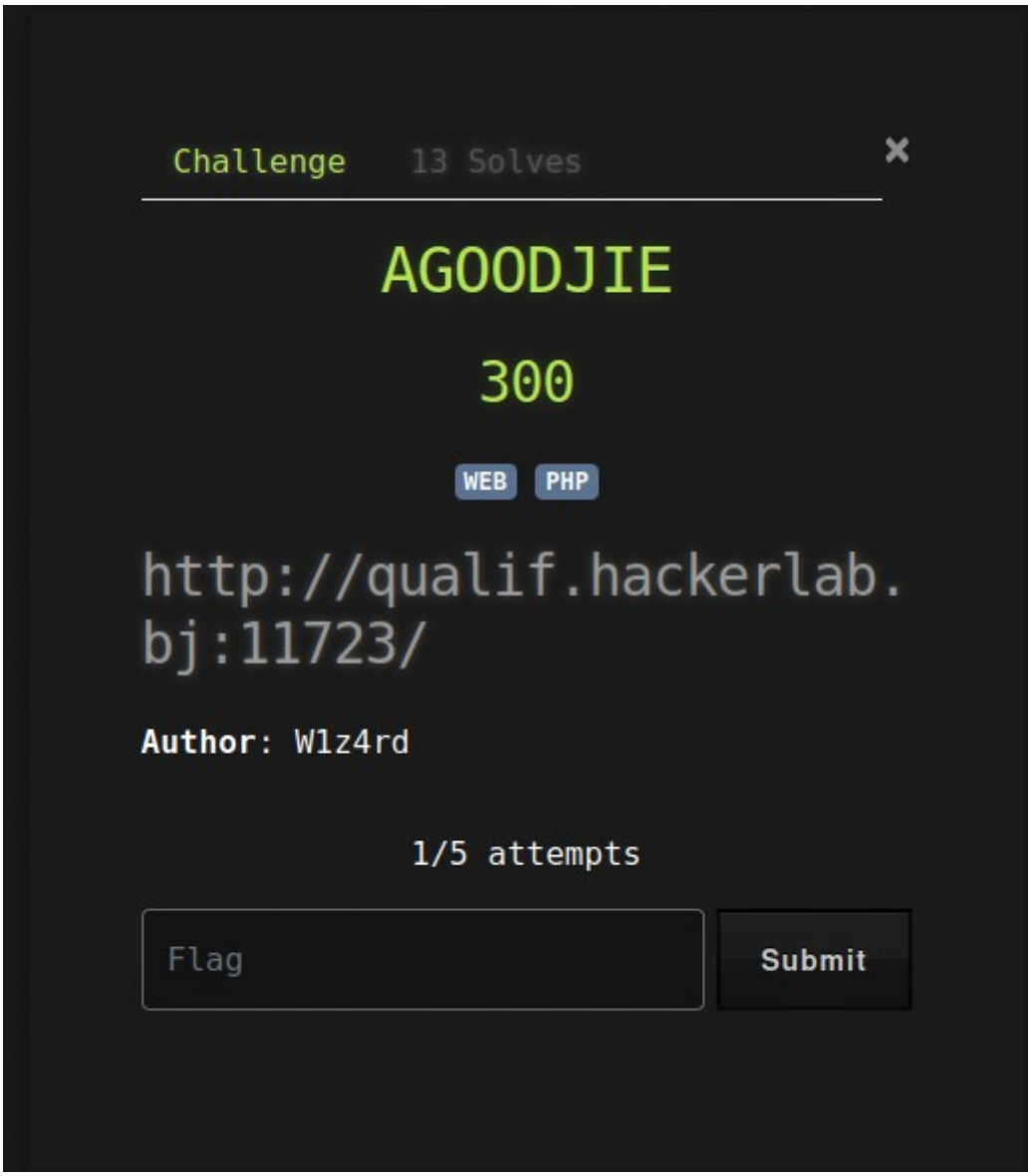
# Writeup

# Mon equipe: Nekketsu

**Challenge:** AGOODJIE

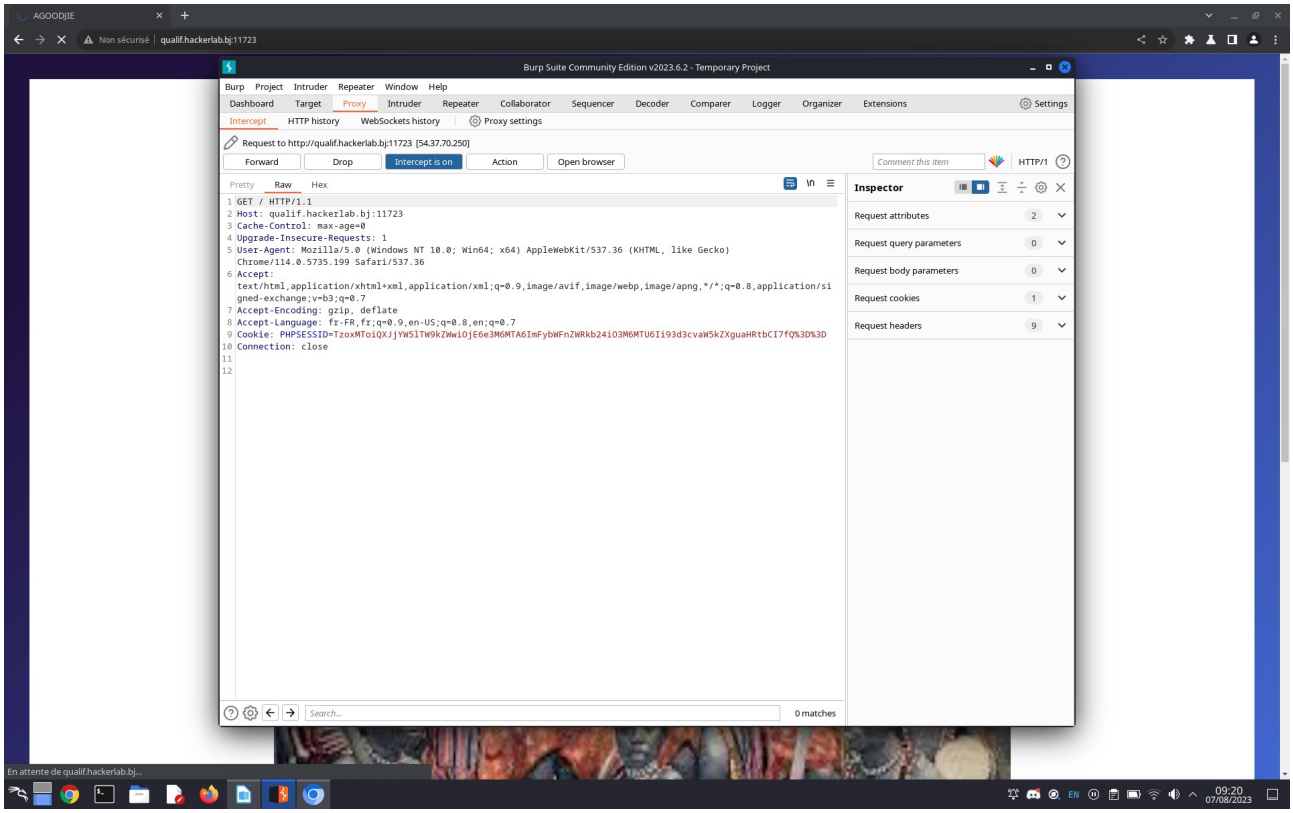
**Auteur:** W1z4rd




Pour ce challenge, il a ete mis a notre disposition le lien suivant: http://qualif.hackerlab.bj:11723/
.

