



API Security

Explorando Vulnerabilidades Reales en
Entornos Modernos

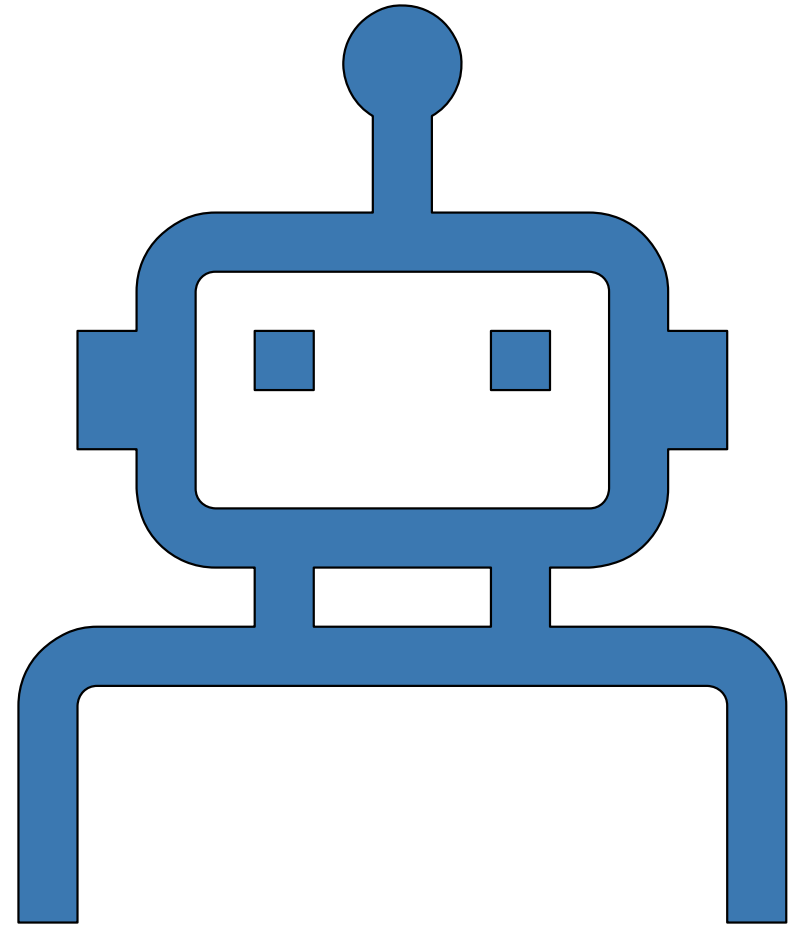
README.MD

- CONSULTOR SENIOR EN LUGAPEL / KRAV MAGA HACKING
- TECHNICAL ACCOUNT MANAGER
- ESPECIALISTA EN CIBERDEFENSA Y OPERACIONES DE CSIRTS (USAF, INCIBE, MDN)
- EX-JEFE DEL CSIRT DE EJÉRCITO
- SPEAKER
- TROTAMUNDOS



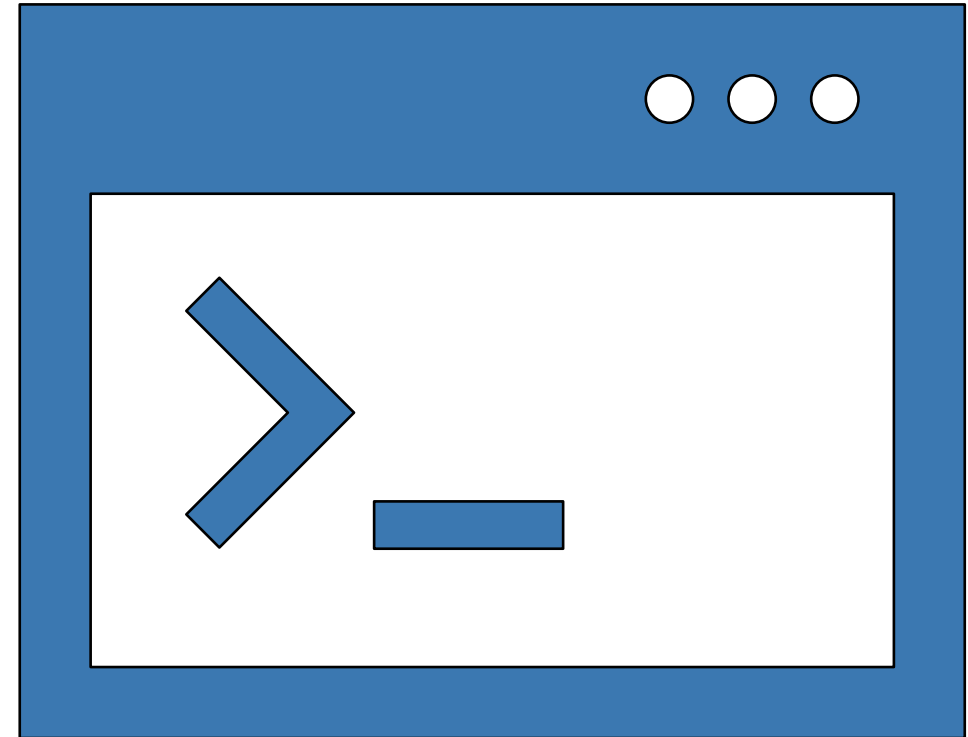
Laboratorio

- Usaremos crAPI
- Simula una web API-Driven, basada en microservicios.
- Contiene vulnerabilidades evidenciadas en aplicaciones modernas de la vida real



Setup

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



Desafíos actuales



92% de las compañías experimentaron un breach debido a una aplicación desarrolladas por ellos.



92% de las compañías han sufrido por lo menos una brecha de seguridad en los últimos 12 meses.



91% de las compañías han desplegado conscientemente aplicaciones vulnerables.

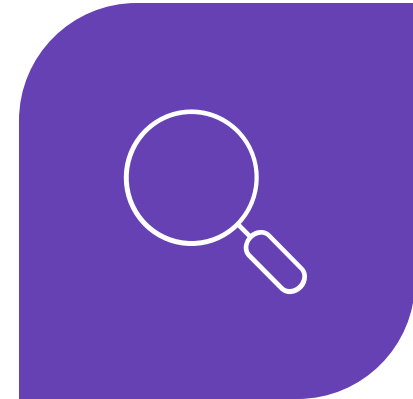
Nuevos desafíos para los CISOs



77% declaran que al menos la mitad del negocio depende de sus aplicaciones.



67% de sus aplicaciones se encuentran hospedadas en la nube.



55% están buscando activamente soluciones que se puedan integrar y automatizar completamente en un ciclo de devops.

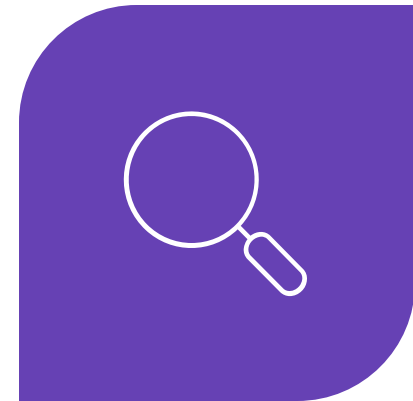
Nuevos desafíos para seguridad



77% declaran que al menos la mitad del negocio depende de sus aplicaciones.



