1. **SQL Injection**
   1. Definition

Une attaque par injection SQL cible les applications utilisant des systèmes de Gestion de base de données.

Lors d’une attaque par injection SQL, l’attaquant fournit un/des segments malicieux de code SQL en tant qu’input transformant la requête SQL initiale en une autre souvent dangereuse. Les attaques par injection SQL sont le plus souvent utilisées pour dérober des informations sensibles de la base de données.

Par une injection SQL, l’attaquant, selon ses capacités peut obtenir des informations confidentielles ou même arriver à modifier ces informations.

* 1. Causes

La cause principale d’une injection SQL est le fait qu’une application accepte des données provenant de sources non sures comme l’utilisateur par exemple (input) ou le navigateur de l’utilisateur (cookies ou headers des requêtes http)

* 1. Vecteurs principaux
* HTTP POST
* HTTP GET
* Cookies
  1. Préventions

Principales :

* Input Validation
* Encodage
* Requêtes préparées

Supplémentaires :

* Réduire la surface d’attaques en donnant le moins de privilèges
* Crypter toutes les données sensibles
* Se méfier des headers http

