|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nombre de la práctica** | **Privilegios de usuarios** | | | **No.** | **8** |
| **Asignatura:** | **Taller de base de datos** | **Carrera:** | **Ingeniería en sistemas computacionales** | **Duración de la práctica (Hrs)** | **2** |

**NOMBRE DEL ALUMNO**: Sandra Alcántara Cruz

GRUPO:3502

**I. Competencia(s) específica(s):** **Construye esquemas de base de datos para proyectar las necesidades de un cliente en base a las reglas sintácticas del lenguaje de definición**

**de datos.**

**II. Lugar de realización de la práctica (laboratorio, taller, aula u otro): Aula**

**III. Material empleado:**

* **Computadora**
* **Navicat**

**IV. Desarrollo de la práctica:**

**Privilegios de Usuarios en MySQL**

En MySQL, los privilegios determinan qué operaciones puede realizar un usuario sobre las bases

de datos y los objetos de la base de datos. Los privilegios se asignan a los usuarios cuando se

crean o mediante el uso de los comandos GRANT y REVOKE . Estos privilegios pueden ser

generales, para toda la base de datos, o específicos para una tabla, columna o incluso una

consulta.

**Tipos de Privilegios en MySQL**

Los privilegios en MySQL se dividen en varias categorías, según el nivel de acceso y la operación

que se permita realizar.

**1. Privilegios Generales (Globales)**

Estos privilegios se aplican a todas las bases de datos del servidor MySQL y afectan a todas las

acciones de los usuarios en el servidor.

**ALL PRIVILEGES**: Otorga todos los privilegios disponibles.

**CREATE**: Permite crear nuevas bases de datos y tablas.

**DROP**: Permite eliminar bases de datos y tablas.

**PROCESS**: Permite ver los procesos del servidor.

**FILE**: Permite leer y escribir archivos en el sistema de archivos del servidor.

**GRANT OPTION**: Permite al usuario conceder a otros usuarios los privilegios que posee.

**SUPER**: Permite ejecutar operaciones que afectan al servidor MySQL, como el kill de procesos,

cambiar variables globales, etc.

**RELOAD**: Permite recargar las tablas de privilegios y otras configuraciones globales.

**Ejemplo:**

**2. Privilegios de Base de Datos**

Estos privilegios afectan a todas las tablas y objetos dentro de una base de datos específica.

**SELECT**: Permite seleccionar (leer) datos de las tablas.

**INSERT**: Permite insertar datos en las tablas.

**UPDATE**: Permite modificar datos existentes en las tablas.

**DELETE**: Permite eliminar datos de las tablas.

**CREATE**: Permite crear nuevas tablas dentro de la base de datos.

**DROP**: Permite eliminar tablas dentro de la base de datos.

**ALTER**: Permite modificar la estructura de las tablas existentes (como agregar o eliminar

columnas).

**INDEX**: Permite crear y eliminar índices de tablas.

**REFERENCES**: Permite crear claves foráneas (foreign keys) en las tablas.

**CREATE TEMPORARY TABLES**: Permite crear tablas temporales dentro de la base de datos.

**LOCK TABLES**: Permite bloquear tablas para evitar que otros usuarios las modifiquen durante

una operación.

**Ejemplo:**

**3. Privilegios de Tabla**

Estos privilegios se aplican a una tabla específica dentro de una base de datos. Son útiles

cuando deseas restringir el acceso de un usuario a tablas individuales dentro de una base de

datos.

**SELECT**: Permite leer los datos de la tabla.

**INSERT**: Permite insertar datos en la tabla.

**UPDATE**: Permite modificar los datos de la tabla.

**DELETE**: Permite eliminar los datos de la tabla.

**ALTER**: Permite modificar la estructura de la tabla.

**INDEX**: Permite crear y eliminar índices en la tabla.

**REFERENCES**: Permite la creación de claves foráneas en la tabla.

**LOCK TABLES**: Permite bloquear la tabla para operaciones de lectura o escritura.

**Ejemplo:**

**4. Privilegios de Columna**

Estos privilegios permiten controlar el acceso a las columnas dentro de una tabla. Son más

específicos y permiten un control granular sobre los datos.

