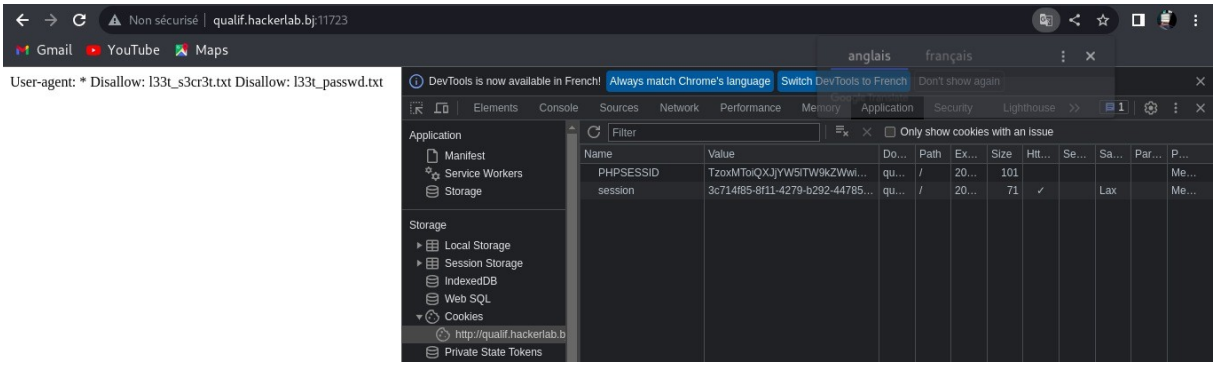
Writeup AGOODJIE N4t10n

Apres une premiere enumeration, On trouve un fichier robots,txt et il index deux fichier txt, L'un contient des mots de passe, Le second est chiffré. Son décodage nous donne un fichier zip mais il est vérroullé. Avec **john** et la liste des mots de passe, on réussit a le déverrouller. Le decodage des fichier qui s'y trouvaient nous dirige vers une vidéo youtube qui reviens souvant dans les CTF et un text qui nous demande d'aller en profondeur dans l'enumération

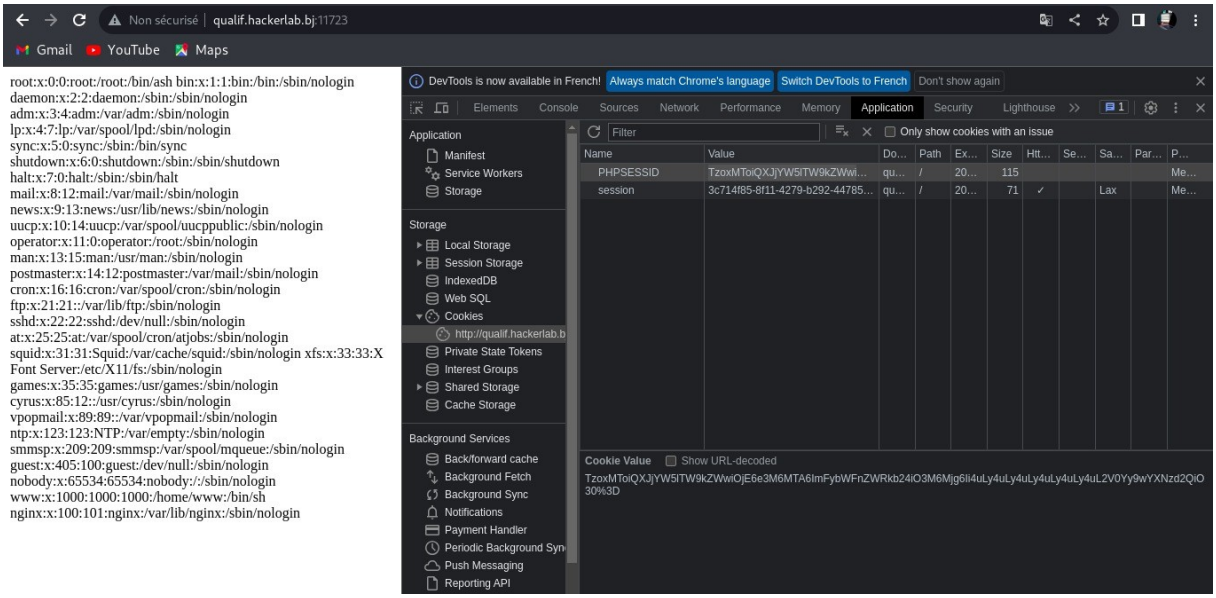
Apres de nombreuse énumération et inspections sans succès, nous avons voulu essayer avec le décodage du sessid TzoxMToiQXJjYW5lTW9kZWwiOjE6e3M6MTA6ImFybWFnZWRkb24iO3M6MTU6Ii93d3cvaW5kZXguaHRtbCI7fQ%3D%3D ce qui nous donne O:11:"ArcaneModel":1:{s:10:"armageddon";s:15:"/www/index.html";} .

