Seguridad básica: despliegue y prueba

Implementa la seguridad de tu API Rest con Spring Boot



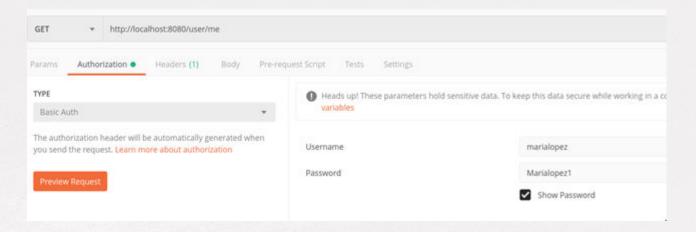
Comprobemos que nuestra API funciona

- POSTMAN o curl
- Probamos a hacer una petición sin autenticación
 - Debemos obtener un error 401
- Probamos a hacer una petición autenticados como USER
- Probamos a hacer una petición autenticados como ADMIN



POSTMAN

Petición con datos correctos





POSTMAN

• Si pulsamos *Preview Request* podemos ver la cabecera generada antes de enviar la petición.

GET + http://localhost:8080/user/me			
Params Authorization • Headers (1) Body Pre-request Script Tests Settings			
▼ Headers (0)			
KEY	VALUE	DESCRIPTION	
Key	Value	Description	
▼ Temporary Headers (1)			
KEY	VALUE	VALUE	
Authorization	Basic bWFyaWFsb3BfejpNYXjpYt	Basic bWFyaWFsb3BiejpNYXlpYWxxcGV6MQ==	

POSTMAN issue

- A día de hoy, POSTMAN tiene algunas dificultades con la autenticación Básica
- En ocasiones, una vez ejecutado el programa, solo nos dejará utilizar las primeras credenciales que usemos.
- Las peticiones siguientes, aunque modifiquemos las credenciales, se realizarán con las primeras que hayamos utilizado.
- Mientras solucionan, podemos utilizar curl

Error 403

- Se produce cuando estamos correctamente autenticados, pero no tenemos privilegio (ROL) para hacer una determinada tarea.
- El error producido tiene el formato estándar
- Si lo queremos modificar, necesitamos proporcionar un AccessDeniedHandler personalizado.
- Refactorizamos para incluirlo, siguiendo el esquema utilizado con el AuthenticationEntryPoint.