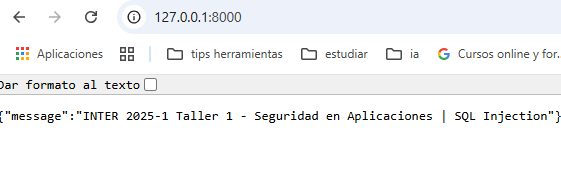
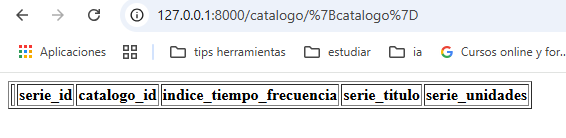
**Taller: Inyección SQL Básica – Practica**

**Se documenta el proceso de inyección**

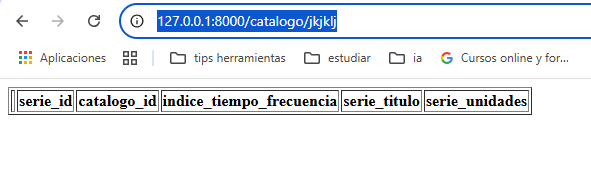
1. Mensaje de Bienvenida



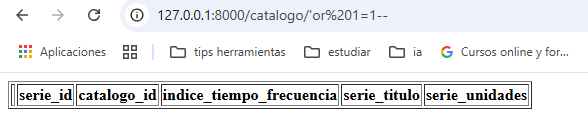
1. Se utiliza /catalogo/{catalogo} Mostrando solo los títulos de las columnas



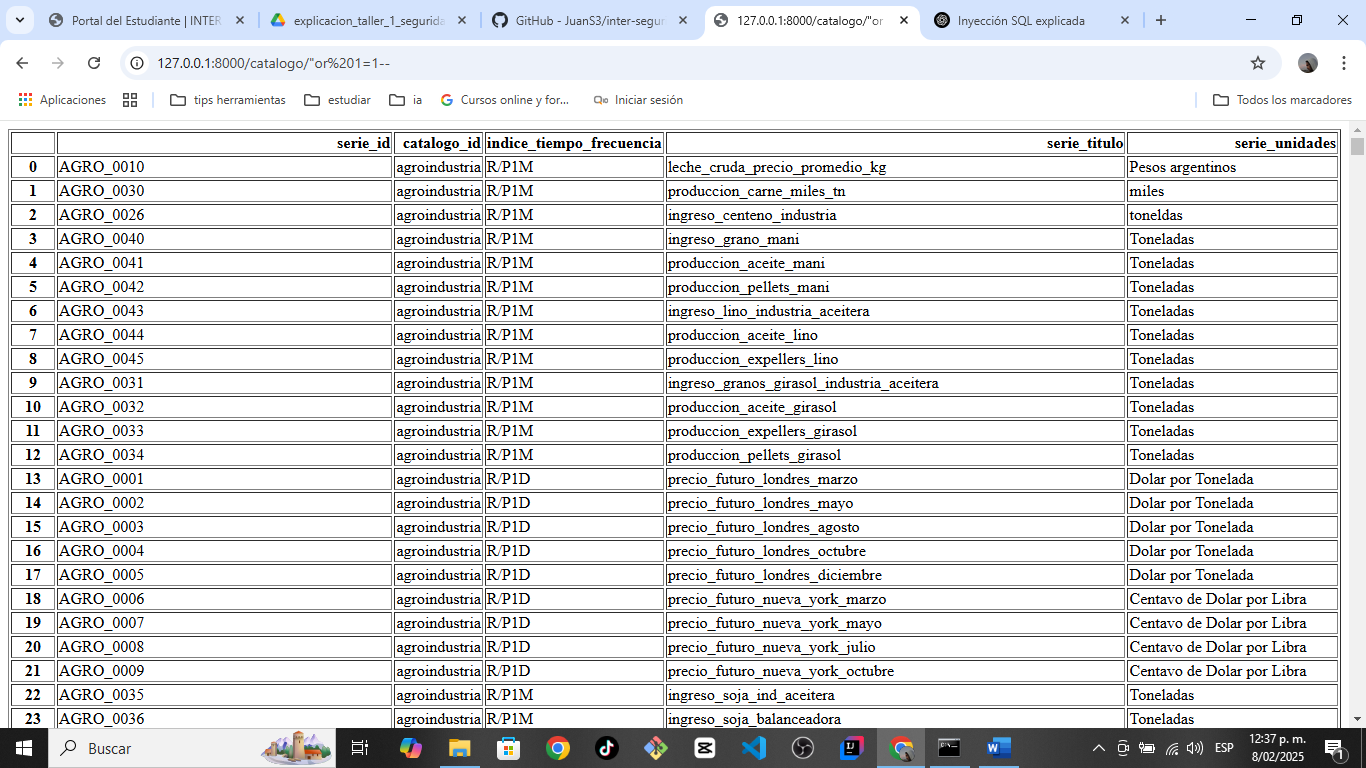
1. Se utiliza <http://127.0.0.1:8000/catalogo/jkjklj> Mostrando solo los títulos de las columnas

