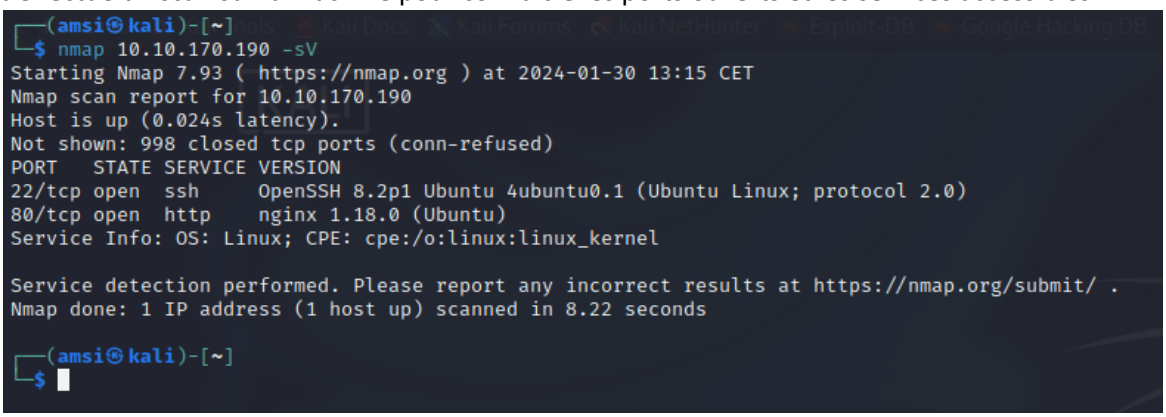
1. Phase de reconnaissance

On me donne le scope de notre attaque : 10.10.170.190

J'effectue un scan sur la machine pour connaître les ports ouverts et les services accessibles :



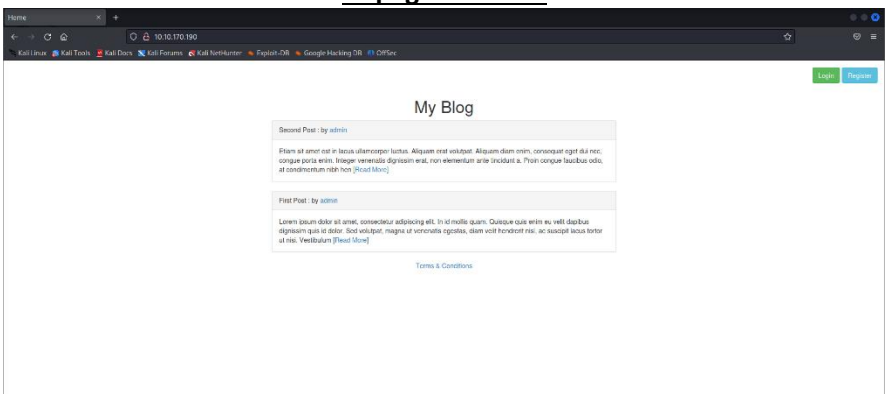
Je vois qu'il y a 2 services de disponible :

- SSH
- WEB

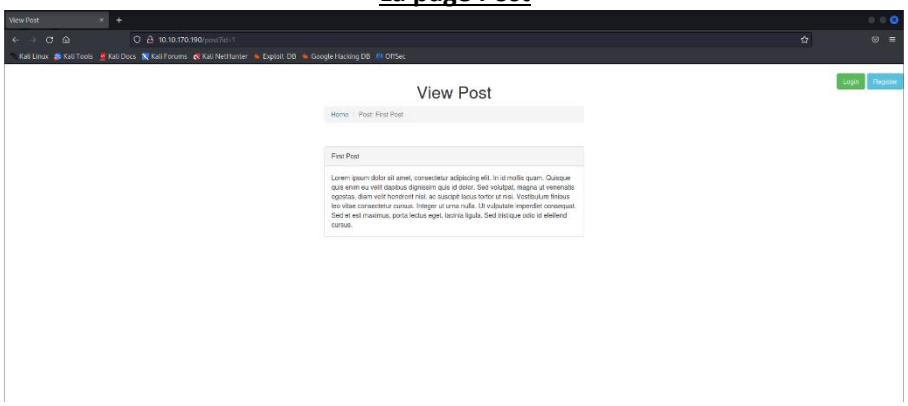
2. Exploitation

J'accède sur le site web, je navigue entre les pages etc :

