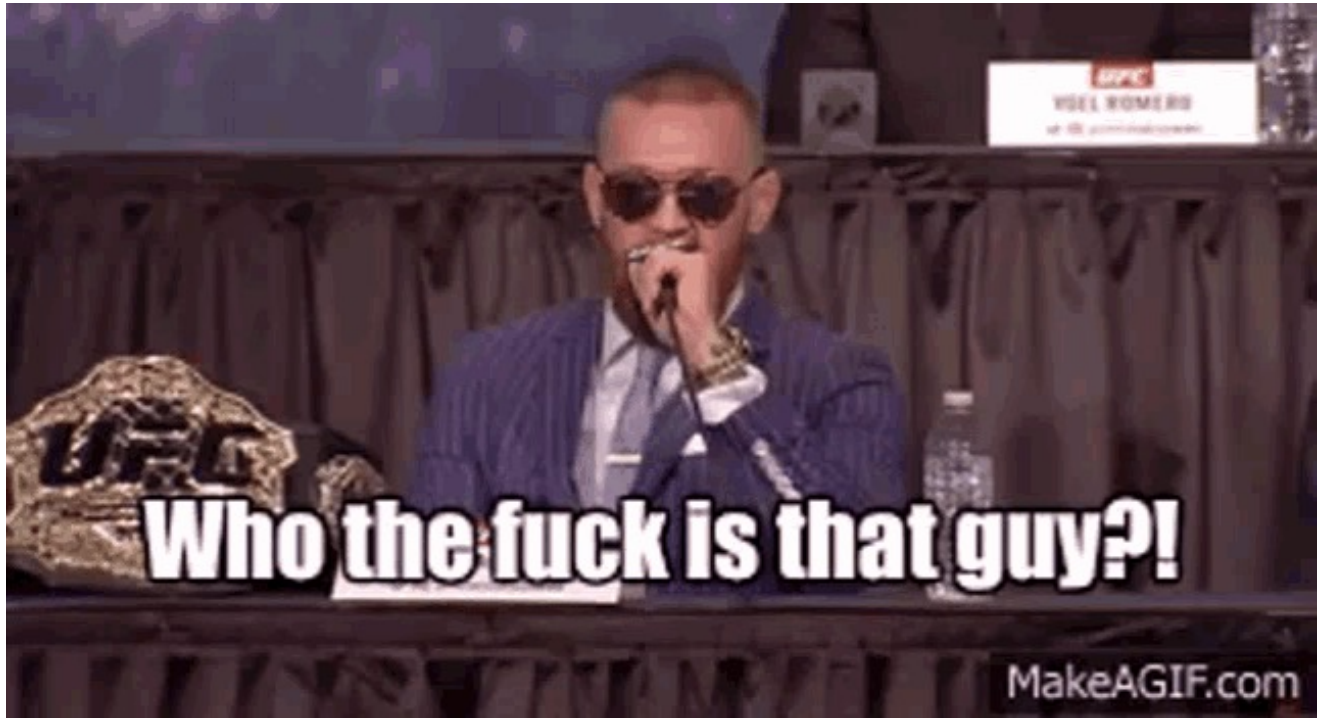

API SECURITY

MATO FERREIRA

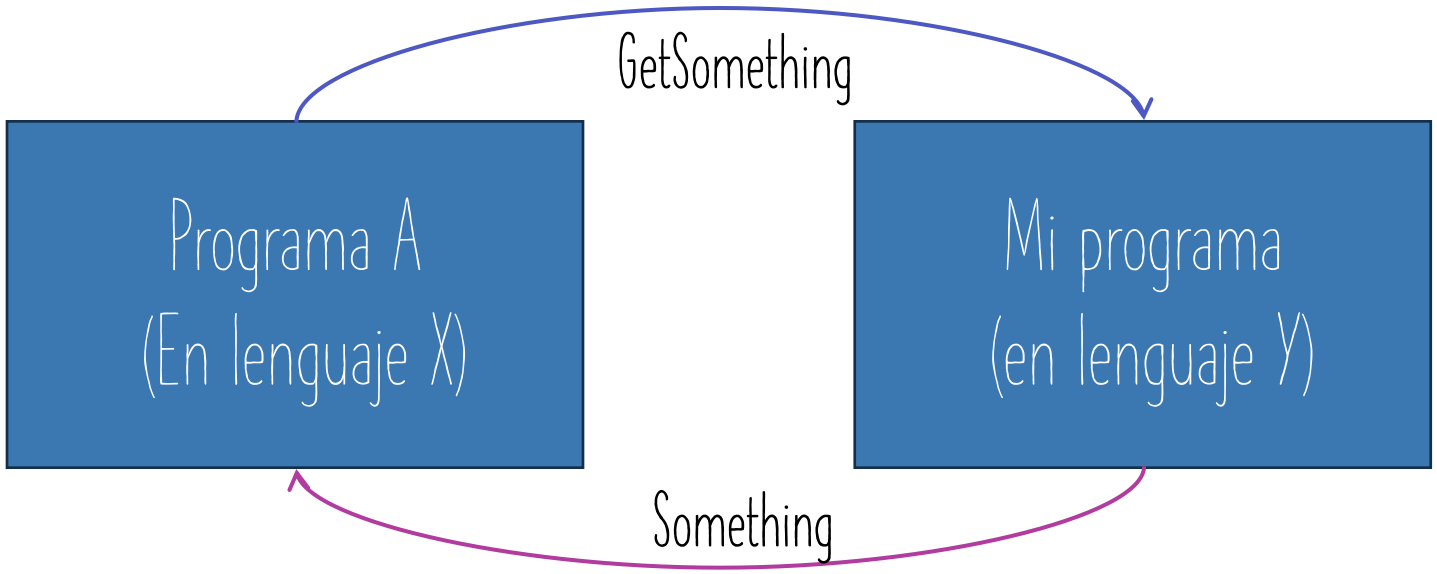
KRAV MAGA HACKING

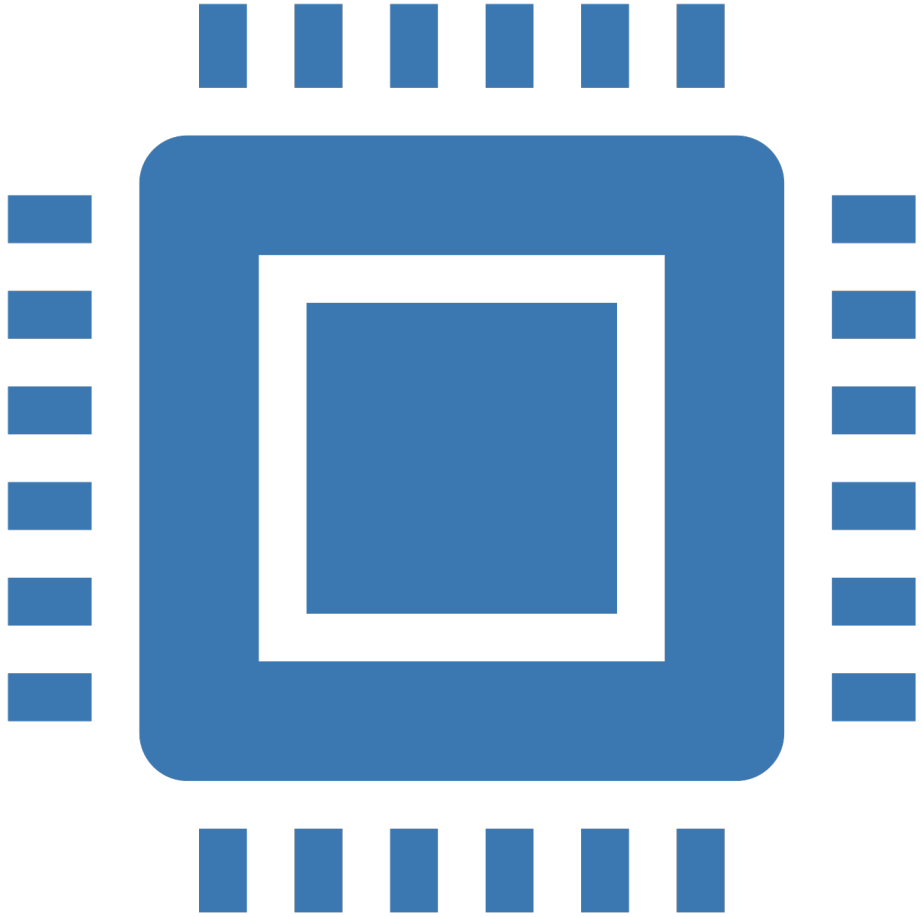
LUGAPEL
APPLICATION SECURITY



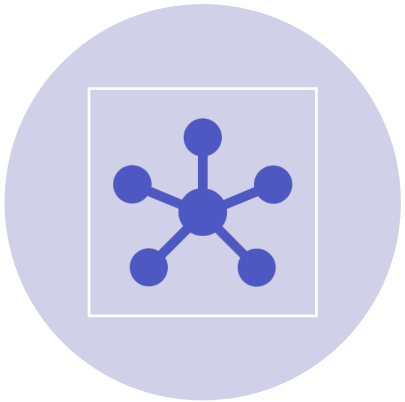
INTRODUCCIÓN A LAS APIS

- Conjunto de protocolos, rutinas y herramientas para intercambiar información entre aplicaciones.





