Injection SQL :

L'injection SQL consiste en la transmission de code malveillant parmi les données entrantes qu'un serveur web utilise pour formuler une requête à destination d'une base de données. Cette classe d'attaques occasionne une perte de contrôle sur les données en base, ce qui peut mener à leur exfiltration, altération ou suppression.

Comment se mettre à l'abri d'une injection SQL ?

L'approche recommandée pour éviter ce type de vulnérabilité consiste à recourir soit à des couches d'abstraction de la base de données qui prennent en charge ce problème, soit à utiliser des requêtes préparées et fortement typées. Tous les langages web couramment employés permettent le recours à de tels mécanismes.

- PDO permet de définir le typage des données entrées
- Utiliser Htmlspecialchars

Faille XSS :

La faille XSS ou Cross Site Scripting réside sur le principe d'intégrer du code Javascript dans un navigateur. Il est possible d'effectuer des actions malveillantes tels que :

- Les données injectées ont la forme de langages interprétés par le navigateur tels que JavaScript ou HTML. Une attaque XSS cible les utilisateurs du site et vise en général à récupérer des secrets émis ou reçus par ceux-ci (sessions, coordonnées, mots de passe, informations bancaires, etc.), ou bien à effectuer des actions en leur nom

- récupérer l'ID d'une session en cookie qui était stocké en base de données via la commande output=”+document.cookie;” l'attaquant pourra se faire passer pour la victime et accéder à son ID de session. Les failles XSS se trouvent souvent dans les commentaires d'un site.

- A l'aide d'une requête Javascript l'attaquant a un contrôle total de la page, peut faire cliquer un bouton à l'insu de l'utilisateur et même envoyer un formulaire et effectuer n'importe quelle action à l'insu de l'user et ceci est encore plus grave si l'user se trouve être l'admin.

Comment se mettre à l'abri d'une faille XSS ?

- Il faut vérifier chaque champs ou l'utilisateur peut entrer des données;
- utiliser la fonction htmlspecialchars() qui filtre les '<' et '>' (cf. ci-dessus).
- utiliser la fonction htmlentities() qui est identique à htmlspecialchars() sauf qu'elle filtre tous les caractères équivalents au codage HTML ou JavaScript.

File inclusion / Faille File upload :

Il est possible d'être attaqué par le biais d'une inclusion de fichier, en effet l'utilisateur peut chercher à exploiter ce fonctionnement pour y inclure un fichier qu'il maîtrise ou qui contient du code malveillant.

Ce type d'attaque peut aussi servir à lire et à afficher le contenu de fichiers a priori inaccessibles sur le serveur par traversée de l'arborescence du système de fichiers. Les fichiers du site deviennent accessibles.

Comment se mettre à l'abri de cette faille ?

- requérir une taille de fichier maximum et un type de fichier spécifique (.jpg/.png/.jpeg)

Faille humaine :

Comme grossièrement expliqué, il est important de ne pas faire confiance aux utilisateurs mais également à ses employés. En effet, l'abus de confiance est un facteur important car beaucoup de cybercriminels savent abuser de la confiance des gens. En entreprise, il est fréquent qu'un technicien informatique appelle l'un de ses clients au téléphone et lui demande son mot de passe.
Soit parce que cela facilite la télémaintenance, soit pour gagner du temps, voire pour éviter de se déplacer. Et généralement, le correspondant lui indique son mot de passe sans sourciller.

Spam et Phishing :

La faille la plus classique de la sécurité informatique est toujours très populaire ! Il est donc toujours fortement déconseillé d'ouvrir par curiosité les pièces jointes de mails provenant d'expéditeurs inconnus ou encore d'activer un lien réclamant un nom d'utilisateur et mot de passe à partir d'un email dont la provenance et l'aspect semblent authentiques (alerte Microsoft, Apple ou autres).
Ces erreurs continuent de causer des pertes annuelles qui se comptent en milliards pour les entreprises.

La connexion d'une clé USB inconnue :

La curiosité pousse certaines personnes à connecter à leur ordinateur des clés USB trouvées par hasard, sans en connaître l'origine. Un cybercriminel dispose pourtant de multiples opportunités avec une simple clé USB. Il peut par exemple utiliser un fichier infecté pour accéder à des données et des mots de passe (ingénierie sociale) ou exploiter une faille sans correctif connu et en faire profiter son réseau. Il peut même configurer une clé USB pour que celle-ci se fasse passer auprès de l'ordinateur pour un clavier qui exécute des commandes via des entrées de touches simulées.

COOKIE & RGPD :

Il est important de savoir que les cookies sont sujet à controverses ces temps-ci, en effet ils portent atteinte à la liberté de l'utilisateur. C'est pourquoi actuellement il est obligatoire de laisser à l'utilisateur le choix d'accepter ou non l'utilisation des cookies.