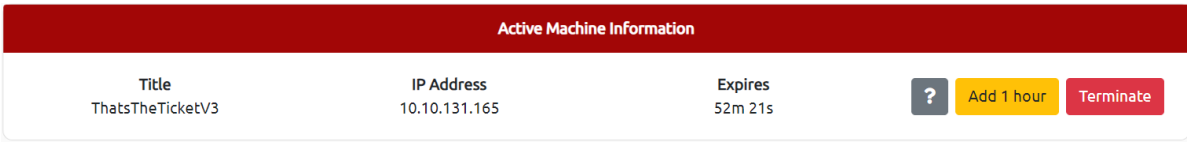
1. Phase de reconnaissance

On me donne le scope de notre attaque : 10.10.131.165



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

```
┌──(amsi㉿kali)-[~]
└─$ nmap 10.10.131.165 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-31 16:14 CET
Nmap scan report for 10.10.131.165
Host is up (0.034s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.63 seconds

┌──(amsi㉿kali)-[~]
└─$
```

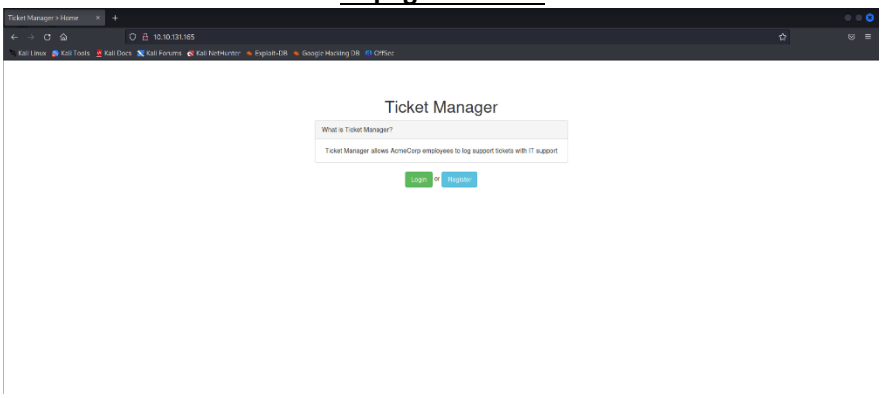
Je vois qu'il y a 2 services de disponible :