EL ROL DE LAS APIS EN EL DESARROLLO MODERNO

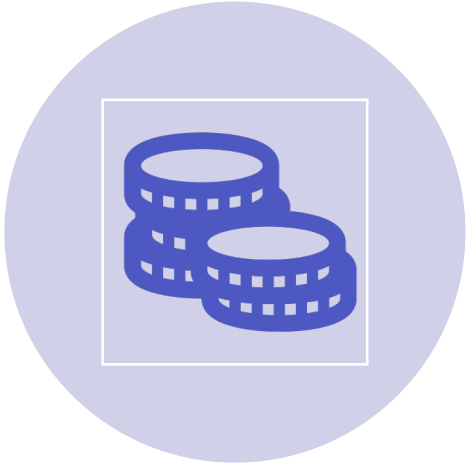


INTEGRACIÓN E INTEROPERABILIDAD

INNOVACIÓN Y ECOSISTEMA EN EXPANSIÓN

ARQUITECTURA DE MICROSERVICIOS

EL ROL DE LAS APIS EN EL DESARROLLO MODERNO



IMPACTO ECONÓMICO

APIs COMO PRODUCTOS

IMPORTANCIA DE API SECURITY

EL ROL DE SEGURIDAD EN LAS APIs

- Ubicuidad de las APIs
- Aumento de la superficie de ataque

RIESGOS Y CONSECUENCIAS

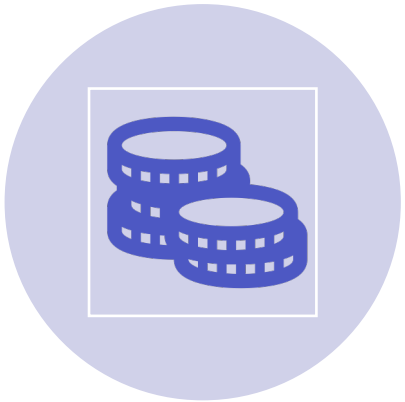
DATA BREACHES

DISRUPCIÓN DE SERVICIOS

PROBLEMAS LEGALES / COMPLIANCE

PÉRDIDA DE CONFIANZA Y REPUTACIÓN

API SECURITY COMO NECESIDAD DE NEGOCIO



IMPACTO ECONÓMICO

VENTAJA COMPETITIVA

IMPULSA INNOVACIÓN

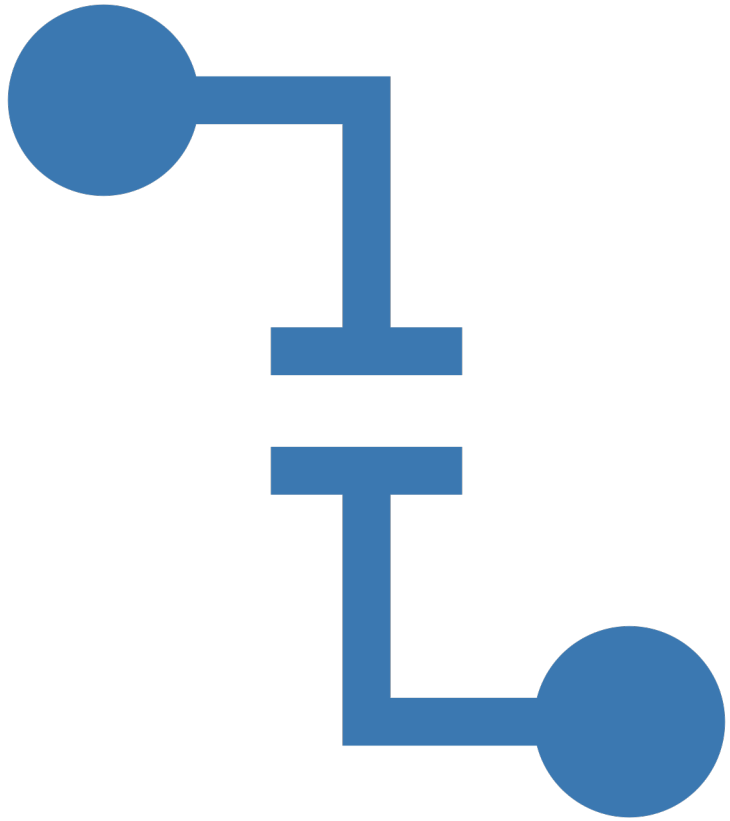
AMENAZAS COMUNES A LA SEGURIDAD DE LAS APIS

AUTORIZACIÓN Y AUTENTICACIÓN INSUFICIENTE PARA EL ACCESO A DATOS

- Broken Object Level Authorization
- Broken Authentication
- Broken Object Property Level Authorization

ACCESO SIN RESTRICCIÓN A RECURSOS, FUNCIONES Y FLUJOS

- Unrestricted resource consumption
- Broken Function Level Autorization
- Unrestricted Access to Sensitive Business Flows



AUSENCIA DE VALIDACIÓN, ERRORES DE CONFIGURACIÓN, MANEJO INAPROPIADO DE INVENTARIO Y RECURSOS

- Server-Side Request Forgery
- Security Misconfiguration
- Improper Inventory Management
- Unsafe Consumption of APIs

MEJORES PRÁCTICAS PARA API SECURITY

Inventario de APIs

Modelado de datos, diseño seguro, threat modelling

Análisis de seguridad y auditoría continua

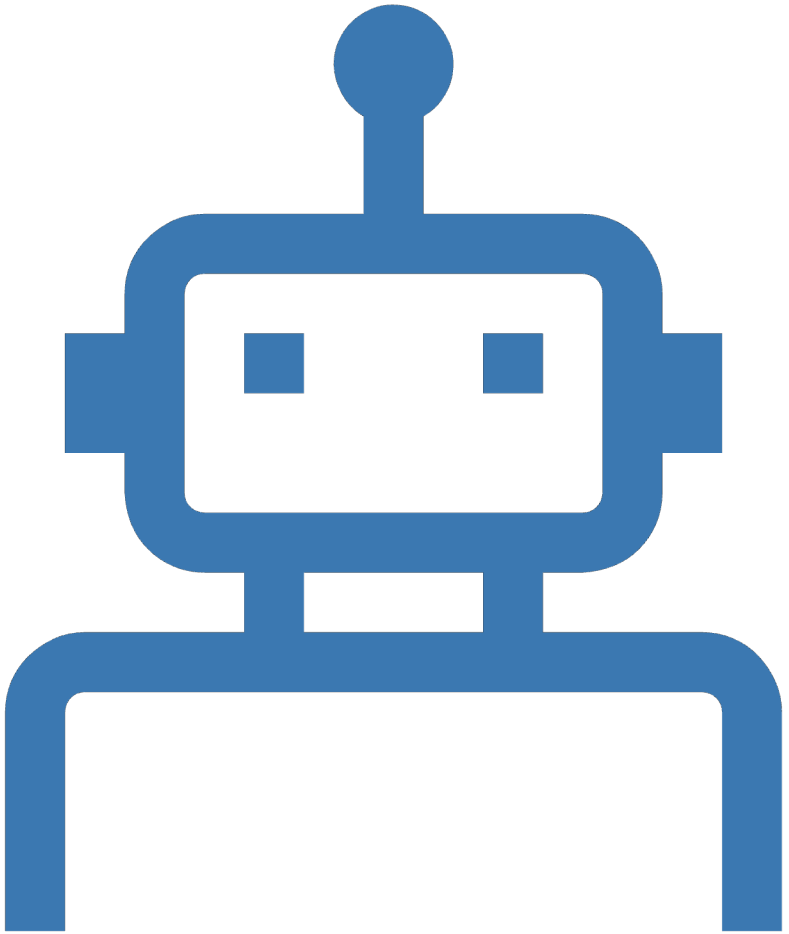
Técnicas de Autenticación y Autorización

