**Práctica 4. Optimización, Transacciones y Seguridad**

**Asignatura:** Sistemas Informáticos I (Prácticas de Laboratorio)

**Grupo:** 1363

**Pareja:** 4

**Nombres:** Sanchez Redondo, Pablo; Solana Vera, Antonio

**Parte A. Optimización.**

**Ejercicio A: Índices**

En primer lugar, mediremos el rendimiento de una consulta SQL y estudiaremos distintos planes de ejecución, comparándolos entre sí, mediante el uso del comando EXPLAIN. Para ello, hemos creado el fichero *“clientesDistintos.sql”* (adjunto a esta memoria de prácticas). En la consulta, hemos mostrados el número de clientes distintos que tienen pedidos en un mes dado y hemos creado distintos índices aplicados a las columnas o atributos en orderdate, totalamount y en ambas. Así, la Tabla 1 muestra los principales resultados obtenidos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Consulta Base | Índice en columna orderdate | Índice en columna totalamount | Índice en ambas |
| **Coste total** | 5636 | 5636 | 4496 | 5636 |
| **Número total de operaciones** | 6 | 6 | 6 | 6 |

Tabla 1. Rendimiento del uso de un índice sobre una consulta SQL.

En general, los resultados obtenidos muestran que la creación de un índice en la columna totalamount mejora el rendimiento de la consulta en un 20% (en función del coste total). Así, la consulta totalamount tuvo un número total de operaciones de 4496, mientras que la consulta base tuvo un número total de operaciones de 5636 contra la base de datos. Como conclusión, podemos decir que el uso de índices acelera las búsquedas y mejora el rendimiento para los resultados obtenidos.

**Ejercicio B: Preparar consultas**

|  |  |  |
| --- | --- | --- |
|  | Con indice | Sin indice |
| **Con prepare** | 57 | 409 |
| **Sin prepare** | 57 | 494 |