- SSH
- WEB

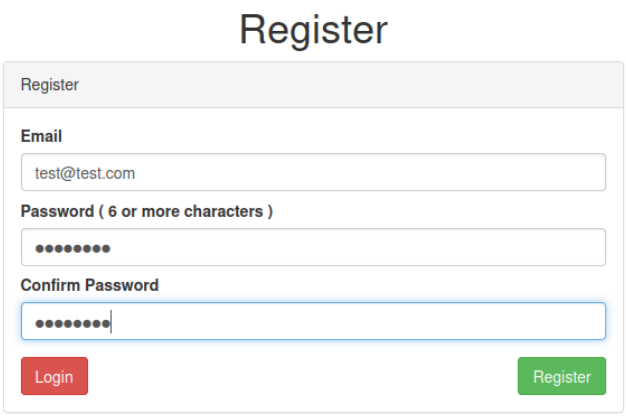
2. Exploitation

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

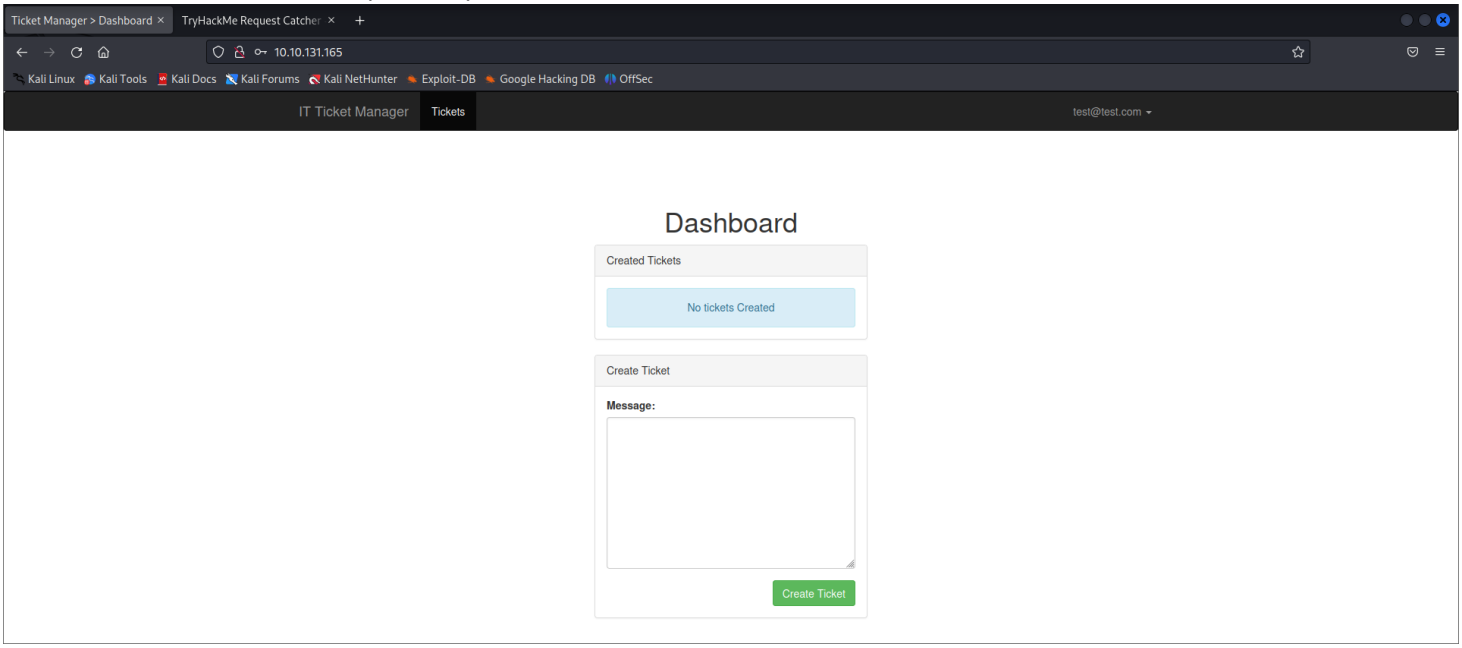
La page d'accueil



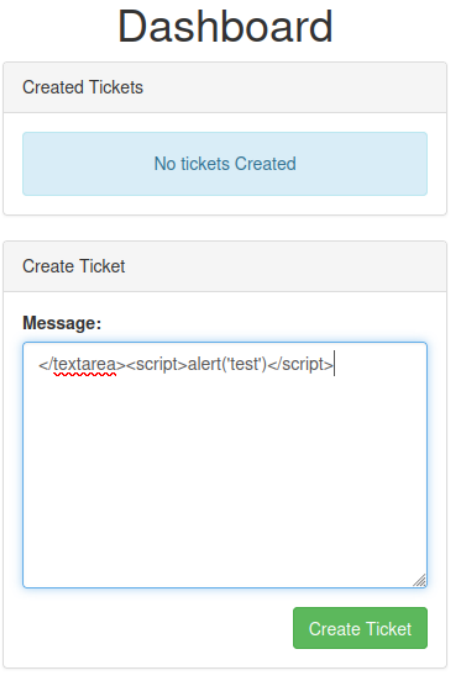
Je me crée un compte de test :



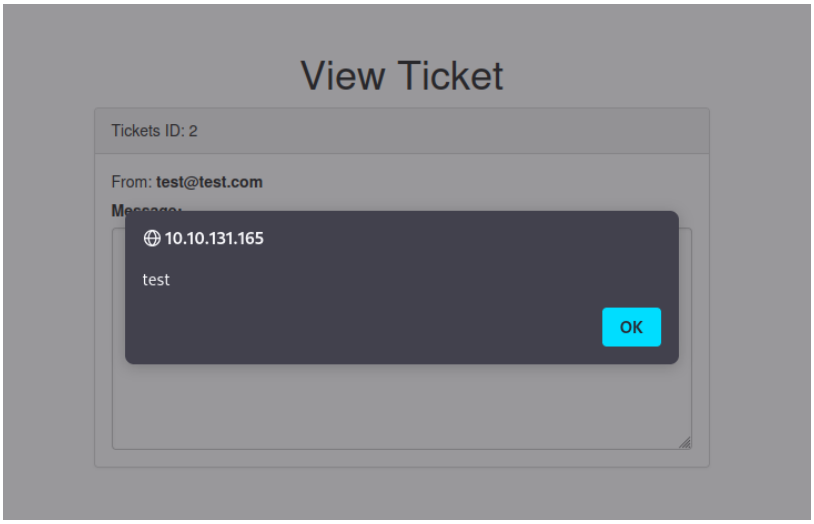
Je me connecte avec mon compte test pour voir l'interface :