Validación de datos y sanitización

Implementación de Throttling y Rate Limiting

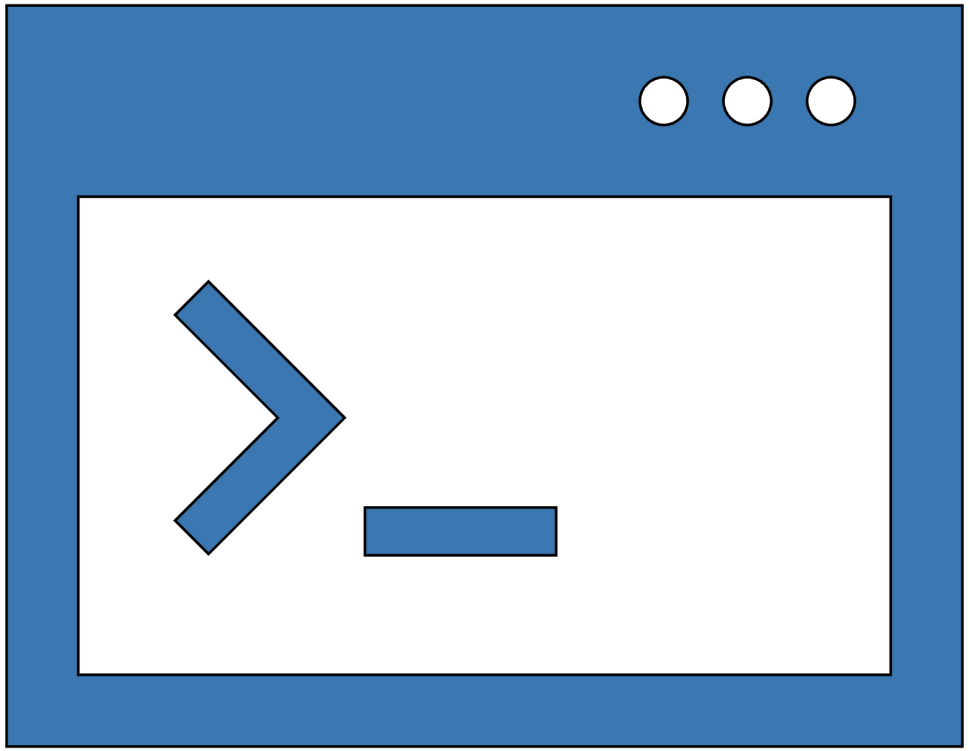
LABORATORIO

- Usaremos crAPI
- Simula una web API-Driven, basada en microservicios.
- Contiene las vulnerabilidades comunes que pasan en aplicaciones modernas basadas en vulnerabilidades de la vida real



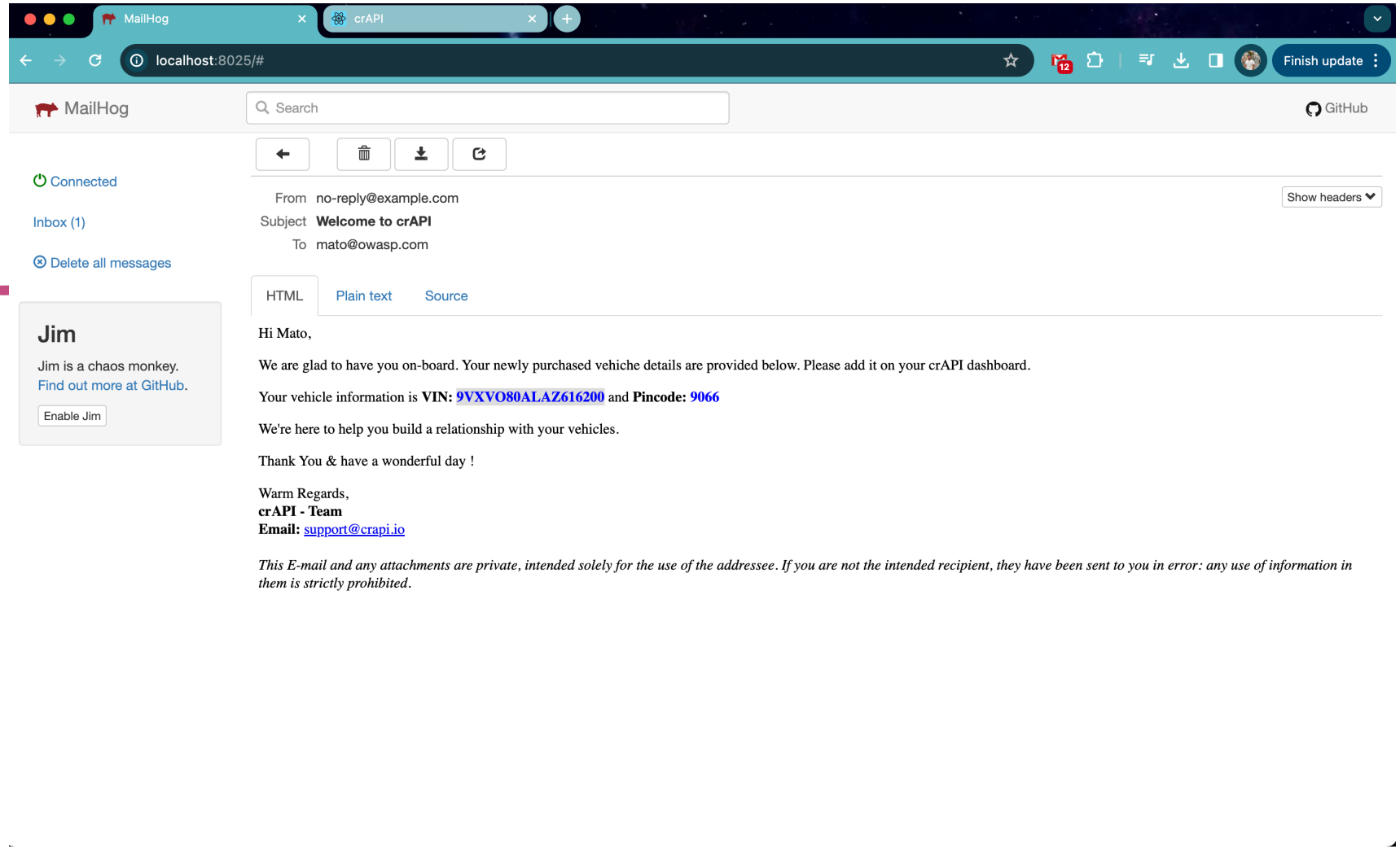
SETUP

- Repo: https://github.com/OWASP/crAPI
- Setup a través de:
  - Docker
  - Vagrant
  - Kubernetes
  - Build personal
- Burp Suite