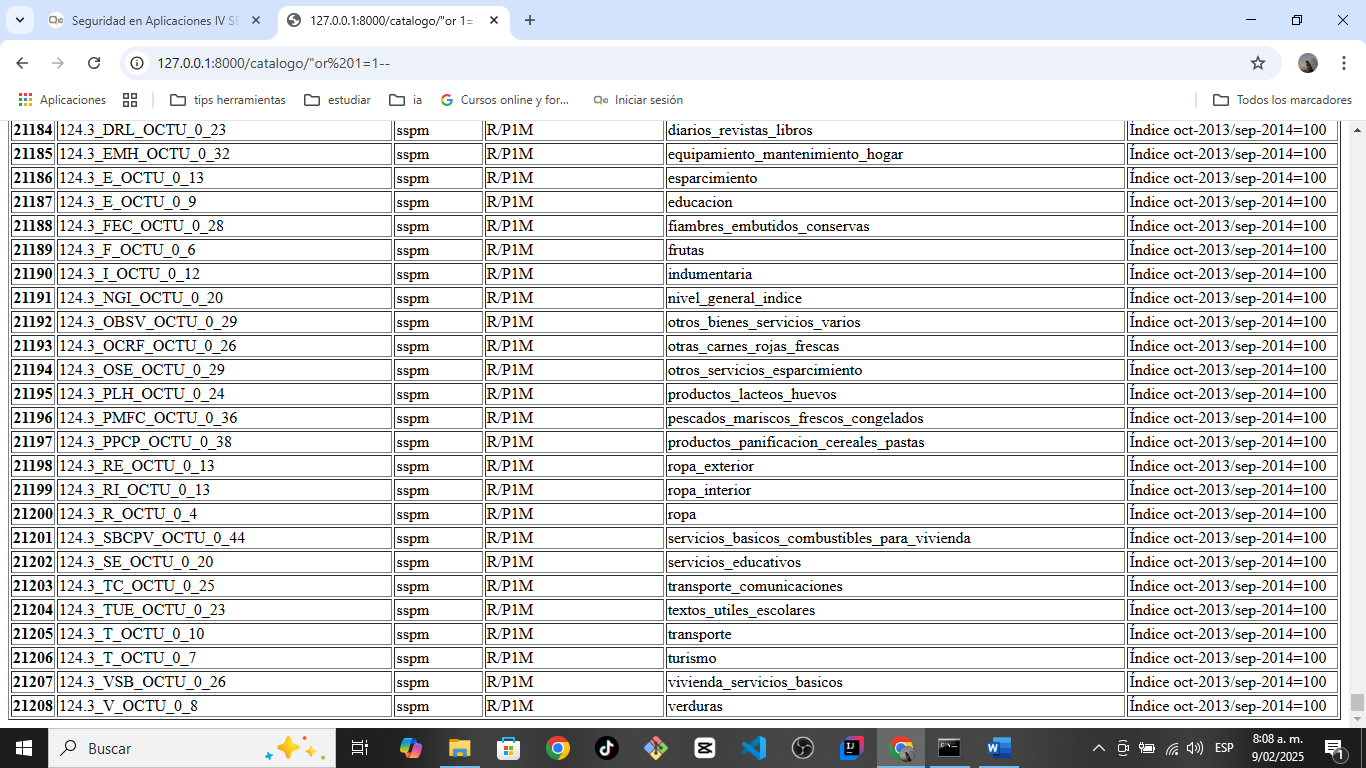


1. Para inyectar código se hizo pruebas con 'or 1=1— mostrando solo los títulos de las columnas

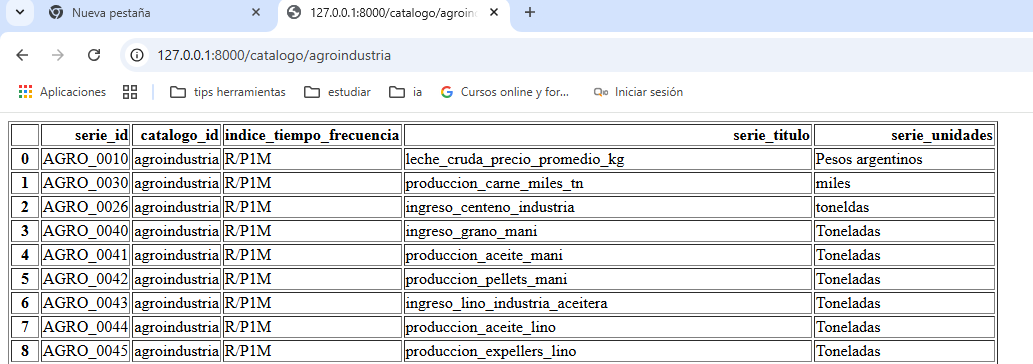


1. Cuando se usa con comillas doble "or 1=1-- si entrega información se mostró toda la información de la tabla