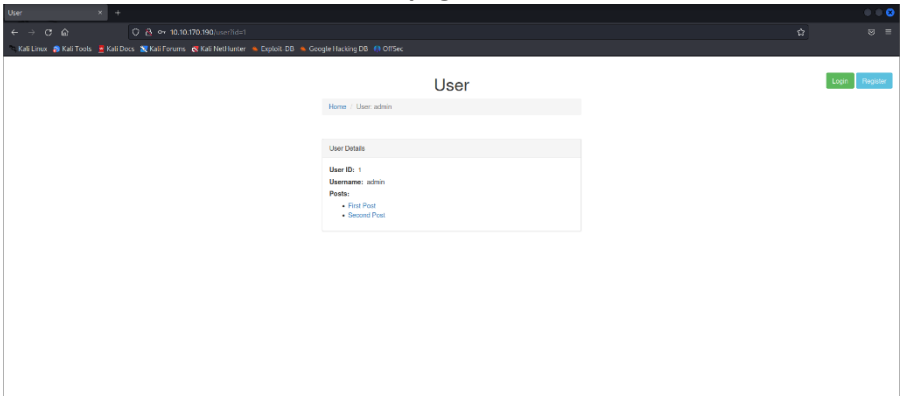
La page d'accueil



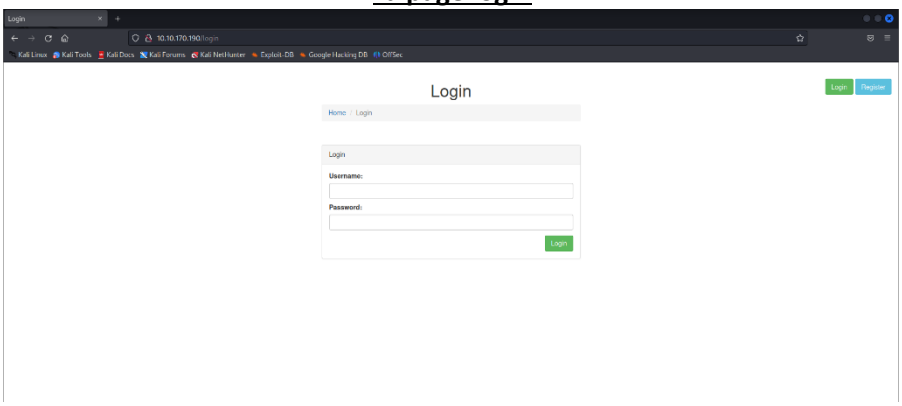
La page Post



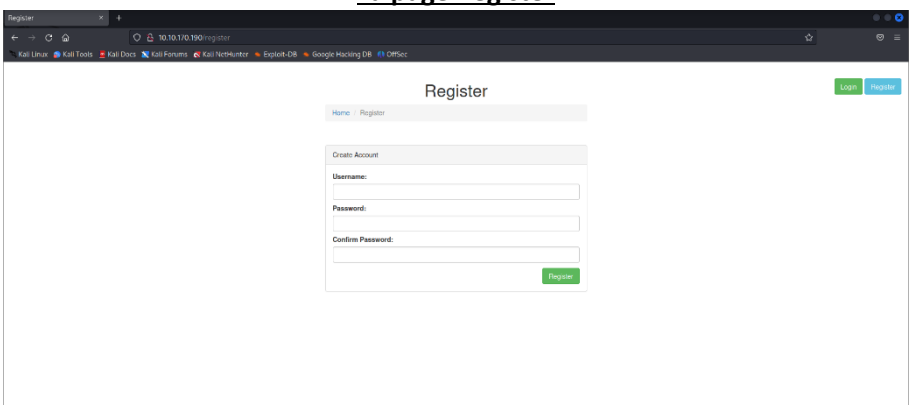
La page User



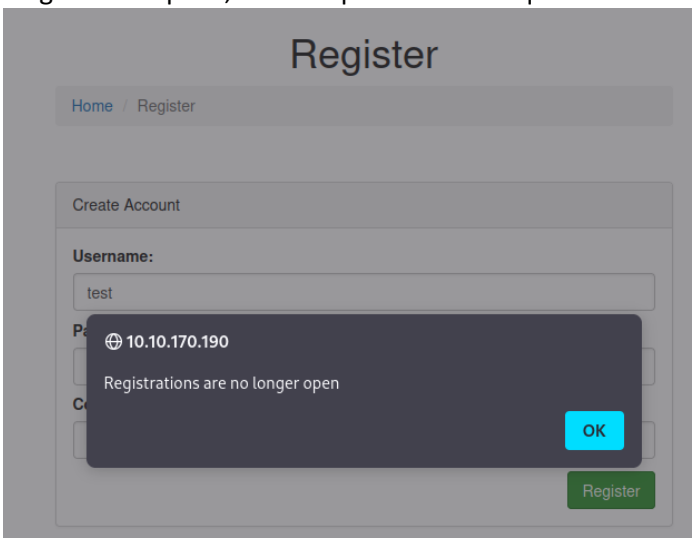
La page login



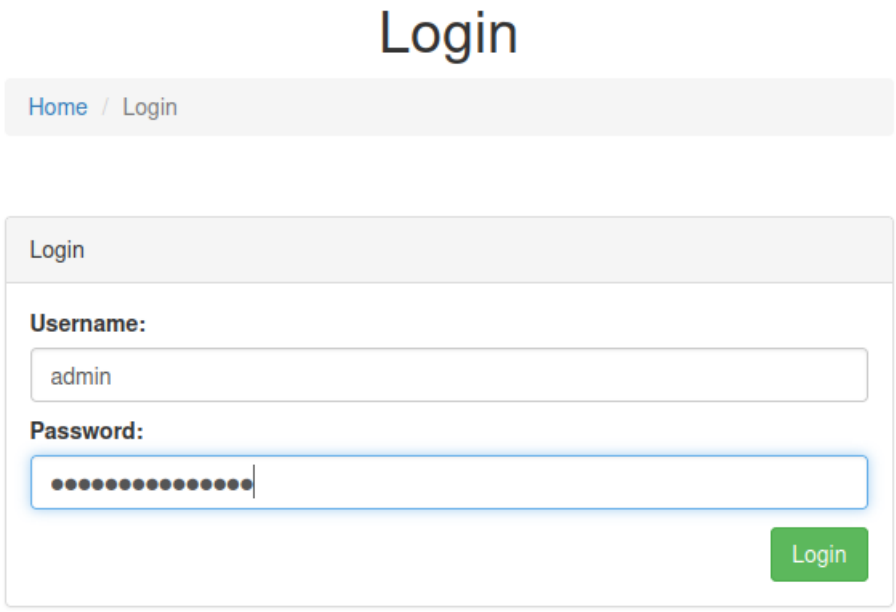
La page Register