Nous avons ensuite essayé de comprendre le fonctionnement de cette ligne, ce qui nous a pousser à essayer de lire autre fichier que le /www/index.html .cependant nous avons modifié le chemin du répertoire par /www/robots.txt ce qui a effectivement marché et nous a permis de lire le contenu du fichier robots.txt



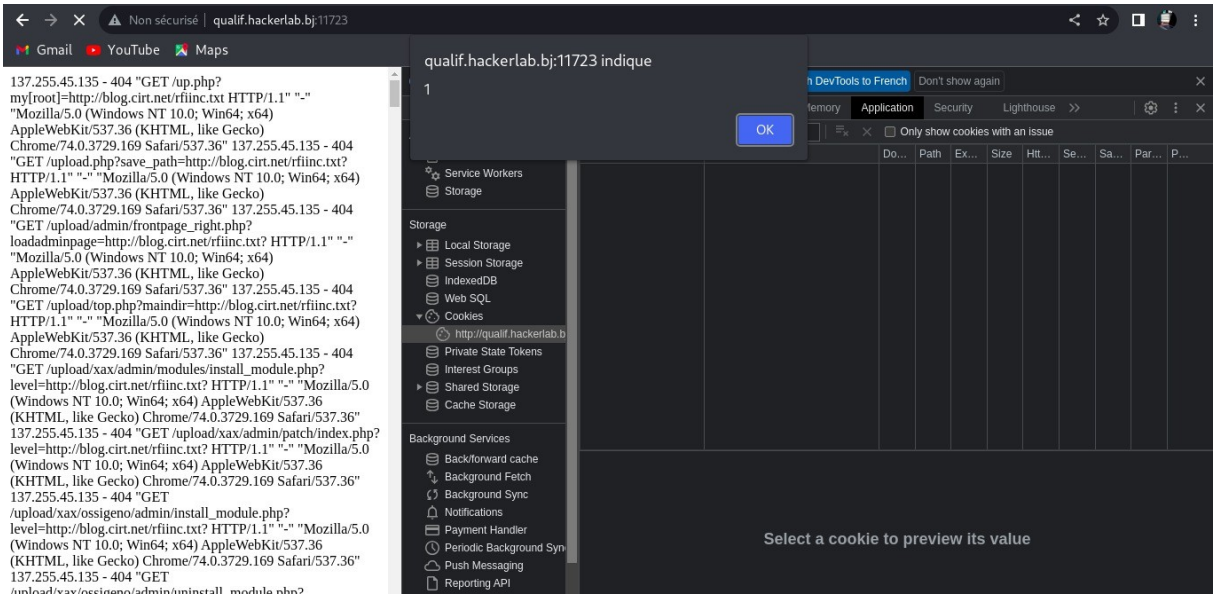
Cette réponse du serveur nous a automatique fait pensez à un LFI. Du coup nous avons essayé de multiple payloads jusqu'à ce que nous essayons avec le ../../../../../../etc/passwd ce qui donne ceci : O:11:"ArcaneModel":1:{s:10:"armageddon";s:28:"../../../../../../etc/passwd";} .

après conversion en base64 et en URL encode, nous avons TzoxMToiQXJjYW5lTW9kZWwiOjE6e3M6MTA6ImFybWFnZWRkb24iO3M6Mjg6Ii4uLy4uLy4uLy4uLy4uLy4uL2V0Yy9wYXNzd2QiO30%3D ce qui nous retourne le contenu du fichier /etc/passwd .

