La sécurité d’un site Web

Afin de traiter ce sujet nous énumérerons les attaques, les motivations des attaquants, ainsi que les solutions pour se protéger.

Table des matières

Les attaques DDoS (Distributed Denial of Service attack)

Le but d’une attaque DDoS est de submerger un site web de requête afin de le mettre hors-service.

Les pirates utilisent souvent des milliers d’ordinateurs dits « zombies ». Il s’agit d’ordinateur ne leur appartenant pas. Ils ont pris le contrôle de ces ordinateurs par différents moyens et s’en servent pour attaquer un site.

A travers ce moyen, le pirate peut être employé par une société A afin de rendre le site du concurrent B inaccessible.

Pour s’en protéger, il est possible de louer un serveur d’hébergement web (OVH, AWS, etc.) et l’hébergeur se chargera alors de vous en protéger. Cependant si vous héberger votre site sur votre propre serveur, la principale méthode pour s’en protéger est de bloquer l’adresse IP d’une machine qui enverrait trop de requêtes à la seconde. Par ce moyen, la machine attaquante qui enverrait une requête n’obtiendrait alors plus de réponse du serveur, donc ne le ralentirait plus.

Les attaques MitM (Man in the Middle)

Le principe de cette attaque est de pouvoir se glisser entre le serveur et le client afin de pouvoir dérober des informations telles que des ID de session ou des adresses IP. Par ce biais il serait alors possible pour le pirate de se faire passer pour le client aux yeux du serveur.

En se faisant passer pour le client, le pirate pourrait alors avoir accès aux cookies ainsi qu'aux informations confidentielles du client. Il lui serait alors possible de commander des choses avec la carte du client si celle ci est renseignée sur le site.

Afin de se propager au sein du réseau, le pirate a besoin que la page ne soit pas sécurisée (HTTP), il faut alors forcer l'utilisation d'un protocole sécurisé (HTTP**S**). Par ce biais, il ne sera alors plus possible de subir des attaques de types MitM.

Les attaques visant les mots de passe

Les pirates affectionnent tout particulièrement ces attaques, étant donné qu'elles leur permettent d'avoir accès au mot de passe de la victime, donc à son compte. Il existe deux méthodes de crackage de mot de passe :

- les attaques par force brute qui testent toutes les combinaisons de mots de passe.

- les attaques par dictionnaire qui utilisent un dictionnaire des mots de passe les plus fréquents.

Afin de s'en protéger, tout comme les attaques DDoS, on peut bloquer les adresses IP qui effectuent trop de tentatives par seconde. On peut également utiliser un système de hashage de mot de passe qui fait perdre quelques millisecondes pour un utilisateur lambda, mais qui peut faire perdre des heures à un pirate qui fait plusieurs millions de tentatives par seconde.

Les injections SQL

L'injection SQL vient du langage SQL servant à manipuler des données dans des bases de données (MySQL, PostgreSQL, etc.). L'injection en elle même consiste dans un champ d'entrée (input) à écrire une requête ou un bout de requête. Par ce biais, il pourrait avoir accès à des informations contenues dans la base de données.

Le meilleur moyen pour s'en prémunir est d'utiliser la classe PDO qui va traiter toutes les données afin de les rendre sans danger pour la base de données. Si l'utilisation de PDO est impossible, il est alors possible avant de rentrer les données dans la base, d'utiliser des fonctions pour en vérifier le contenu et enlever ce qui pourrait être problématique (–, ‘, ‘’, etc.). Dans le langage PHP la fonction principale est **mysqli_real_escape_string()**.

Les failles XSS

Les failles XSS (Cross site scripting) sont très dangereuses. Il existe trois sous parties dans ces attaques :

- Les attaques XSS stockées : Le pirate envoie du code malicieux, celui-ci est stocké dans une base de donnée et est retourné à tous les utilisateurs naviguant sur le site par la suite.
- Les attaques XSS reflétées : Le pirate crée un lien vers un site sain mais rajoute à l'URL une partie de code, qui une fois traitée par le serveur web, va s'exécuter et pourrait servir, par exemple une campagne de phishing.
- Les attaques XSS basées sur le DOM : De nos jours, certains sites / applications web sont complètement réalisés en Javascript. De par ce fait il est alors de possible de manipuler le DOM, qui est l'outil permettant de modifier le contenu d'un navigateur, afin d'exécuter le code que l'on souhaite.

Afin de ce prémunir des 2 premiers types d'attaque XSS, il faut tout comme pour les injections SQL, vérifier le contenu de ce qui est envoyé par le client. Pour la troisième, il faut faire en sorte que le script d'exécution côté client vérifie également tout ce qui est entré par le client.