File Upload

Description

L'upload de fichier consiste à transférer un fichier d'un utilisateur vers un serveur web. Il s'agit de l'opération inverse du téléchargement (download). Ceci peut par exemple permettre à un utilisateur de mettre en ligne des photos, des images etc. L'upload de fichier ou file upload n'est pas une vulnérabilité en soit, mais le fait de ne pas contrôler ce que l'utilisateur upload sur le serveur constitue une vulnérabilité.

En effet, un attaquant peut potentiellement uploader un fichier malveillant tel qu'un web shell qui est une interface shell permettant l'accès et le contrôle à distance d'un serveur Web ainsi que l'exécution de commandes arbitraires.

Pré-requis d'exploitation

Pour exploiter cette vulnérabilité, il est nécessaire d'avoir accès à un serveur web proposant une fonctionnalité d'upload, avec des contrôles et mécanismes de protection insuffisants permettant de télécharger un web shell.

Compétences nécessaires

- Connaissance du protocole HTTP ;
- Connaissance du type MIME ;
- Connaissance sur les types de fichiers et leurs extensions ;
- Connaissance des techniques employées pour contourner certains contrôles.

Ressources nécessaires

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

Flux d'exécution

Explorer

Énumérer les fonctionnalités permettant d'uploader des fichiers et identifier les répertoires dans lesquels ces derniers vont être téléchargés.

Expérimenter

Lister les différentes extensions et les différents type MIME acceptés par le serveur web.

Exploiter

Conséquences potentielles

Le succès de ce type d'attaque peut permettre :

- L’exécution de commandes sur l'hôte de l'application avec le niveau de privilège de l'utilisateur exécutant le service web ;
- L'utilisation de l'hôte de l'application comme machine de rebond pour mener des attaques sur le réseau interne, ou sur Internet ;
- L'utilisation de l'hôte de l'application pour miner de la cryptomonnaie ;
- Le déploiement d'une backdoor pour maintenir un accès persistant sur l'hôte de l'application.

Contres-mesures

Les contre-mesures suivantes peuvent être mises en œuvre :

- S'assurer que le serveur web est à jour avec tous les correctifs pour être protégé contre les vulnérabilités connues ;
- S'assurer que les autorisations de fichiers dans les répertoires du serveur web à partir desquels les fichiers peuvent être exécutés sont définies sur les paramètres de **moindre privilège**, et que le contenu de ces répertoires est contrôlé par une liste

d'autorisations ;
- Contrôler les extensions des fichiers ainsi que leur MIME-type ;
- Renommer les fichiers uploadés sur le système avec une chaîne de caractère aléatoire ;
- Stocker les fichiers uploadés dans un répertoire sur lequel l'utilisateur du service web n'a pas les droits d'exécution (en dehors de la racine du serveur web) ;
- Filtrer les extensions et type MIME avec un système de liste blanche plutôt que liste noire ;
- Limiter la taille des fichiers uploadés et la taille du nom du fichier, et filtrer les caractères spéciaux dans le nom du fichier ;
- N'autoriser que les utilisateurs authentifiés à utiliser une fonction d'upload.

Retour fiches vulnérabilités

- Cyber fiches vulnérabilités

From:
/ - **Les cours du BTS SIO**

Permanent link:
/doku.php/cyber/vulnerabilite/file_upload?rev=1752237763

Last update: **2025/07/11 14:42**