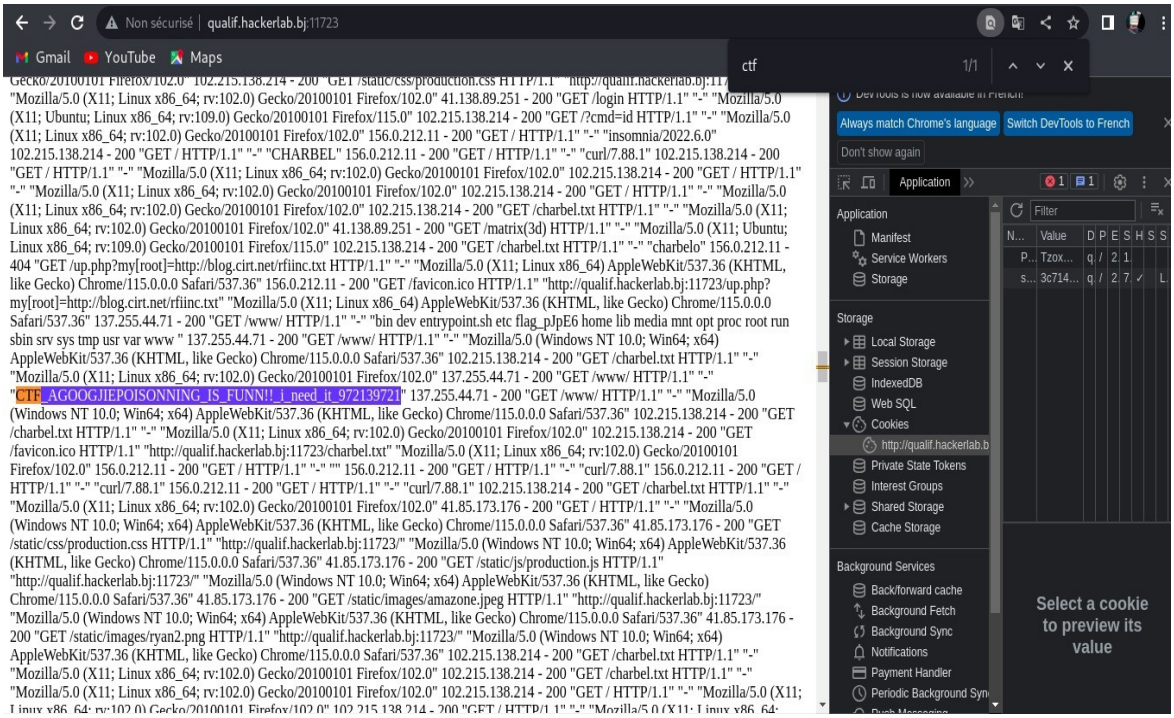


en utilisant cette même méthode nous avons essayé d'ouvrir le fichier flag.txt dans diffèrent répertoire connu d'une machine linux mais sans succès puisque nous n'avons aucune certitude que le fichier flag.txt se situe dans les répertoire que nous entrons. Du coup nous avons pensez à un rce a parti du LFI

Avec quelque recherche , nous sommes tombés sur cet article https://aditya-chauhan17.medium.com/local-file-inclusion-lfi-to-rce-7594e15870e1 qui nous a permis modifier notre sessID et d'essayer à nouveau avec O:11:"ArcaneModel":1:{s:10:"armageddon";s:36:"../../../../var/log/nginx/access.log";} ce qui nous retourne le contenu du access.log



Par curiosité, j'ai essayé de rechercher CTF_ dans le contenu d'access.log en faisant ctrl+F et en tapant dans la barre de recherche CTF_ quand je suis tombé sur le flag : **CTF_AGOOGJIEPOISONNING_IS_FUNN!!_i_need_it_972139721** ce qui m'a permis de valider le challenge.


Non sécurisé | qualif.hackerlab.bj:11723
Gmail
YouTube
Maps
ctf
1/1
Always match Chrome's language
Switch DevTools to French
Don't show again
Application
Manifest
Service Workers
Storage
Storage
Local Storage
Session Storage
IndexedDB
Web SQL
Cookies
http://qualif.hackerlab.b
Private State Tokens
Interest Groups
Shared Storage
Cache Storage
Background Services
Back/forward cache
Background Fetch
Background Sync
Notifications
Payment Handler
Periodic Background Sync
Filter
Select a cookie to preview its value