TP Sécurité : LFI/RFI

Exercice 1 : Attaque LFI de base

1) Utiliser les deux fichiers : lfi.html et index.php, lfi affiche un message simple et correspond à notre script malveillant. L'objectif est que index.php inclue lfi.html. Réalisez cette opération.

2) Une fois que le fichier index.php inclue lfi.html, faite cette même inclusion via un paramètre GET dans l'url.

3) Le fichier /etc/passwd correspond aux mots de passes utilisateurs. Afficher son contenu via le paramètre GET dans le navigateur, même principe que la question précédente.

4) Récupérons le code source ! Il est possible d'utiliser certains wrappers comme les "PHP filters" pour récupérer le code source des fichiers souhaités. Via cette technique, il est possible de récupérer le code source de fichiers PHP !

Remarque : php://filter/read=convert.base64-encode/resource=PAGE et aidons nous de https://www.base64decode.org/

Exercice 2 - Empoisonnement des logs :

1) Sur le même site ouvrez la console de développeur et allez sur l'onglet Réseau. Modifier la requête et modifier le userAgent en y rajoutant du code PHP (un echo ou un phpinfo() par exemple). Envoyer la requête.

2) Afficher les logs apache comme pour l'Ex1 - 2. Votre code s'est il exécuté ?

Exercice 3 - Protection :

1) Trouver un moyen de corriger cette faille sur votre site en utilisant str_replace pour vérifier que la valeur de $_GET ne soit pas une attaque LFI.

Mariot Guillaume – Laloy Pierre – Dutel Louis – Damiens Florent