**SELECT**: Permite leer los datos de una columna específica.

**INSERT**: Permite insertar datos en una columna específica.

**UPDATE**: Permite modificar los datos en una columna específica.

**Ejemplo:**

**5. Privilegios de Procedimientos y Funciones**

Estos privilegios permiten a un usuario ejecutar procedimientos almacenados y funciones dentro

de una base de datos.

**EXECUTE**: Permite ejecutar procedimientos almacenados y funciones.

**ALTER ROUTINE**: Permite modificar un procedimiento almacenado o función existente.

**DROP ROUTINE**: Permite eliminar un procedimiento almacenado o función.

**Ejemplo:**

**6. Privilegios de Gestión de Usuarios**

Estos privilegios permiten administrar otros usuarios y sus privilegios.

**CREATE USER**: Permite crear nuevos usuarios en MySQL.

**DROP USER**: Permite eliminar usuarios.

**GRANT OPTION**: Permite otorgar privilegios a otros usuarios.

**REVOKE**: Permite revocar privilegios de los usuarios.

**Ejemplo:**

**Comandos para Gestionar Privilegios**

**1. GRANT: Asignar Privilegios**

El comando GRANT se utiliza para asignar privilegios a los usuarios. Puedes conceder privilegios

a nivel global, de base de datos, de tabla, o incluso a nivel de columna.

**Ejemplo:**

**2. REVOKE: Revocar Privilegios**

El comando REVOKE se utiliza para revocar privilegios previamente otorgados a los usuarios.

**Ejemplo:**

3. SHOW GRANTS: Ver Privilegios de un Usuario

El comando SHOWGRANTS muestra los privilegios otorgados a un usuario específico.

**Ejemplo:**

**4. FLUSH PRIVILEGES: Recargar Privilegios**

Después de hacer cambios en los privilegios, es necesario ejecutar el comando FLUSH

PRIVILEGES para que los cambios surtan efecto.

**Ejemplo:**

**Ejercicios sobre Privilegios de Usuarios en** MySQL

**Ejercicio 1: Crear un Usuario con Privilegios**

Específicos

**Enunciado:**

1.  Crea un usuario llamado empleado con la contraseña empleado123 .

2.  Asigna al usuario empleado permisos de solo lectura ( SELECT ) sobre la base de datos

empresa\_db .

3.  El usuario empleado no debe poder modificar ni eliminar datos en empresa\_db .

CREATE USER 'empleado'@'localhost' IDENTIFIED BY 'empleado123';

GRANT SELECT ON empresa\_db.\* TO 'empleado'@'localhost';

FLUSH PRIVILEGES;

**Ejercicio 2: Revocar Privilegios y Modificar Permisos**

**Enunciado:**

1.  El usuario empleado anteriormente tenía permisos de solo lectura sobre la base de datos

empresa\_db .

2.  Ahora, revoca el privilegio SELECT al usuario empleado y asigna el privilegio INSERT para que

pueda agregar datos a las tablas de empresa\_db .

REVOKE SELECT ON empresa\_db.\* FROM 'empleado'@'localhost';

GRANT INSERT ON empresa\_db.\* TO 'empleado'@'localhost';

FLUSH PRIVILEGES;

**Ejercicio 3: Asignar Privilegios Globales**

**Enunciado:**

1.  Crea un usuario llamado admin\_db con la contraseña admin123 .

2.  Asigna al usuario admin\_db privilegios globales para crear y eliminar bases de datos ( CREATE

y DROP ), así como para gestionar usuarios ( CREATE USER y DROP USER ).

CREATE USER 'admin\_db'@'localhost' IDENTIFIED BY 'admin123';

GRANT CREATE, DROP ON \*.\* TO 'admin\_db'@'localhost';

GRANT ALL PRIVILEGES ON \*.\* TO 'admin\_db'@'localhost' WITH GRANT OPTION;

FLUSH PRIVILEGES;

**Ejercicio 4: Ver Privilegios de un Usuario**

**Enunciado:**

1.  El usuario admin\_db tiene privilegios para crear y eliminar bases de datos.

2.  Usando el comando adecuado, verifica los privilegios asignados al usuario admin\_db en el

servidor MySQL.

SHOW GRANTS FOR 'admin\_db'@'localhost';

**V. Conclusiones:**