Deuxième année

Cours 2: Pourquoi les injections SQL existent-elles toujours ?

Les injections SQL représentent toujours une menace sur les applications WEB (*en tête du classement TOP 10 de l'OWASP*)

Burp Suite

Pour *réaliser ou simuler une attaque* de ce genre, on peut utiliser ce **logiciel** très utilisés dans le monde de la cybersécurité. Il permet d'effectuer des tests de pénétration. **C'est une suite complète d'outils de cybersécurité**.

Pour sécurisé son application WEB – >

Interface utilisateur (partie HTML)

Sécuriser au maximum le formulaire en limitant les actions et les saisies de l'utilisateur.

- Limiter le nombre de caractères (minlength, maxlength)
- Définir le bon type de champs (text, email, password)
- Ajouter les attributs nécessaires (required, pattern)

pattern – > permet de préciser une expression régulière. (la valeur du champs devra respecter la contrainte du formulaire)

Interactions locales (partie JS)

Créer des fonctions de vérifications des champs du formulaire:

- format valide de l'adresse mail
- caractères autorisés ou non
- limiter l'expérience utilisateur quand nécessaire (interdire la modification d'un champs / interdire l'envoi d'un champs vide)

Interrogation serveur

- Utilisation de PDO avec PHP (requêtes préparées puis exécutées)
- Créer des fonctions de vérification des données

ORM (Object-Relational-Mapping)

Méthode d’accès aux données d’une BDD qui utilise une syntaxe orientée objet au lieu d’utiliser le langage SQL.

- **Créer les classes objet pour que la BDD corresponde aux objets** (utilisation de framework / architecture MVC)