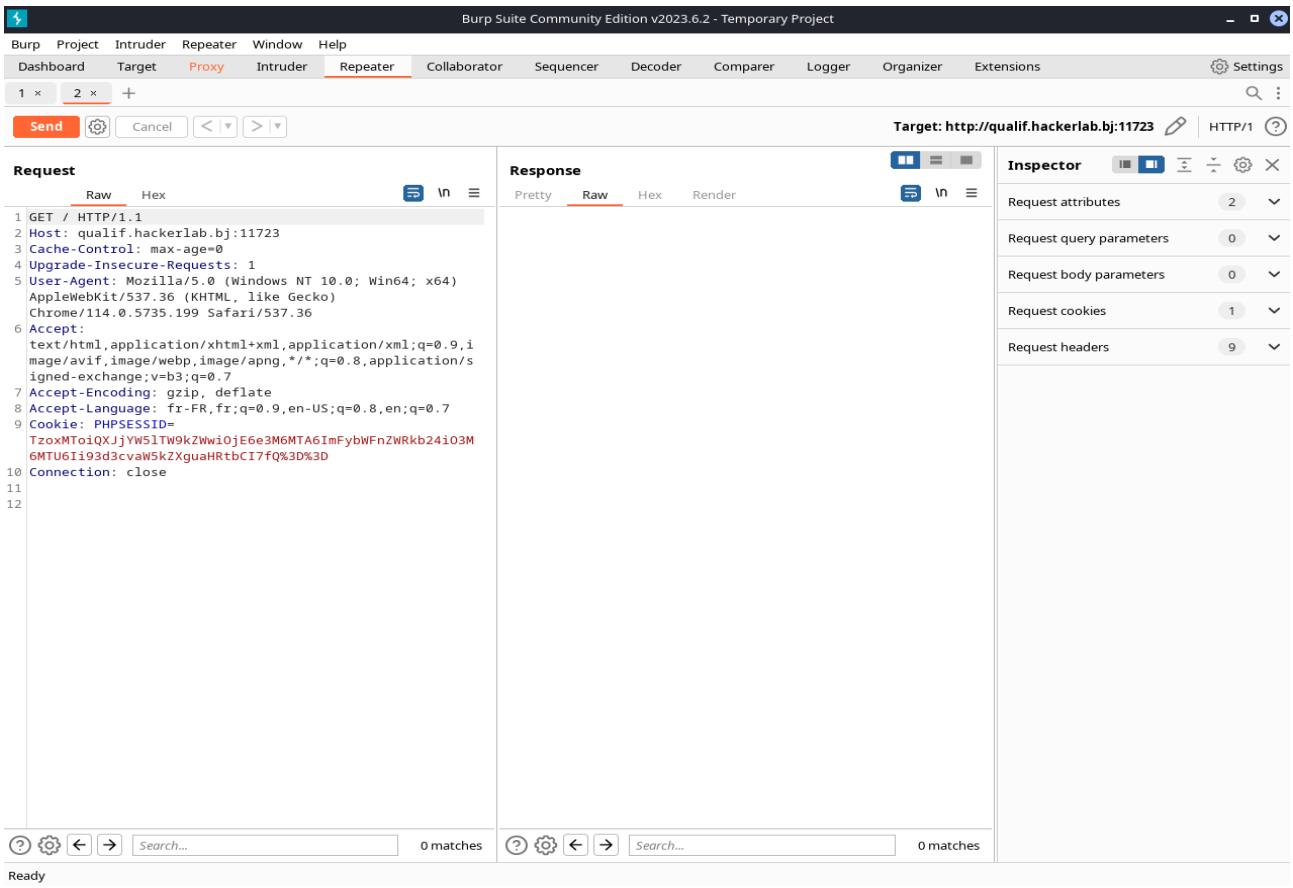
Pour commencer, le premier reflexe que j’ai eu etait de verifier le fichier robots.txt mais malheureusement, c’etait un leurre puisqu’au final il y avait un faux flag.
Merde!!! Un brute-force pour rien.

Bah suite a cet echec, le reflexe etait de verifier les cookies. J’ai donc attaque mon burpsuite.




On obtient un PHPSESSID chiffre en base64. Lorsque je l’ai decode j’ai obtenu O:11:"ArcaneModel":1:{s:10:"armageddon";s:14:"/www/index.html";}