mostrando principalmente las siguientes categorías AGROINDUSTRIA / DEFENSA / ENERGIA / SALUD / SIEP /SSPM

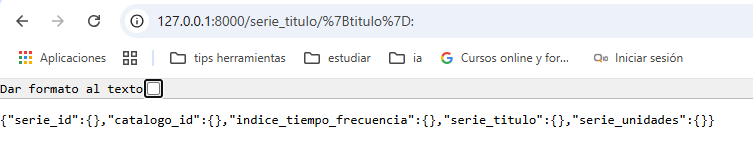




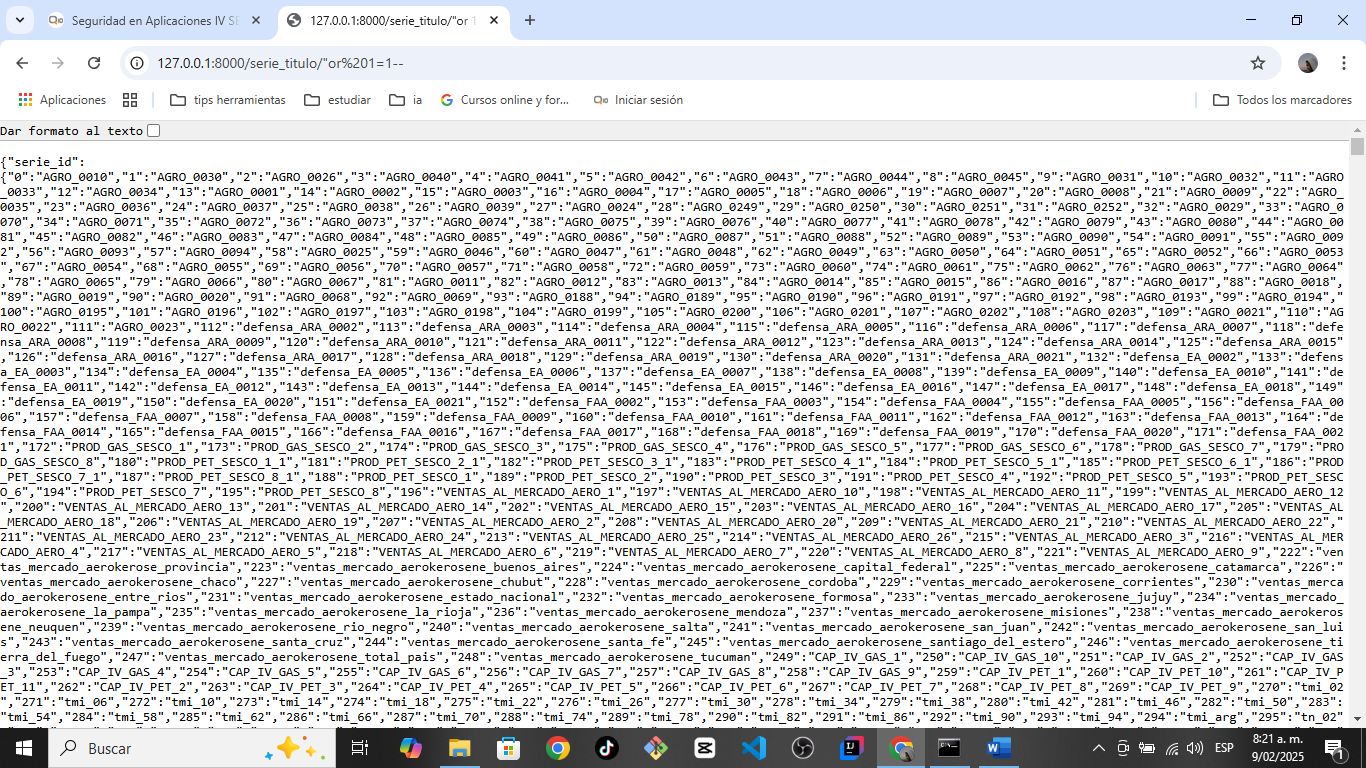
1. Ya teniendo la base completa se puede empezar a filtrar por el nombre del catálogo ejemplo agroindustria



