Sécuriser un projet web – La Fnac

1.Injection XSS (Cross-Site Scripting) et utilisation de cookie d'identification

L'injection XSS consiste à insérer du code JavaScript malicieux dans un formulaire, où en l'occurrence l'espace commentaire d'un produit Fnac, qui sera ensuite exécuté dans le navigateur d'autres utilisateurs. Les scripts sont souvent utiliser pour récupérer les cookies d'identifications et voler leurs sessions

Solutions :

- Utiliser l'attribut HttpOnly sur les cookies pour les rendre inaccessibles par JavaScript.
- Utilisation et configuration de certain Framework comme Apache2.

2. Injection SQL

Consiste à insérer des méthodes SQL dans les formulaires de la Fnac, ce qui peut donner accès à la base de données de Fnac.

Solutions :

- Utiliser la validation des entrées pour empêcher l'injection de code.
- Paramétrer les variables pour séparer le code SQL des données.
- Utiliser un ORM (Object Relational Mapping) pour générer automatiquement les requêtes SQL sécurisées.

3. Brute force

Consiste à répéter toutes les combinaisons possibles d'un mot de passe pour l'hacker, souvent à l'aide d'un malware.

Solutions : Utiliser des algorithmes de hachage (exemple :ARGON2) et/ ou salage qui est une donnée aléatoire rajouté lors du hachage pour crypter les mots de passe.