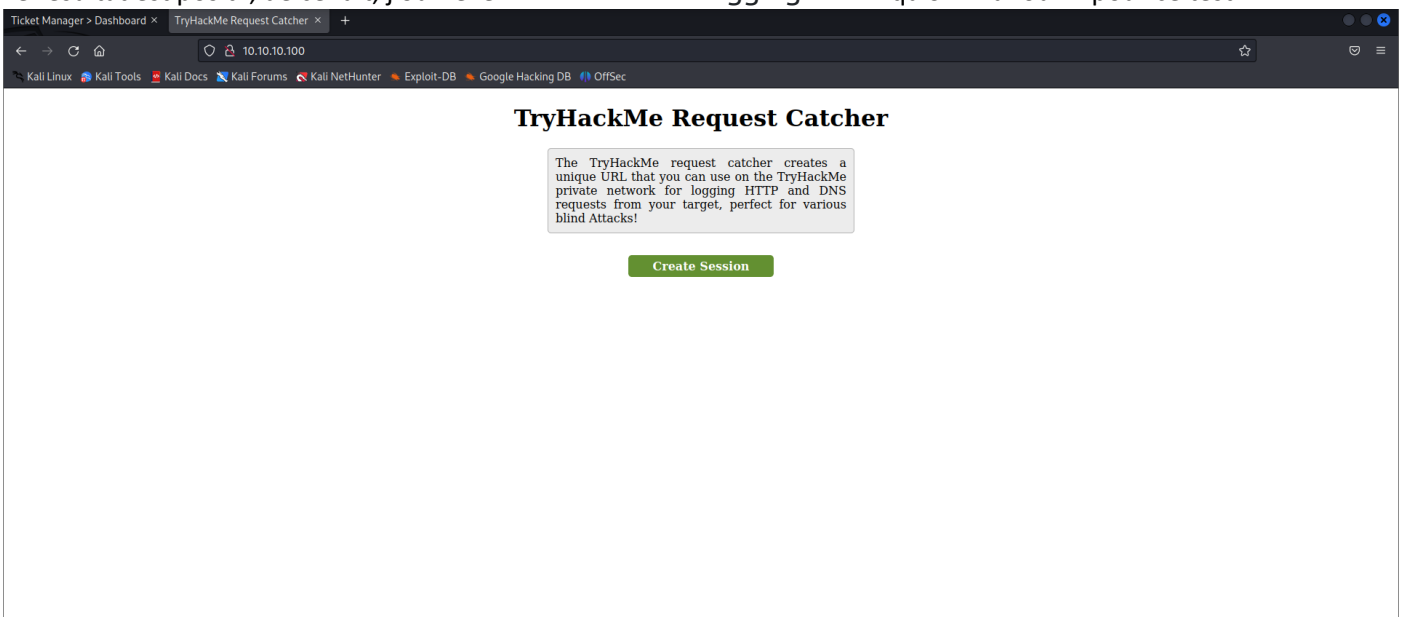
Je vais créer un ticket en tentant une injection XSS :