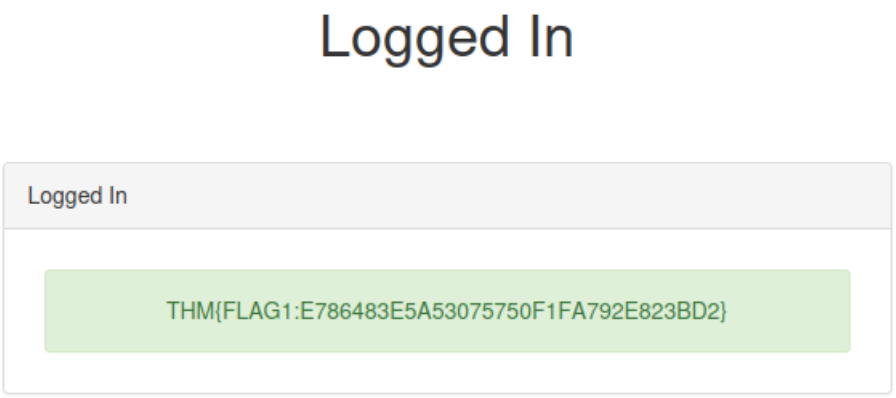
Je remarque la page user, c'est une gestion de paramètre qui affiche un contenu en fonction de la valeur du paramètre. Donc je considère qu'il y'a une base de données.
Je tente de m'inscrire mais à ma grande surprise, les inscriptions sont bloquées :