67% de sus aplicaciones se encuentran hospedadas en la nube.



55% están buscando activamente soluciones que se puedan integrar y automatizar completamente en un ciclo de devops.

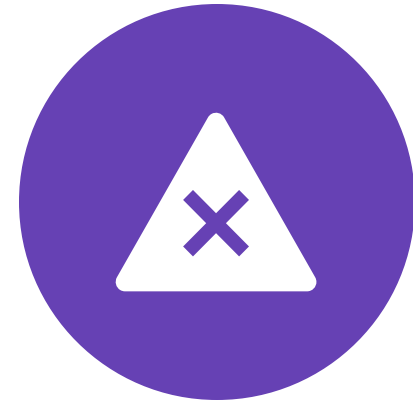
¿Y en producción?



18% - Esperaba que la vulnerabilidad no fuera explotable.



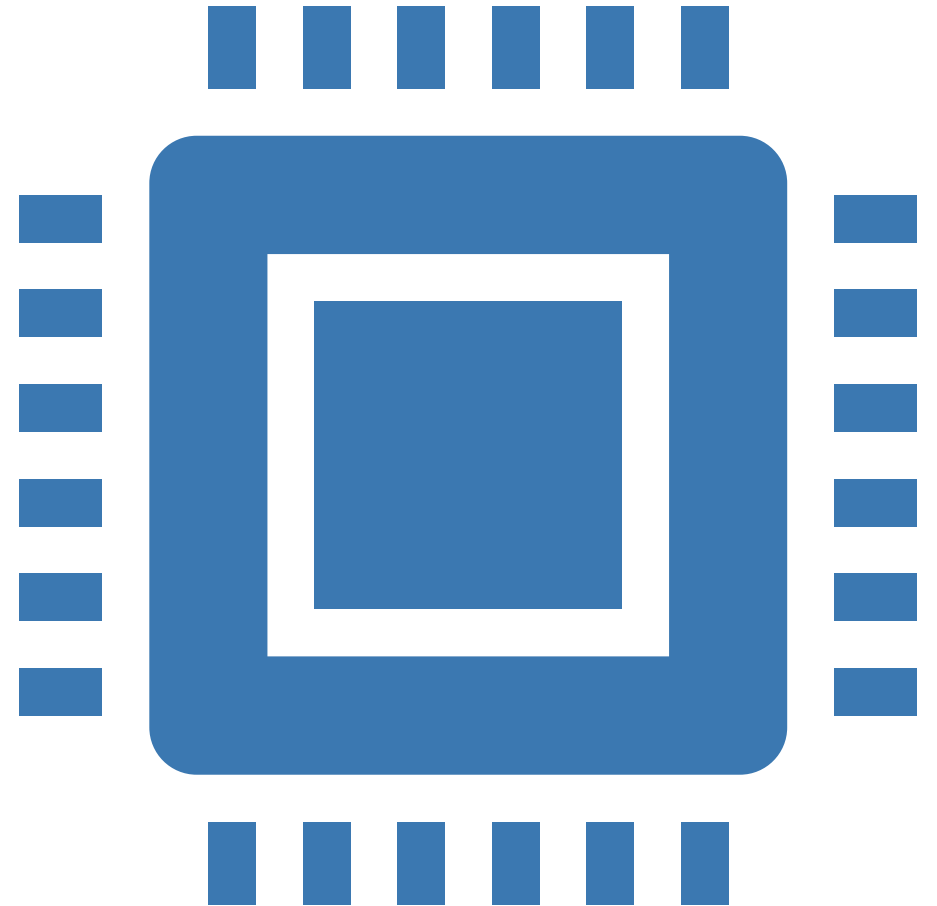
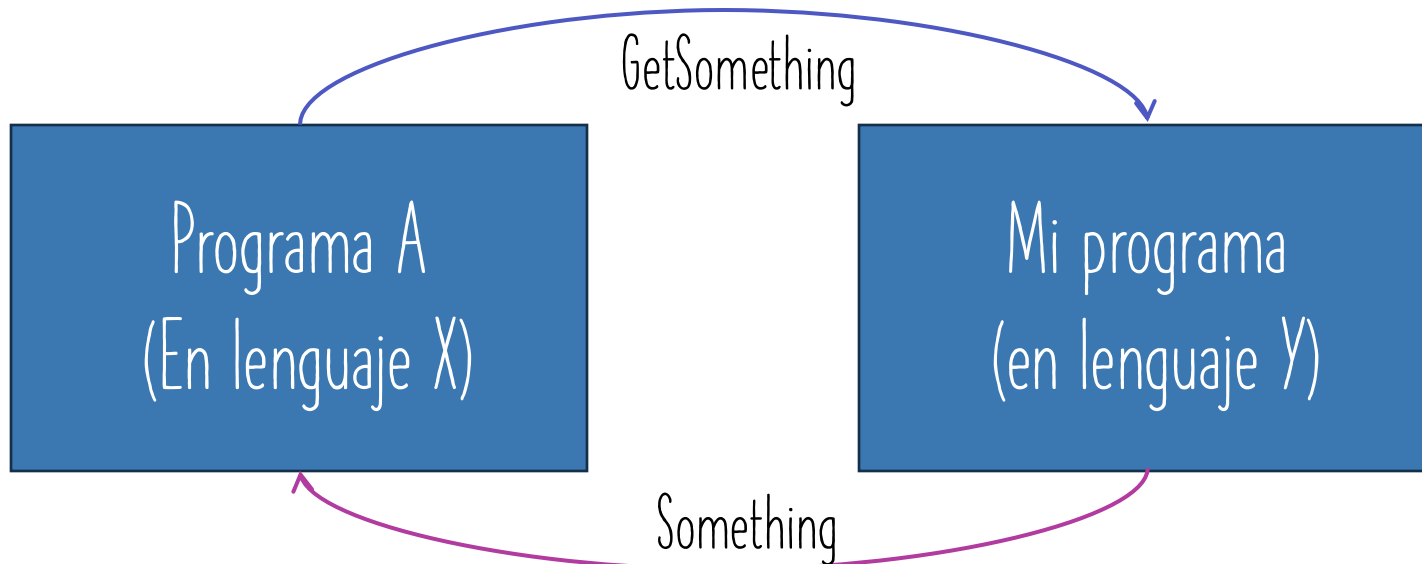
18% - Para cumplir con un deadline de negocio, feature o seguridad.



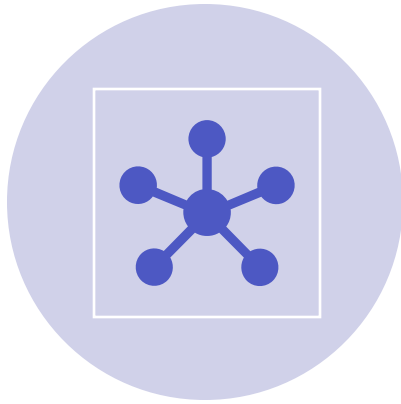
14% - La vulnerabilidad no era explotable.

