Auditoría de seguridad de las aplicaciones para móviles de Ferrocarrils de la Generalitat Valenciana

Autor:
Correo:
Fecha: 17 de diciembre de 2018

Índice

1. Introducción

Este documento describe la auditoría de seguridad realizada a los componentes que conforman la aplicación para dispositivos móviles de Ferrocarrils de la Generalitat Valenciana.

Antes de comenzar, es conveniente comprender la arquitectura básica de la aplicación, que es distribuida. Una aplicación distribuida es aquella que requiere más de un componente para funcionar. Dichos componentes se ejecutan en entornos separados e interactúan entre sí, normalmente a través de una red.

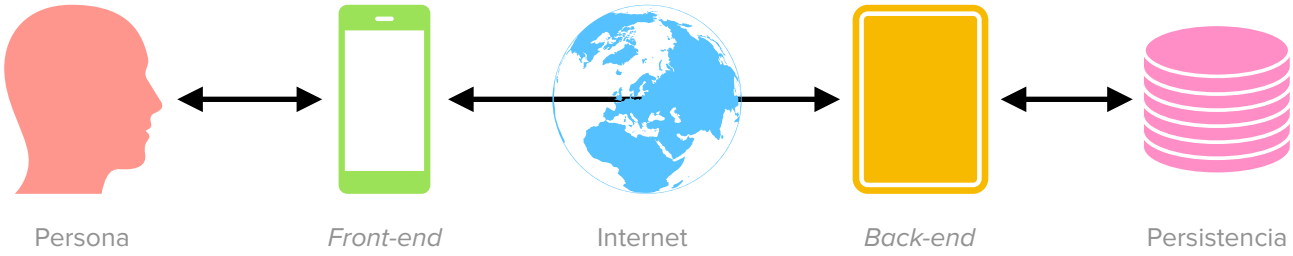


Figura 1. Flujo de interacción típico de una aplicación distribuida.

Por ejemplo, la aplicación de Metrovalencia está formada por dos componentes: el cliente, también llamado *front-end*, que se se ejecuta en un dispositivo móvil, y el servidor, también llamado *back-end*, que se ejecuta en la infraestructura de FGV y está conectado a internet. El *back-end* expone una interfaz pública a internet con la que cualquier dispositivo con conexión a dicha red puede interactuar.

Dicha interfaz se llama API (interfaz de programación de aplicaciones, por sus siglas en inglés) y debe diseñarse e implementarse, al igual que todo producto de software, por profesionales cualificados. De lo contrario, ocurre lo que se expone en este documento.

1.1. Motivación

El respeto de los derechos de las personas y el cumplimiento de la ley son requisitos fundamentales para garantizar un marco de convivencia sano y democrático. Es obligación de los ciudadanos denunciar las situaciones en las que no se garantizan estas condiciones, mientras que es derecho de la sociedad conocerlas y que los organismos competentes actúen debidamente.

1.2. Objetivos

Son objetivos de esta auditoría:

- Dar a conocer a la sociedad, los organismos oficiales y los medios de comunicación el presunto incumplimiento grave de la legislación en materia de protección de datos por parte de Ferrocarrils de la Generalitat Valenciana y/o sus empresas adjudicatarias.
- Hacer llegar la información al máximo número de personas, utilizando un lenguaje accesible para todo el mundo, sin requerir conocimientos avanzados de informática.
- Sustentar los hechos mediante la argumentación y la aportación de pruebas concluyentes.
- Informar a Ferrocarrils de la Generalitat Valenciana sobre los hechos para que cumplan la ley con la mayor celeridad posible.
- Concienciar a la sociedad sobre la gravedad de los hechos y la situación actual de la informática en el sector público.

2. Auditoría

El proceso de auditoría consiste en analizar el *front-end*, que en este caso puede ser cualquiera de las aplicaciones de FGV para móviles (Metrovalencia o TRAM), para entender cómo interactúa con el *back-end* y descubrir si dichos componentes han sido diseñados e implementados debidamente.