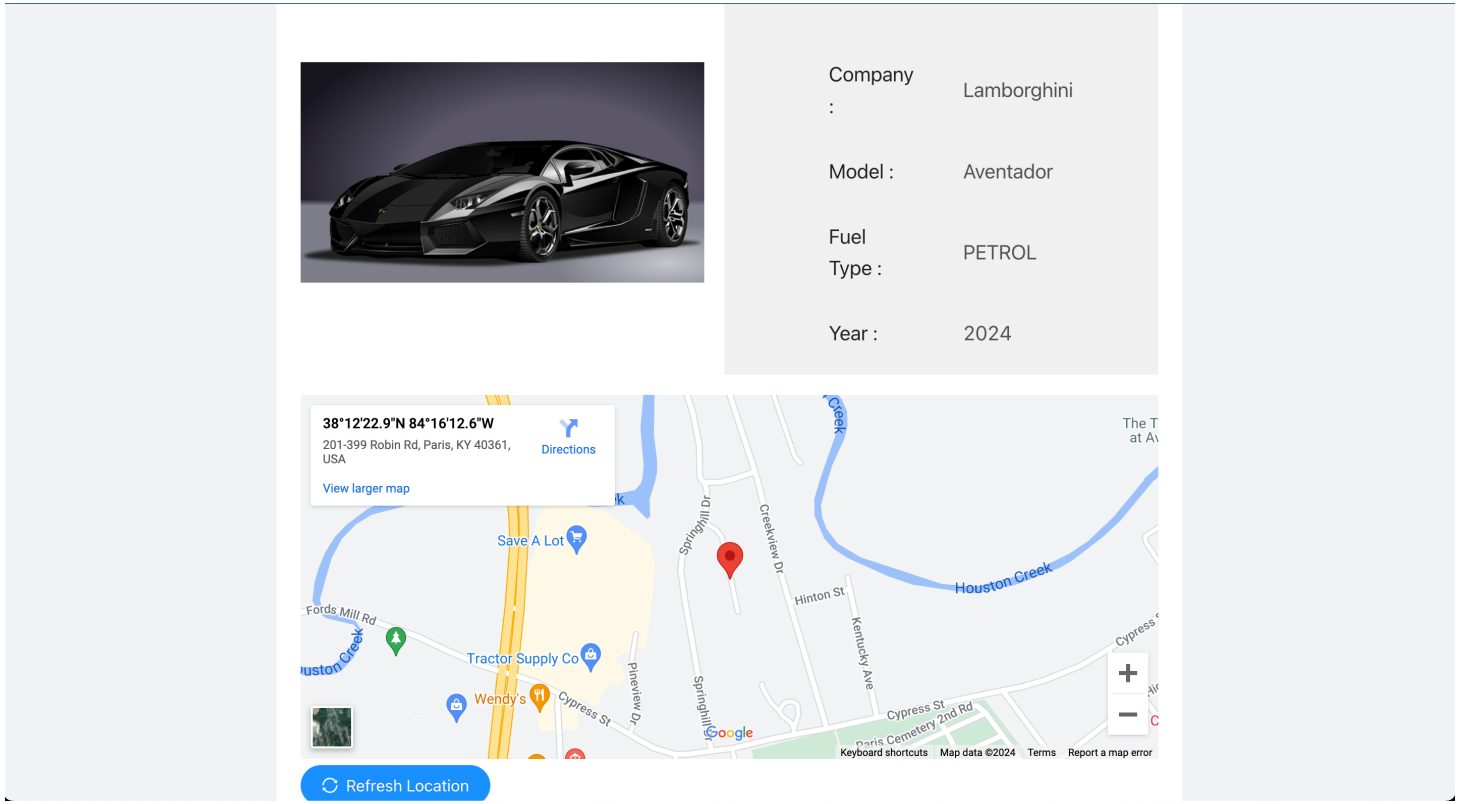
EJERCICIO 1 - BOLA WALKTHROUGH

- Acceder a localhost:8088 y crear una cuenta
- Acceder a localhost:8025 para ver los datos del vehículo a registrar
- Hacer login y agregar vehículo