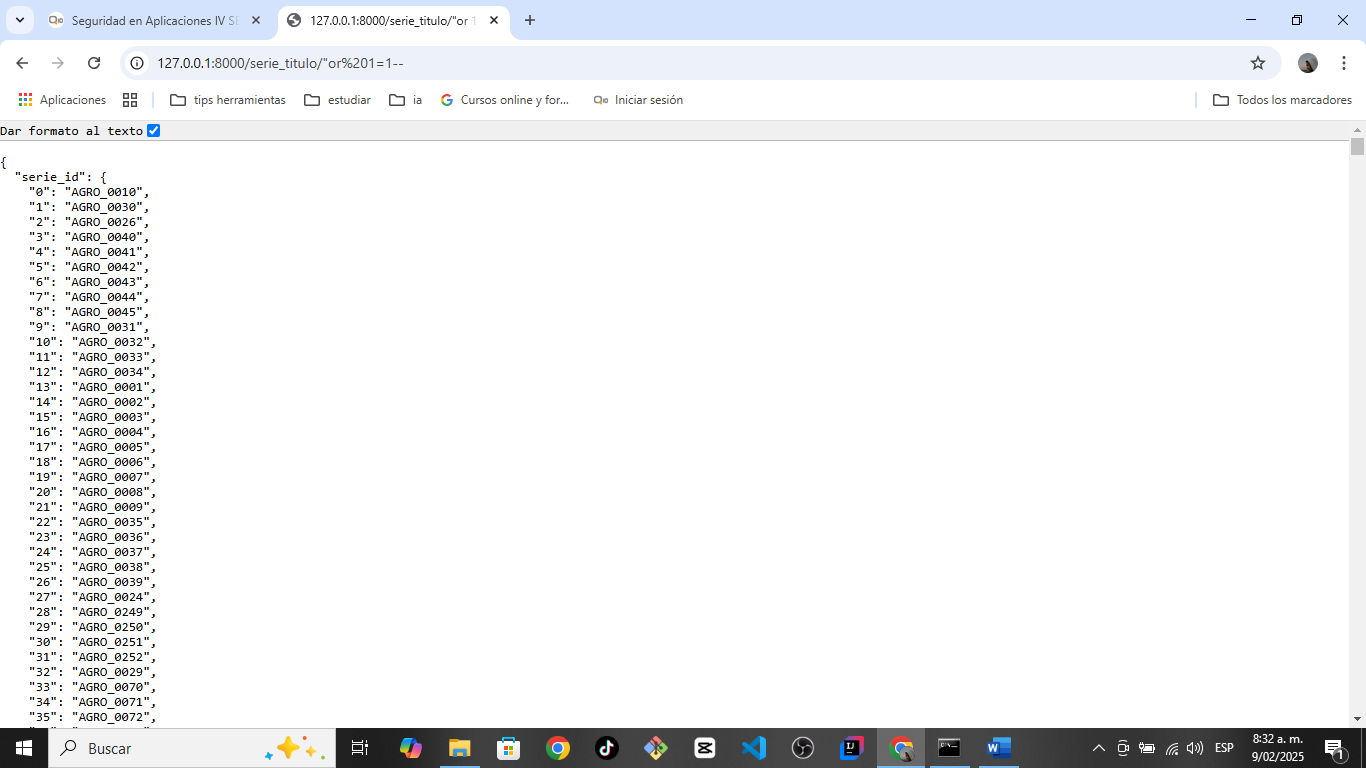
1. Ahora se utilizara el end point /serie\_titulo/{titulo}:  Mostrando un jason sin ningún contenido adentro