Los usuarios tienen derecho a conocer qué hacen las aplicaciones que instalan en sus dispositivos, siempre y cuando tengan permiso para obtenerlas, instalarlas y utilizarlas, que es el caso. Por tanto, cualquier persona tiene derecho a realizar toda inspección que considere oportuna para estudiar su comportamiento, no así a copiar ni distribuir su código fuente, cosa que podría violar la licencia del software y los derechos de autor.

> Por respeto a los derechos de las personas y a la ley, durante esta auditoría no se ha almacenado ningún dato personal. Además, toda la información sensible ha sido ocultada en las pruebas. En cualquier caso, hay que tener presente que toda esa información seguirá siendo pública hasta que FGV tome las medidas pertinentes.

2.1. Preparación

El primer paso es descargar el paquete de la aplicación para Android (APK) de Metrovalencia o TRAM, que puede encontrase en Google Play Store. Existen diversas herramientas que permiten, respectivamente, descargar un archivo APK de Play Store y extraer sus contenidos.

Para conocer los diferentes puntos de entrada (*endpoints*, en inglés) de la API únicamente es necesario inspeccionar las clases `com.fgv.transporte.Config` y `com.fgv.transporte.Comunication.ApiMethods`. Recorriendo la clase `ApiMethods` y apoyándose en la información de la clase `Config` es posible listar todos los puntos de entrada.

> Si el objetivo de la lectura es contrastar la veracidad de los hechos que se exponen en la auditoría, es recomendable importar la colección de Postman en la aplicación antes de continuar. Véase el anexo 1.

2.2. Análisis

Existe un punto de entrada cuya supuesta funcionalidad es autenticar a un cliente (`POST https://www.metrovalencia.es/ap18/api/public/api/v1/V/oauth/login`). Sin embargo, este únicamente devuelve el identificador numérico del usuario autenticado en caso de éxito. El resto de puntos de entrada no comprueban la identidad de la petición, por lo que en realidad el *back-end* no dispone de autenticación. De lo anterior se puede concluir que el software incumple presuntamente lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

A continuación se analizan los puntos de entrada (*endpoints*, en inglés) más relevantes. En el anexo 2 se adjuntan algunas capturas de pantalla a modo de demostración.

> Si el objetivo de la lectura es valorar qué aspectos del software incumplen la legislación en materia de protección de datos, los *endpoints* relevantes van del 1 al 5, inclusive, y probablemente el 7.

2.2.1. Obtener usuario

Este punto de entrada permite acceder a los datos personales de todos los usuarios registrados en Metrovalencia sin autenticación, incluyendo la dirección de correo electrónico, NIF, nombre completo, género, fecha de nacimiento, dirección postal completa y números de teléfono.

Como la API tiene un límite de 60 peticiones por minuto, sería posible descargar los datos personales de todos los usuarios, uno a uno, en menos de 17 horas desde un único dispositivo. En caso de realizar una descarga distribuida, el tiempo podría reducirse sustancialmente.

Método	`GET`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/usuarios/perfil/{user_id}`
Parámetros de la URL	- **`user_id`**. Identificador numérico del usuario a consultar. En el momento de redactar el documento, de 1 a 59894.
Cabeceras	`Authorization: FGV-20171220`

2.2.2. Obtener las tarjetas de transporte de un usuario

Desde este *endpoint* es posible listar todas las tarjetas de transporte de un usuario en concreto.

Método	`GET`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/tarjetas-transporte/listado/{user_id}`
Parámetros de la URL	- **`user_id`**. Identificador del usuario que posee las tarjetas.
Cabeceras	`Authorization: FGV-20171220`

2.2.3. Obtener los movimientos de una tarjeta de transporte

Este punto de entrada posibilita la obtención de los movimientos de una tarjeta de transporte. Como es posible conocer a quién pertenece una tarjeta de transporte, es posible saber dónde ha estado cada usuario en todo momento.

