PE-2.3: Seguridad Avanzada en APIs

Laboratorio de Programación de Microservicios Basados en Datos

Configuración Auth0

Domain: No proporcionado

Client ID: No proporcionado

Checkpoints Completados

- [x] Node.js verificado y proyecto copiado
- [x] Dependencias de seguridad instaladas
- [x] Migración a ESM completada
- [x] Auth0 configurado
- [x] Archivo .env creado
- [x] Rutas protegidas con JWT
- [x] Rate Limiting verificado
- [x] Headers de seguridad verificados

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": 4,
  "operation": "add"
}
```


Análisis y Conclusiones

Gracias a esta practica pudimos ver como delegar la autenticación a un proveedor como Auth0 facilita el manejo de usuarios y reduce riesgos, ya que no es necesario administrar directamente contraseñas en el sistema. Además, vimso otras herramientas como Helmet ayudan a reforzar la seguridad básica de la API mediante configuraciones automáticas, mientras que el rate limiting evita abusos al controlar la cantidad de solicitudes. En conjunto, estas medidas permiten que la API sea más segura y estable sin complicar el desarrollo.