Sur la page user je vois qu'il y'a un admin de créer, je tente une injection SQL classique pour contourner le Mot de Passe : ' OR 1=1 -- -';



Je réussi à connecter en tant qu'admin :



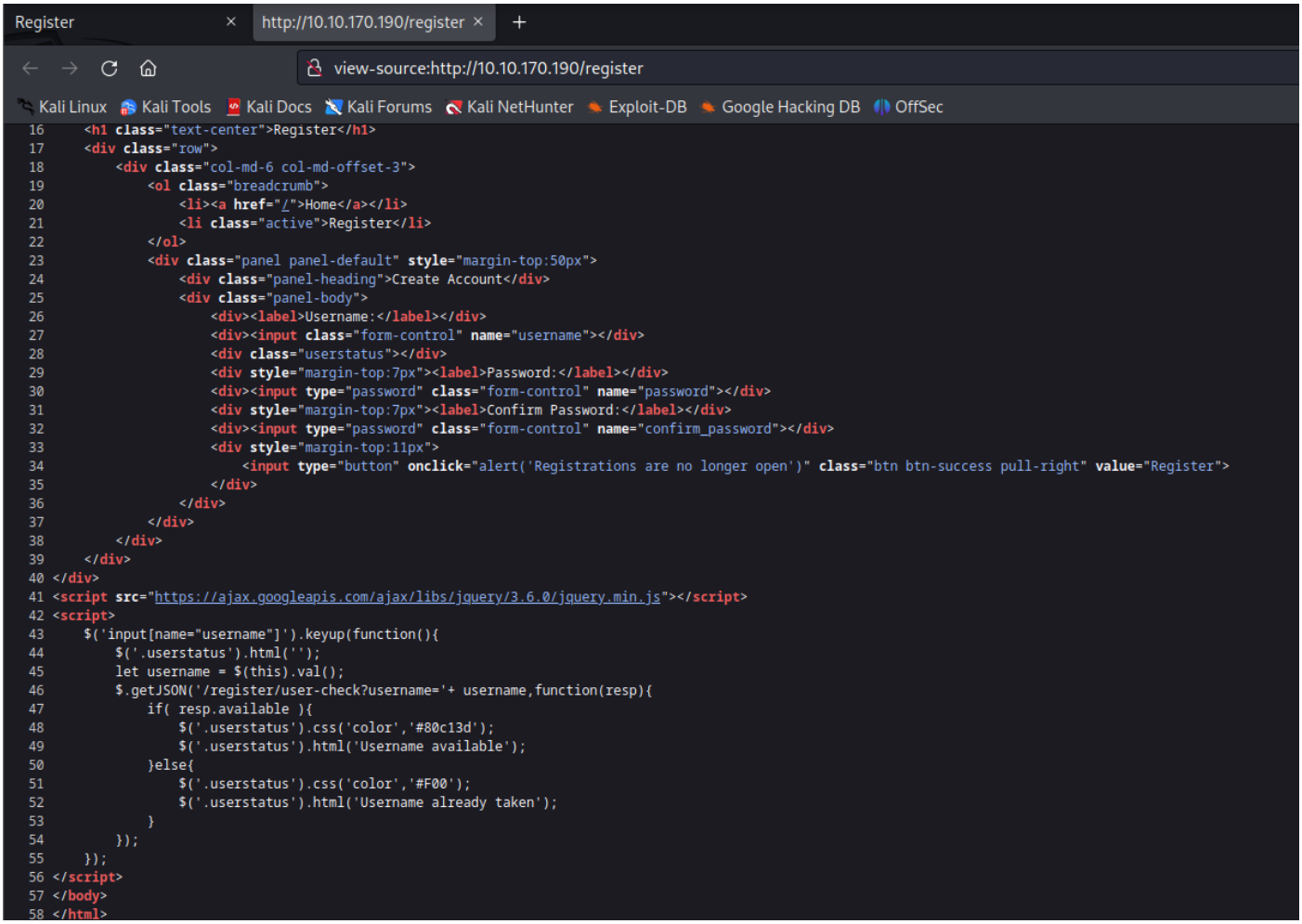
Penchons sur le cas de la page post car il a un paramètre dans l'url donc je peux tenter une injection avec sqlmap :

```
┌──(amsi㉿kali)-[~]
└─$ sqlmap -u http://10.10.170.190/post?id=1 -p id -dump
```

