UPLOAD FILE

Beaucoup de sites Web offrent la possibilité aux clients d'y uploader des fichiers comme des photos, des vidéos, des CV... Donc il ne s'agit pas vraiment d'une vulnérabilité, mais c'est le fait de ne pas contrôler ce que le client charge sur le serveur qui constitue une vulnérabilité très dangereuse.

Le principe de l'attaque est très simple. Le pirate essaie d'uploader un fichier qui contient du code malveillant ou un code PHP de sa création. Si la faille est là alors le fichier finira pas atterrir sur le serveur. Il suffit ensuite au pirate d'appeler son fichier pour que celui-ci s'exécute.

Bien entendu une telle attaque peut avoir de graves conséquences comme par exemple:

- Espionnage des fichiers et dossiers du site
- Accès au fichiers systèmes et fichiers confidentiels
- Destruction ou altération de données existantes sur le serveur
- Prise de contrôle du serveur

Comme d'habitude, la vulnérabilité est due au mauvais contrôle des entrées de l'utilisateur, alors qu'il suffisait de vérifier si le type/Mime du fichier uploadé correspond bien à une image JPEG ou PNG en utilisant le code suivant par exemple:

```
<?php
   if(preg_match("#jpeg|png#",$_FILES["photo"]["type"]))
      // Accépter l'upload
   else
      echo "Format du fichier invalide.";
?>
```