Sécurité des systèmes d'information

TD 3 : Injection SQL

1 Mise en place de l'environnement

1. Télécharger l'archive TPinjectionSQL.tar.gz
2. Décompresser l'archive

   ```
   tar xvf TPinjectionSQL.tar
   ```

3. Copier les fichiers de l'application web vers le répertoire

   ```
   sudo mkdir /var/www/html/TPinjectionSQL
   ```

4. Copier les fichiers de l'application web vers le répertoire TPinjectionSQL

   ```
   sudo cp *.css *.php *.html /var/www/html/TPinjectionSQL
   ```

5. Importer les données fournies dans le script Users.sql

   ```
   $ mysql -u root -p
   mysql> CREATE DATABASE Users;
   mysql> quit
   $ mysql -u root -p Users < Users.sql
   ```

6. Parcourir le contenu de l'ensemble des fichiers de du répertoire TPinjectionSQL et comprendre le cheminement de l'application.
7. Modifier le mot de passe utilisé pour établir la connexion à la BD depuis le code php par celui défini lors de l'installation de mysql.
8. Lancer le serveur apache

   ```
   sudo service apache2 start
   ```

9. Voici un version simlifier (et avec les "vrais" mots de passe) de la table importée dans la base "Users" :

User	Employee ID	Password	Salary	Birthday	SSN	Nickname	Email	Address	Phone#
Admin	99999	seedadmin	400000	3/5	43254314				
Alice	10000	seedalice	20000	9/20	10211002				
Boby	20000	seedboby	50000	4/20	10213352				
Ryan	30000	seedryan	90000	4/10	32193525				
Samy	40000	seedsamy	40000	1/11	32111111				
Ted	50000	seedted	110000	11/3	24343244				

2 Injection SQL (select)

1. Réaliser une injection sql qui permet de s'authentifier en tant que Boby. Pour cette question nous supposons que disposez de l'ID de Boby qui est 20000.
2. Réaliser une injection sql qui permet de s'authentifier sans connaitre aucun ID. Quelle est l'employé affecté par cette attaque ?
3. Répéter l'attaque précédente pour obtenir des information sur chaque employé.
4. Pour cette question, on souhaite se connecter en tant d'administrateur sans connaitre son ID. On sait uniquement que "Admin" est le nom utilisé par l'administrateur. L'approche de la question précédente peut être fastidieuse si le nombre d'employé est élevé. Pour cette question on pourra procéder comme suit :
   (a) Faire une injection SQL permettant de récupérer le nom de la table.
   (b) Faire une injection SQL permettant de récupérer le nom des différentes colonnes de la table.
   (c) Faire une injection SQL permettant de récupérer l'ID de l'administrateur.
   (d) Faire une injection SQL permettant de se connecter en tant qu'administrateur.
5. En vous inspirant de la question précédente, obtenez une information contenue dans une autre table de la base. Quelle bonne pratique aurait pu limiter l'impacte de votre attaque ?

3 Injection SQL (update)

1. Réaliser une injection sql qui permet à Ryan de modifier son salaire. Pour cette on connait l'ID de Ryan (30000) ainsi que son mot de passe (seedryan).
2. Réaliser une injection sql qui permet à Alice de modifier de numéro de téléphone de Ryan.
3. Est-ce que Alice peut modifier le mot de passe de Ryan ?