Estudante: Enrico Bernz Reichow Santos;

Turma: 2B;

Componente Acadêmico: Arquitetura de Banco de Dados;

Professor: Antônio D Viniski;

Trabalho Acadêmico: TDE 3.

TE06:

1. Qual conta é atribuída como a detentora de uma relação em um banco de dados? Quais são os privilégios que o detentor de uma relação detém?

R: A conta responsável por uma conexão é a conta de usuário que a iniciou. Quem está à frente dessa conexão possui certos privilégios especiais, os quais englobam a habilidade de conceder ou revogar privilégios associados a essa tabela. Além disso, eles têm a capacidade de efetuar modificações na tabela ou excluí-la, mesmo que não detenham explicitamente os privilégios requeridos.

2. De que maneira o mecanismo de visão é empregado como um mecanismo de autorização em sistemas de bancos de dados?

R: A função do mecanismo de visão é utilizada como um mecanismo de autorização, o que possibilita que o criador da visão estabeleça as permissões de acesso aos dados subjacentes. As visões podem ser empregadas para ocultar informações confidenciais ou conceder acesso somente leitura a uma parte específica dos dados, oferecendo assim um controle minucioso sobre o que os usuários têm permissão para visualizar.

3. Qual é o significado da concessão de um privilégio e da revogação de um privilégio em SQL?

R: Outorgar um privilégio envolve a permissão dada a um usuário ou função para executar uma ação específica em um elemento do banco de dados, como realizar

operações de SELECT, INSERT, UPDATE ou DELETE. Por outro lado, revogar um privilégio refere-se à anulação dessas autorizações previamente concedidas.

4. Enumere os tipos de privilégios disponíveis em SQL.

R: Os diversos tipos de privilégios disponíveis em SQL abrangem:

GRANT: Capacita a concessão de privilégios a outros usuários.

DROP: Permite a remoção de objetos no banco de dados.

REVOKE: Possibilita a anulação de privilégios anteriormente cedidos.

CREATE: Habilita a criação de objetos no banco de dados, como tabelas e visões.

INSERT: Possibilita a inserção de novos dados em uma tabela.

SELECT: Permite a leitura de dados de uma tabela.

DELETE: Permite a exclusão de dados de uma tabela.

UPDATE: Faculta a modificação de dados em uma tabela.

5. Qual é a distinção entre controle de acesso discricionário e controle de acesso obrigatório em sistemas de bancos de dados?

R: O controle de acesso discricionário depende das políticas estabelecidas pelos donos dos objetos, ao passo que o controle de acesso obrigatório é ditado por políticas de segurança externas e permanece imutável perante os proprietários dos objetos.

6. Quais são os diversos tipos de ataques de Injeção de SQL que podem afetar sistemas de bancos de dados?

R: Há várias categorias de ataques de Injeção de SQL, que incluem:

Injeção de SQL clássica: Essa tática envolve a inserção de código SQL malicioso em campos de entrada com o objetivo de explorar vulnerabilidades no sistema.

Injeção de SQL baseada em tempo: Este tipo de ataque se aproveita dos atrasos no processamento do servidor para deduzir informações sensíveis.

Injeção de SQL cega: Nesse cenário, consultas booleanas são usadas para inferir informações do banco de dados.

Injeção de SQL fora de banda: Aqui, os dados são transferidos para um local controlado pelo atacante, permitindo que eles obtenham informações do sistema.

TE07:

1. Explore as características de atomicidade, durabilidade, isolamento e preservação da consistência de uma transação em um banco de dados.

R: As propriedades de uma transação em um banco de dados, como atomicidade, durabilidade, isolamento e preservação da consistência, são comumente referidas como propriedades ACID. A atomicidade garante que uma transação seja tratada como uma entidade indivisível. A durabilidade assegura que as modificações efetuadas por uma transação sejam permanentes. O isolamento cuida da gestão da concorrência entre transações, e a preservação da consistência garante que uma transação leve o banco de dados de um estado consistente a outro.

2. Analise como a serialização é utilizada para aplicar o controle de concorrência em um sistema de banco de dados. Por que a serialização às vezes é vista como excessivamente restritiva no que diz respeito à exatidão dos agendamentos de transações?

R: A serialização é utilizada para aplicar o controle de concorrência em um sistema de banco de dados, assegurando que as transações sejam executadas de forma sequencial. No entanto, a abordagem serializada pode ser percebida como excessivamente restritiva, uma vez que pode ocasionar bloqueios entre transações

simultâneas, resultando em uma menor concorrência e potencialmente prejudicando o desempenho do sistema.

3. Descreva os quatro níveis de isolamento no SQL.

R: Os quatro níveis de isolamento no SQL compreendem: READ UNCOMMITTED, READ COMMITTED, REPEATABLE READ e SERIALIZABLE. Cada um desses níveis proporciona diferentes níveis de controle de concorrência e consistência de dados.

4. Defina as violações causadas por cada um dos seguintes fenômenos: leitura suja, leitura não repetitiva e fantasmas.

R: Violações causadas por:

Leitura suja (dirty read): Esta situação ocorre quando uma transação lê dados que foram alterados por outra transação que ainda não foi confirmada, o que pode levar a informações imprecisas.

Leitura não repetitiva (non-repeatable read): Isso acontece quando uma transação lê os mesmos dados duas vezes, mas os valores são diferentes devido a modificações feitas por outra transação no intervalo entre as leituras, o que pode levar a inconsistências nos resultados.

Fantasmas (phantom): Estas violações ocorrem quando uma transação lê um conjunto de linhas que atendem a uma condição de pesquisa e, posteriormente, outra transação insere ou exclui linhas que atendem à mesma condição, resultando em resultados imprevistos e não consistentes.

5. O que é o protocolo de bloqueio em duas fases e como ele garante a serialização?

R: O protocolo de bloqueio em duas fases é um método de controle de concorrência que assegura a serialização das transações. Ele compreende duas fases: a aquisição de bloqueio, na qual as transações adquirem os bloqueios necessários, e a liberação de bloqueio, na qual os bloqueios são liberados após a conclusão da transação. Isso garante a serialização, uma vez que as transações aguardam a obtenção dos bloqueios antes de avançar, prevenindo assim conflitos entre elas.