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

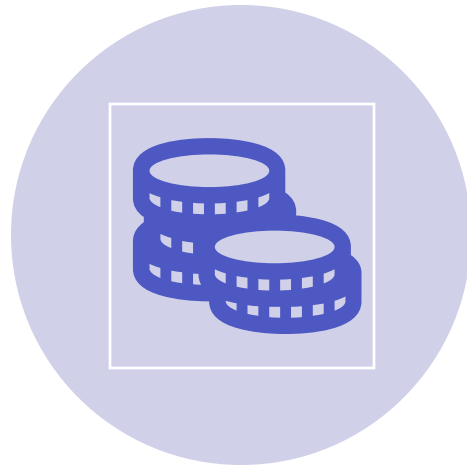


INNOVACIÓN Y ECOSISTEMAS
EN EXPANSIÓN

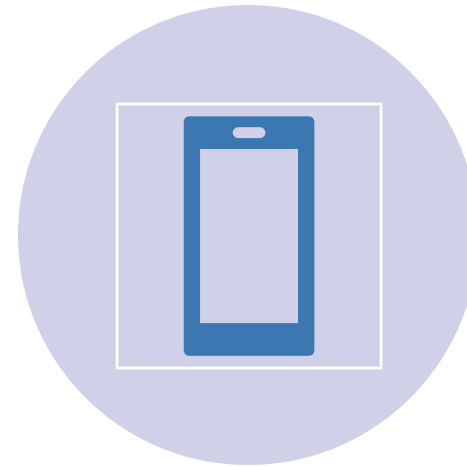


ARQUITECTURA DE
MICROSERVICIOS

El Rol de las APIs en el Desarrollo moderno



IMPACTO ECONÓMICO



APIs COMO
PRODUCTOS



La 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

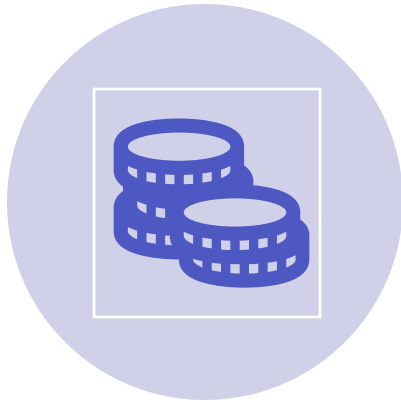


PROBLEMAS
LEGALES



PÉRDIDA DE
CONFIANZA Y
REPUTACIÓN

API Security como necesidad de negocio



IMPACTO
ECONÓMICO



VENTAJA
COMPETITIVA



REGULACIONES Y
CUMPLIMIENTOS

WASP API Security
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



Request

PrettyRawHex

ln

1 GET

/identity/api/v2/vehicle/f89b5f21-7829-45cb-a650-299a61090378/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 eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJtYXRvQGx1Z2FwZWwuY29tIiwicm9sZSI6InVzZXIiLCJpYXQiOiE3MTM3NDYyNTUsImV4cCI6MTcxNDM1MTA1NX0uV3p9gXjFpHA1yhCE6vK_xpc4qrTLvwBTgCx8VE-RqULrea9RH0dxqsPLkBXfz6My8Te20FuD-nax0rgdGF8A4FE0A-JJ5XZmt0CDwM2sCsXWFEzVEQ23m9w0hmyt10bLQX1L0A54DZv7hPLATjT6nAaurZGNG-ZspqNF7psxly9Y6hCftH2ymqdKQo3Qfd8RTXLZ7ZhAlt7Lox6ecHERr5FnK0oWradDQ4REskZ1WXJ9iV5FuRenVpjc-I8gUFceU10DUwF70tdLCh4Y4grI4Fd8rYtQIk3fAVuXp7yqBS_g7uFMFg3EVA66Id9C_ix8uNs2zbYGOPIdILL_L68rzQ

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

Response

PrettyRawHexRender

ln

1 HTTP/1.1 200

2 Server: openresty/1.17.8.2

3 Date: Mon, 22 Apr 2024 00:44:55 GMT

4 Content-Type: application/json

5 Connection: close

6 Vary: Origin

7 Vary: Access-Control-Request-Method

8 Vary: Access-Control-Request-Headers

9 X-Content-Type-Options: nosniff

10 X-XSS-Protection: 1; mode=block

11 Cache-Control: no-cache, no-store, max-age=0, must-revalidate

12 Pragma: no-cache

13 Expires: 0

14 X-Frame-Options: DENY

15 Content-Length: 142

16

17 {

"carId":"f89b5f21-7829-45cb-a650-299a61090378",

"vehicleLocation":{

"id":14,

"latitude":"32.778889",

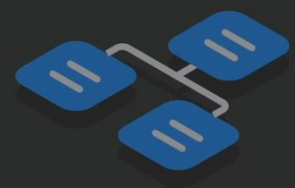
"longitude":"-91.919243"

},

"fullName":"Adam"

