TP : Étude de la faille LFI / RFI

DUREE 2H

EPISEN - ITS
Université Paris-Est Créteil

LFI / RFI

1. Objectifs pédagogiques :

Sécurisé un système d'information est sans conteste une tâche ardue et il est inenvisageable de penser en faire le tour en une série de TP. Cette série de TP est donc conçue comme une série de challenges qui répondent, chacun, à un objectif différent. Le but espéré est de vous pousser à la réflexion et à approfondir les sujets étudiés.

L'étude de ces failles informatiques est uniquement à but pédagogique et ne vise pas à pousser à l'illégalité. L'objectif pédagogique de cette activité est de sensibiliser les étudiants aux vulnérabilités des failles informatiques les plus classiques.

2. Prérequis :

Avant de commencer le TP nous recommandons fortement de lire et comprendre le cours relatif à la vulnérabilité étudiée. En plus de comprendre le fonctionnement de la faille, ses risques et ses enjeux ceci vous permettra d'acquérir de la facilité dans la réalisation du TP.
Après la réalisation de ce TP, nous vous encourageons à tester vos connaissances via le QCM présent sur la plateforme.

3. TP :

1) Quelles sont les différences entre une faille LFI et RFI ?

2) Que peut-on faire avec une faille LFI ? Et RFI ?

Dans un premier temps nous allons mettre en place un serveur PHP contenant une faille LFI. Pour cela, vérifiez que votre VM est en accès par pont. Cela va permettre d'accéder au site web de la VM sur votre PC.

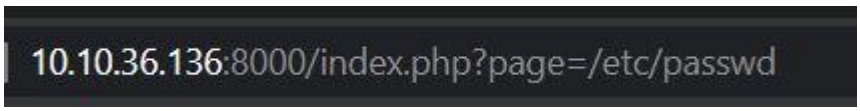
Sur votre VM, créez un fichier index.php contenant le code suivant :

```
 GNU nano 2.7.4                    File: index.php

<?php
if(isset($_GET['page']) && !empty($_GET['page'])){
        include($_GET['page']);
}

?>


<html>
<p> Bienvenue </p>
</html>
```

Pour lancer le serveur local PHP avec la page index.php, lancez la commande suivante : *php –S ipEth0:8000 index.php*

Pour accéder au site web, il vous suffit d'écrire l'URL suivante : *ipEth0:8000/index.php*
Vous devriez voir apparaitre le texte "Bienvenue" affiché.

Pour effectuer une attaque LFI, modifiez l'URL en ajoutant à la fin de l'URL : *?page=/etc/passwd*



3) Quel est le résultat de cette URL ?

4) A quoi cela correspond ? Quelles sont les informations importantes présentes ?

5) Que pouvez-vous faire avec ces informations ?

6) Essayez d'atteindre d'autres données sensibles sur la VM hébergeant ce site web.

7) Comment résoudre cette faille ? Mettez en place les mesures nécessaires pour enlever la faille. Vérifiez si votre solution est fonctionnelle.

8) Avec une attaque comme celle-ci, est-il possible de mettre en place un reverse shell ? Si oui, expliquez comment ? Quel est son intérêt ?

9) En reprenant l'exemple donné avec la faille LFI, comment serait-il possible de mettre en place une attaque RFI ? Mettez en place un exemple simple avec une redirection vers le site de Google.

10) Quel serait l'intérêt pour une personne malveillante de mettre en place une attaque RFI ? Expliquez en détail un cas d'utilisation possible.

4. Approfondir la réflexion :

Pour en savoir plus sur le reverse shell via LFI :
https://a3h1nt.medium.com/from-local-file-inclusion-to-reverse-shell-774fe61b7e1e