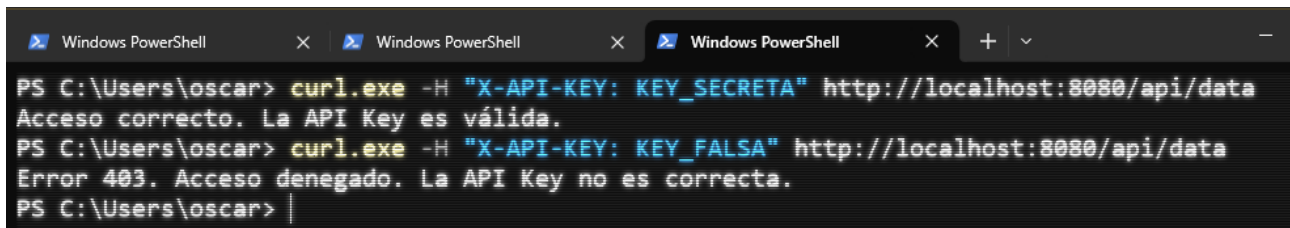


Seguridad en APIs mediante KEY

En mi caso he definido mi API Key como "KEY_SECRETA" y, como podemos ver, el acceso funciona correctamente.



```
PS C:\Users\oscar> curl.exe -H "X-API-KEY: KEY_SECRETA" http://localhost:8080/api/data
Acceso correcto. La API Key es válida.
PS C:\Users\oscar> curl.exe -H "X-API-KEY: KEY_FALSA" http://localhost:8080/api/data
Error 403. Acceso denegado. La API Key no es correcta.
PS C:\Users\oscar> |
```

Dejo adjunto el proyecto, el cual simplemente se debe ejecutar con *mvn spring-boot:run* en el terminal y, desde otro terminal, podremos enviar las cabeceras con curl como en la imagen.

El proyecto consta de un Main y 3 Clases:

- ApiController: Define el endpoint /api/data que responde con éxito si la API Key es válida.
- ApiKeyFilter: Intercepta las solicitudes entrantes, valida la API Key en la cabecera y devuelve 403 si es incorrecta.
- SecurityConfig: Configura la seguridad de Spring Boot, registra el filtro y permite que las solicitudes lleguen al endpoint protegido.

También el pom.xml con las dependencias correspondientes y el application.properties para definir el puerto y la API Key.