scenario ctf2

Cyprien Leschi, Hugo Sarazin, Jérémy Richard, Haroune Samouche, Steven Jaman

December 2021

1 CTF 2

La cible de l'attaque est le site de RockIt, un grand festival de rock.

Pour parvenir à s'introduire sur le serveur, l'attaquant devra exploiter une **LFI (Local File Inclusion)** couplée à un **PHP filter**, dans le but de récuperer le fichier de configuration du site web. Ce fichier contient les identifiants de l'administrateur ainsi que son mot de passe hashé, qu'il est possible de cracker avec la liste Rockyou.

Une fois connecté sur le dashboard administrateur, un formulaire d'upload permet à l'attaquant **d'uploader un shell PHP**. Cependant, le serveur change les noms des fichiers uploadés par des mots aléatoires de longueur 5 ou 6. L'attaquant devra alors réaliser un **brute force pour trouver le nom de son shell**.

Une fois introduit sur le serveur, l'attaquant sera dans un docker en tant que www-data, il peut alors récupérer le premier flag dans */var/www/flag.txt*. Pour obtenir le flag root, il faut tout d'abord devenir root dans le docker. Pour cela, l'attaquant devra exploiter une vulnérabilité de l'interprétation des **wildcards ('*')**. Ensuite, il devra réaliser un **docker escape** grâce à la **CVE-2019-14271**.