Método	`GET`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/tarjetas-transporte/movimientos/{transport_card_id}`
Parámetros de la URL	- **`transport_card_id`**. Identificador de la tarjeta de transporte, que se puede obtener listando las tarjetas de transporte de un usuario en concreto.
Cabeceras	`Authorization: FGV-20171220`

2.2.4. Obtener las compras de un usuario

Este *endpoint* permite conocer las recargas de tarjetas de transporte que ha realizado cada usuario.

Método	`GET`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/compra-venta/compras/{user_id}`
Parámetros de la URL	- **`user_id`**. Identificador del usuario que posee las compras.
Cabeceras	`Authorization: FGV-20171220`

2.2.5. Obtener las tarjetas bancarias de un usuario

Desde este punto de entrada es posible listar las tarjetas de bancarias de cada usuario. Estas tarjetas se utilizan para realizar las recargas de las tarjetas de transporte.

Únicamente se muestra la marca (Visa o MasterCard, por ejemplo) y la fecha de caducidad. En cualquier caso, dicha información es confidencial y puede ser utilizada para realizar ingeniería social con el objetivo de obtener los datos completos de una tarjeta.

Método	`GET`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/tarjetas/obtener/{user_id}`
Parámetros de la URL	- **`user_id`**. Identificador del usuario que posee las tarjetas bancarias.
Cabeceras	`Authorization: FGV-20171220`

2.2.6. Añadir o eliminar una tarjeta de transporte

Desde estos *endpoints* se puede añadir y eliminar una tarjeta de transporte a un usuario sin su consentimiento.

Método	`POST`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/tarjetas-transporte`
Parámetros del cuerpo	- **`ID`**. Identificador del usuario al que asignar las tarjetas. - **`NUM_SERIE`**. Número de la tarjeta de transporte a asignar. - **`REGISTRAR`**. Desconocido (numérico).
Cabeceras	`Authorization: FGV-20171220`

Método	`POST`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/tarjetas-transporte/desasignar`
Parámetros del cuerpo	- **`NUM_SERIE`**. Número de la tarjeta de transporte a desasignar.
Cabeceras	`Authorization: FGV-20171220`

2.2.7. Recargar una tarjeta de transporte

Este punto de entrada permite recargar la tarjeta de transporte de un usuario realizando el pago con su tarjeta bancaria (si tiene alguna añadida), suponiendo que la pasarela de pago no requiera autenticación de doble factor. Como es ilegal auditarlo, queda como algo puramente teórico.

Por otra parte, también permite realizar una recarga indicando importes distintos de cobro y de recarga, por lo que se entiende que es posible recargar 10 € en una tarjeta pagando solo 0,01 €, por ejemplo.

Método	`POST`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/compra-venta/recarga`
Parámetros del cuerpo	- **`usuario_id`**. Identificador del usuario. - **`num_serie`**. Número de serie de la tarjeta de transporte. - **`tarjeta_id`**. Identificador de la tarjeta bancaria. - **`importe`**. Importe a cobrar, que no tiene por qué coincidir con el importe a recargar. - **`saldo_a_incrementar`**. Importe a recargar en la tarjeta de transporte.
Cabeceras	`Authorization: FGV-20171220`

2.2.8. Cambiar la contraseña de un usuario

También es posible que cualquier persona modifique la contraseña del usuario que desee. El sistema confía en que cada persona sea quien dice ser.

Método	`POST`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/usuarios/cambiar-password`
Parámetros del cuerpo	- **`id`**. Identificador del usuario. - **`pwd`**. Nueva contraseña.
Cabeceras	`Authorization: FGV-20171220`

2.2.9. Devolver pago

Este punto de entrada permite realizar la devolución de cualquier pago dado su identificador.

Método	`GET`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/tarjetas/devolver-referencia/{payment_id}`
Parámetros de la URL	- **`payment_id`**. Identificador del pago a devolver.
Cabeceras	`Authorization: FGV-20171220`

2.2.10. Añadir o eliminar una tarjeta bancaria

Por último, también es posible añadir tarjetas bancarias a un usuario o eliminarlas sin su consentimiento.