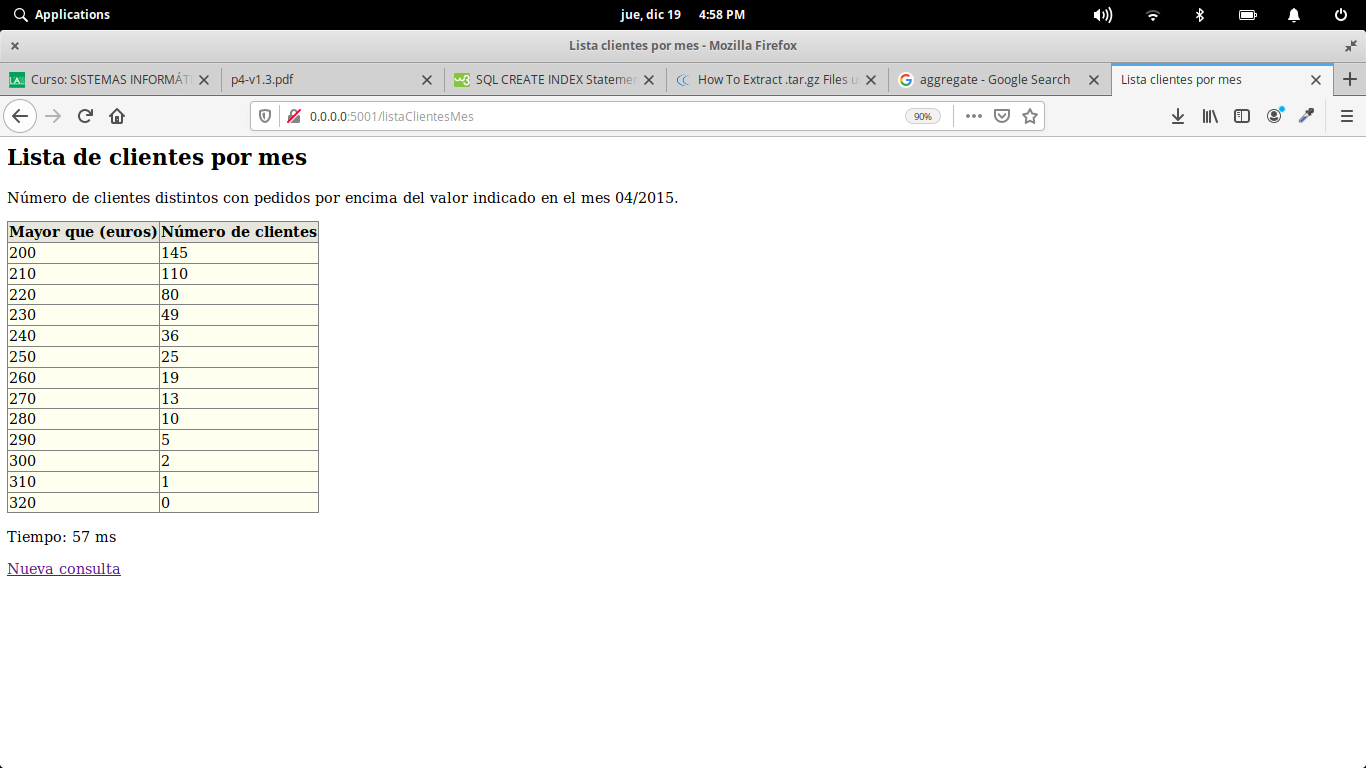
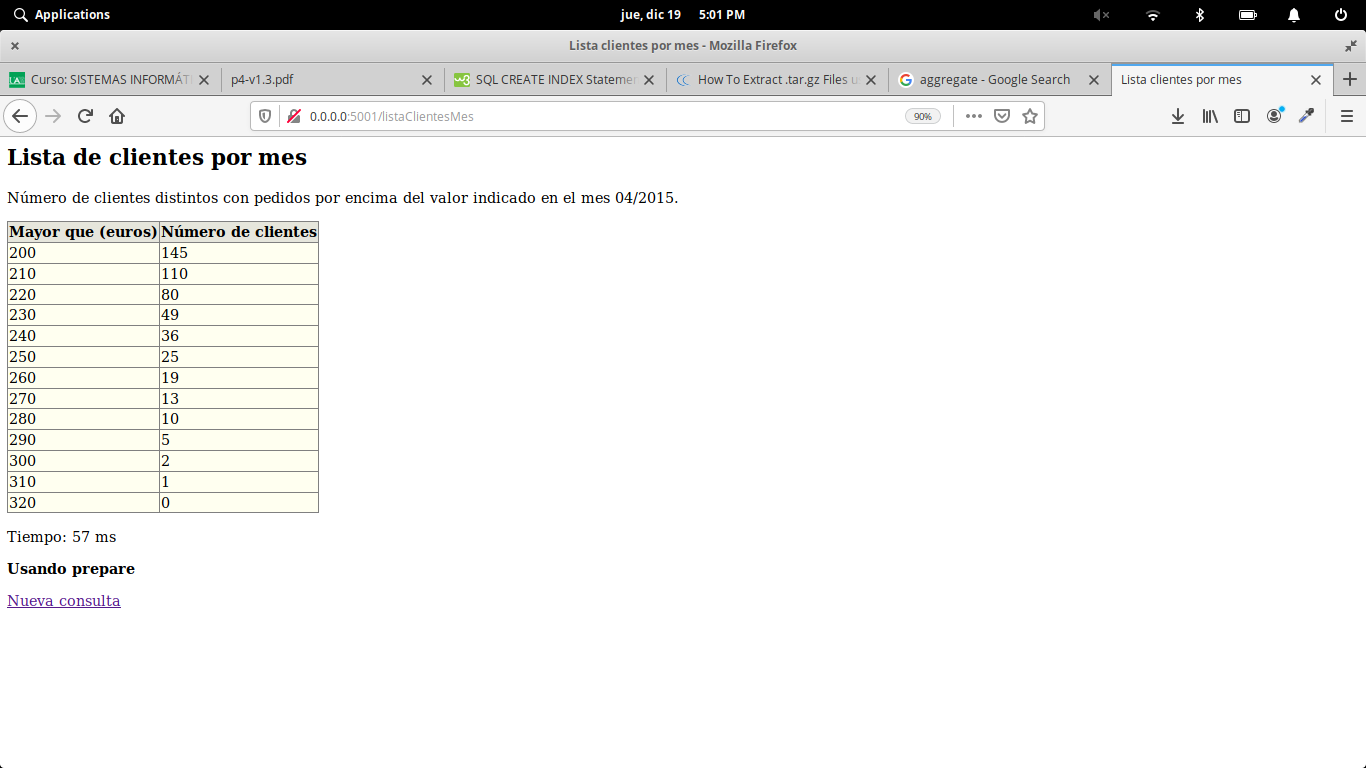
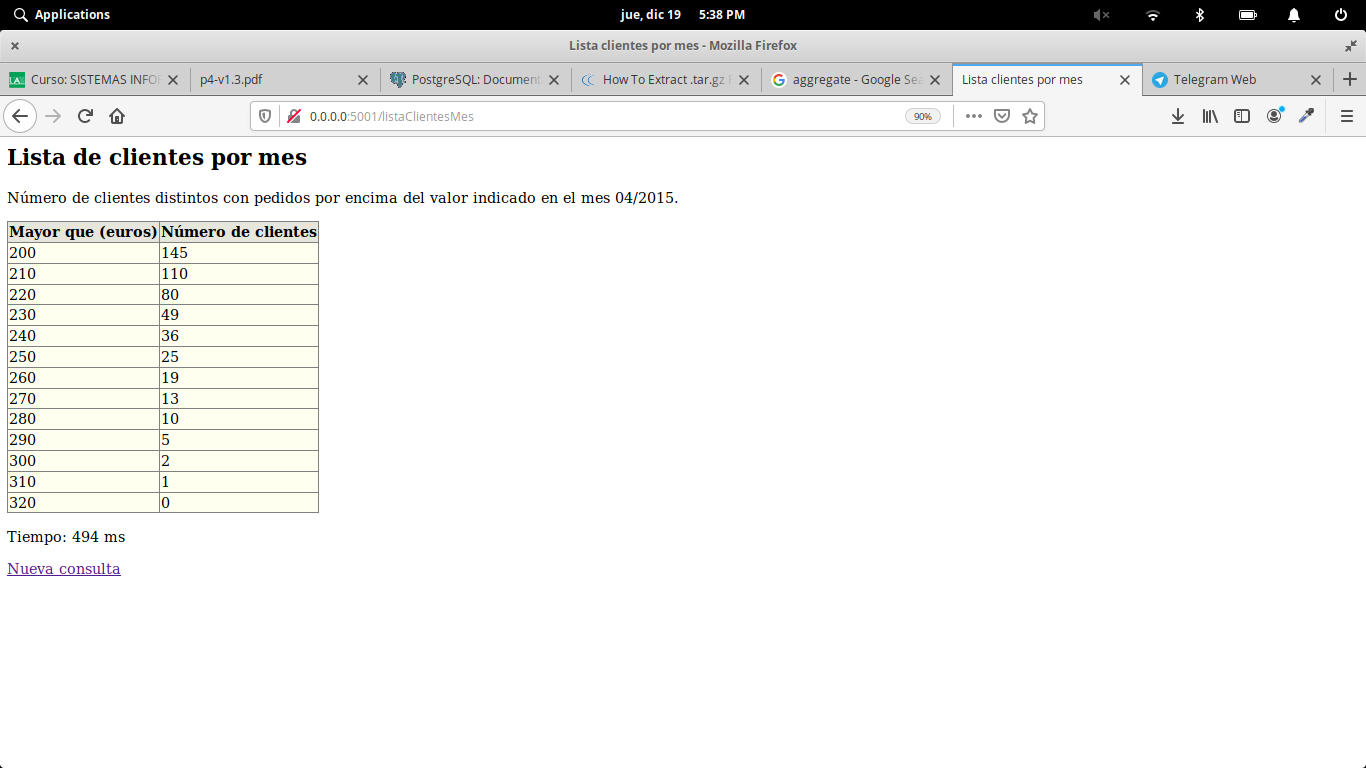
Tabla 1. Rendimiento del uso de un índice y/o un prepare sobre una consulta SQL.

