C'est quoi une faille Upload ?

Vous connaissez sûrement la balise HTML qui permet l'upload de fichier :

<input type="file" />

La faille upload est une faille permettant d'uploader des fichiers avec une extension non autorisée, cette faille
est due à la mauvaise configuration du script d'upload ou à l'absence complète de sécurité. Celle-ci est généralement
présente dans les scripts d'upload d'images.

Le but de cette faille est d'uploader un fichier avec une extension non autorisée. (Par exemple un code php)
de façon à avoir un accès au serveur cible.

Il existe plusieurs méthodes pour passer les protections, si protection il y a.

Vous pouvez altérer le fichier au moment de l'upload avec 'Tamper Data', un outil du naviagteur de firefox.
Grâce à ces outils vous allez pouvoir upload le fichier en tant qu'image. Une fois le fichier upload vous
n'avez plus cas y accéder et l'exécuter avec l'URL.

Deuxième méthode, la double exention.

Certains sites vérifie l'extention du fichier que vous voulez upload, il existe un moyen de contournée cette sécurité,
la double extention. L'idée c'est d'intégrer du code php dans un fichier .gif. Tout d'abord crée un fichier .gif avec
paint par exemple, ensuite ouvrez se fichier avec un éditeur hexadécimal. Ajouter votre code PHP dans le .gif,
est ajouté l'extension .php, ce qui nous donne "file.php.gif". Maintenant l'upload va s'effectuer sans soucis !
On se rendra notre fichier.php.gif ?

http://monsite.com/fichier.php

Voila !

Comment se sécuriser face a une faille upload ?

-Ne jamais se fier à ce que peut envoyer le client.
-Vérifier la configuration d'Apache afin d'agir en conséquence.
-Ne pas placer le .htaccess dans le répertoire d'upload
-Ne pas permettre l'écrasement de fichier
-Générer un nom aléatoire pour le fichier uploadé et enregistré le nom dans une base de données.
-Ne pas permettre de voir l'index of du répertoire d'upload.
-Assigner les bonnes permissions au répertoire.
-Vérifier le mime-type avec getimagesize() et l'extension du fichier.

Détection d'une faille upload ?

Voici des outils pour détecter ces failles :

-ScanMyServer

ScanMyServer propose l'un des rapports le plus complet en matière de test de sécurité comprenant l'injection SQL, la faille XSS,
l'injection de code PHP, l'injection d'en-tête HTTP, etc. Le rapport d'analyse vous est adressé par courriel avec un résumé du niveau global de vulnérabilité de votre site web.

-Quttera

Quttera vérifie votre site et détecte les malware et les failles de sécurité éventuelles. Vous aurez une vue complète sur les fichiers infectés,
les fichiers douteux, les fichiers à risque, etc.

Les pratiques a prendre pour éviter une faille upload :

Il suffit de contrôler les informations rentrées par l'utilisateur, dans le cas d'un formulaire qui permettrait d'envoyer des photos,
il faut être certains que les extensions des fichiers qui sont envoyés soient en JPEG, PNG etc…, voici un exemple de code en PHP qui permet de vérifier l'extension du fichier.

```
if(preg_match("#jpeg|png#",$_FILES["image"]["type"])){
     echo "fichier envoyé !";
}else{
     echo "Fichier non valide.";
}
```

Il est aussi important de vérifier les droits de lecture / écriture (CHMOD) de vos fichiers sur le serveur pour
éviter à un utilisateur d'accéder à certains fichiers / répertoires.

Ou se mettre a jour ?

Futura sciences (https://www.futura-sciences.com/tech/cybersecurite/actualites/)