Classes d'attaques

BAC

Broken Access Control

Description :

Actions d'utilisateurs en dehors des autorisations qui leur sont accordées :

- Utilisateur non authentifié accédant à des parties requérant l'authentification
- Utilisateur authentifié ayant accés à des parties auxquelles il ne devrait pas avoir le droit compte tenu de son rôle

Défaillances cryptographiques

Description :

Exposition (en clair ou non suffisamment protégées) de données nécessitant une protection (voir RGPD) : mots de passe, numéros de carte de crédit, dossiers médicaux, informations personnelles, informations internes d'entreprises

Conception non sécurisée

Description :

En phase de conception, absence de profilage des risques inhérents au logiciel ou au système en cours de développement, et donc incapacité à déterminer le niveau de sécurité requis

Défaut de configuration lié à la sécurité Description :

L'application ou l'un de ses composants est mal configurée et devient vulnérable compte tenu d'une configuration inappropriée.

XSS

Cross Site Scripting (XSS)

Description :

- Injection de code (HTML, JS) côté client (navigateur)
- Pollution (visuelle, comportementale)
- Récupération d'informations ((sessions, coordonnées, mots de passe, informations bancaires, etc)
- Exécution d'action (à l'insu de l'utilisateur authentifié)

CSRF

Cross Site Request Forgery (XSRF)

Description :

- Utilisateur authentifié (session valide) sur un site (sensible)
- La navigation sur un site externe “malveillant” provoque une requête vers le site

Cross Site Request Forgery

SSRF

Server-Side Request Forgery (SSRF)

Description : Equivalent, côté serveur, du CSRF. Il s’agit, pour un attaquant, de demander au serveur vulnérable d’effectuer des requêtes vers des destinations choisies par l’attaquant en profitant éventuellement des privilèges du serveur (par exemple, l’accès à un réseau privé)

SQLi

Injections SQL (SQLi)

Description :

- Transmission de code malveillant (SQL partiel) parmi les données entrantes
- Le serveur web utilise ces données pour créer une requête à destination d’une base de données
- Exfiltration, altération ou suppression de données

Liens :

Tutoriel Injections SQL (zestedesavoir)

Session hijacking

Description : Vol d'id de session par l'un des moyens suivants :

- Predictable session token;
- Session Sniffing;
- Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc);
- Man-in-the-middle attack
- Man-in-the-browser attack

voir https://owasp.org/www-community/attacks/Session_hijacking_attack