Local File Inclusion

Description

Les LFI pour Local File Inclusion sont des vulnérabilités qui peuvent permettre à un attaquant d'inclure des fichiers locaux dans une application Web vulnérable.

Cela signifie que l'attaquant peut arbitrairement charger un fichier local présent sur le système cible, comme par exemple des fichiers de configuration, des journaux du système ou encore des fichiers contenant des informations sensibles telles que des mots de passe.

Pré-requis d'exploitation

Pour exploiter cette vulnérabilité, il est nécessaire d'avoir accès à une application Web vulnérable utilisant des fonctionnalités d'inclusion de fichiers locaux.

Connaissances nécessaires

- Connaissances des bonnes pratiques et mesures de sécurité en langage de programmation (PHP, Perl, Python).

Outils nécessaires

- Outils de modification et/ou d’interception de requêtes (Burp, Curl).

Flux d'exécution

Explorer

Pour identifier les endpoints et/ou pages vulnérables à une LFI, il est important de naviguer sur l'application de manière exhaustive. Les pages dynamiques qui prennent en charge les paramètres utilisateur doivent être examinées attentivement pour détecter les vulnérabilités LFI. Les points d'entrée vulnérables peuvent être identifiés en recherchant des chaînes de caractères spécifiques telles que “file=app.php” ou “inc=func”.

Expérimenter

Une fois les points d'entrée identifiés, l'attaquant peut tenter d'inclure des fichiers locaux sensibles sur le système pour extraire des informations. Les fichiers les plus couramment inclus sont les fichiers de configuration et les journaux de système. En exploitant une LFI, l'attaquant peut récupérer des informations telles que les mots de passe ou des clés d'API. L'attaquant doit ensuite analyser le comportement de l'application pour comprendre comment ces informations peuvent être exploitées pour compromettre d'avantage le système ciblé.

Exploiter

Conséquences potentielles

Une exploitation réussie de ce type de vulnérabilité peut permettre :

- La fuite de données confidentielles, telles que des informations utilisateurs comme des mots de passe ou des secrets de l'application comme des fichiers de configuration ;
- Une potentielle escalade de privilège afin d'obtenir un contrôle à distance sur le serveur cible ;
- Une attaque par déni de service (DoS) par la surcharge du serveur.

Contre-mesures

Les contre-mesures suivantes peuvent être mises en œuvre :

- Utiliser des fonctions sécurisées et connues ;

- Valider toutes les entrées d'URL pour s'assurer qu'elles ne peuvent pas être injectées ;
- Filtrer les caractères spéciaux dans toutes les entrées.

Comment cela fonctionne

Le scénario suivant peut être joué via l'exploitation de cette vulnérabilité :

- Exécution de code malveillant : un attaquant peut inclure un fichier PHP malveillant contenant du code malveillant dans une page Web vulnérable à une LFI.

Exemple 1

Voici un exemple de code PHP vulnérable à une Local File Inclusion :

```php
<?php
    $file = $_GET['page'];
    include($file);
?>
```

Ce code PHP permet à un utilisateur de spécifier la page à inclure via un paramètre GET nommé "page". Si l'attaquant peut contrôler la valeur de ce paramètre, il sera en mesure d'inclure des fichiers locaux qui ne devraient pas être accessibles, tels que des fichiers de configuration contenant des informations sensibles.

Par exemple, si l'attaquant demande la page "https://example.com/vuln.php?page=/etc/passwd", le code PHP inclura le contenu du fichier "/etc/passwd" dans la réponse, divulguant ainsi des informations sensibles du système. Pour éviter cette vulnérabilité, il est recommandé de limiter les chemins d'accès aux fichiers inclus ou d'utiliser une fonction telle que realpath() pour valider les chemins d'accès absolus.

Exemple 2

Voici un exemple de code PHP vulnérabilité à une Local File Inclusion en null byte :

```php
<?php
    $file = $_GET['file'];
    include('/var/www/html/' . $file . '.php');
?>
```

La variable $file est définie à partir de la valeur du paramètre GET nommé "file". La fonction include() est utilisée pour inclure un fichier PHP en utilisant le chemin absolu "/var/www/html/" et le nom du fichier $file. L'extension ".php" est ajoutée à la fin de la variable $file pour s'assurer que le fichier inclus est un fichier avec l'extension ".php".

Cependant, cette technique d'inclusion de fichiers locaux peut être vulnérable à une attaque d'inclusion avec l'utilisation d'un null byte. Un attaquant peut inclure un fichier malveillant en envoyant une valeur $file contenant un caractère null byte (\0), qui est utilisé comme marqueur de fin de chaîne de caractères. Cela peut permettre à l'attaquant d'inclure un fichier malveillant en dehors du répertoire cible.

Voici un exemple d'exploitation de cette page PHP vulnérable : https://example.com/index.php?file=../../../../../../etc/passwd%00

L'attaquant utilise le caractère null byte (%00) pour terminer la chaîne de caractères et inclure le fichier /etc/passwd situé en dehors du répertoire cible. L'utilisation à plusieurs reprises de "../" permet de remonter dans l'arborescence du système de fichiers.

Pour empêcher cette famille de LFI utilisant un null byte, il est possible d'utiliser la fonction basename() pour extraire le nom du fichier sans le chemin et ainsi vérifier que le nom du fichier est autorisé avant de réaliser l'inclusion.

Voici un exemple de correction du code PHP vulnérable :

```php
<?php
    $file = basename($_GET['file']);
    $allowed_files = array('page1', 'page2', 'page3'); // Liste des fichiers autorisés
    if (in_array($file, $allowed_files)) {
        include('/var/www/html/' . $file . '.php');
    } else {
        echo "Fichier non autorisé";
    }
?>
```

CWEs

- CWE-98 : Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')
- The PHP application receives input from an upstream component, but it does not restrict or incorrectly restricts the input before its usage in “require,” “include,” or similar functions.

References

URL :

- https://repository.root-me.org/Exploitation%20-%20Web/EN%20-%20Local%20File%20Inclusion.pdf
- https://www.idc-online.com/technical_references/pdfs/information_technology/Understanding_LFI_and_RFI_Attacks.pdf

Retour fiches vulnérabilités

- Cyber fiches vulnérabilités