}

Broken object level authorization



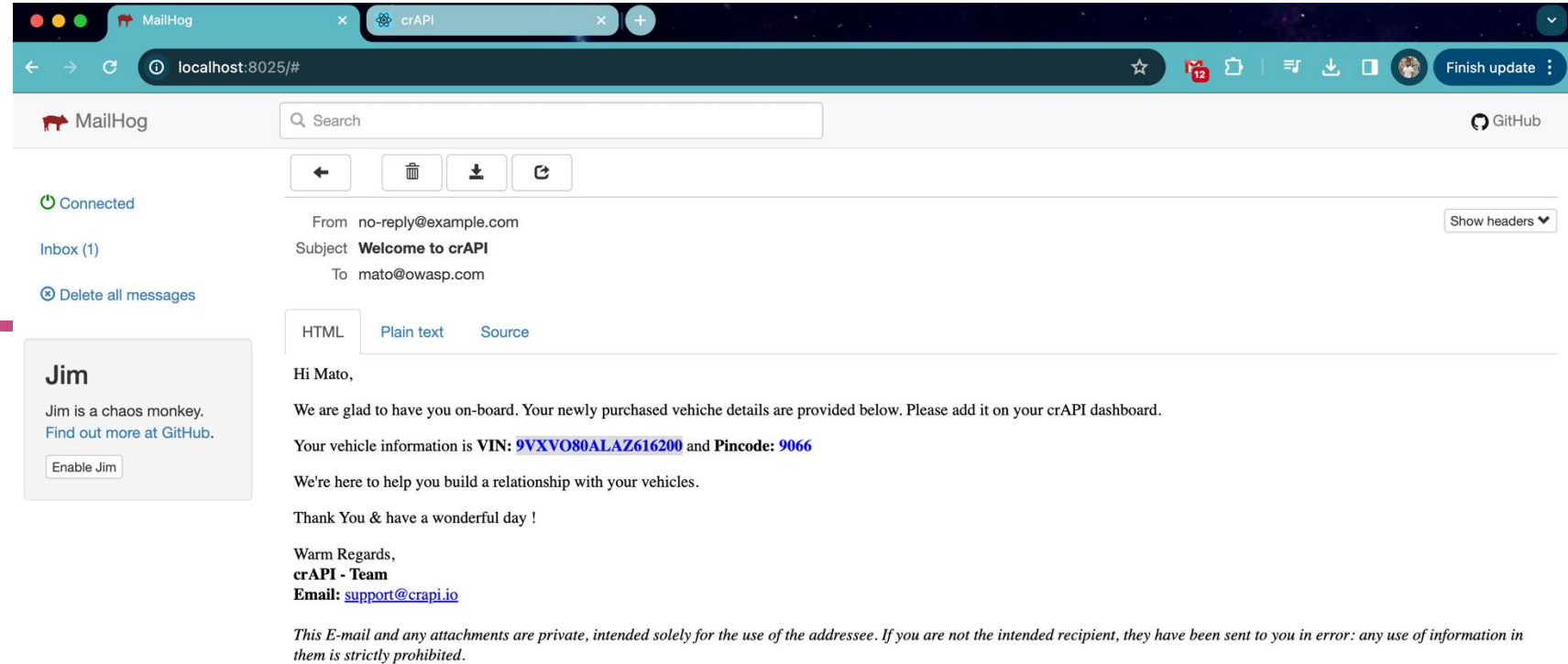
Site map is empty

The site map displays information about the contents of your target applications, along with any issues that have been discovered. This is automatically populated during scans and while you browse using Burp's browser.

[Learn more](#)[Open browser](#)


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



Company : Lamborghini

Model : Aventador

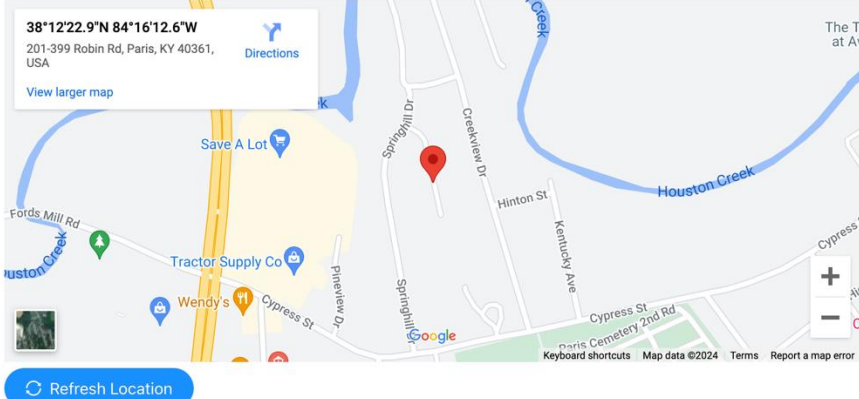
Fuel Type : PETROL

Year : 2024

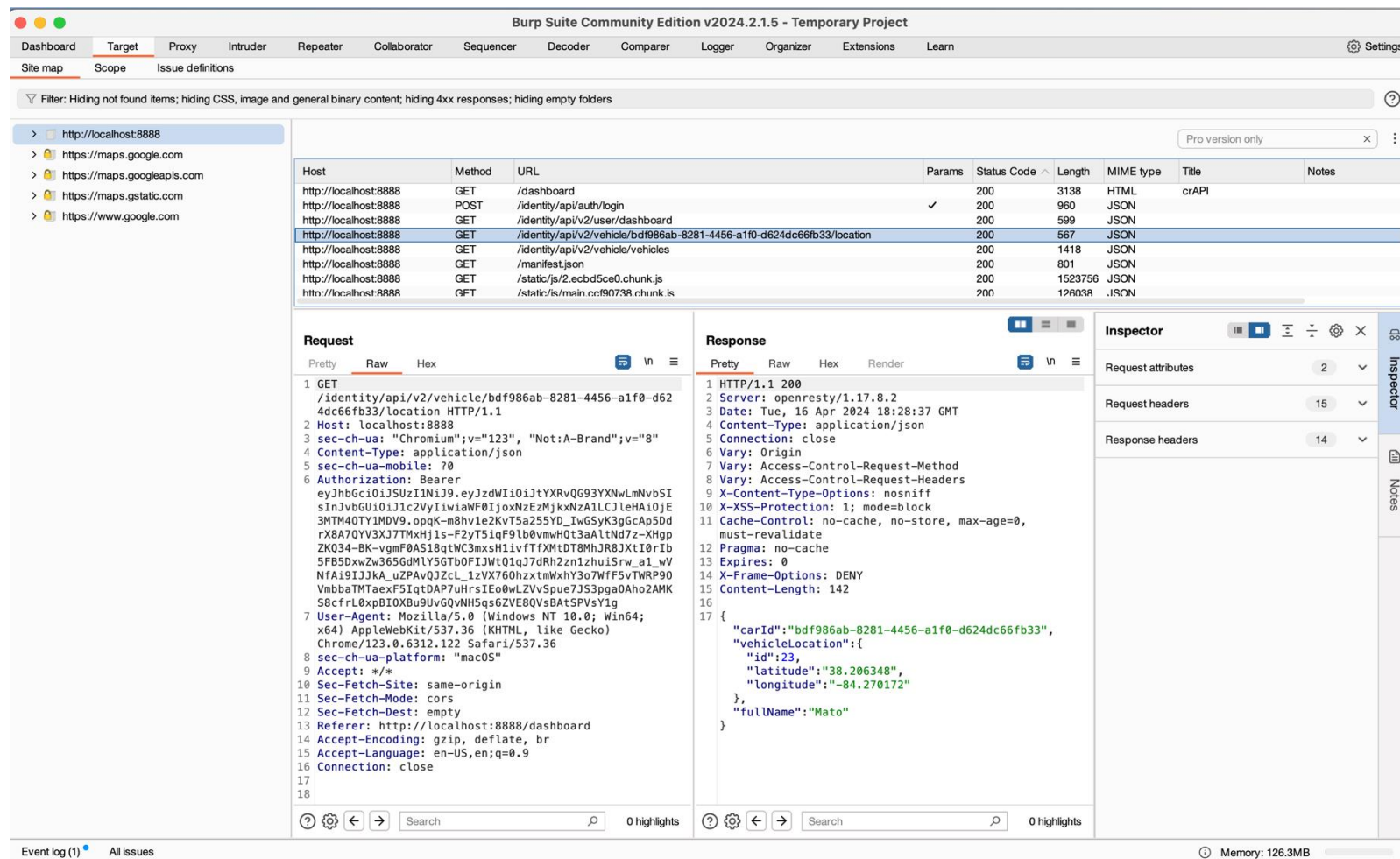
38°12'22.9"N 84°16'12.6"W
201-399 Robin Rd, Paris, KY 40361, USA