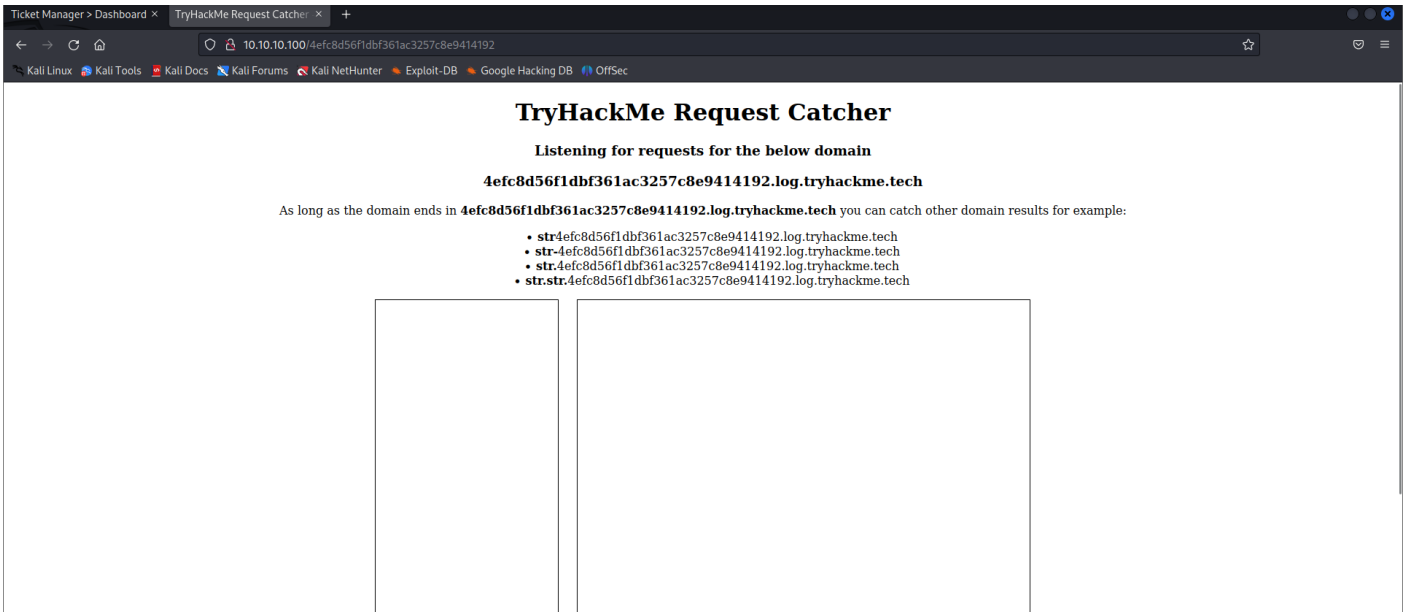
Voici le résultat :



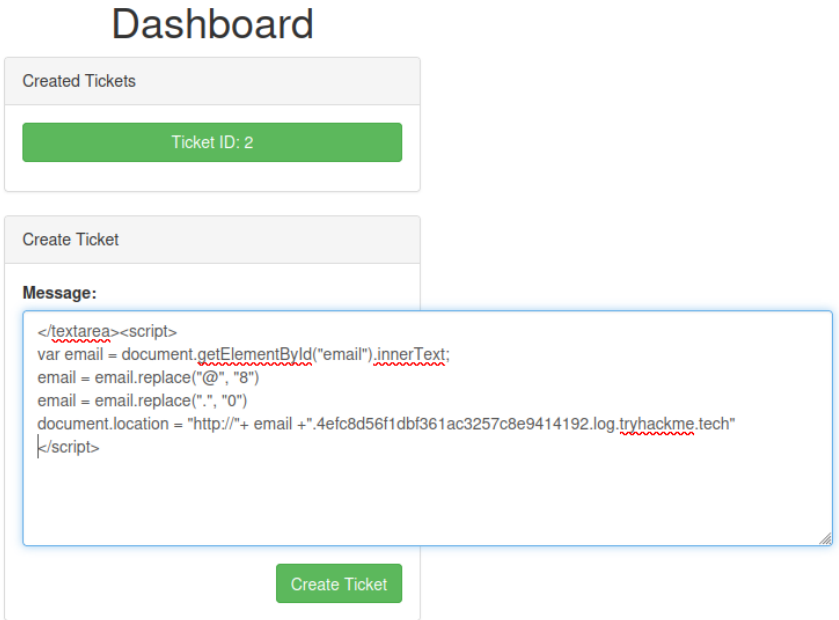
Le résultat est positif, de ce fait, j'ouvre le « HTTP & DNS Logging tool » qu'on m'a fourni pour ce test :



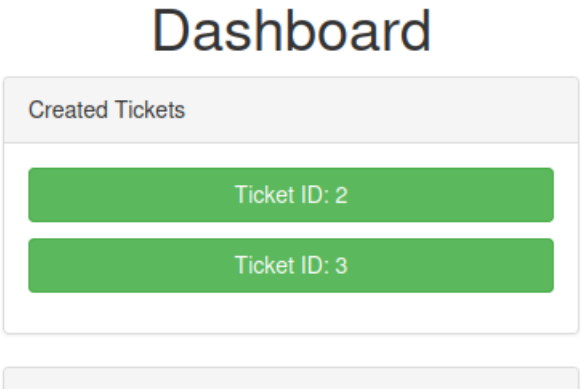
Je crée une session :