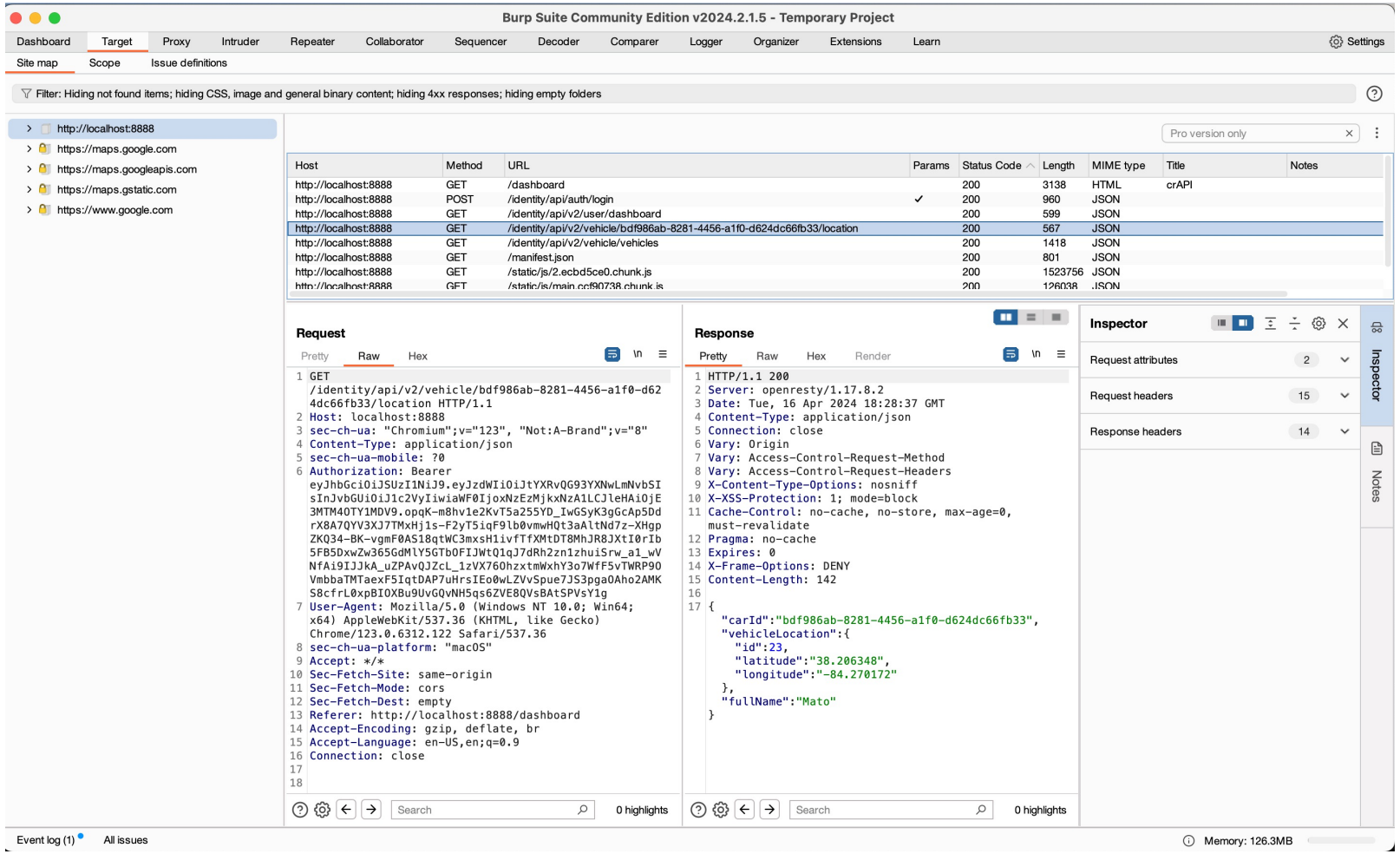
WALKTHROUGH

- Registrar vehículo
- Desde el proxy a elección (Burp), entrar al dashboard y darle a refresh location
- Analizar el request



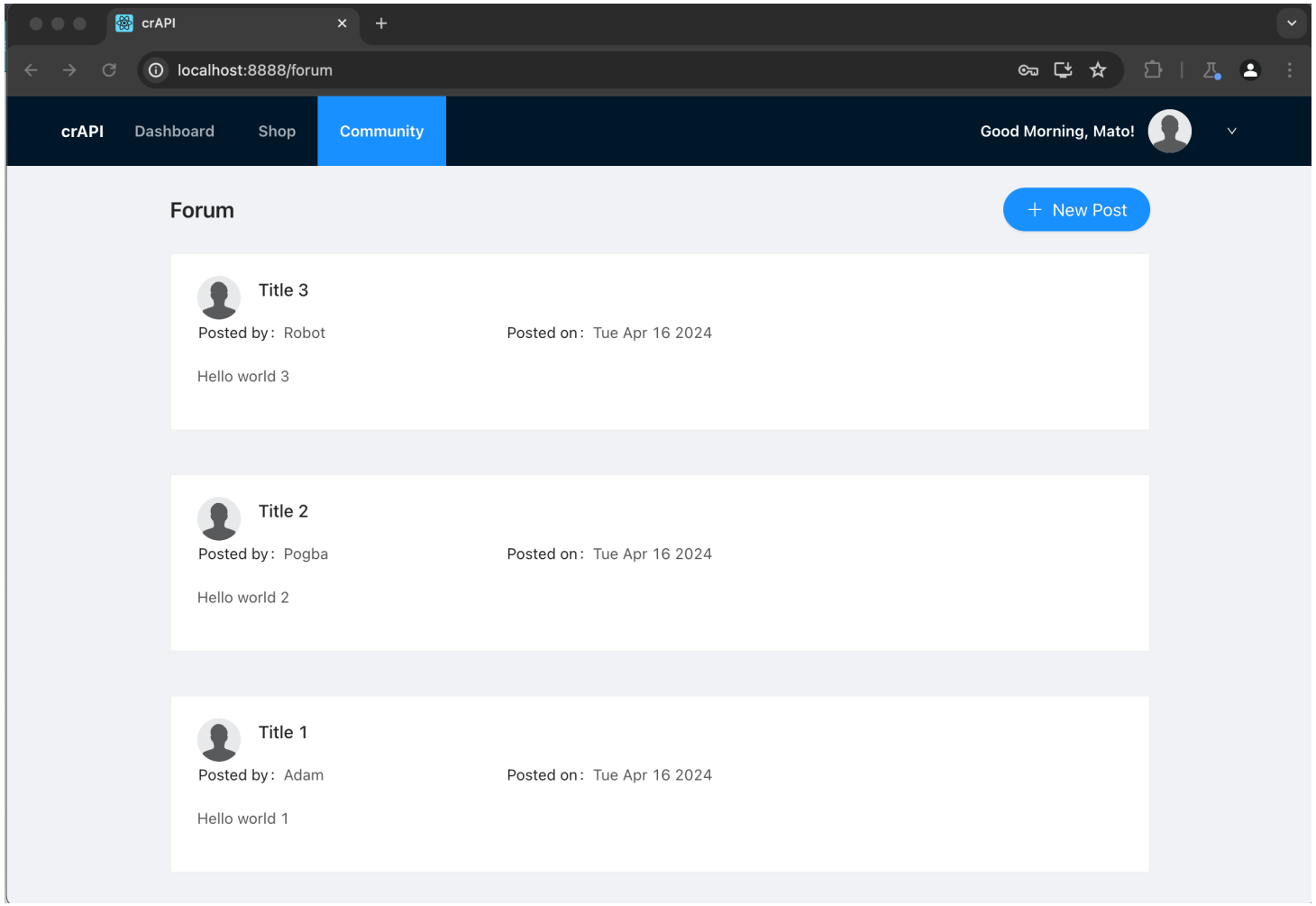
WALKTHROUGH

- Analizamos el request
- El endpoint usa el id de vehículo
- GET /identity/api/v2/vehicle/bdf986ab-8281-4456-a1f0-d624dc66fb33/location