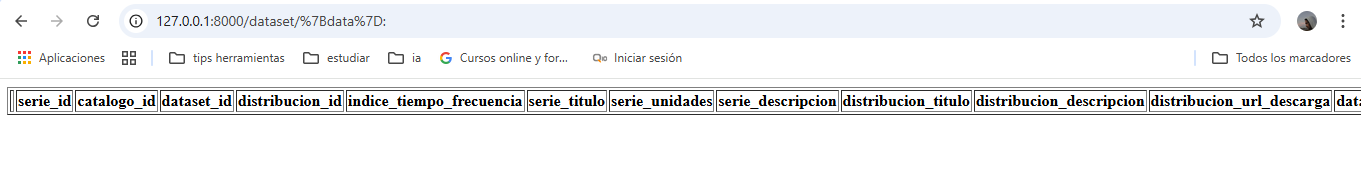
1. Ahora se utilizara la inyección /serie\_titulo /"or 1=1— Mostrando ya la información que se encuentra dentro de los jasson que son el id de la serie , catalodo\_id, índice\_tiempo\_frecuencia, serie\_titulo, serie\_unidades, que son los títulos que aparecieron en la anterior consulta



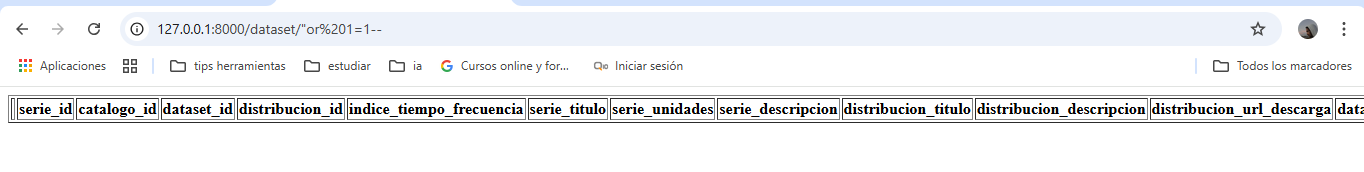
1. Dentro de la página tiene la opción de dar formato al texto mostrando mas claramente el contenido Aquí se aprecia la siguiente información