Imagen 1. Rendimiento de la consulta sin PREPARE y con INDEX en la web.

Imagen 2. Rendimiento de la consulta sin PREPARE y con INDEX en la web.

Imagen 3. Rendimiento de la consulta sin PREPARE y sin INDEX en la web.

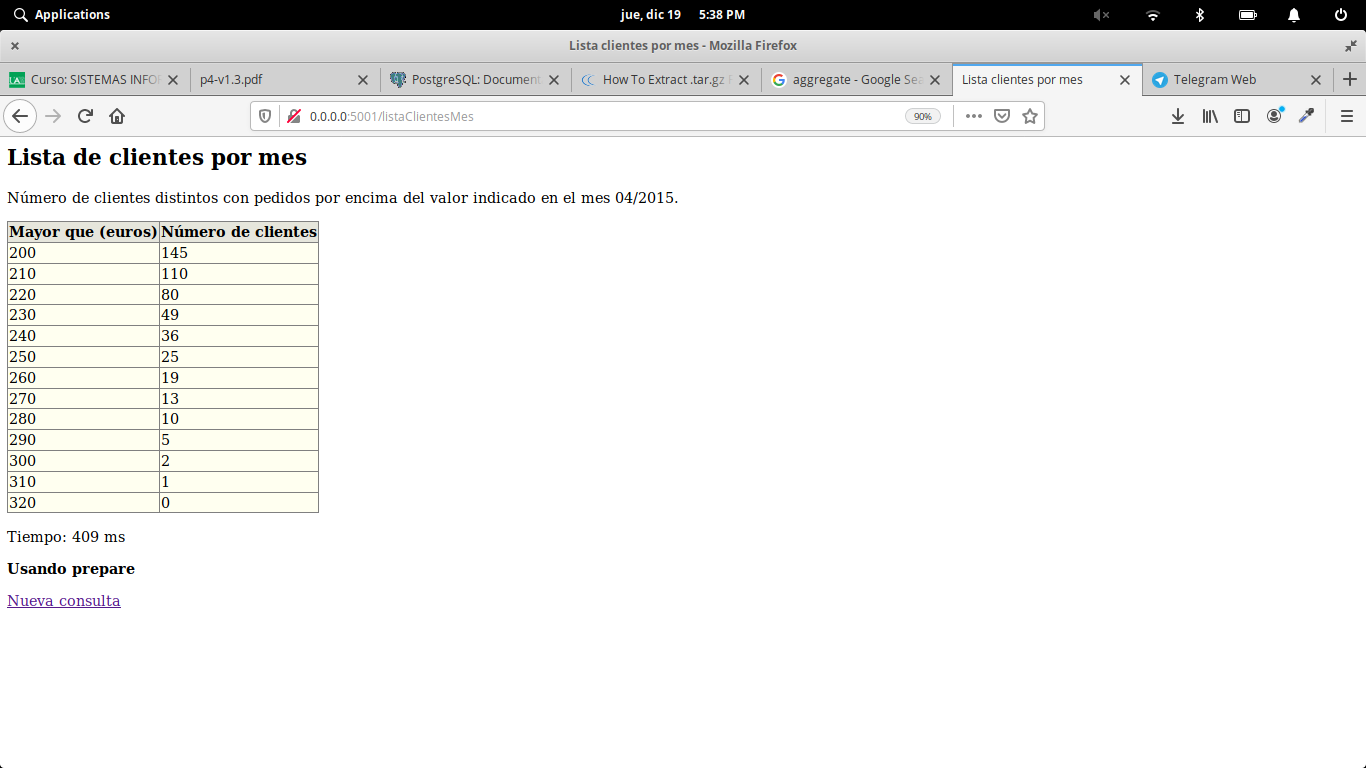


Imagen 4. Rendimiento de la consulta sin PREPARE y sin INDEX en la web.

Se puede observar que con los prepare no causan ninguna diferencia usando INDEX dado que la velocidad de ejecucion de la consulta ya es muy rapida. En cambio a falta de un INDEX se puede notar una ligera diferencia (una mejora de un 18%).

