

Giovany da Silva Santos 2018007758
Webster Aurélio Carvalho Ramos 2018014716

1)a)

create or replace function geraRelatorio(numeroPedido integer)

returns table(

 identificador_pedido integer,

 consumidor varchar,

 cidade varchar,

 data_pedido timestamp,

 valor_total numeric)

as \$\$

begin

return QUERY

```
SELECT o.orderid as identificador_pedido, companyname as consumidor,
       city as cidade_consumidor, o.orderdate as data_pedido,
       sum(unitprice*quantity-discount) as valortotalpedido
  from northwind.orders o join northwind.order_details od on
 (o.orderid=od.orderid and o.orderid=10248) join northwind.customers
    c on (o.customerid=c.customerid) group by(o.orderid,c.companyname,c.city);
```

end;

\$\$ language plpgsql

select * from geraRelatorio(10248)

b)

create role gerente;

create role gestor;

create user giovany with password '12345';

create user webster with password '1234';

grant gerente to giovany;

grant gestor to webster;

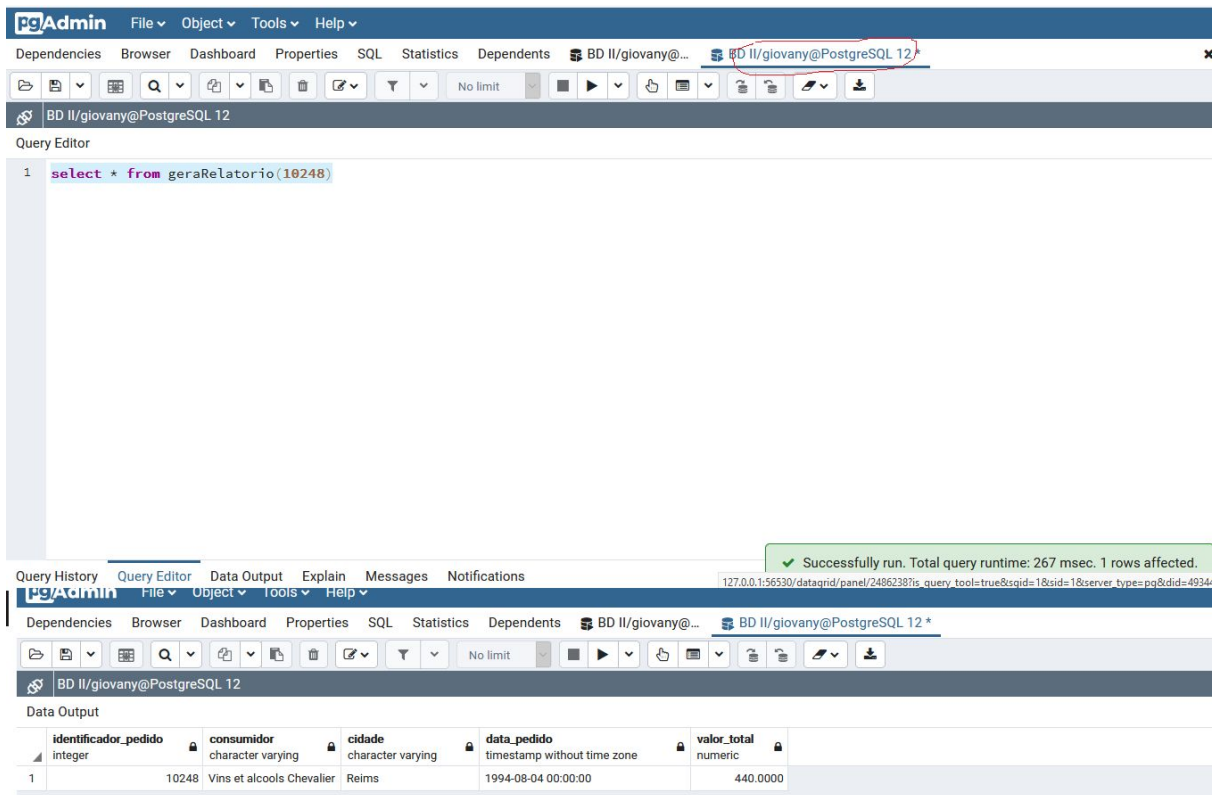
grant usage on schema northwind to gerente;

grant usage on schema northwind to gestor;

grant execute on function geraRelatorio(numeroPedido integer) to gerente;

c) Com os comandos dados pelos determinados usuários podemos observar os retornos dado pelo Postgresql como abaixo:

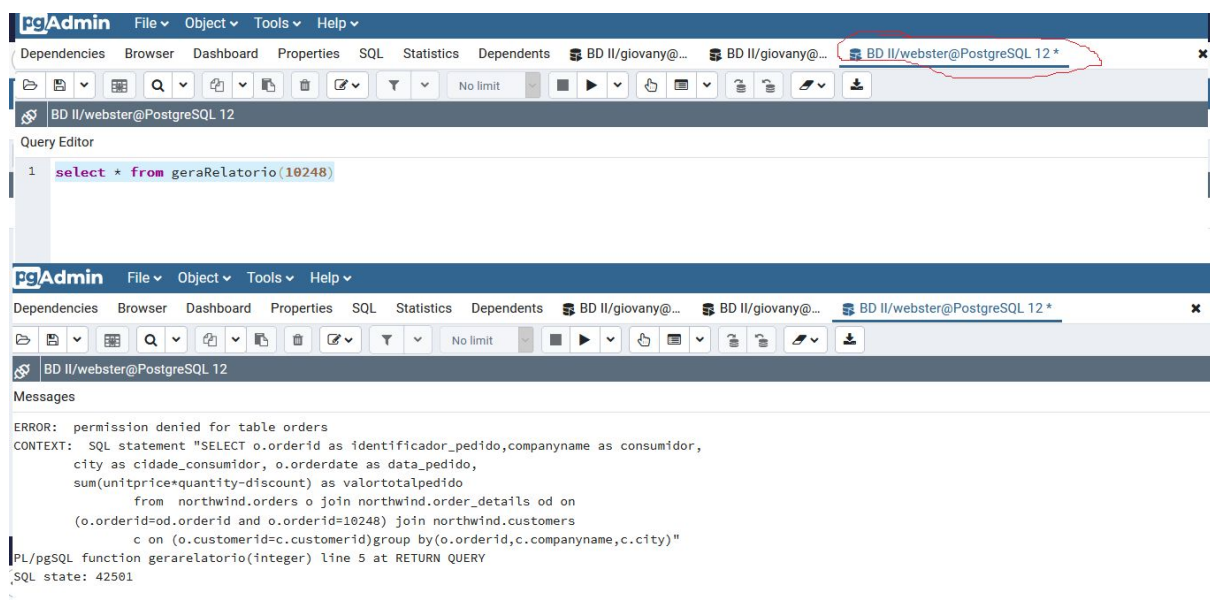
Usuário giovany(gerente):



The screenshot shows the pgAdmin interface for user 'giovany' connected to 'BD II/giovany@PostgreSQL 12'. The Query Editor contains the SQL command: `select * from geraRelatorio(10248)`. A green message bar at the bottom indicates: 'Successfully run. Total query runtime: 267 msec. 1 rows affected.' Below the Query Editor, the 'Data Output' tab is active, displaying a table with 6 columns and 1 row of data.

identificador_pedido	consumidor	cidade	data_pedido	valor_total	
integer	character varying	character varying	timestamp without time zone	numeric	
1	10248	Vins et alcools Chevalier	Reims	1994-08-04 00:00:00	440.0000

Usuário:webster(gestor)



The first screenshot shows the pgAdmin interface for user 'webster' connected to 'BD II/webster@PostgreSQL 12'. The Query Editor contains the same SQL command: `select * from geraRelatorio(10248)`. The second screenshot shows the 'Messages' tab with an error message: 'ERROR: permission denied for table orders'. The context provided is: 'SQL statement "SELECT o.orderid as identificador_pedido, companyname as consumidor, city as cidade_consumidor, o.orderdate as data_pedido, sum(unitprice*quantity-discount) as valortotalpedido from northwind.orders o join northwind.order_details od on (o.orderid=od.orderid and o.orderid=10248) join northwind.customers c on (o.customerid=c.customerid) group by (o.orderid, c.companyname, c.city)". PL/pgSQL function gerarelatorio(integer) line 5 at RETURN QUERY SQL state: 42501'.

2) O SQL Injection é uma técnica de ataque baseada na manipulação do código SQL, onde o invasor pode inserir ou manipular consultas criadas pela aplicação, que são enviadas diretamente para o banco de dados relacional. Pode ser realizada por meio de telas de login, mensagens de erro, entre outras maneiras. Os métodos de prevenção são: sempre validar os dados digitados pelo usuário (de modo a aceitar somente dados que são conhecidamente válidos), nunca retornar as mensagens do servidor SQL para o usuário (estas mensagens podem revelar informações importantes), remover objetos que não serão utilizados e habilitar logs de segurança no servidor.

3) No phpmyadmin rodamos os comandos:

```
create database BD_II
```

```
drop table if exists 'usuario';
```

```
create table 'usuario' (
```

```
    'usuario' varchar(20) default null,
```

```
    'senha' varchar(20) default null
```

```
) engine = InnoDB default charset = latin1;
```

```
-- Inserindo dados na tabela usuario --
```

```
lock tables 'usuario' write;
```

```
insert into 'usuario' values ('giovany', '123');
```

```
insert into 'usuario' values ('webster', '1234');
```

```
unlock tables;
```

Link do github: <https://github.com/websterramos/AtividadePraticaBD2>

Link do vídeo do funcionamento: <https://youtu.be/4QSJY140fiw>