CERTIF ACADEMY

1. Les attaques MITM : HTTPS
2. Le phishing : Eduquer les visiteurs
3. Les attaques CSRF : Token CSRF
4. Les modifications du DOM : Faire les vérifications au backend
5. Les injections : Figer la forme de la requete SQL et désactiver les balises HTML
6. Le brute force : Mettre une limite sur le nombre d‘essais

CERTIF
ACADEMY

CERTIF ACADEMY

Que sont les injections ?

CERTIF ACADEMY

PREVENTION

Il faut désactiver le code SQL ou HTML dans les données que l‘on recoit au niveau du payload.

Si nous ne les désactivons pas, on s‘expose au risque que les codes injectés peuvent s‘exécuter.

CERTIF ACADEMY

1. Injections SQL : pour désactiver le code SQL, il exite 2 manières : soit on utilise les requêtes préparées, soit on utilise la fonction quote pour désactiver les codes SQL directement

2. Injections XSS : désactiver le code HTML dans les variables - utiliser la fonction htmlentities pour désactiver les codes HTML directeement

CERTIF ACADEMY

Désactivation du code SQL en entrée

CERTIF ACADEMY

Utiliser les requêtes préparées pour figer la forme de la requête

Les requêtes préparées sont des requêtes précompilées.

CERTIF ACADEMY

Hibernate, qui est une implémentation de JPA, utilise déjà des requêtes préparées dans sa forme la plus simple si vous n’avez pas écrit vos propres requêtes SQL.

CERTIF ACADEMY

Désactivation du code HTML en entrée

CERTIF ACADEMY

Il faut échapper les caractères < et > !

CERTIF ACADEMY

Spring Security fournit plusieurs en-têtes de sécurité par défaut. Il inclut l'en-tête X-XSS-Protection. X-XSS-Protection indique au navigateur de bloquer ce qui ressemble à XSS. Spring Security peut automatiquement ajouter cet en-tête de sécurité à la réponse.

CERTIF
ACADEMY