Sécurité des systèmes d'information

TD 2 : Gestion des autorisations

1 Prérequis

Installation :

```
sudo apt install apache2 php mysql-server libapache2-mod-php php-mysql
```

Pour se connecter à mysql en tant que root :

```
mysql -u root -p
```

Crétion d'une base de données :

```
CREATE  DATABASE TP1;
```

Choisir la base de données devant être utilisées :

```
USE TP1;
```

Création d'un utilisateur :

```
CREATE USER test@localhost IDENTIFIED BY test;
```

Exercice 1

1. Quels sont les privilèges nécessaire à un utilisateur souhaitant exécuter la command SQL suivante sur les tables Employe(ID, nom) and Projet(ID_emp, nom_proj) ?

```
Delete From Employe
Where ID In (Select ID_emp From Projet Group By ID_emp Having Count(*) > 3)
```

2. Quels sont les privilèges nécessaire à un utilisateur souhaitant exécuter la command SQL suivante sur les tables Employé(ID, salaire, grade,deptID) et Département (ID, catégorie) ?

```
Update Employee E1
Set salaire = (Select Avg(salaire) From Employee E2 Where E1.grade = E2.grade)
Where deptID In (Select ID from Département Where catégorie = 'Vente')
```

3. On considère un utilisateur U1 qui a créé la table Employé (ID, salaire, département). Cet utilisateur souhaite autoriser U2 à accéder (sans pouvoir modifier) l'information des employés ayant un salaire inférieur à 30 000 et qui travaillent dans un département ayant moins de 10 employés. Donner les commandes SQL que U1 doit réaliser.

4. On considère deux tables Employe(ID, nom) et Projet(ID_emp, nom_proj). On considère les commandes suivantes réalisées par le propriétaire des deux tables :

```
Create View EmpAffectProj As
  Select Distinct ID From Employe, Projet Where Employe.ID = Projet.ID_emp;

Grant Delete on EmpAffectProj to U With Grant Option;
```

Pourquoi ce grant n'est pas autorisé dans le standard SQL ? Ecrire deux commandes équivalentes qui seront acceptées.

Exercice 2

On considère une BD décrivant une petite entreprise. La BD décrit :
— les employés : nom, salaire, nom du département,
— les départements : nom, nom du responsable.
Les utilisateurs de la BD sont ses employés :
— Alice est l'administratrice de la BD,
— Odile est la directrice du personnel,
— Pierre est l'agent comptable,
— Alain est responsable du département Informatique,
— Isabelle est une employé du département Informatique.
On considère les contraite de contrôle d'accès suivantes :
— Alice crée une vue *affectation* qui associe chaque employé à son département.
— Alice transmet à tous les utilisateurs le privilège de consulter les affectations.
— Alice crée une vue *mon_ employe* qui donne le nom et le salaire de chaque employé du département dont l'utilisateur de cette vue est le responsable.
— Alice transmet à Alain, responsable du département Informatique, le privilège de consulter le salaire des employés de ce département.
— Alice transmet à Odile, la directrice du personnel, le privilège de modifier le département dans lequel travaille un employé .
— Alice transmet à Odile le privilège de modifier responsable d'un département.
— Alice transmet à Pierre, l'agent comptable, les privilèges de consulter et de modifier le salaire des employés.
— Alice révoque le privilège de Pierre de modifier le salaire d'un employé.

1. Donner le schéma de la base de donnée en précisant les clé primaires et étrangères.
2. Créer les utilisateurs de la bases de données.
3. Donner les différentes commandes que l'administrateur doit effectuer pour créer les tables et les vues.
4. Donner les différentes commandes que l'administrateur doit effectuer pour respecter les contraintes d'accès.
5. A chaque commande effectuer les insertions minimales permettant de vérifier que les règle d'accès son bien respectées.

Exercice 3

Soit le schéma de base de données suivant :

Employé (Num , Nom, Prénom, Département, Salaire, Tel, Email)
Département (DeptId, Nom, Directeur)
EmployeDept (DeptId, NumEmploye)
Projet (ProjetId, ResponsableProjet, NomProjet, Status)
MembreProjet(ProjetID, NumEmploye)

Un directeur et un responsable de projet sont des employés (clé étrangère de l'attribut Num de la relation Employé).

Nous considérons la politique d'accès définit par les contraintes suivantes :

1. Un employé peut accéder à ses données personnelles enregistrées dans la relation Employé.
2. Un employé peut modifier son numéro de téléphone ainsi que son email.
3. Un directeur peut modifier les salaires de tous les employés de son département sauf le sien.
4. Un responsable de projet peut ajouter ou supprimer des employés à un projet dont il est responsable.
5. Un responsable de projet peut créer un nouveau projet.
6. Le directeur d'un département peut connaître le nombre d'employés de son département assignés à chaque projet.
7. Un employé peut accéder aux informations des autres employés de son département à l'exception du salaire.
8. Un employé peut connaître la moyenne des salaires de chaque département.

Les utilisateurs utilisent comme login leur numéro d'employé. En d'autres termes lorsque l'employé 123 est connecté la fonction USER() retourne la valeur 123@localhost.

1. Donner les différentes commandes que l'administrateur doit effectuer pour respecter les contraintes d'accès.
2. A chaque commande effectuer les insertions minimales permettant de vérifier que les règle d'accès son bien respectées.
3. Discuter les problèmes que peut induire la dernière règle d'autorisation (8).