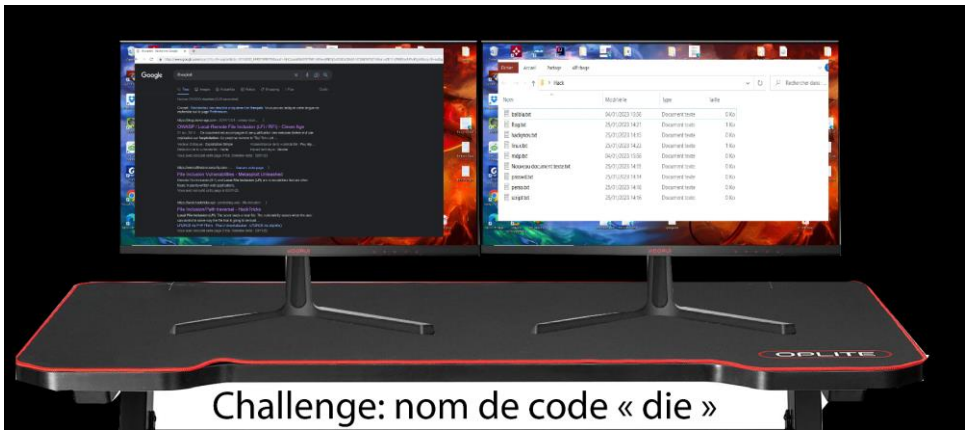
Chall nom de code “DIE”

Table des matières

Partie 1 : Présentation du challenge



Domaine : web

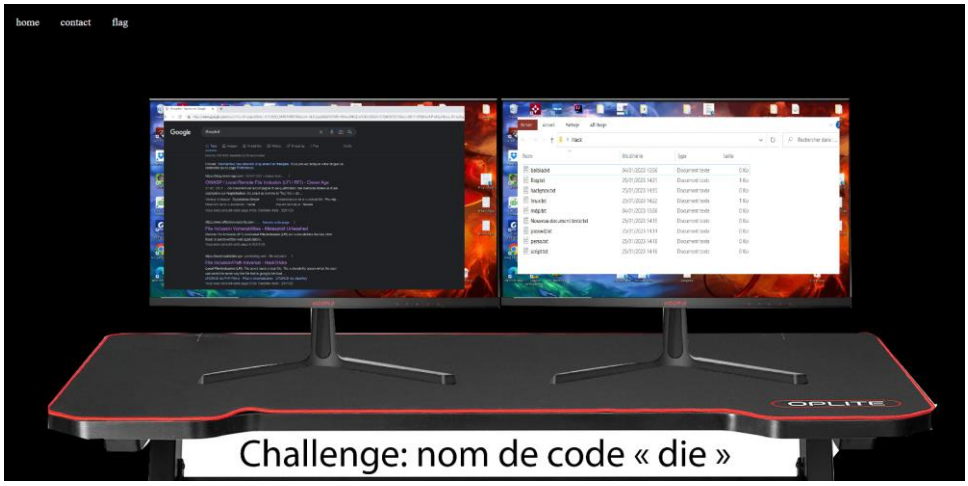
Difficulté :

Auteur : Mounier Matthieu

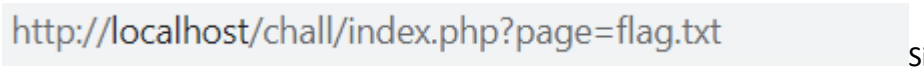
Description : bob viens de trouver une faille sur un site, il pense qu'il y a moyen de récupérer des infos mais il toujours pas réussi.

(Soyez attentif à chaque détaille)

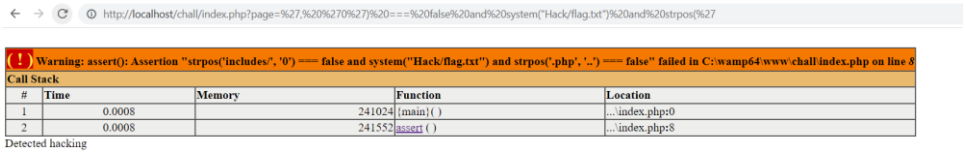
Partie 3 : Résolution



On arrive sur cette page au début de chall, dedans se cache des indices comme le début de la faille qui l'image de gauche avec la recherche lfi, l'image de droite a comme indice le nom du fichier ou il y a le flag et le nom du dossier. Le nom du chall est pas anodin le mot die correspond a la commande qu'il faut faire



Si on tente une simple lfi rien ne se passe pour se faire il faut faire des recherches pour trouver la faille php:assert().

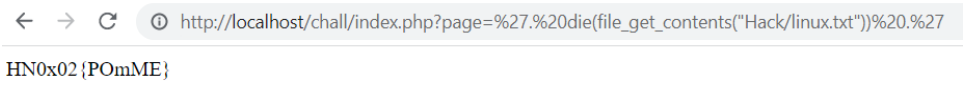


Une fois renseigner sur php:assert() on trouve une commande a mettre dans l'URL qui est ?page=', '0') ===

false and system("Hack/linux.txt") and strpos('

Mais si on le fait on a une erreur et la seule commande qui marche est

?page='. die(file_get_contents("Hack/linux.txt")) .'



Et voilà une fois la bonne commande avec le bon chemin du fichier on a le flag

Flag : HN0x02{POmME}