Voici le résultat :

```
[13:46:47] [INFO] table 'sqhell_5.posts' dumped to CSV file '/home/amsi/
[13:46:47] [INFO] fetching columns for table 'flag' in database 'sqhell_
[13:46:47] [INFO] fetching entries for table 'flag' in database 'sqhell_
Database: sqhell_5
Table: flag
[1 entry]
+----+-----------------------------------------+
| id | flag                                    |
+----+-----------------------------------------+
| 1  | THM{FLAG5:B9C690D3B914F7038BA1FC65B3FDF3C8} |
+----+-----------------------------------------+
```

L’intrigue que la page de « Register » est fermée m’a poussé à vérifier le code source de celui-ci :

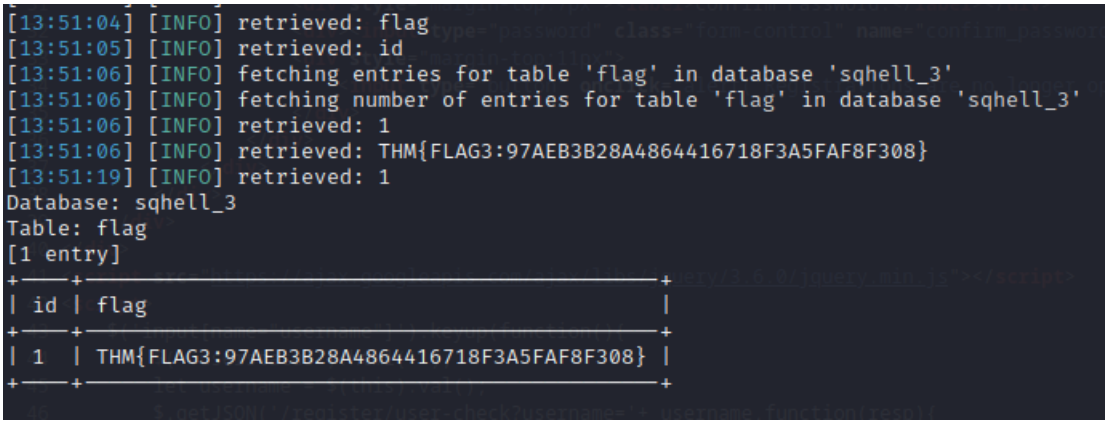


J’ai remarqué que dans le script de formulaire à la ligne 46, la requête s’envoyer vers :