**Lista de ficheros adjuntos**

* *database.py*: Contiene las sentencias ejecutadas en las mediciones del ejercicio (a traves de la interfaz web)

**Ejercicio C: Impacto de la forma de consultas**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Consulta 1 | Consulta 2 | Consulta 3 |
| **Coste total** | 3961 | 4537 | 0 |
| **Número total de operaciones** | 2 | 4 | 6 |

i. La tercera consulta devuelve el resultado de forma inmediata por que el coste de ejecucion es cero.

ii. La segunda puede ser ejecutada en paralelo despues del agregate. La tercera puede ser paralelizada sin ningun problema porque es una operación de append repetida multiples veces.

**Ejercicio D: Estudio del impacto de las estadisticas**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Consulta 1 | Consulta 2 | Consulta 3 |
| **Coste total** | 3961 | 4537 | 0 |
| **Número total de operaciones** | 2 | 4 | 6 |

i. La tercera consulta devuelve el resultado de forma inmediata por que el coste de ejecucion es cero.

ii. La segunda puede ser ejecutada en paralelo despues del agregate. La tercera puede ser paralelizada sin ningun problema porque es una operación de append repetida multiples veces.

**Lista de ficheros adjuntos**

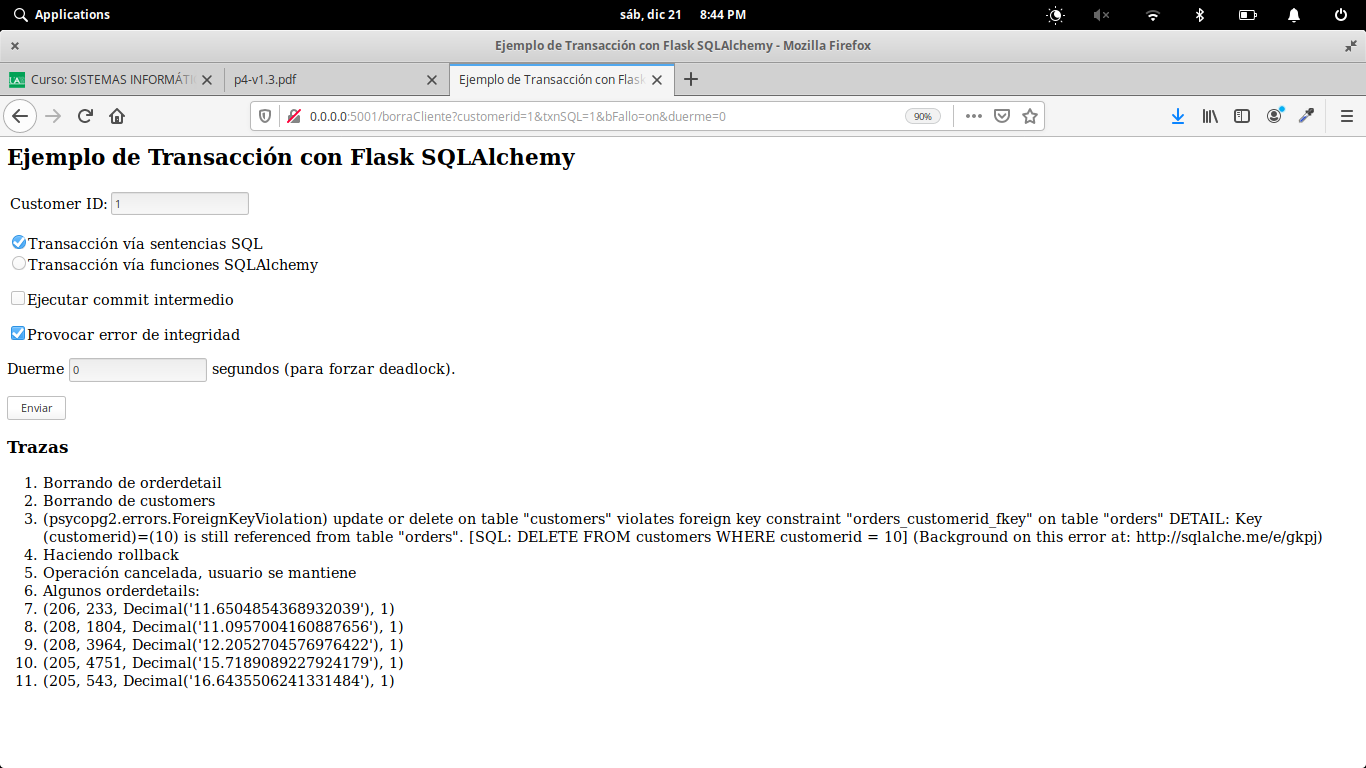
*countStatus.sql*: Contiene las sentencias ejecutadas en las mediciones del ejercicio.