Directions

View larger map

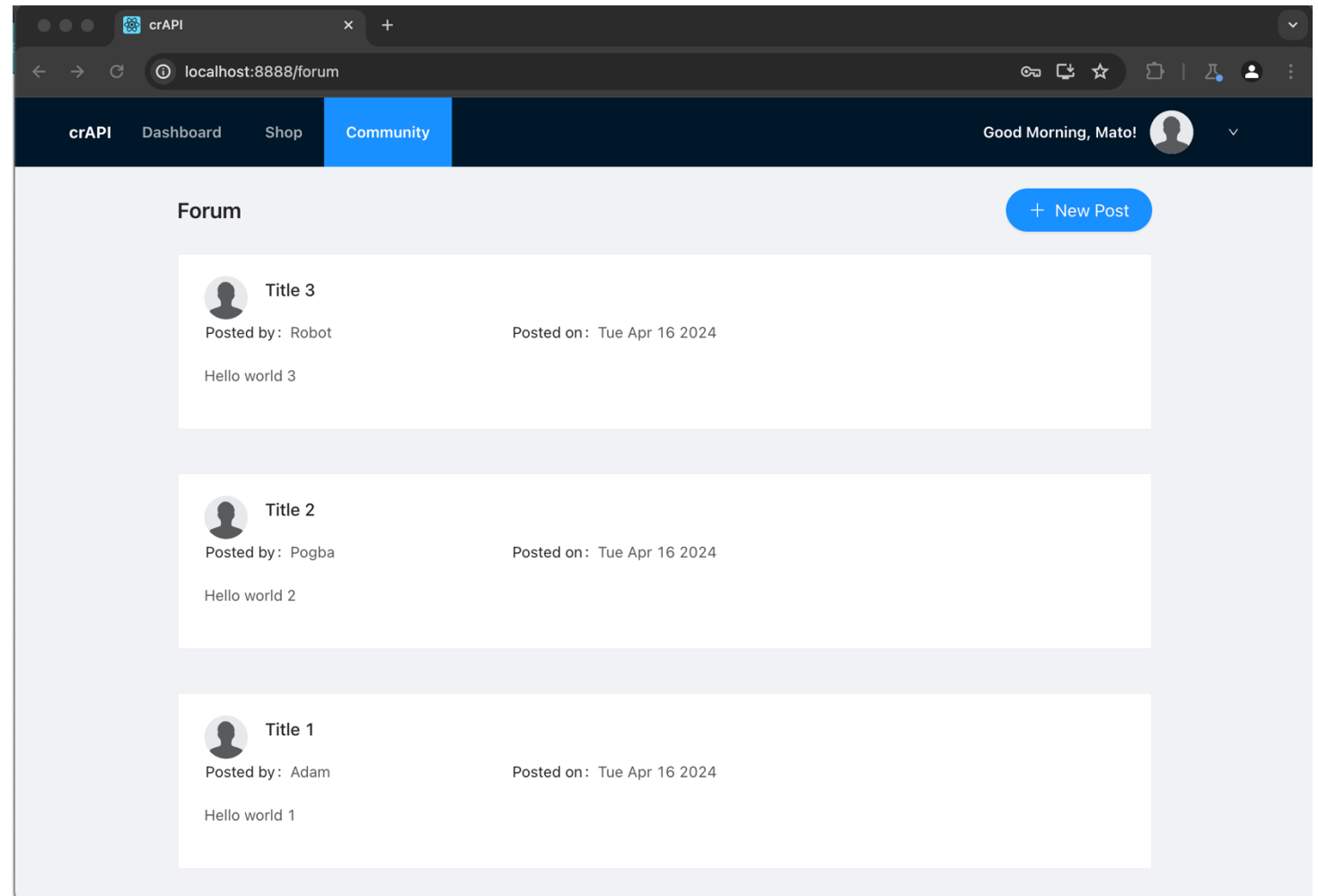


- Analizamos el request
- El endpoint usa el id de vehículo
- GET
/identity/api/v2/vehicle/bdf986ab-8281-4456-a1f0-d624dc66fb33/location



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.

The screenshot displays the Burp Suite Community Edition v2024.2.1.5 interface. The top menu bar includes options like Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The 'Target' tab is active, showing a list of targets on the left, including http://localhost:8888, https://maps.google.com, https://maps.googleapis.com, https://maps.gstatic.com, and https://www.google.com.

The main panel shows a list of requests. The selected request is a GET request to /community/api/v2/community/posts/recent. The response is a JSON object containing user information, including a vehicle ID.

Request Details:

```
1 GET /community/api/v2/community/posts/recent
2 HTTP/1.1
3 Host: localhost:8888
4 sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"
5 Content-Type: application/json
6 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpzZXQ6OTY3YXNwLmNvbSI...
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
```

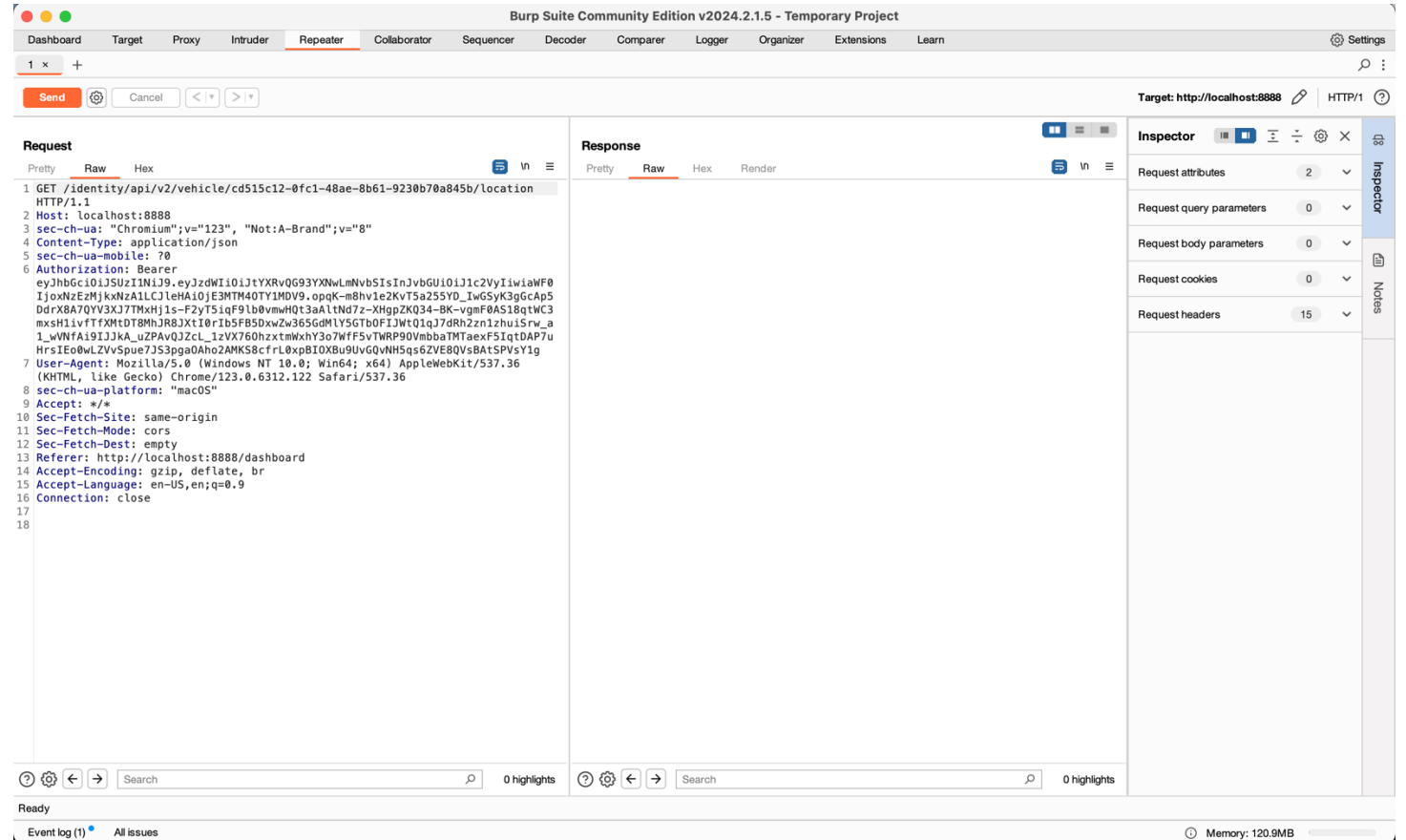
Response Details:

```
1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Tue, 16 Apr 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 {
  "id": "NLxP5wDdbSBsNvGemRRR",
  "title": "Title 3",
  "content": "Hello world 3",
  "author": {
    "nickname": "Robot",
    "email": "robot001@example.com",
    "vehicleId": "4bae9968-ec7f-4de3-a3a0-ba1b2ab5e5e5",
    "profile_pic_url": "",
    "created_at": "2024-04-16T12:43:00.665Z"
  },
  "comments": [
  ],
  "authorId": 3,
  "CreatedAt": "2024-04-16T12:43:00.665Z"
},
12
```