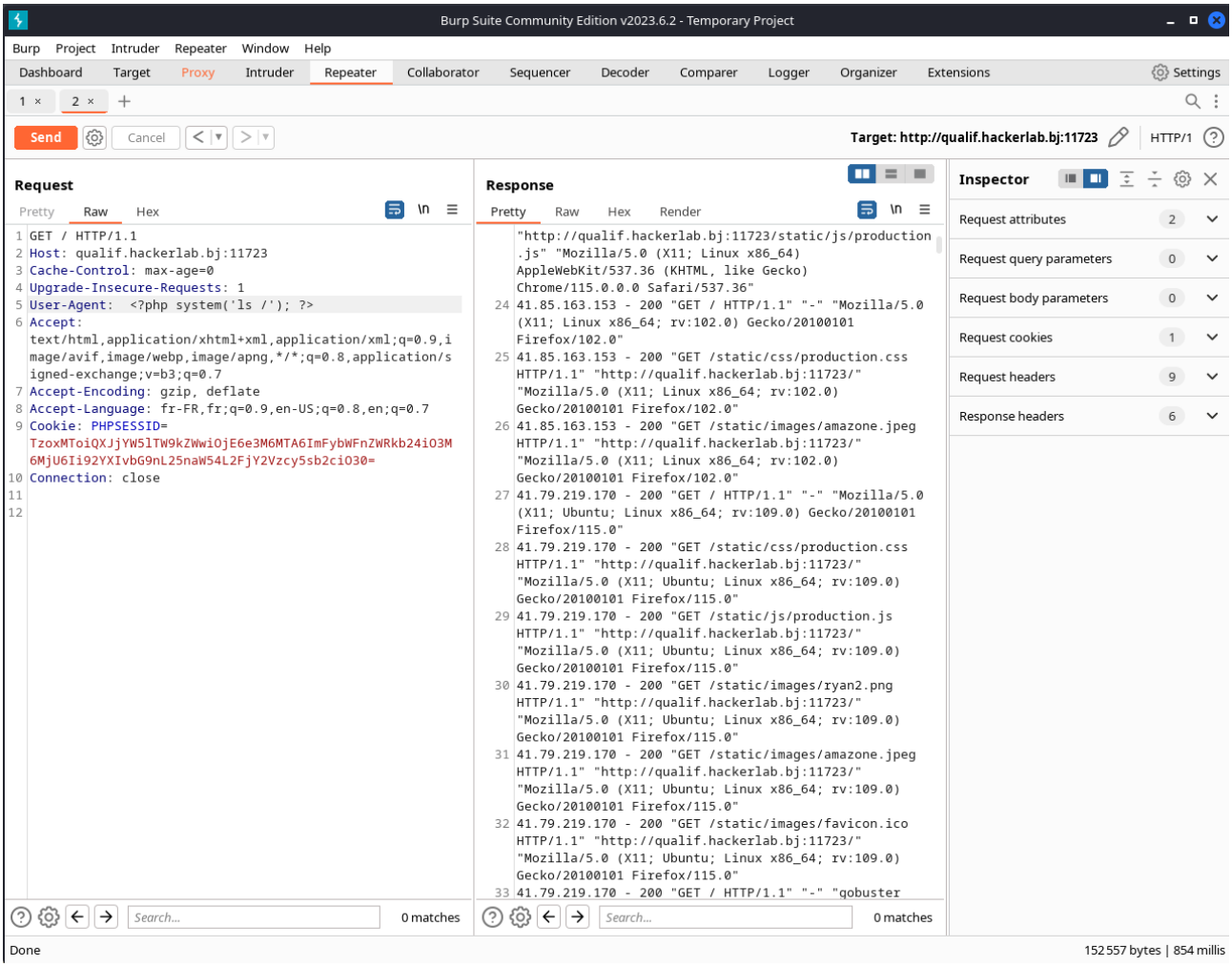
Je me suis donc mis a essayer quelques tenatives au niveau du PHPSESSID pour voir s’il y avait une vulnerabilite. Etant donne qu’on ne peut pas le faire directement au niveau du proxy, nous avions utilise le repeter en cliquant sur «send to repeter».




Voici en quelques etapes, les modifications que j’ai apporte au niveau du PHPSESSID.

Etape 1:

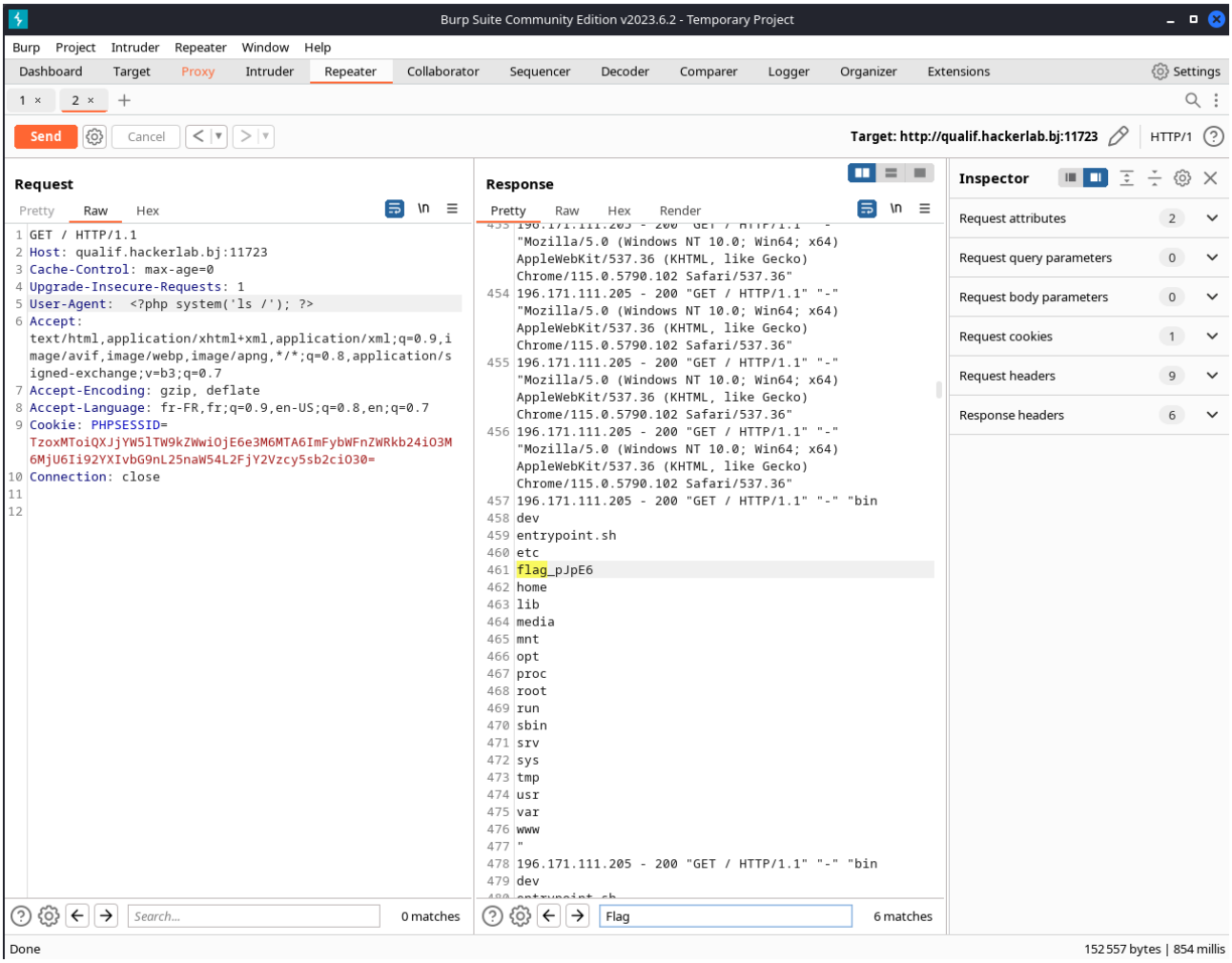
J’ai remplace sa valeur par «O:11:"ArcaneModel":1:{s:10:"armageddon";s:25:"../../../../../etc/passwd";}» ce qui donne «TzoxMToiQXJjYW5lTW9kZWwiOjE6e3M6MTA6ImFybWFnZWRkb24iO3M6MjU6Ii4uLy4uLy4uLy4uLy4uL2V0Yy9wYXNzd2QiO30=» en base64.




Comme resultat on obtient le contenu du repertoire /etc/passwd ce qui m'a fait conclu que le serveur etait vulnerable au LFI.

Etape 2:

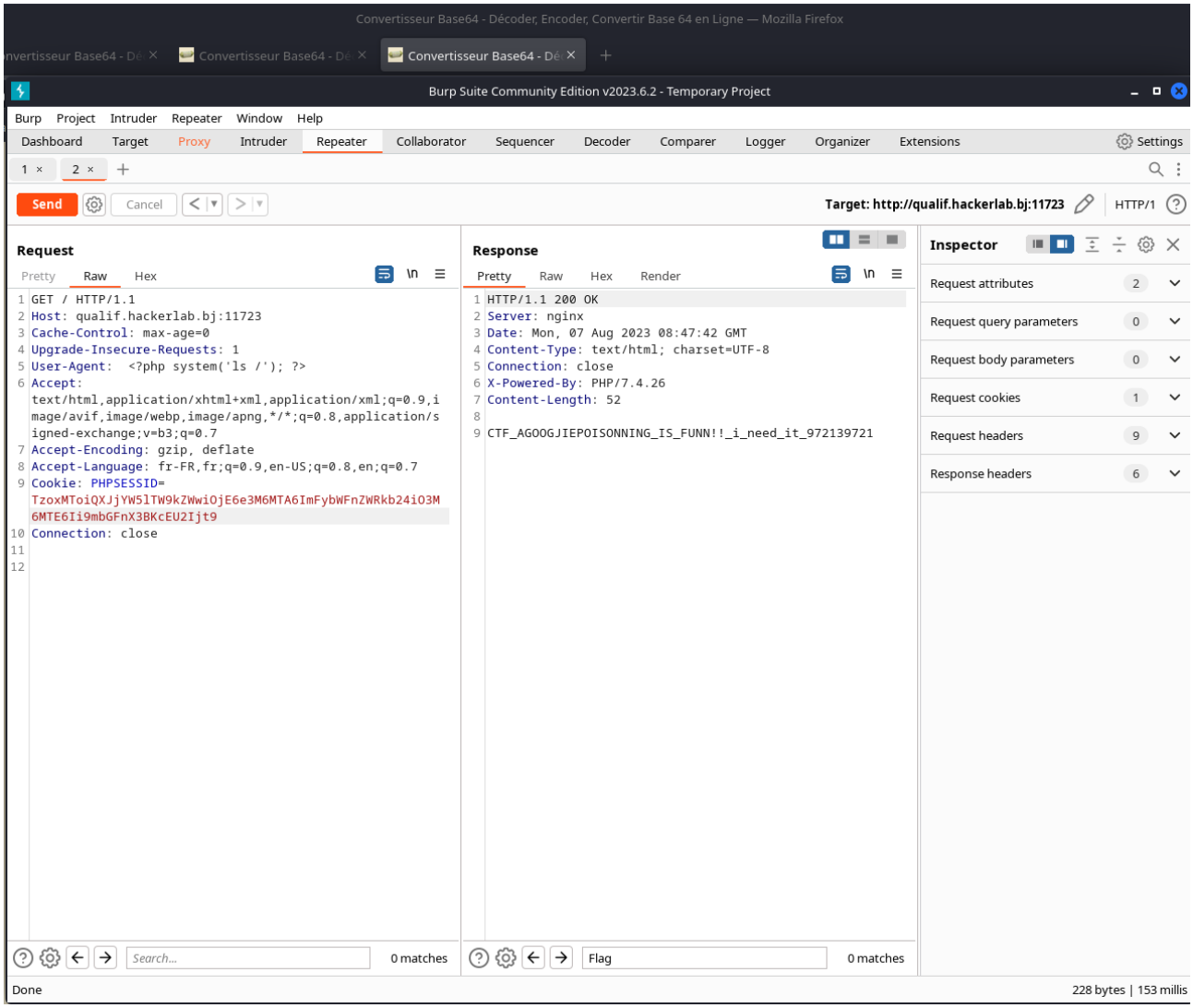
Etant donne que le serveur est vulnerable au LFI, j'ai essaye d'accede au log de notre serveur pour voir les actions qui ont ete effectue. J'ai donc modifie le PHPSESSID en «O:11:"ArcaneModel":1:{s:10:"armageddon";s:25:"/var/log/nginx/access.log";}». Ensuite j'ai modifie le User-agent en «User-Agent: <?php system('ls /'); ?>».
Ces modifications me permettra d'afficher les logs ainsi que les repertoires du dossier racine.




Comme resultatj'ai eu les logs comme je le voulais. Cependant ce qui m'interessait etait le flag; j'ai donc effectue une rcherche dans les logs pour voir si un fichier nomme flag a ete cree ou modifie. Ce qui etait le cas.

Etape 3:

Cette etape etait la derniere puisque je savais déjà qu'il y avait un fichier nomme Flag_pJpE6. J'ai donc affiche le contenu de ce fichier en ramenant la valeur du User-agent a la valeur initial et en modifiant la valeur du PHPSESSID par «O:11:"ArcaneModel":1:{s:10:"armageddon";s:11:"/flag_pJpE6";}».




**Flag:** **CTF_AGOOGJIEPOISONNING_IS_FUNN!!_i_need_it_972139721**