Método	`POST`
URL	`https://www.metrovalencia.es/ap18/api/public/es/api/v1/V/tarjetas/registrar`
Parámetros de la URL	- **`usuario_id`**. Identificador del usuario al que añadir la tarjeta. - **`numero_tarjeta`**. Numeración de la tarjeta bancaria. - **`fecha_caducidad`**. Fecha de caducidad de la tarjeta bancaria. - **`cvv2`**. CVV de la tarjeta bancaria. - **`nombre`**. Nombre completo del titular de la tarjeta bancaria.
Cabeceras	`Authorization: FGV-20171220`

3. Medidas

Conocida y probada la situación, deberían tomarse medidas correctivas, preventivas y depuradoras por los diferentes organismos involucrados con la mayor celeridad posible.

Ferrocarrils de la Generalitat Valenciana debería:

- Desactivar los servicios afectados con efecto inmediato hasta que cumplan con la legislación vigente.
- Realizar una investigación para descubrir si la información pública ha sido descargada y/o explotada por terceras partes.
- Volver a emitir de forma gratuita y con nueva numeración todas las tarjetas de transporte de los usuarios afectados para garantizar que terceras partes que hayan descargado la información no sean capaces de seguir monitorizando sus movimientos por la red de transporte.
- Depurar responsabilidades dentro de la propia empresa y de las empresas adjudicatarias del software si procediese.
- Pedir disculpas a los usuarios afectados y a la sociedad en general, ya que el daño cometido es irreparable en la práctica.
- Auditar todo su software e infraestructura, y poner a disposición de la sociedad los resultados de dichas auditorías.

Por los organismos competentes (Agencia Española de Protección de Datos y fiscalía):

- Investigar la situación, previa denuncia o de oficio, para descubrir si hay infracción administrativa, responsabilidad civil y/o responsabilidad penal por parte de los implicados.

Por la sociedad:

- Condenar duramente este tipo de situaciones y exigir que profesionales cualificados se encarguen de diseñar e implementar los productos que la sociedad utiliza en el día a día, siendo la informática una pieza esencial en la misma.

4. Conclusiones

Hasta que Ferrocarrils de la Generalitat Valenciana tome medidas, los datos personales de miles de personas son accesibles por todo el mundo. Desde el momento en el que se expone un servicio a internet, este es público para toda la red. La autenticación, por tanto, es un requisito indispensable en todo software de acceso público que maneja información privada, y en este caso se ha optado por no implementar ningún tipo de autenticación sin pensar en las consecuencias. Se puede afirmar sin lugar a dudas que no se trata de un fallo de seguridad; el software se ha concebido así directamente porque no ha sido desarrollado por profesionales cualificados.

Destaca especialmente la mediocridad de la necesidad de enviar la cabecera `Authorization` con contenido `FGV-20171220` en cada petición, lo cual pone en evidencia que el equipo de desarrollo es absolutamente incompetente para la tarea que ha llevado a cabo. En cualquier caso, la API completa y la aplicación para Android son casos de especial estudio.

Por otra parte, el hecho de aceptar pagos con tarjetas bancarias exige el cumplimiento de unos estándares de seguridad muy estrictos (véase Payment Card Industry Data Security Standards) que ni el software ni la infraestructura de Ferrocarrils de la Generalitat Valenciana cumplen.