The right sidebar shows the 'Inspector' tab, which displays the request and response headers and body. The status bar at the bottom indicates 'Memory: 120.9MB'.

Walkthrough

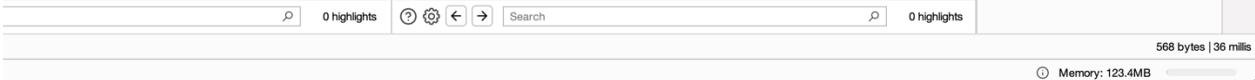
- Seleccionamos el request de location y lo enviamos al repeater de burp
- Modificamos el id del vehículo por el id objetivo
Ej: cd515c12-0fc1-48ae-8b61-9230b70a845b



- Obtenemos como respuesta la ubicación del vehículo objetivo

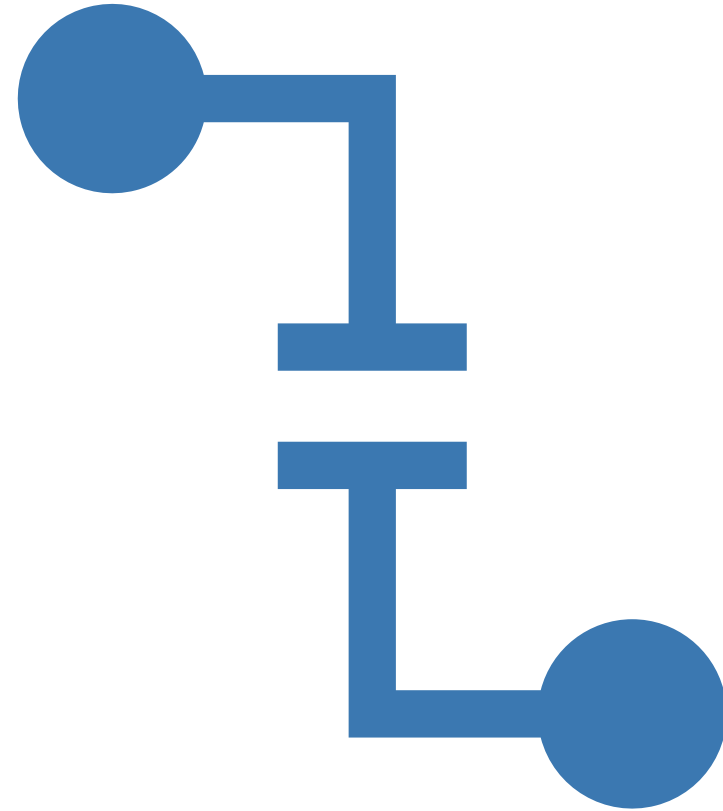
- Obtenemos como respuesta la ubicación del vehículo objetivo

} |



Acceso sin restricción a recursos, funciones y flujos

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



Broken authentication

4. Intruder attack of http://localhost:8888

Attack ▾ Save ▾ ⏸ ?

