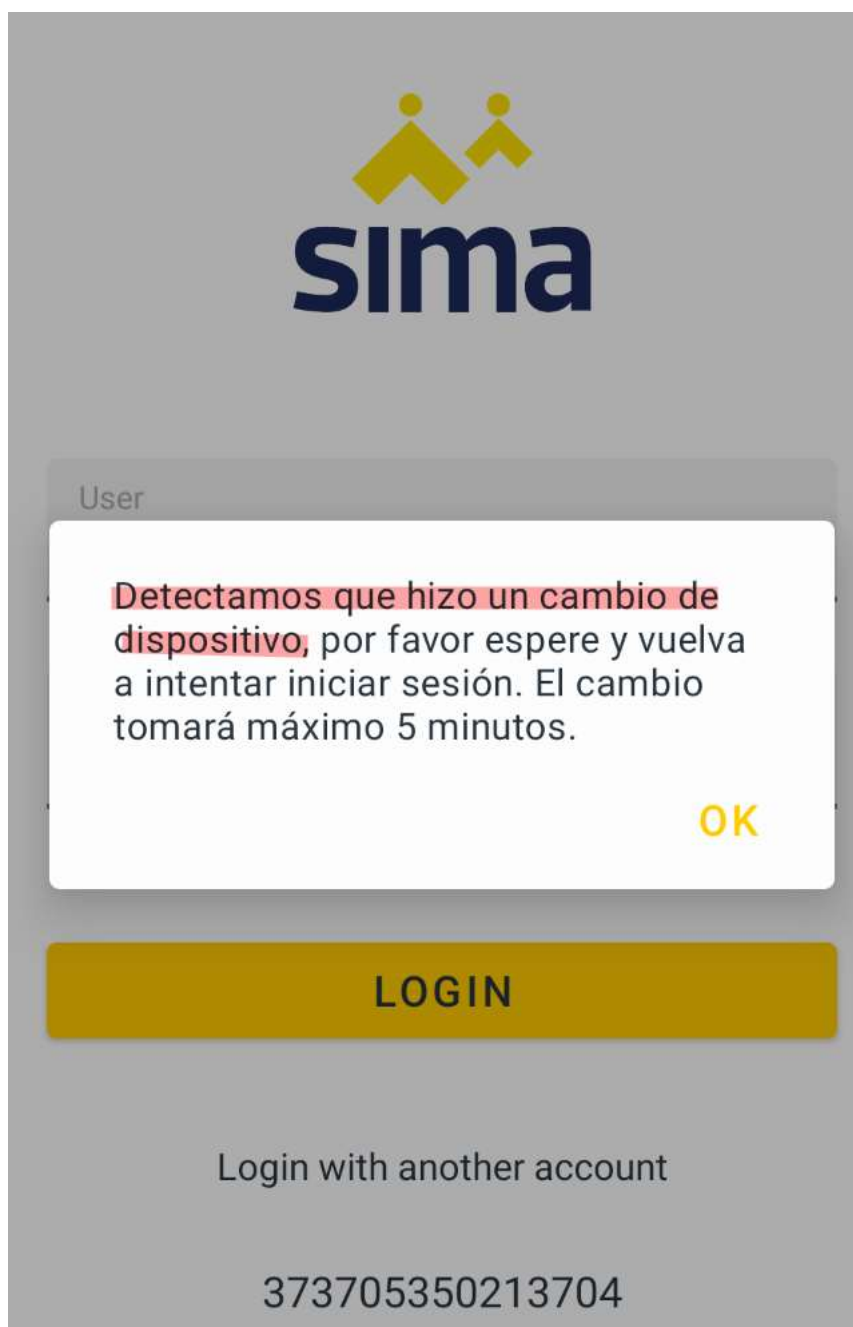
Request to https://app.formiik.com:3034 [70.37.48.30]
Forward Drop Intercept is on Action Open Browser