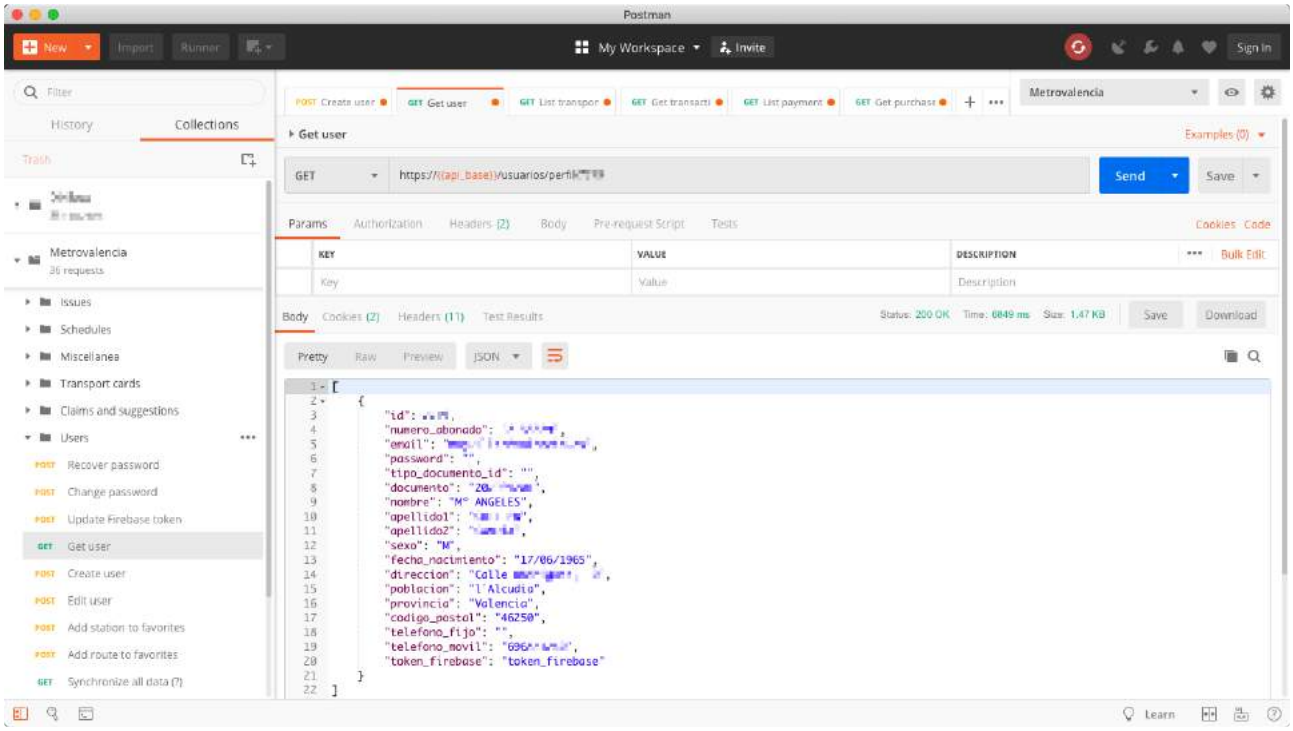
Si el estándar de calidad de FGV es el que ha quedado patente en esta pequeña auditoría, ¿qué garantías tienen los ciudadanos de que el resto de software e infraestructura informática cumplen con la legislación?