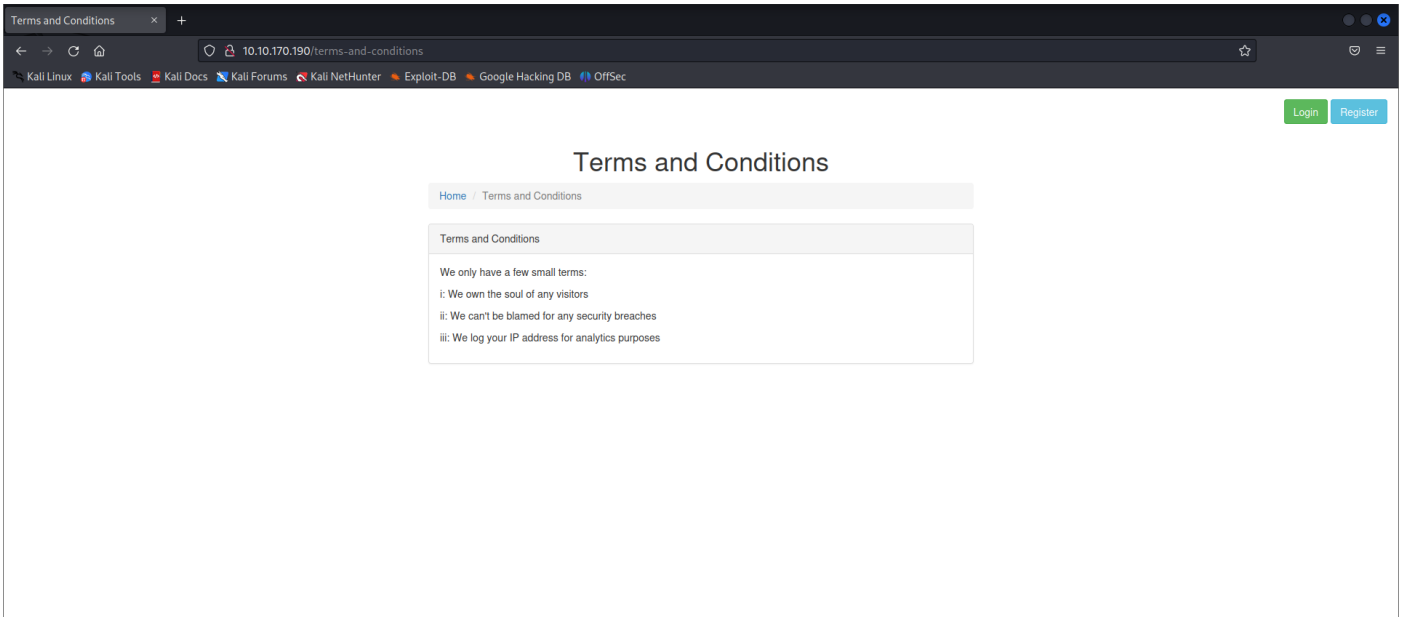
« register/user-check?username= »

J’ai donc tenter une injection sql avec sqlmap :

Voici le résultat :



Grâce à l'astuce donnée par TryHackMe, j'ai cherché dans cette page « Terms and Conditions » :

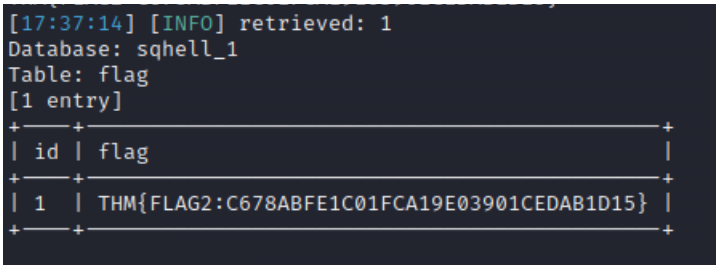


Le 3e points m'a intrigué et j'ai cherché sur internet, de ce que j'ai compris, cela signifie que le site identifie l'adresse IP de l'utilisateur qui se connecte à son serveur web par le biais d'un en-tête HTTP.

Donc j'utilise le X-Forwarded-For qui est un champ d'en-tête HTTP considéré comme standard

Donc j'utilise sqlmap pour modifier le champ d'en-tête :

Voici le résultat :



Je n'ai pas trouvé le 4e Flag, mais le TP a été très long et dur pour ma part car cela m'a pris toute la semaine, en plus des grosses taches qu'on me confie en alternance, et en étant tombé malade cette semaine, c'était impossible pour moi de finir les 2 TP (Sqhell & That's the ticket) surtout qu'à ma grande surprise que le CTF Sqhell m'a pris énormément de temps.

Voici les flags récupérés :