SQL Injection

AND HOW TO EASILY PREVENT IT

Objectif de la présentation

- Comprendre ce qu'est une Injection SQL
- Comprendre comment les prévenir et lutter contre.

Les Injections SQL

Alors c'est quoi une injection SQL ?

Les injections SQL

- Une attaque sur une application web qui permet d'insérer des instructions SQL malveillante dans l'application.
- Le but est de pouvoir accéder à des données sensible, et en tirer profit ou par exemple les supprimer.

On parle « DES » injections SQL, mais quelles sont elles ?

Les Types d'Injections SQL

- Injection SQL In-Band (Même canal utilisé pour insérer le code malveillant et rassembler les résultats)
  - Attaque basée sur l'erreur
  - Attaque basée sur l'union
- Injection SQL Inférentielle (Injection SQL aveugle) (On envoi plusieurs requetes à l'aveugle pour analyser les réponses)
  - Booleéne = « … and 1=1 » or « … and 1=2 »
  - Basée sur le temps Attaque basée sur l'erreur
- Injection SQL Out-of-Band
  - Alternative au InBand pour rassembler les resultats

Les risques d'une Injection SQL

- Comme vous le comprenez, les risques d'une injection SQL sont à la fois nombreux, mais surtout à la fois grave.

  Imaginez une base de données d'utilisateurs sont les informations se retrouvent dans la nature (Nom, adresse, numéro de CB, téléphone etc)

  Ou encore, imaginez que vous BDD est votre gagne pain et que d'un coup, un supprime tous vos utilisateurs ….

Comment se prémunir ?

- J'ai peur

- Mais …

Les bonnes pratiques

- Vérifier les entrées utilisateurs
  - Login.replace(« ; », « »)

- Utiliser les PreparedStatement
  - stmt = conn.prepareStatement(query);
    stmt.setString(1, username);
    stmt.setString(2, password);

Les bonnes pratiques (Bis)

- Voici un bonus des bonnes pratiques:
  - Valider les données et leur format avant de les envoyer en requete
  - Ne pas utiliser de nom communs pour les tables (tbluser, tblaccount)
  - Utiliser Hibernate ou Spring
  - Limiter l'accès à la DB via les permissions et accès
  - Ne pas retourner d'erreur trop précise pouvant donner des infos
  - Utiliser des outils tels que SQLMap pour fix les vulnérabilités

Est-ce que c’est clair ?

Ressources

- https://www.oracle.com/fr/security/injection-sql-attaque.html
- https://www.digitalocean.com/community/tutorials/sql-injection-in-java
- https://kinsta.com/fr/blog/injections-sql/