1. Ahora se utilizare el endppoint /dataset/{data}: Dando el titulo de las columnas de la tabla

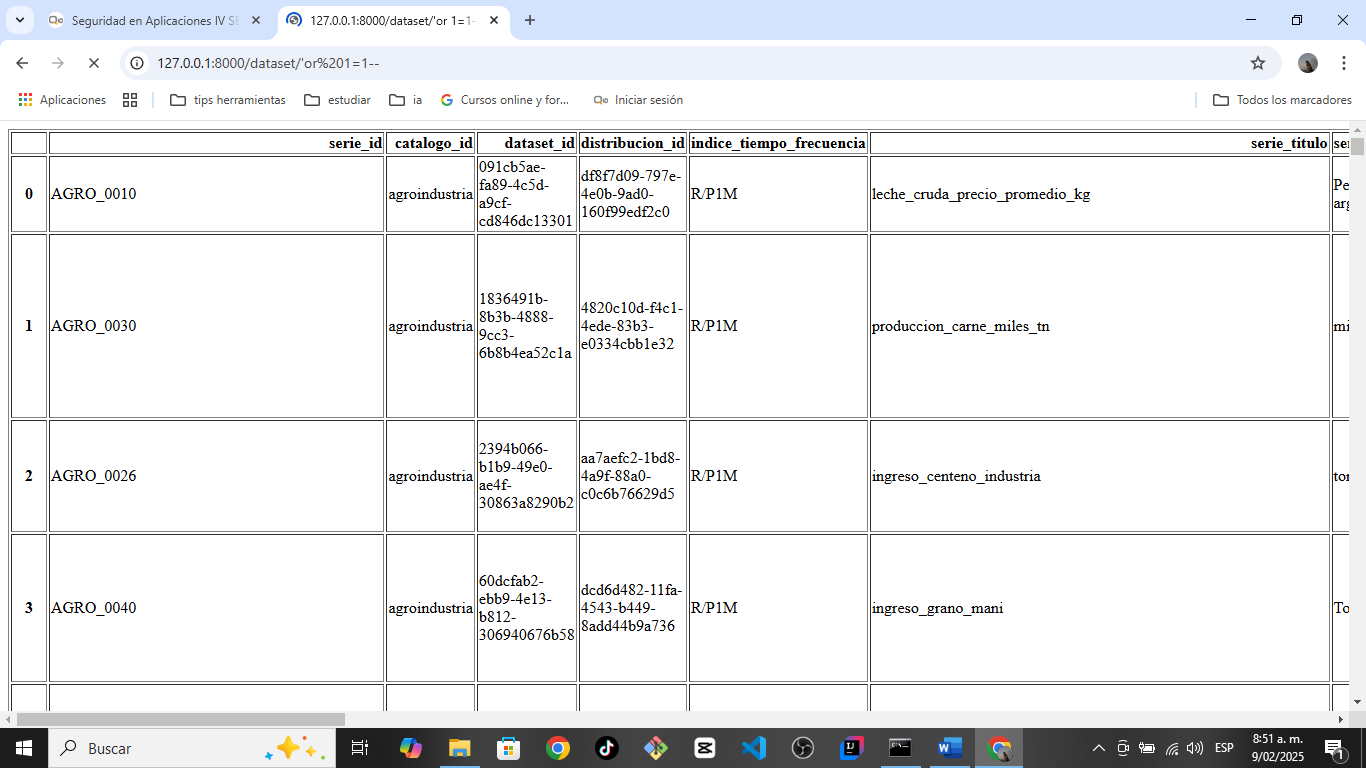


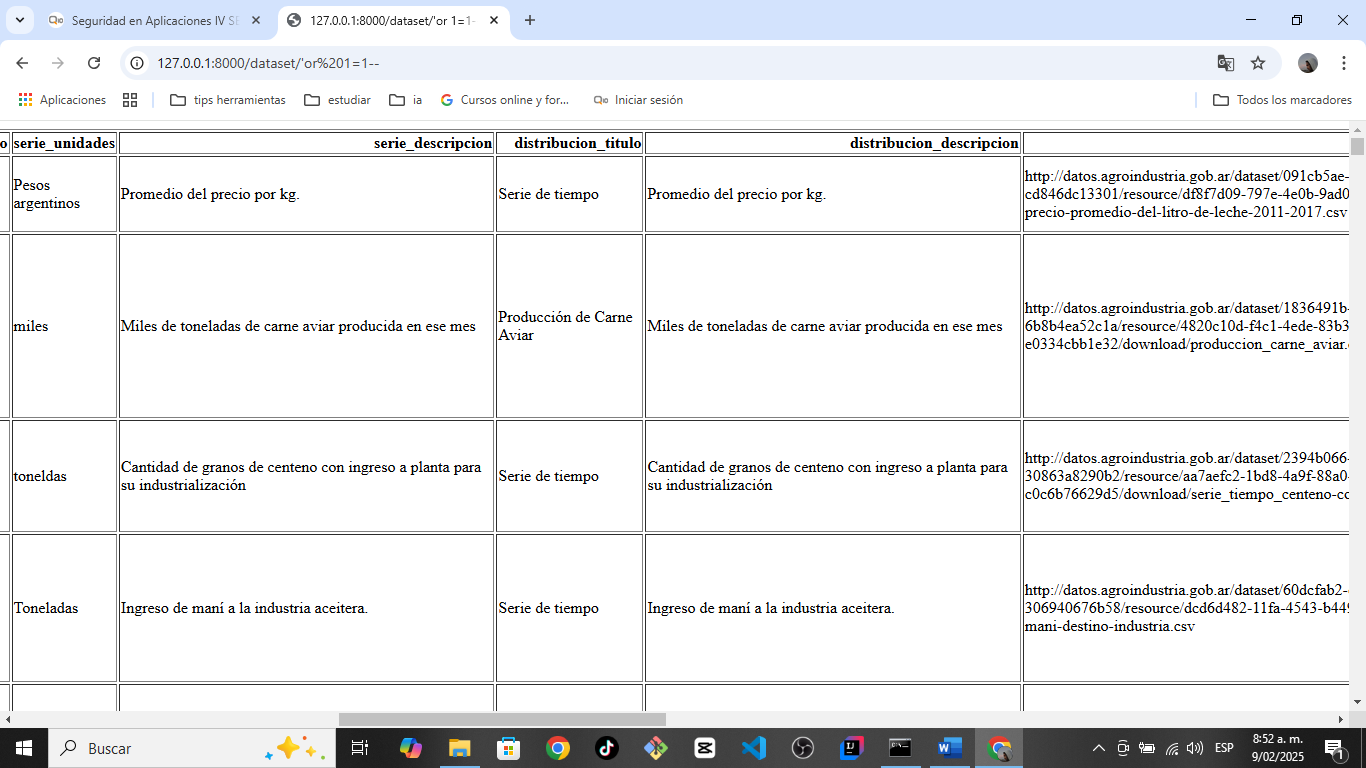
1. Se realizar la inyección /"or 1=1— al anterior endpoint en este caso solo arroja los títulos de las columnas