Anexo 1: Postman y colección de *endpoints*

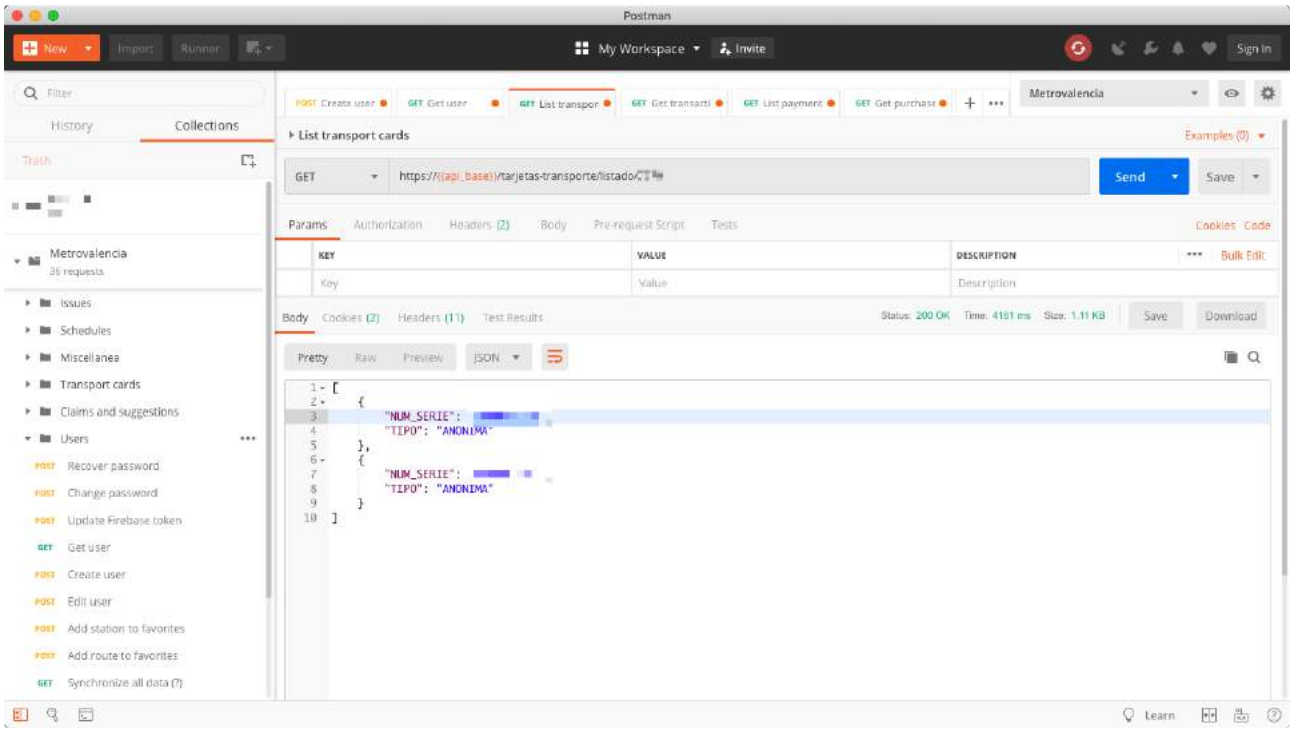
Con el objetivo de facilitar el proceso de auditoría y su posterior corroboración, es posible descargar la aplicación Postman y la colección de *endpoints* de la API de Ferrocarrils de la Generalitat Valenciana desde los siguientes enlaces.

