CRM - Exigences techniques

Procédures de sécurité requises à respecter :

- **Utiliser Python 3**.
- **Empêcher une injection SQL.** Veiller à gérer les entrées des utilisateurs pour prévenir une injection SQL en :
    - utilisant Django ORM ;
    - évitant d'utiliser les requêtes SQL brutes à moins que cela ne soit absolument nécessaire.
- **Garantir l'authentification.**
    - Activer et utiliser le framework d'authentification Django dans les paramètres (django-admin startproject).
    - Mettre en œuvre et faire appliquer le principe du moindre privilège lors de l'attribution de l'accès aux données. Veiller à ce que les utilisateurs n'aient accès qu'aux données dont ils ont besoin.
    - Supprimer les erreurs d'autorisation ou les droits de contrôle d'accès incorrectement configurés qui permettent un accès non autorisé.
- **Mauvaises configurations de sécurité.** S'assurer que toutes les vues disposent de décorateurs et/ou de contrôles de logique pour les configurations de sécurité :
    - Les autorisations d'utilisateur sont appropriées.
    - Les méthodes HTTP utilisées dans la requête sont autorisées.
- **Effectuer le logging et la surveillance.** Toutes les applications doivent consigner les exceptions et les erreurs produites.