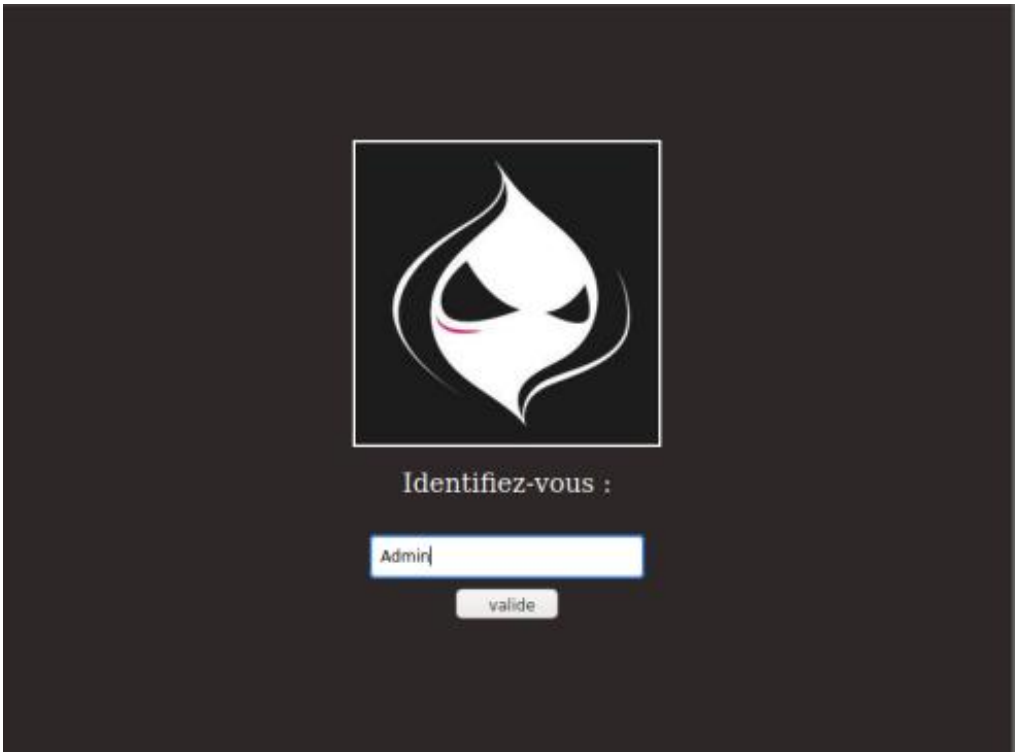
HACKY'NOV

WRITEUP

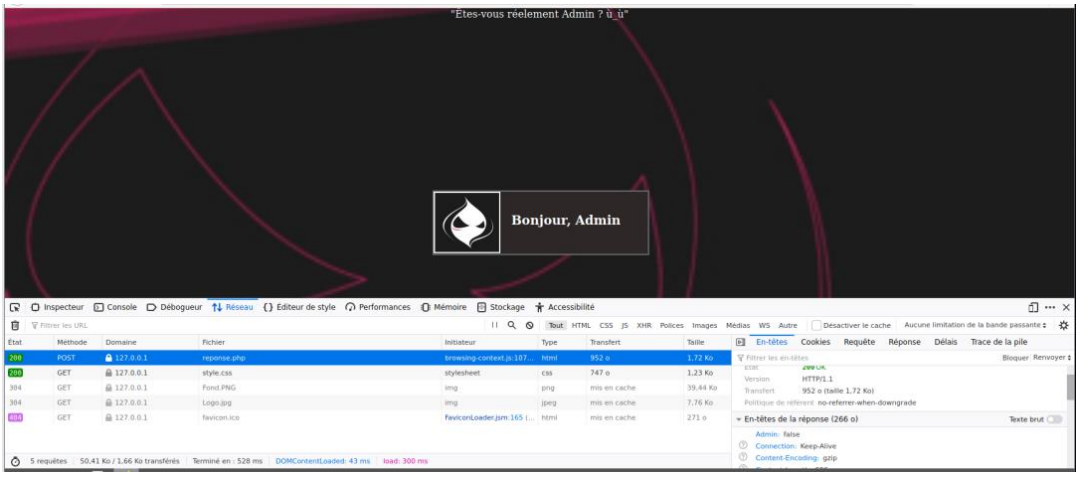
Etape n°1 :

Comme le nom du challenge le laisse désirer, le terme « Administration » en dit beaucoup sur l'objectif à réaliser : se connecter en tant qu'admin. C'est pour cela que l'on arrive sur une page de connexion nécessitant une identification, comme vous pouvez vous en douter, « Admin » (ne pas oublier la majuscule) est le pseudo requit pour accéder à la suite, sinon vous serez redirigé vers une page indiquant que votre pseudo n'est pas dans la base de données.



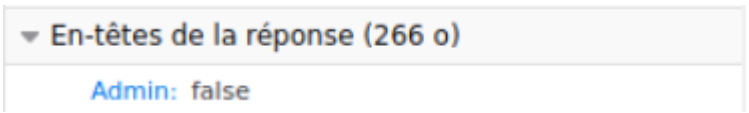
Etape n°2 :

Une fois le bon pseudo rentré, nous arrivons sur une autre page où l'on peut voir le message suivant : "Êtes-vous réellement Admin ? ", nous montrant que le système ne nous reconnait pas entièrement comme tel. De ce fait on fait, il faut regarder les interactions avec le réseau pour remarquer que l'en-tête de la requête possède un argument qui pourrait nous être intéressant.



Etape n°3 :

On s'aperçoit alors que la variable Admin est en false, nous signifiant que nous ne sommes pas réellement admin, il faut donc trouver un moyen pour la passer en true.



Etape n°4 :

Pour passer Admin en true il faut ouvrir un terminal de commande et utiliser la commande curl suivante pour injecter des arguments dans notre requête (en mettant bien Admin avec sa majuscule).

```
curl -X POST -H 'Admin:true' -d 'pseudo=Admin' http://127.0.1.1/reponse.php
```

Une fois la commande validée, le site nous reconnaitra enfin comme un véritable administrateur, nous laissant ainsi la visibilité sur le flag.

```
user@debian:~$ curl -X POST -H 'Admin:true' -d 'pseudo=Admin' http://127.0.1.1/reponse.php
Bravo, le flag est: HACKYNOV{AbRiC0T}<style type="text/css">
```

Bien joue à vous, vous avez trouvez le flag
Flag : HACKYNOV{AbRiC0T}