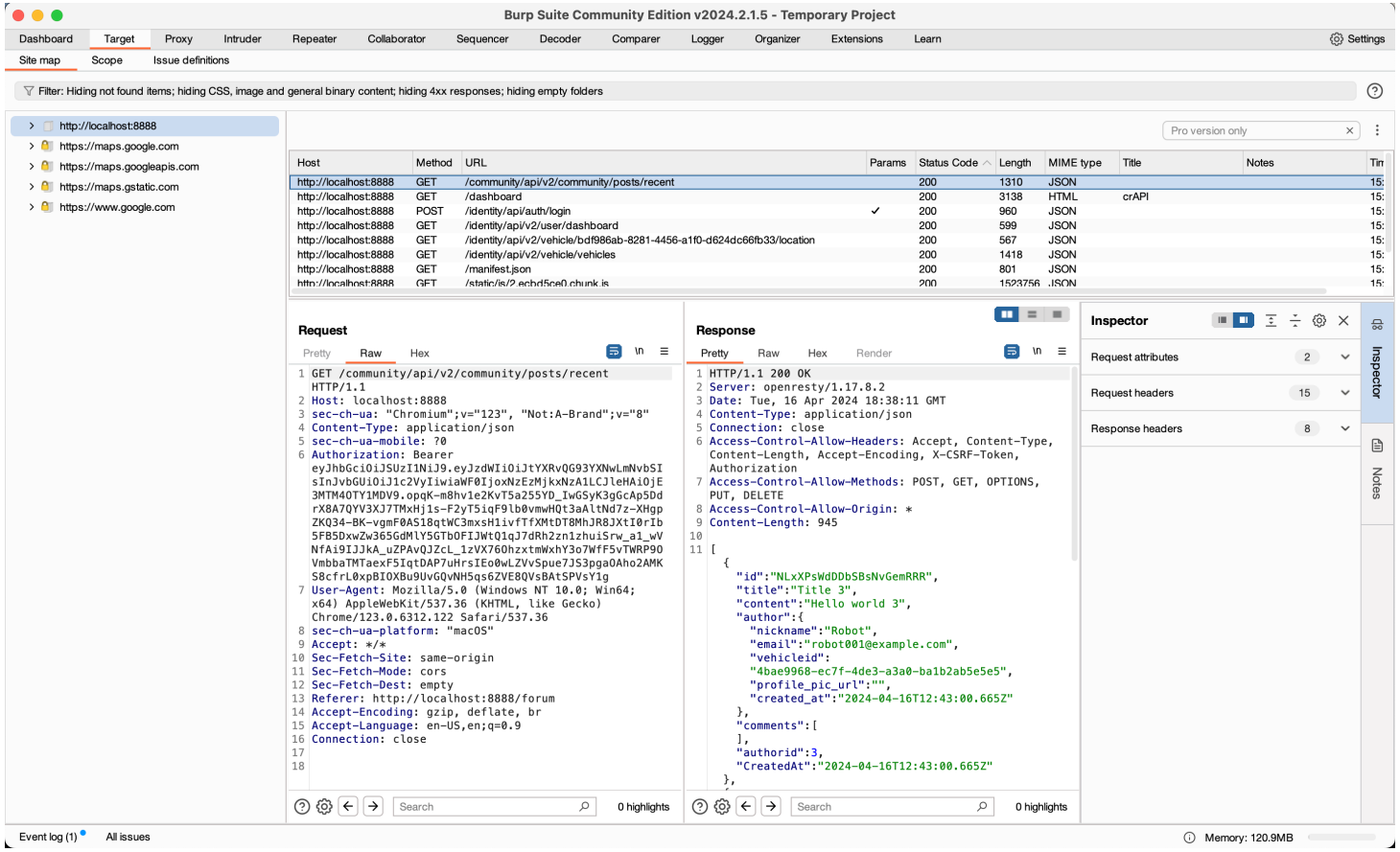
WALKTHROUGH

- Obtengamos la ubicación de otro usuario.
- Vamos a Community



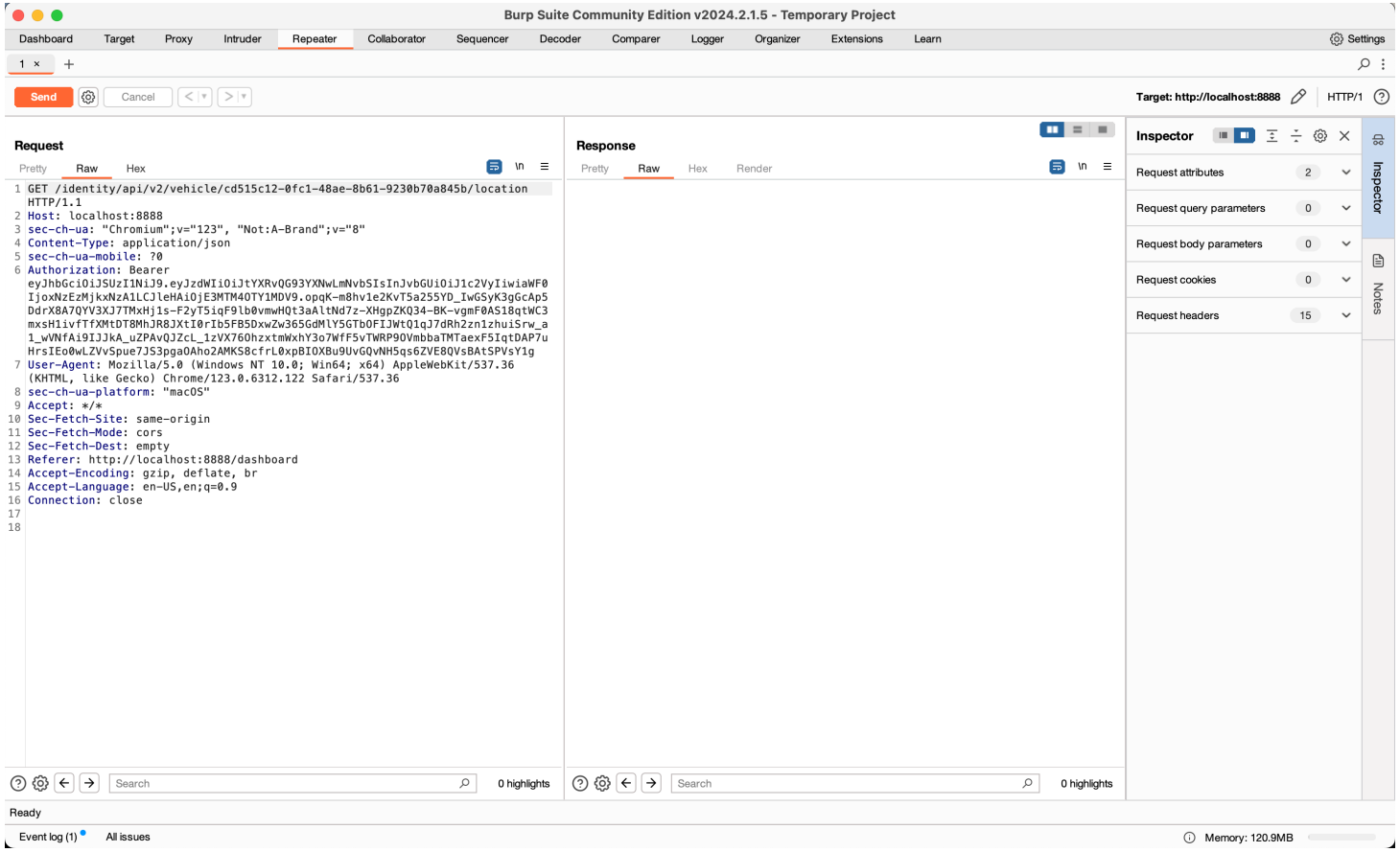
WALKTHROUGH

- Analizamos el request en Burp.
- Vemos que se comparten Vehicle Ids de los usuarios.



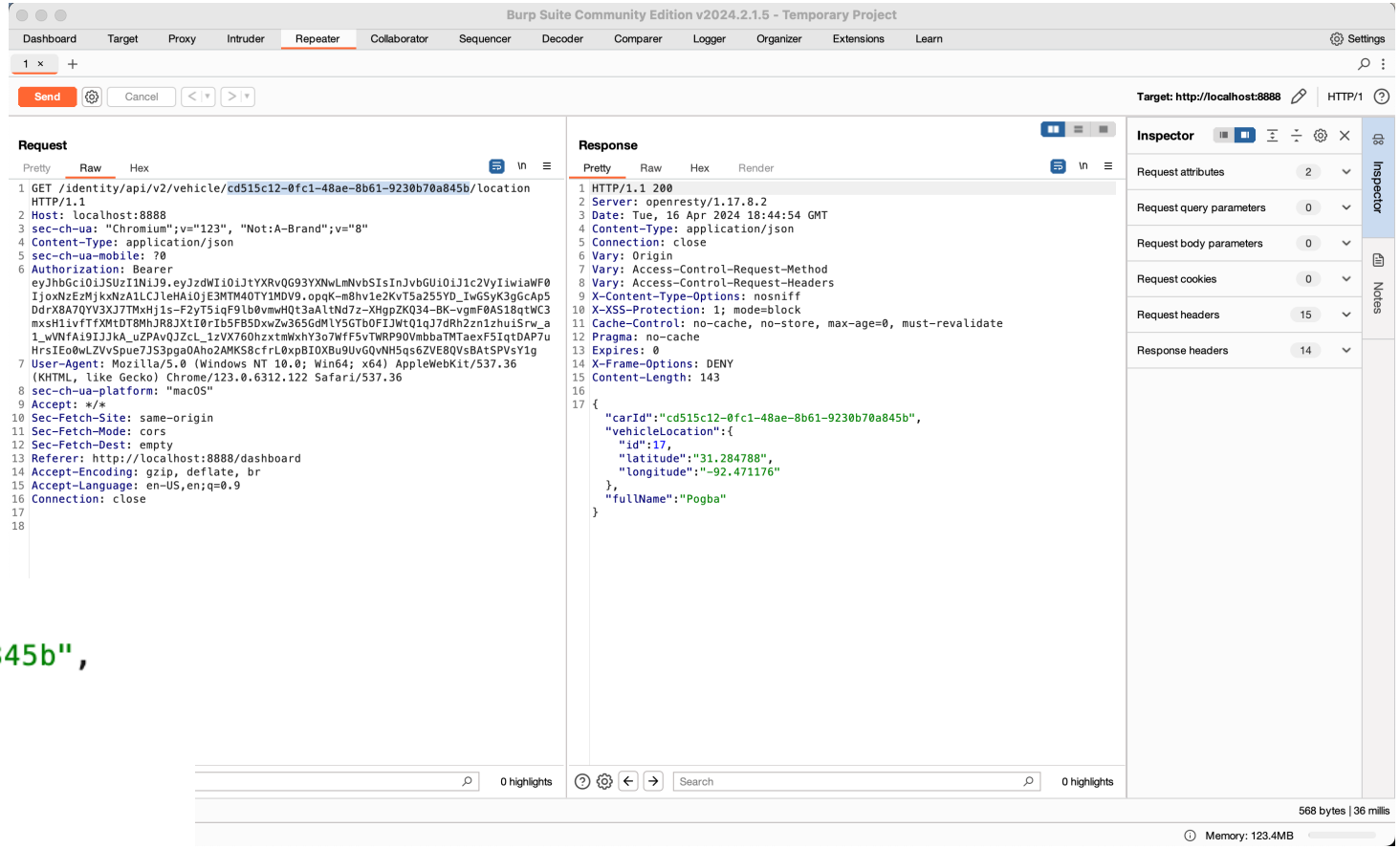
WALKTHROUGH

- Seleccionamos el request de location y lo enviamos al repeater de burp
- Modificamos el id del vehículo por el id objetivo
  Ej: cd515c12-0fc1-48ae-8b61-9230b70a845b



WALKTHROUGH

- Obtenemos como respuesta la ubicación del vehículo objetivo




```
{
  "carId":"cd515c12-0fc1-48ae-8b61-9230b70a845b",
  "vehicleLocation":{
    "id":17,
    "latitude":"31.284788",
    "longitude":"-92.471176"
  },
  "fullName":"Pogba"
}
```

RECURSOS EXTRAS

- Listado de herramientas de Api Security: https://owasp.org/www-community/api_security_tools
- Ejercicios Free: https://application.security/free/owasp-top-10-API
- Repo sobre el workshop: https://github.com/matoferreira/APISecWorkshop

CONTACTO

- mferreira@lugapel.com
- https://www.linkedin.com/in/matoferreira/

FEEDBACK

- https://forms.gle/e6VW2FoWG1KHpgFg7

Q&A