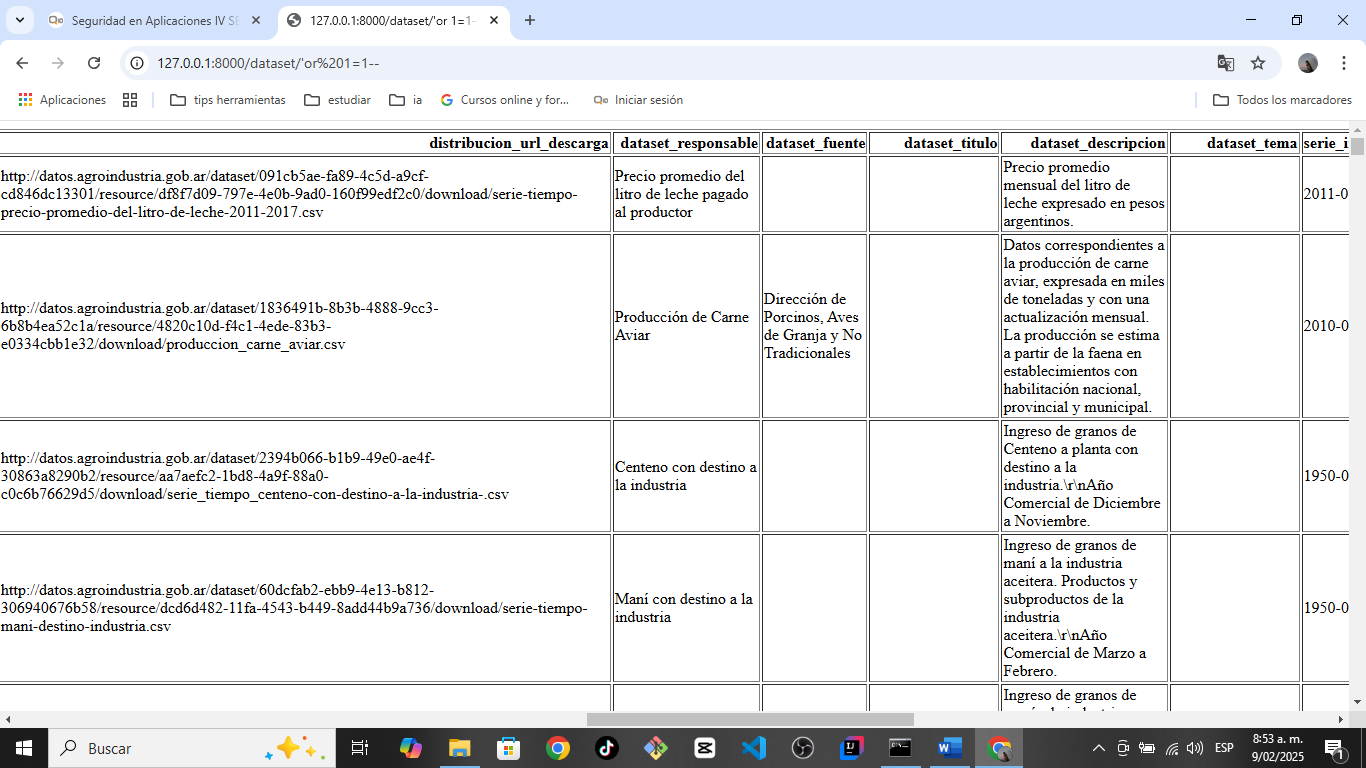


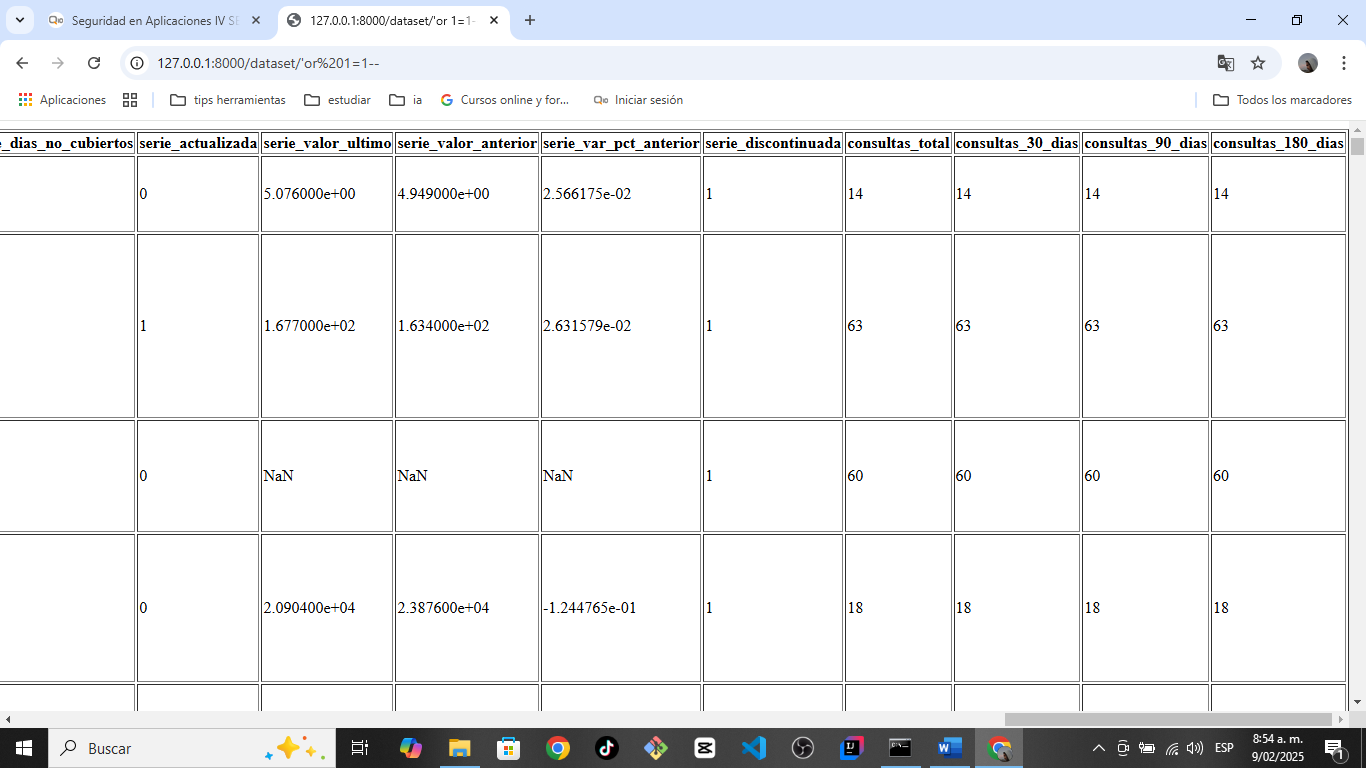
11 Para el anterior endpoint si se usa comilla simple en la inyección si entrega información:

Aquí se observa un información detallada de los productos









**Preguntas generadoras**

* ¿Cómo podrías descubrir la estructura de la base de datos?

R: Ya teniendo la tabla se da una pista con las columnas y los nombres dado a entender que estructura manejan en su formato como puede ser como configuran los Id

* ¿Qué información podría ser sensible en este sistema?

R: Dado que se nota que es información de una empresa toda información es vulnerable ya sea por los competidores o ladrones ejemplo con los precios, la forma que distribuyen su producto, entre otras.

* ¿Cómo probarías si un endpoint es vulnerable a inyección SQL?

R: a travez del código de SQL 'or 1=1— o también Intenta enviar caracteres especiales como comillas ('), comillas dobles ("), o comentarios SQL (--, #).

Ya dentro del sistema se podría ensayar con la información entendiendo parte se su estructura da pista como en este ejercicio que mostro un jason.