Results Positions Payloads Resource pool Settings

Filter: Showing all items

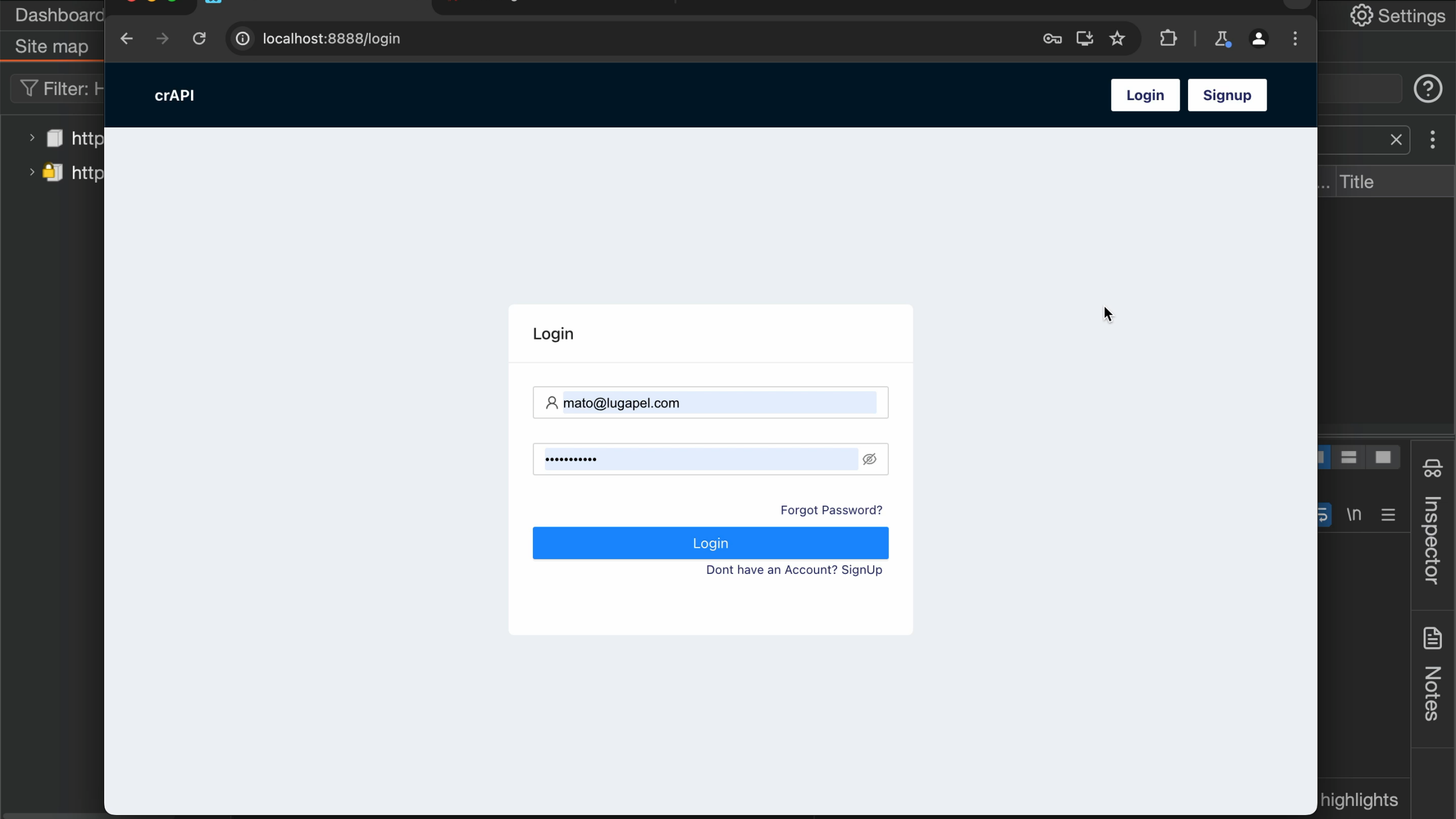
Request	Payload	Status code ^	Response recei...	Error	Timeout	Length	Comment
20	1809	200	141			500	
107	1896	500	23			519	
106	1895	500	19			519	
105	1894	500	18			519	
104	1893	500	23			519	
103	1892	500	21			519	
102	1891	500	24			519	
101	1890	500	20			519	
100	1889	500	17			519	
99	1888	500	139			519	
98	1887	500	18			519	
97	1886	500	22			519	

Request Response

Pretty Raw Hex

```
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:8888/forgot-password
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Connection: keep-alive
18
19 {
  "email": "mato@owasp.com",
  "otp": "1809",
  "password": "test1234!"
}
```

108 of 8210 0 highlights



Vehicles Details

VIN: 6SZPE30HTVG569861

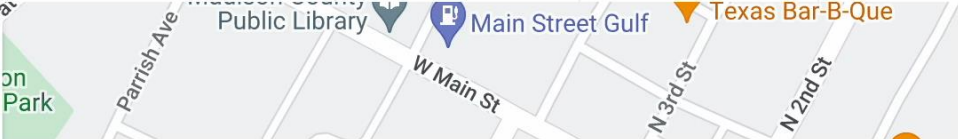
Contact Mechanic



Company :	MG Motor
Model :	Hector Plus
Fuel Type :	PETROL
Year :	2024

37°44'48.8"N 84°18'05.3"W
323 High St, Richmond, KY 40475, USA

Directions



Request

Pretty

Raw

Hex

1

POST /identity/api/auth/forget-password HTTP/1.1

2

Host: localhost:8888

3

Content-Length: 26

4

sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"

5

sec-ch-ua-platform: "macOS"

6

sec-ch-ua-mobile: ?0

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

Content-Type: application/json

9

Accept: */*

10

Origin: http://localhost:8888

11

Sec-Fetch-Site: same-origin

12

Sec-Fetch-Mode: cors

13

Sec-Fetch-Dest: empty

14

Referer: http://localhost:8888/forgot-password

15

Accept-Encoding: gzip, deflate, br

16

Accept-Language: en-US,en;q=0.9

17

Connection: close

18

19

{

"email": "mato@owasp.com"