Aplicación Postman	Colección de *endpoints*
	
https://www.getpostman.com	https://bit.ly/2LngJKN

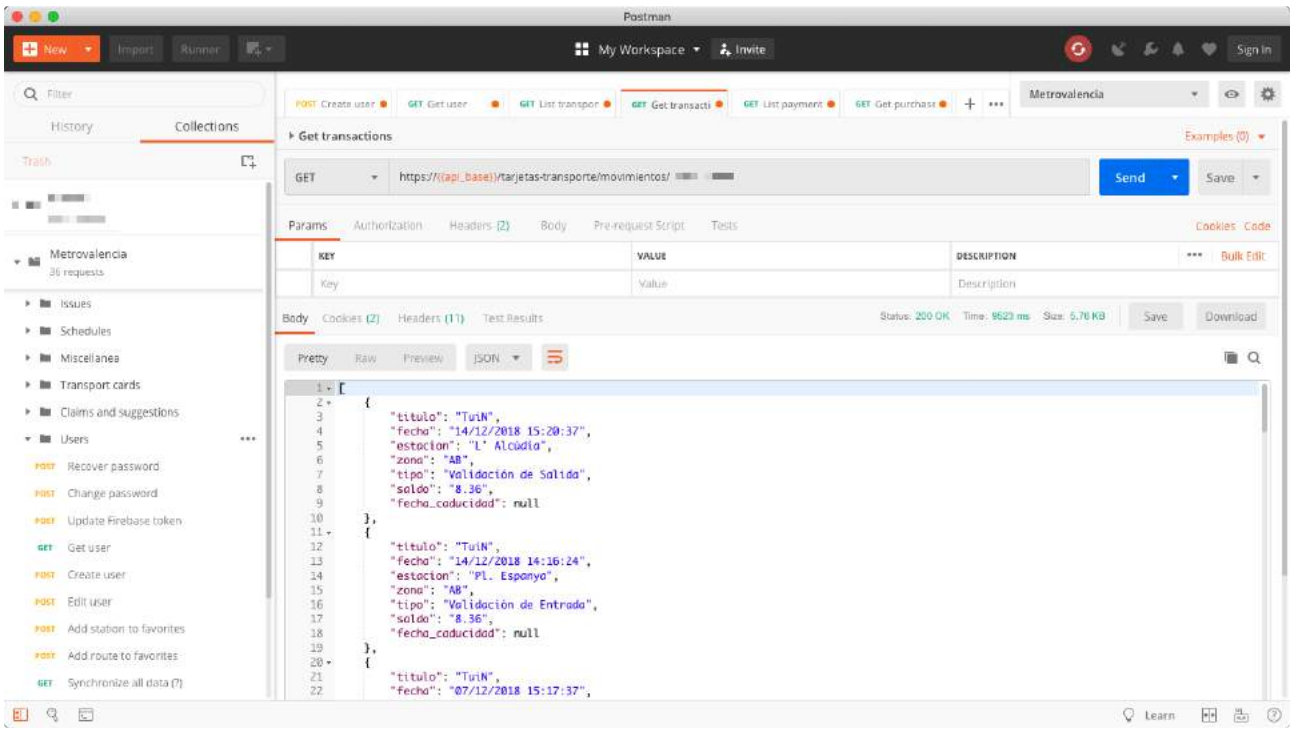
Anexo 2: capturas de pantalla



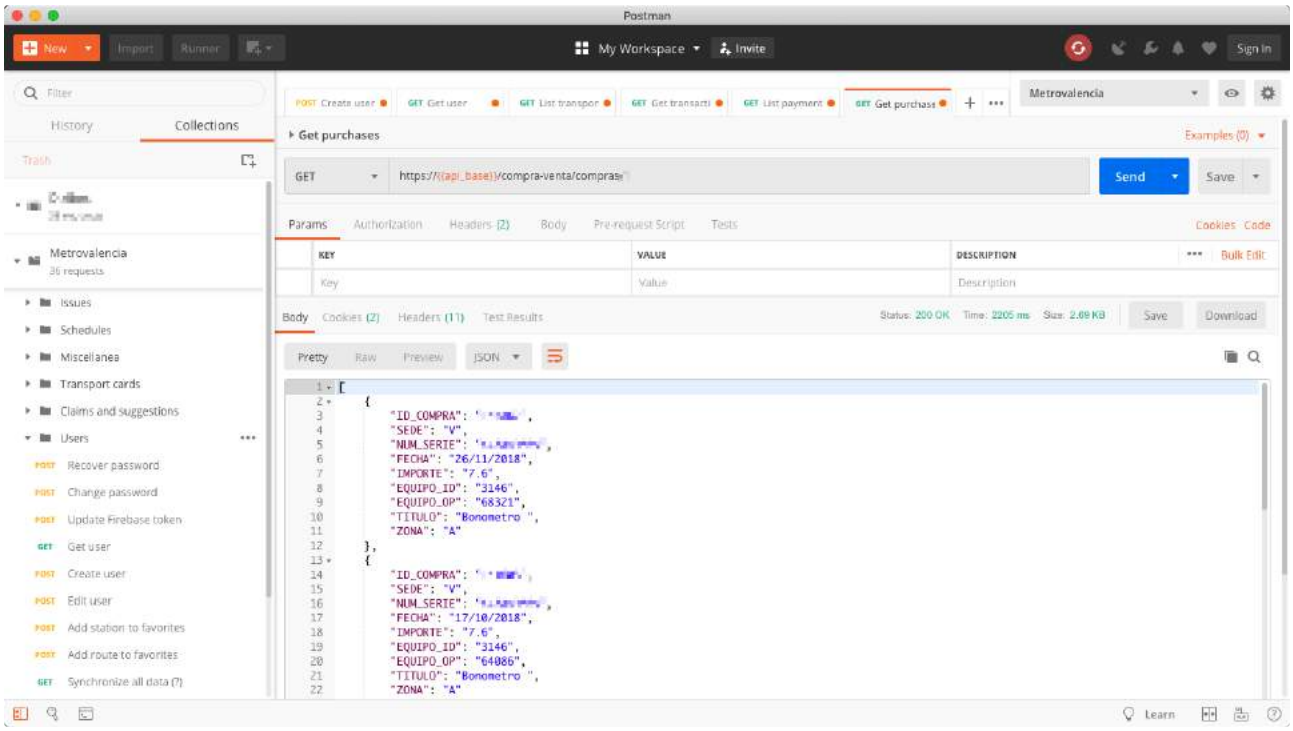
Captura 1: obtención de todos los datos de un usuario.



