Banco de Dados II
Prática 1

Profª. Vanessa Souza

Assunto: Segurança – Aula Prática

Essa prática deve ser executada no SGBD PostgreSQL.
REFERÊNCIAS DO POSTGRESQL:

- ROLES : https://www.postgresql.org/docs/12/user-manag.html
- GRANT : https://www.postgresql.org/docs/12/sql-grant.html
- REVOKE : https://www.postgresql.org/docs/12/sql-revoke.html

Questão 1: Restaure o banco de dados Northwind.

Questão 2: Seguindo as boas práticas de segurança, você deve criar perfis de usuário no banco e posteriormente adicionar usuários a esses perfis.

a) Crie uma role chamada 'programadores', com o privilégio de CRUD em todas as tabelas do banco.
b) Crie uma role chamada 'gerente'. Daremos privilégios para essa role nas próximas questões.

Questão 3 : Criação de usuário no banco de dados.

a) Crie um usuário com seu nome no banco de dados Northwind
b) Faça *login* com esse novo usuário
c) Simule falhas de conexão
d) Verifique os privilégios do usuário

Questão 4: Concedendo privilégios ao usuário.

a) Considere que o usuário que você criou na questão 3 é um usuário do tipo 'programador'. Insira ele na role criada na questão 2.
b) Verifique o que é possível realizar no banco
c) Simule falhas associadas a falta de privilégios por esse usuário.

Questão 5: Removendo privilégios do usuário.

a. Remova da role 'programadores' o privilégio de realizar 'delete' na tabela 'Categories'.
b. Teste a remoção do privilégio.

Questão 6 : É possível conceder privilégios sobre *Views*. A associação dos comandos GRANT e VIEW permite que se limite o acesso de registros a usuários (e não apenas a

nível de coluna, como no GRANT). É possível também permitir que usuários tenham acesso apenas a relatórios. Testaremos essa funcionalidade nessa questão.

a. Crie uma *view* chamada 'relatorio', sobre as tabelas *Orders e OrderDetails*, cujo resultado seja idêntico à figura 1. Onde:
    - Total_produtos é o total de produtos comprados no pedido
    - Total_pedido é a soma dos valores de todos os produtos comprados

	orderid [PK] integer	customerid character varying (5)	employeeid integer	total_produtos bigint	total_pedido numeric
1	11038	SUPRD	1	3	46.9000
2	10782	CACTU	9	1	12.5000
3	10725	FAMIA	4	3	40.6500
4	10423	GOURL	6	2	54.0000
5	10518	TORTU	4	3	287.4500
6	10356	WANDK	6	3	58.0000
7	10963	FURIB	9	1	34.0000
8	10596	WHITC	8	3	89.6500
9	10282	ROMEY	4	2	36.3000

b. Conceda o privilégio de leitura sobre a View para a role 'gerente'.
c. Crie o usuário 'gestor' e adicione ele na role
d. Teste os privilégios do usuário gestor no banco de dados.

Questão 7: O banco de dados PostgreSQL é do tipo 'objeto-relacional'. Isso significa que ele implementa conceitos da orientação objeto em seu modelo. Dessa forma, tabelas, roles, usuários, são objetos no banco e possuem 'um dono'. Ou seja, quem criou aquele 'objeto' tem direitos sobre ele. No caso dos comandos SQL GRANT e REVOKE, isso tem diversas implicações. Vamos testá-las nessa atividade.

a) Crie uma role, cujo perfil é de 'DBA de Banco de Dados'. Ou seja, ela terá todos os privilégios sobre o banco Northwind.
b) Crie um usuário e associe ele a esse perfil.
c) Faça login no banco com o perfil criado e execute a seguinte operação no banco: inserir uma coluna na tabela 'categories'.
d) Qual o resultado da operação executada na letra c?
e) Ainda logado como o usuário criado na letra b (que é um DBA), remova da role 'programadores' o privilégio de realizar 'delete' na tabela 'Orders.
f) Qual o resultado da operação executada na letra e?

Questão 8: Testando o 'WITH GRANT OPTION'.

a) Crie um novo usuario no banco chamado 'user1' e dê a ele privilégios de CRUD nas tabelas categories, customers e products. Utilize o 'with grant option'.
    a. Lembrem-se que essa não é uma boa prática de segurança! Estamos utilizando apenas para testes!!!!

b) Crie um novo usuario no banco chamado ‘user2’ e dê a ele privilégios de CRUD nas tabelas orders e orderdetails. Utilize o ‘with grant option’.
c) Crie um novo usuario no banco chamado ‘user3’ e dê a ele privilégios de SELECT em todas as tabelas do schema *northwind*.
d) Agora, o user1 vai repassar os privilégios dele para o user3.
e) De forma análoga, o user2 repassará os privilégios dele para o user3.
f) Qual o efeito das operações executadas nas letras d e e no banco?
g) Logado como postgres, remova os privilégios no user3. O que acontece? Como resolver?