**Transacciones y Deadlock.**

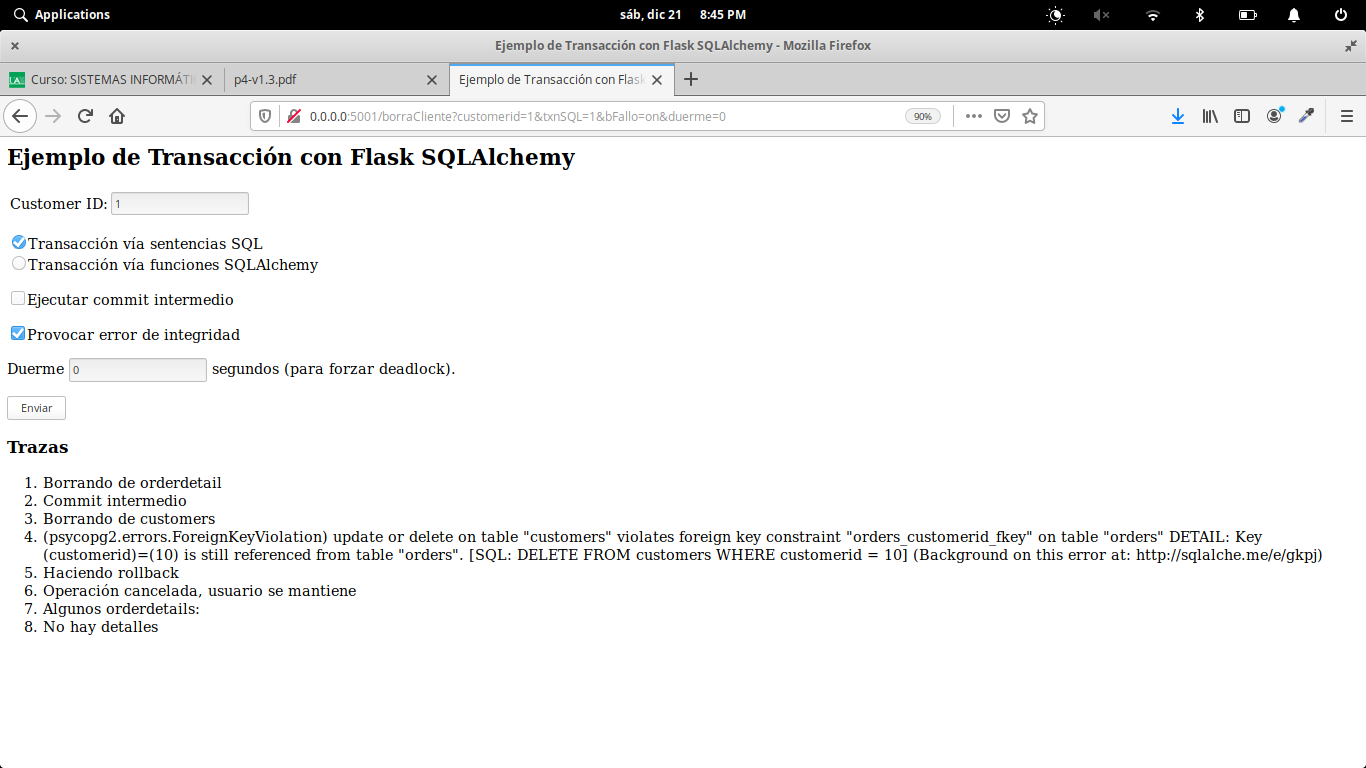
**Ejercicio E: Estudio de Transacciones**

Para eliminar a un usuario el orden correcto es: orderdetail, orders y por último customers, porque orderdetail tiene una foreign key a orders y, a su vez orders tiene una foreign key con customers. Para el fallo, eliminamos orderdetails, hacemos el commit o no, y luego eliminamos de la tabla customers, por lo que salta un error.

El resultado en la web sin commit:

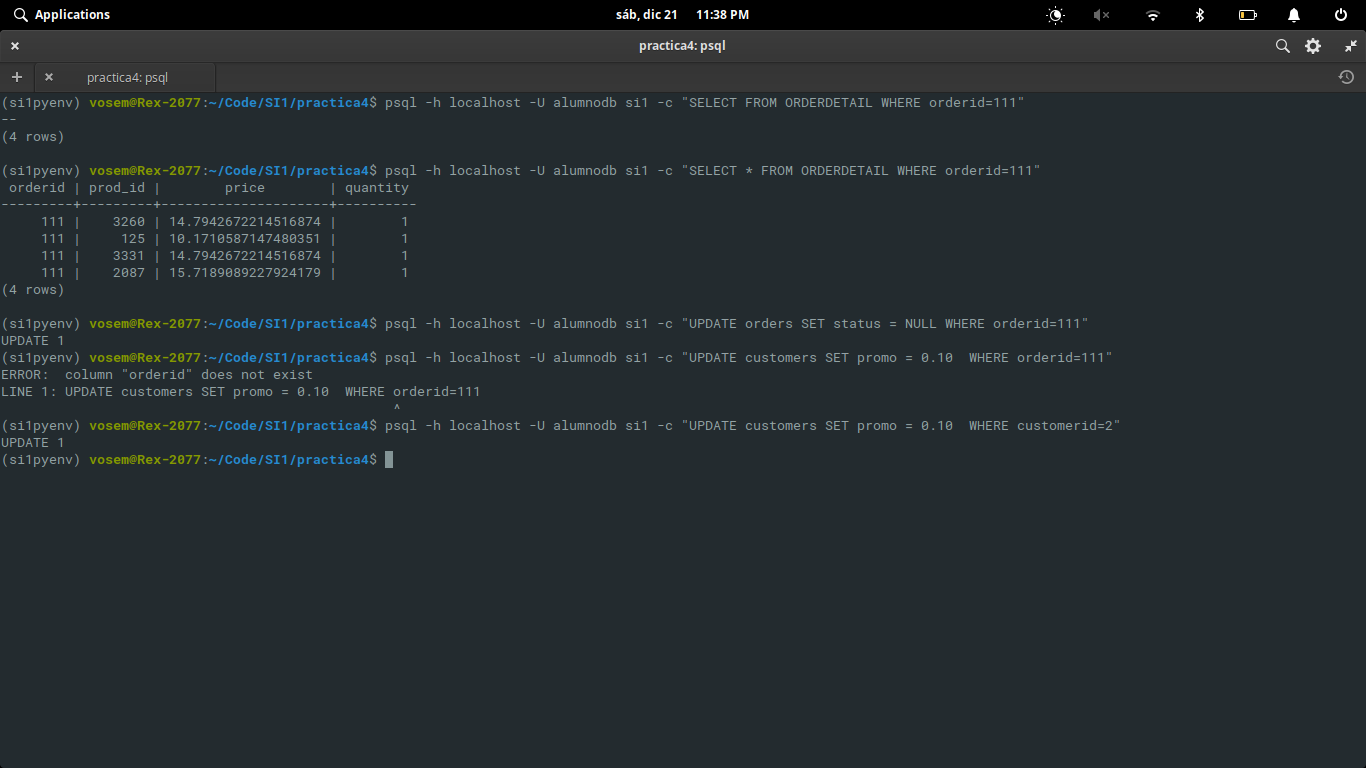


Resultado con el commit en orderdetail:

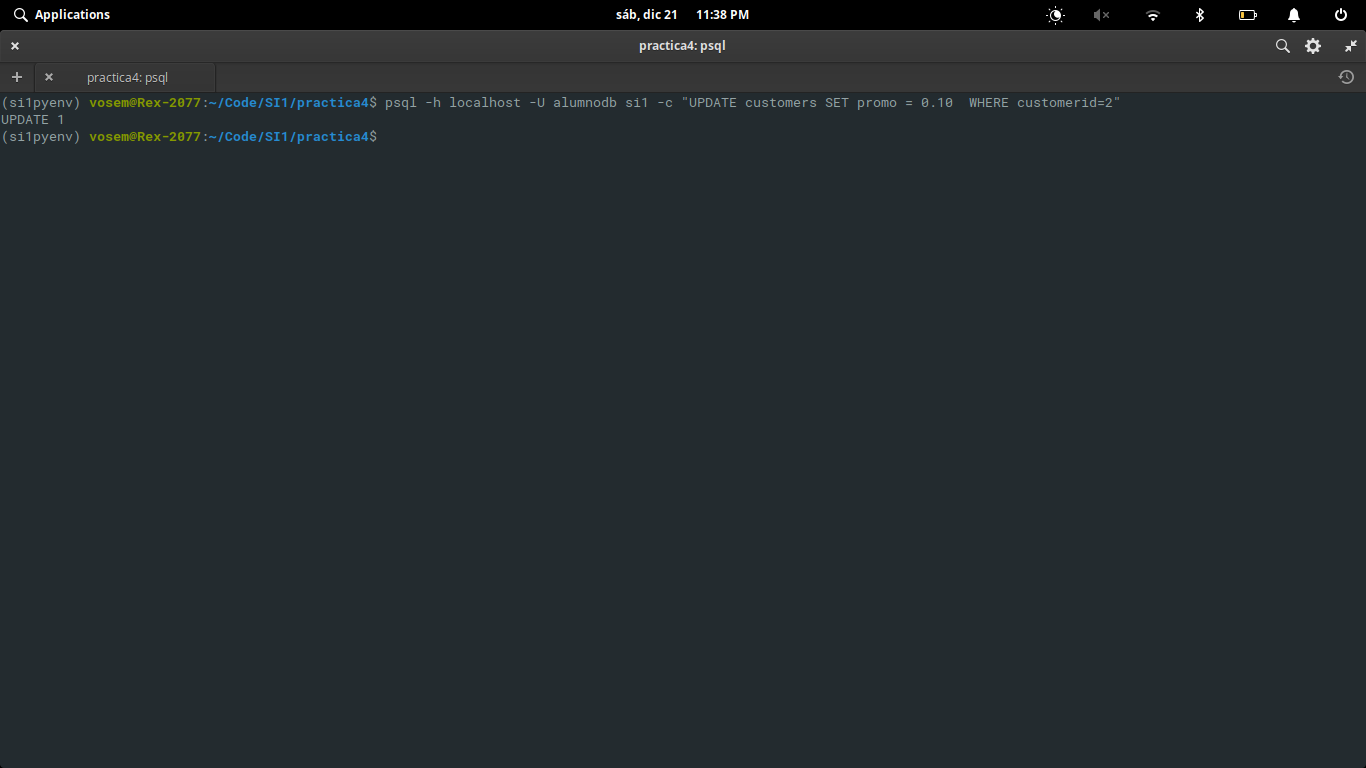
****

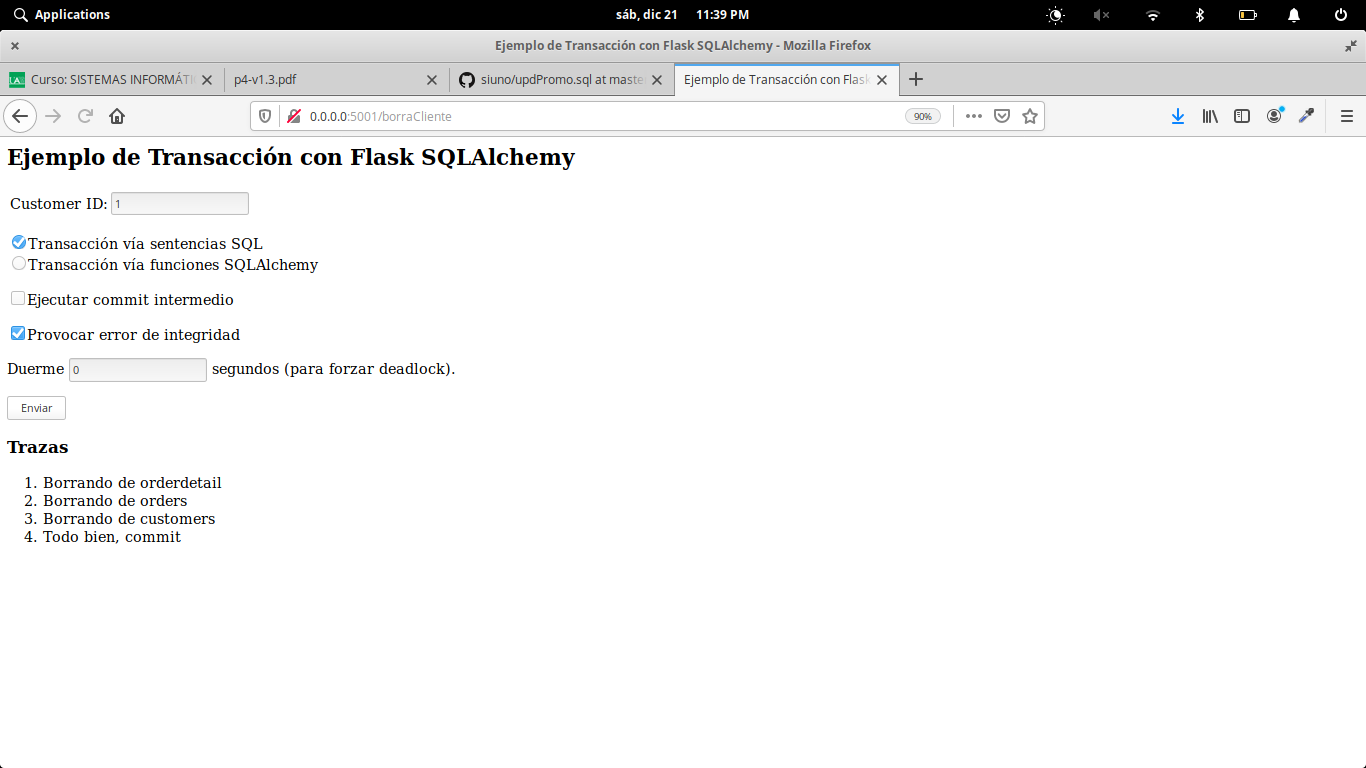
**Ejercicio F: Estudio de Bloqueos y Deadlocks**

Creacion de carritos:



Eliminar usuario 2 y updatear promo al mismo tiempo con el deadlock:



****

**Lista de ficheros adjuntos**

*updPromo.sql:* Creación de la columna promo y trigger que la actualiza

**Seguridad.**

**Ejercicio G: Login**

La parte del código que es vulnerable es la siguiente:

A screenshot of a computer screen

Description automatically generated

Imagen 5. Código vulnerable a inyección SQL.

De forma más precisa, la línea vulnerable es la 88, cuando guardamos en query un texto con input de usuario sin sanear.

Para saltarnos el proceso de login, podemos introducir lo siguiente:

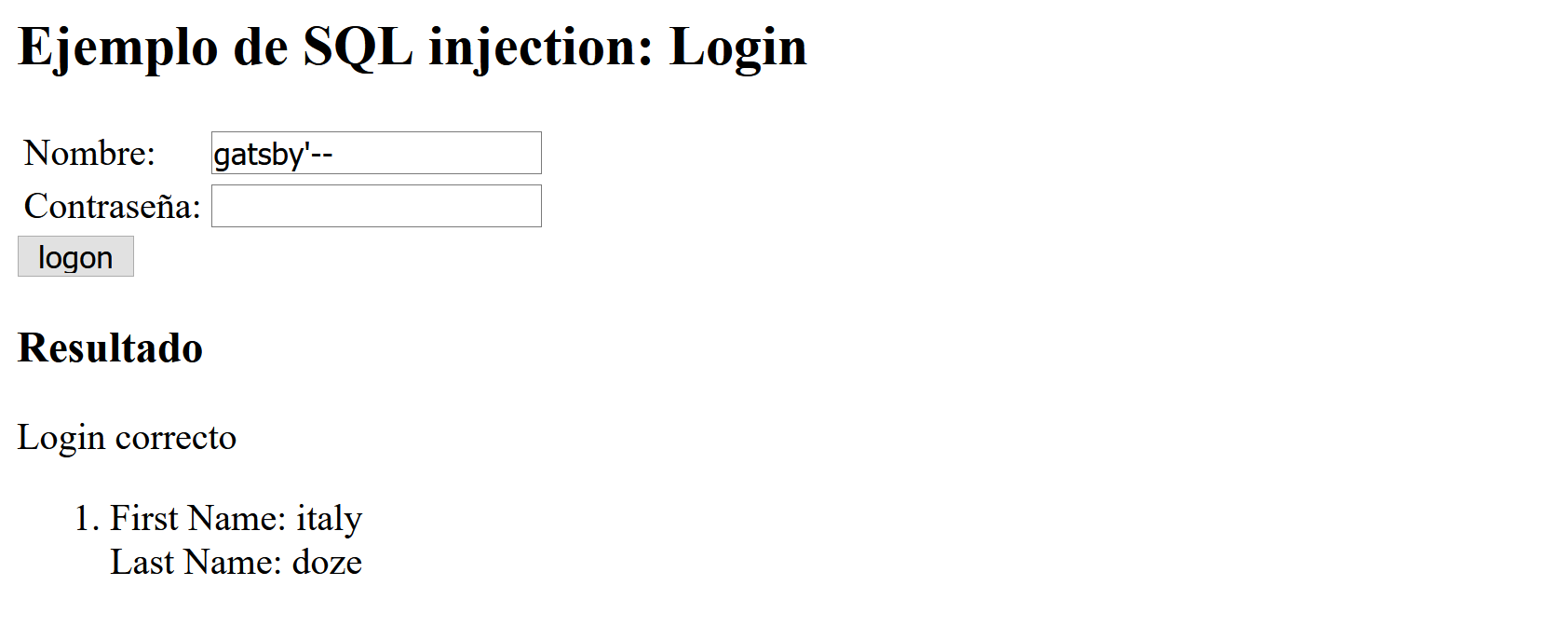


Imagen 6. Demostración de vulnerabilidad en la web con nombre de usuario.

Este texto funciona porque el doble guión del final deja comentada la comprobación de la contraseña.

También podemos realizar un login correcto sin conocer un nombre de usuario empleando la siguiente técnica:

A screenshot of a cell phone

Description automatically generated

Imagen 7. Demostración de vulnerabilidad en la web sin nombre de usuario.

Esta vez hemos dejado la query de la siguiente manera:

SELECT \* FROM customers WHERE username=’’ OR 1=1

No nos ha importado cual es el usuario y hemos puesto un 1=1 al final de la query por que sabemos que de esta manera siempre nos va a devolver un usuario (que es el único requerimiento para hacer login correcto). Como en el código solo seleccionamos el primer resultado de la query, el usuario que nos muestra la web es el primero que ha encontrado.

A screen shot of a computer

Description automatically generated Imagen 8. Código funcional no vulnerable.

En este ejemplo no vulnerable en vez de insertar directamente el input del usuario en nuestra query, le pasamos por un lado la query y por otro los valores a insertar a la función “execute” de SQLAlchemy. Esta función se ocupa por nosotros de sanear el input del usuario, previniendo así una inyección SQL.

Otra forma más correcta de realizar la consulta hubiera sido no usar “raw” SQL, y utilizar las funciones de SQLAlchemy.

**Ejercicio H: Acceso a información.**

De nuevo tenemos el mismo problema que en el apartado anterior, estamos ejecutando una query con el input del usuario sin sanear.

A screenshot of a cell phone

Description automatically generated

Imagen 9. Código vulnerable para buscar películas.

Podemos ver en la imagen 10, como utilizando el mismo truco de 1=1 para que siempre se cumpla la query, podemos seleccionar todas las películas de la base de datos.

A screenshot of a cell phone

Description automatically generated

Imagen 10. Demostración de la vulnerabilidad.

Para filtrar información de la base de datos nos hemos con un problema: no conocemos el nombre de la variable que muestra las películas por pantalla, o si son varias. Si lo supiéramos o acertáramos probando podríamos ejecutar la siguiente query:

A screenshot of a cell phone

Description automatically generated

Imagen 11. Mostramos todas las tablas del sistema.

No solo eso, si queremos ver solo las del usuario podemos obtener su OID con la siguiente query:

A screenshot of a cell phone

Description automatically generated

Imagen 12. Obtenemos el OID del usuario.

Y una vez conocido el “relowner” de las tablas que nos interesan podemos ejecutar esta para ver todas las tablas del usuario:

A screenshot of a social media post

Description automatically generated

Imagen 13. Obtenemos las tablas del usuario con su OID.

Viendo estas tablas podemos asumir que lo que nos interesa es la tabla “customers” que probablemente tenga la información confidencial que buscamos.

Ahora necesitamos los nombres de las columnas de la tabla. Podemos acceder fácilmente a través de “information\_schema.columns” como se ve en la imagen:

A screenshot of a social media post

Description automatically generated

Imagen 14. Acceso al nombre de las columnas de una tabla.

Una vez obtenido el nombre de las columnas, usando “AS movietitle” y “CONCAT()” podemos obtener cualquier información de los clientes de la base de datos. En la imagen 15 se puede observar el nombre, apellido y tarjeta de crédito de todos los clientes.

A screenshot of a cell phone

Description automatically generated

Imagen 15. Obtenemos información de los clientes de la base de datos.

Para resolver este problema no podemos usar un “combobox” porque podemos seguir haciendo las mismas peticiones, aunque ya no de forma manual desde el navegador. Usar post nos deja en la misma posición, no cambia nada ya que el usuario puede seguir usando el navegador u otras herramientas para hacer una inyección SQL.

Un atacante con un proxy como burpsuite puede realizar estas operaciones sin importar cual sea la interfaz mostrada al usuario o el método HTTP utilizado para mandar los datos al servidor.

Para resolver el problema debemos realizar los mismos cambios que en el apartado G (Imagen 8).

Nosotros proponemos la siguiente solución para evitar este tipo de problemas en el futuro. En lugar de utilizar las funciones de acceso a la base de datos de forma directa, podemos crear un nuevo archivo wrapper que nos obligue a pasarle por un lado la query y por otro los parámetros, de manera que sea imposible que aparezcan nuevas vulnerabilidades en el futuro.