Deuxième année

Cours 1: La protection des applications web

OWASP (Open Web Application Security Project)

– > **Communauté qui travaille sur la sécurité des applications web**

Son but – > **publier des recommandations de sécurisation** des sites web et proposer des outils permettant de tester la sécurité des applications web.

Projet TOP 10

– > vise à lister les **10 risques de sécurité et vulnérabilités les plus critiques** affectant les applications Web.

Ce classement a pour but d'**informer l'existence de ces vulnérabilités et de fournir les guides simplifiés** sur les bonnes pratiques pour s'en prémunir.

Broken Access Control

Le contrôle d'accès applique une stratégie pour que les utilisateurs ne puissent pas agir en dehors de leurs autorisations prévues. On place les utilisateurs dans des groupes où la gestion de profil est possible.

Motivations des attaquants – > *divulgation d'informations, modification ou la destruction de données, l'exécution d'une fonction quelconque qui n'était pas attribuée à l'utilisateur*

Vulnérabilités courantes – >

- Contournement des restrictions
- Permettre à la clé primaire d'être remplacée par l'enregistrement d'une autre utilisateur
- Élévation de privilège en manipulant les métadonnées
- Forcer la navigation vers des pages authentifiées ou privilégiées

Injection SQL

Type de cyberattaque dans lequel l'attaquant insère son propre code dans un site web ou une application qui utilise le langage SQL pour manipuler ses informations dans la base de données. – > **le pirate peut ainsi accéder aux informations potentiellement sensibles.**

Exemple: ‘ OR 1=1 # (“1=1” est toujours vraie”)

Quelques solutions – >

- refuser par défaut l’accès aux fonctionnalités/applications
- le test manuel est le meilleur moyen de détecter le contrôle d’accès manquant ou inefficace
- on peut ajouter aussi des logiciels de scan de vulnérabilité des applications (VST) ou des outils de test de sécurité des applications statiques (SAST)