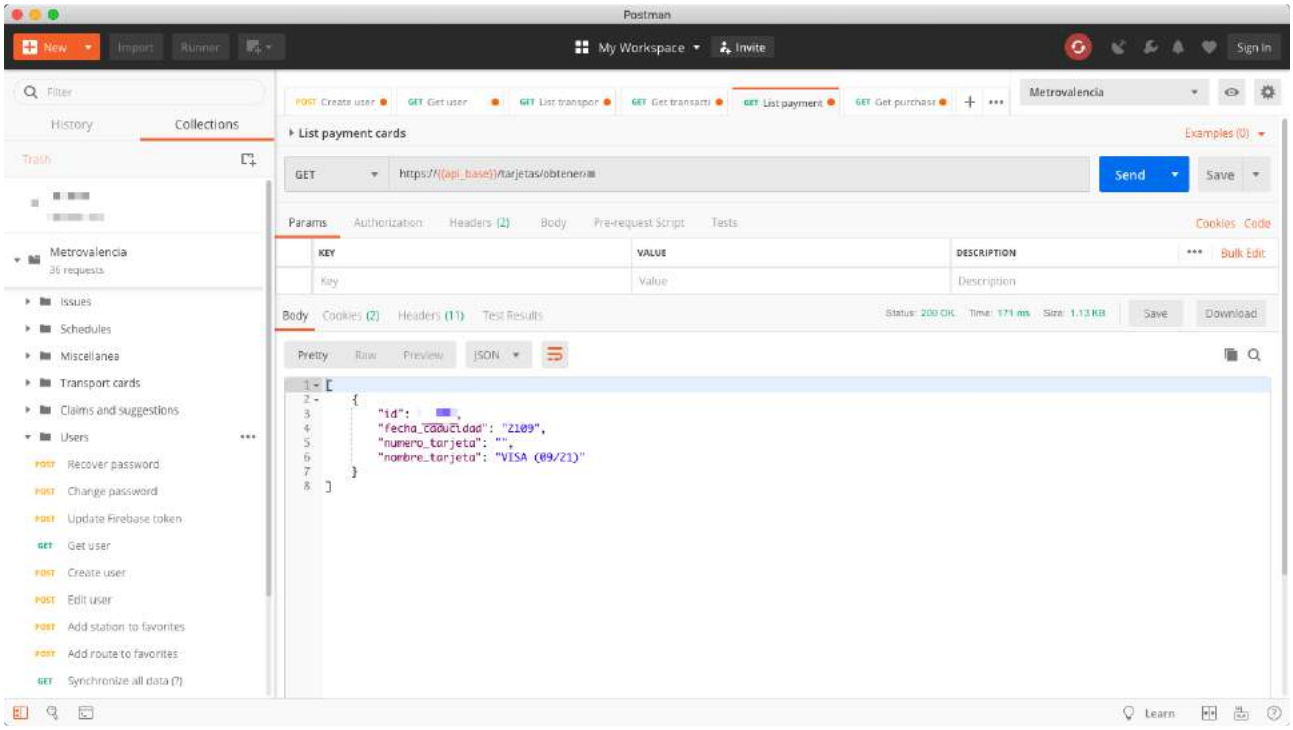
Captura 2: obtención de todas las tarjetas de transporte de un usuario.



Captura 3: obtención de todos los movimientos de una tarjeta de transporte.



Captura 4: obtención de todas las compras de un usuario.



Captura 5: obtención de todas las tarjetas de pago de un usuario.