

PE-2.3: Seguridad Avanzada en APIs

Laboratorio de Programación de Microservicios Basados en Datos

Estudiante: Luis Eduardo Poma Medina

Configuración Auth0

Domain: No proporcionado

Client ID: No proporcionado

Checkpoints Completados

- ' 1.1 Env preparado y copiado
- ' 1.2 package.json type:module
- ' 1.3 tsconfig.json ESNext
- ' 1.4 Imports con extensión .js
- ' 2.1 Deps de seguridad instaladas
- ' 2.2 Hardening (Helmet/Rate-Limit) implementado
- ' 2.3 Configuración .env, Cookies y JWT
- ' 3.1 Decorador authenticate implementado
- ' 3.2 Auth0 y Rutas registradas

Evidencias de Pruebas

Test 401 Unauthorized:

```
{  
  "statusCode": 401,  
  "error": "Unauthorized",  
  "message": "Token JWT inválido o no proporcionado. Por favor, autentícate en /login"  
}
```

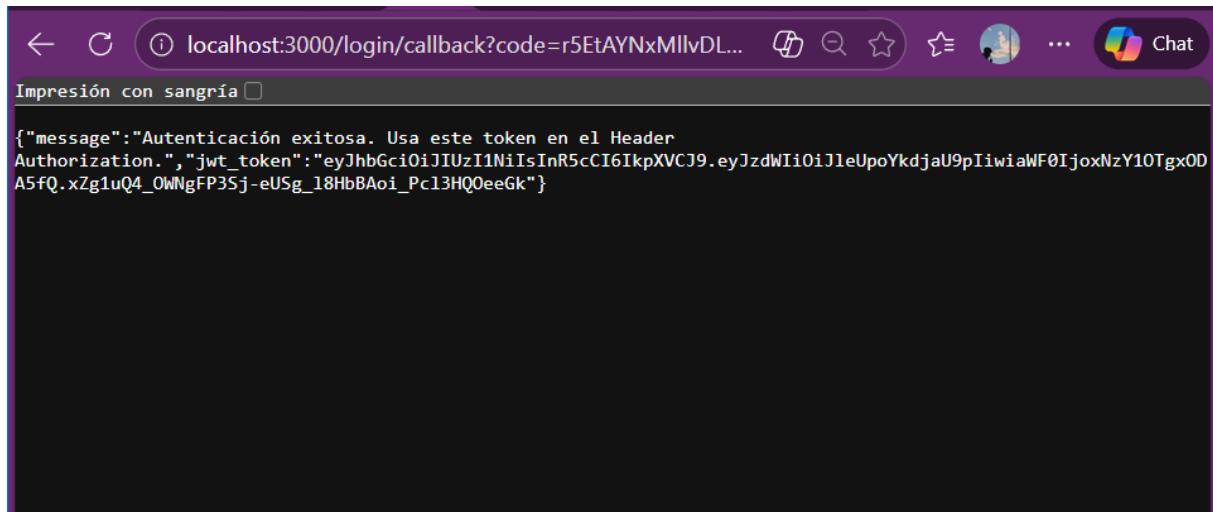
Test 200 OK con JWT:

```
{  
  "result": 18,  
  "operation": "multiply"  
}
```

Análisis y Conclusiones

El Helmet añade headers de protección evitando evita sniffing de MIME y reforzando políticas de seguridad, y el Rate Limit evita el abuso de peticiones haciendo que este colapse y de esa manera protege a tu servidor de posibles ataques como son los ataques de fuerza bruta

Evidencia de Login (Token)



A screenshot of a web browser window titled "localhost:3000/login/callback?code=r5EtAYNxMllvDL...". The main content area displays a JSON object with the following message and token:

```
{"message": "Autenticación exitosa. Usa este token en el Header Authorization.", "jwt_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJleUpoYkdjaU9pIiwiaWF0IjoxNzY1OTgxODA5fQ.xZg1uQ4_0WNgFP3Sj-eUSg_l8HbBAoi_Pcl3HQ0eeGk"}
```