LES FAILES DE SECURITE

Les 5 failles de sécurité les plus courantes d’un site web

1ere faille web

La faille XSS

Une faille XSS consiste à injecter du code qui pourra être interprété directement par le navigateur Web. Ce dernier ne fera ainsi aucune différence entre le code du site et celui injecté par le pirate. Les effets sont bien entendu assez embêtants puisque vous risquez de faire face à des redirections vers un autre site, du vol de cookies ou encore une modification du code de votre page.

Pour vous protéger des XSS, vous devez remplacer les caractères pouvant être compris par le navigateur comme des balises par leur entité HTML. En procédant ainsi, le navigateur affichera mot à mot le caractère et ne cherchera plus à l'interpréter. En PHP, vous pouvez utiliser les fonctions htmlentities ou htmlspecialchar.

2ème faille web

La faille include

Il s'agit d'une faille très dangereuse. Comme son nom l'indique, elle exploite une mauvaise utilisation de la fonction include. La plupart du temps, cette fonction est utilisée pour exécuter du code PHP qui se situe dans une autre page, permettant de se connecter à une base de données. Il existe deux type de failles include :

A distance : il s'agit de la faille include par excellence. C'est à la fois la plus courant et la plus facilement exploitable.

En local : cela revient à inclure des fichiers qui se trouvent sur le serveur du site. Une personne mal intentionnée pourra donc s'emparer, assez facilement, de votre fichier contenant vos mots de passes.

Pour se protéger de cette faille, rien de mieux que de la tester ! Il vous suffit d'inclure une page qui n'existe pas. Si l'URL de celle-ci est vulnérable, un message d'erreur vous sera transmis venant de PHP.

3ème faille web

La faille upload

Cette faille peut apparaître lors de l'upload de fichiers sur un site : photo de profil, document pdf, image dans un message, etc. Elle profite de l'action effectuée pour mettre en ligne des fichiers malveillants PHP qui vont permettre au « hacker » de prendre le contrôle total de notre site.

Pour éviter cette vulnérabilité, il est important de :

Empêcher les utilisateurs d'envoyer des fichiers lorsque cela n'est pas une fonction primordiale pour votre site ou application

Interdire l'exécution de code depuis le dossier dans lequel sont stockés les fichiers uploadés sur votre site

Vérifier et autoriser l'extension des fichiers que vous tolérez via une liste blanche

4ème faille web

Injection SQL

Cette faille survient lors de la modification d'une requête SQL et consiste à injecter des morceaux de code non filtrés, généralement pas le biais d'un formulaire. Cela revient à détourner la requête et lui faire faire autre chose que ce pour quoi elle a été conçue. Cette manipulation donne donc accès à vos données telles que les login, mots de passe ou adresses e-mail.

5ème faille web

Attaque par force brute

Cette méthode consiste à trouver le mot de passe ou la clé cryptographique d'une personne afin de pouvoir accéder à un service en ligne, à des données personnelles, voire à un ordinateur. Il est donc indispensable d'utiliser des mots de passe forts pour vos sites et comptes utilisateurs afin de rendre complexe l'attaque par une personne tiers.

3 conseils utiles pour renforcer vos mots de passe :

Utiliser des lettres minuscules, des majuscules, des chiffres et des caractères spéciaux (notez qu'il existe des générateurs automatiques de mots de passe sur internet)

Renouveler souvent ses mots de passe

Utiliser des mots de passe différents pour chaque site

Des sources pour rester informé sur les nouvelles failles

https://www.cert.ssi.gouv.fr/

https://vigilance.fr/?langue=1

https://security.stackexchange.com/

https://owasp.org/