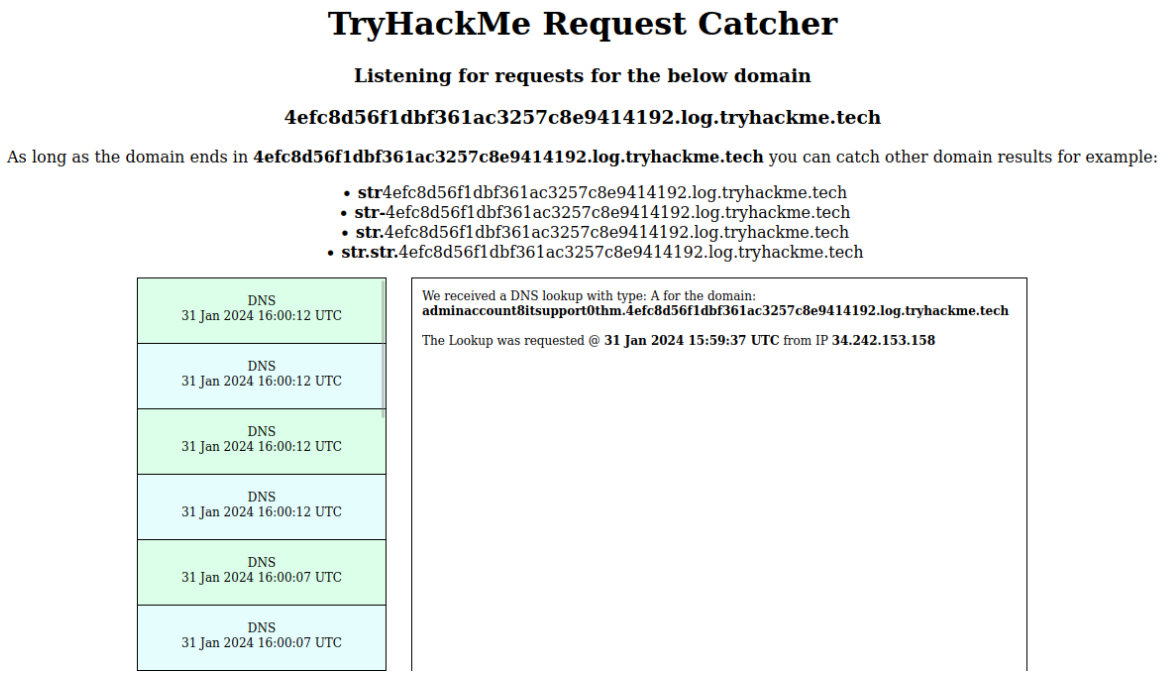
Je retourne sur le site pour tenter de récupérer l'adresse Email de l'admin en redirigeant ces infos sur la session http crée :



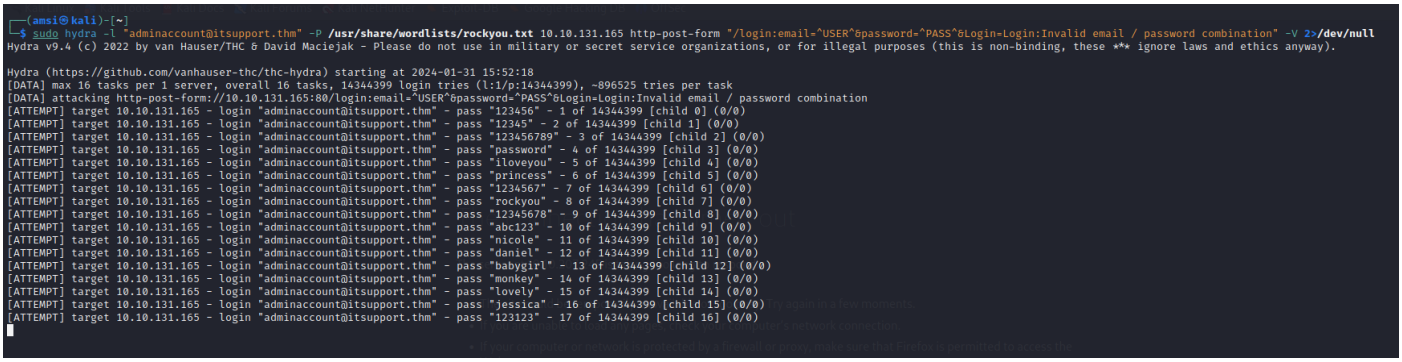
Je viens de remarquer que mon premier ticket commence par l'ID 2 et non par 1, donc j'en déduis qu'il existe déjà un ticket 1 :