}

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 200

2

Server: openresty/1.17.8.2

3

Date: Mon, 22 Apr 2024 15:45:16 GMT

4

Content-Type: application/json

5

Connection: close

6

Vary: Origin

7

Vary: Access-Control-Request-Method

8

Vary: Access-Control-Request-Headers

9

Access-Control-Allow-Origin: *

10

X-Content-Type-Options: nosniff

11

X-XSS-Protection: 1; mode=block

12

Cache-Control: no-cache, no-store, max-age=0, must-revalidate

13

Pragma: no-cache

14

Expires: 0

15

X-Frame-Options: DENY

16

Content-Length: 73

17

18

{

"message": "OTP Sent on the provided email, mato@owasp.com",

"status": 200

}

Inspector

Request attributes

2

▼

Request query parameters

0

▼

Request cookies

0

▼

Request headers

16

▼

Response headers

15

▼

Inspector

Notes

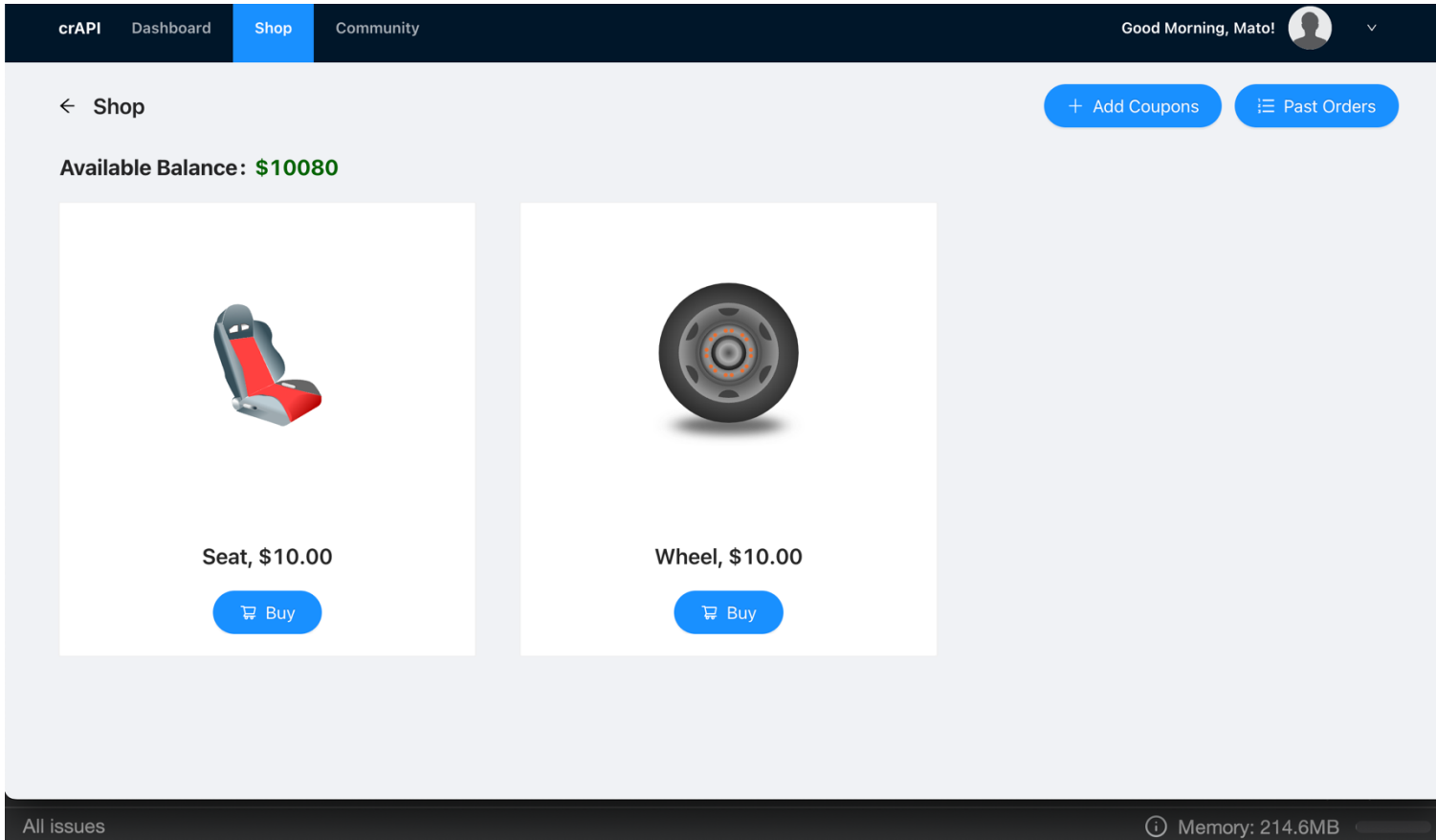
0 highlights

0 highlights

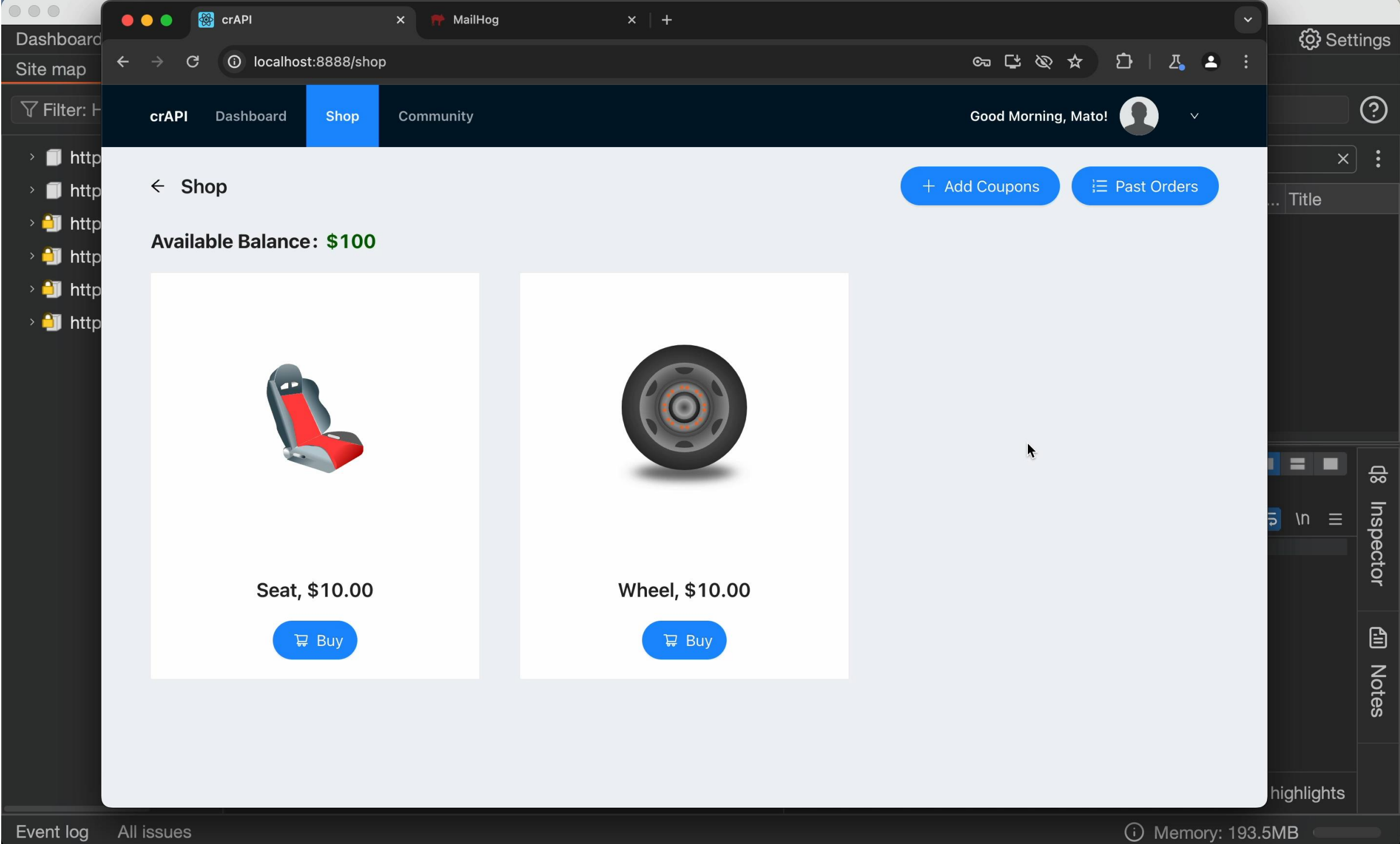
Ausencia de validación, errores de configuración, Manejo inapropiado de inventario y recursos

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





Broken Object Property Level Authorization



DashboardSite map

Filter: H

> http

> http

> http

> http

> http

> http

Event logAll issues

crAPI

MailHog

localhost:8888/shop

crAPIDashboardShopCommunity

Good Morning, Mato!

Settings

?

×

Title

Inspector

Notes


highlights

← Shop

+ Add Coupons


☰ Past Orders

Available Balance: \$90



Seat, \$10.00

Buy



Wheel, \$10.00

Buy

DashboardSite mapFilter: H


crAPIDashboardShopCommunity

Good Morning, Mato!

← Shop


+ Add CouponsPast Orders

Available Balance: \$90



Seat, \$10.00

Buy



Wheel, \$10.00

Buy

Settings

InspectorNotes

Event logAll issuesMemory: 198.8MB

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

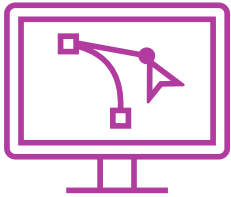


Validación de datos
y sanitización



Implementación de
Throttling y Rate
Limiting

Necesidad de análisis



API Security
Posture



API Security
Testing



API Security
Runtime

Key takeaways

Business

Cloud

DevSecOps

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/>