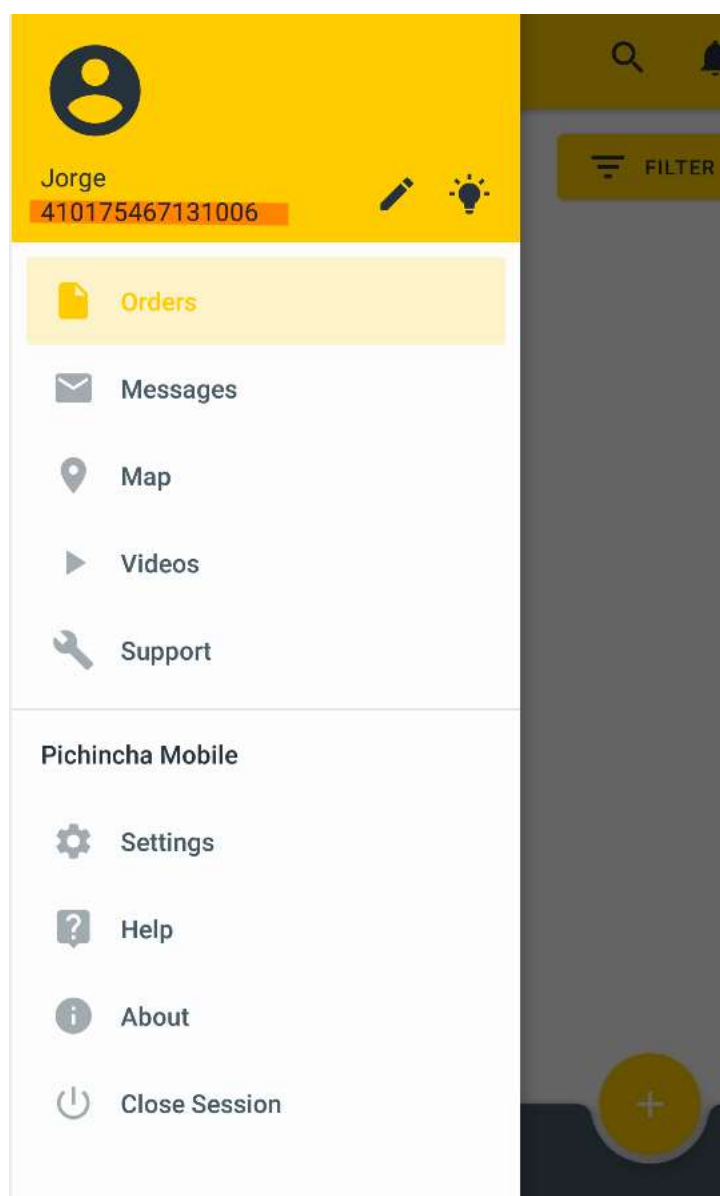
Pretty Raw Hex

```

1 POST /SecurityPipeRest.svc/Login HTTP/2
2 Host: app.formiik.com:3034
3 Accept: text/json
4 Content-Type: application/json
5 Content-Length: 537
6 Accept-Encoding: gzip, deflate
7 User-Agent: okhttp/4.0.1
8
9 {
10   "localDateTime": "2022-02-04 00:01:39",
11   "password": "MjDoBuXGwtv-VkEhq8AR6Kjmb5UoG_CyD4pL-MFjClk,",
12   "operatingSystemVersion": "8.1.0",
13   "deviceModel": "Android SDK built for x86",
14   "pushDeviceId": "cR5q74ngQguSFvpweY03bE:APAS1bEGgtExmla0PBCKyJ4qpsGETYxducgavZWoc3k0sCGOR5T1Uz1S_HkeyaUsgD0eY8EsaUfctyPj7r7J5nqlmi2FkjDtlKAPR0tQEz6-b1Yf4pKA4vCgeQHucf7oojBHRjMdfJMSv",
15   "pushDeviceType": "0.0",
16   "deviceManufacturer": "Google",
17   "operatingSystem": "Android",
18   "version": "7.3.5-p",
19   "username": "bp\\jorcedil",
20   "deviceSerialNumber": "373705350213704",
21   "pushType": "FCM_v1"
22 }

```





Conclusiones

y oportunidades de mejora

Conclusiones

- La aplicación posee un modelado de amenazas, ya que a nivel de arquitectura y diseño posee controles importantes de seguridad como el control de IMEI de dispositivos, con un esfuerzo adicional es posible Bypass este control de integridad.
- Se evidencia credenciales de APIs quemadas en la aplicación, un atacante puede intentar usarlas sin consentimiento.
- La aplicación posee control de detección de root, que evita que la APP se ejecute en dispositivos rooteados, realizando un esfuerzo adicional es posible Bypass este control.
- La aplicación posee controles de contra ataques MITM, con un poco de esfuerzo adicional es posible inyectar un certificado y poder capturar todo el tráfico que genera la aplicación, manipular y conocer su estructura.
- La aplicación no posee controles que mitiguen ataques de ingeniería reversa.
- La aplicación no posee controles de detección de emuladores virtuales o dispositivos físicos.
- La aplicación no realiza pruebas de integridad de sus archivos, lo que permitió hacer un proceso de decompilación, alteración de archivos con librerías maliciosas y re-empaquetamiento y complicación de una nueva app alterada.

Oportunidades de mejora

- La aplicación debe implementar controles que eviten o dificulten procesos de ingeniería inversa como ofuscación de código
- Inyectar en tiempo de ejecución los valores de las APIs, para evitar que las credenciales de las APIs sean encontradas en la aplicación.
- En la aplicación se deben implementar controles que no permitan la ejecución en entornos virtualizados, esto facilita el reconocimiento y la explotación de debilidades en la ejecución de las pruebas dinámicas
- La aplicación debe mejorar los controles de certificados SSL y root detection, la combinación de estas vulnerabilidades, puede ocasionar que un atacante manipule los datos de la aplicación al vuelo, alterando el flujo de la aplicación.