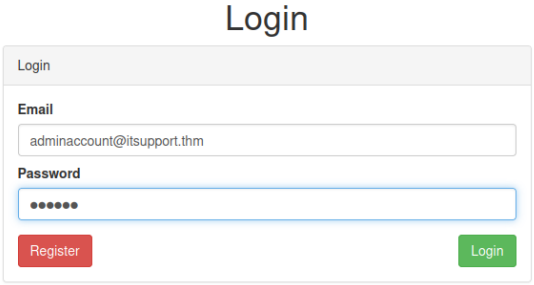
Je regarde les résultat reçus sur le serveur HTTP :



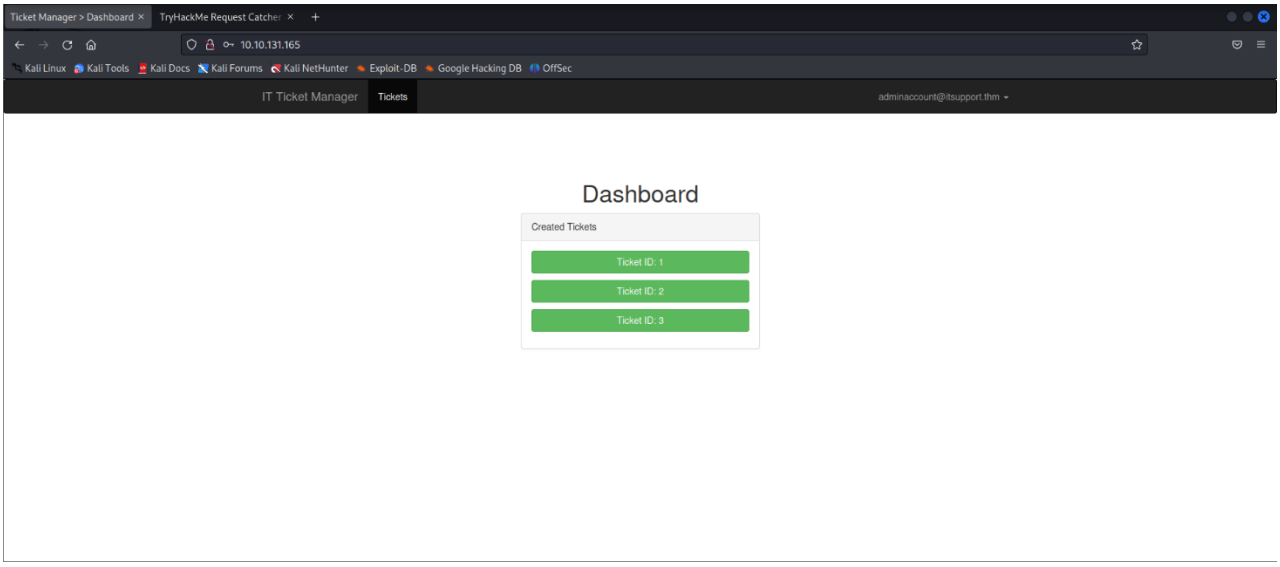
Je vois que j'ai reçu l'adresse mail de l'admin, donc je tente un brute force avec Hydra :



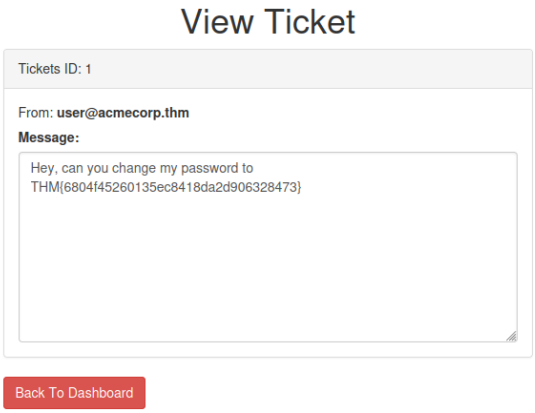
Je tente de me connecter en essayant les mots de passe cité par Hydra :



J’ai réussi à me connecter en admin :



Je vais donc voir le contenu du ticket 1 :



Je pris beaucoup de temps à trouver les flags, mais le TP a été fastidieux. J’ai appris une autre facette d’Hydra, J’ai pris énormément de temps à trouver le 1 Flag, mais une fois trouvé, les autres Flags se suivent mutuellement.

Voici les flags récupérés :