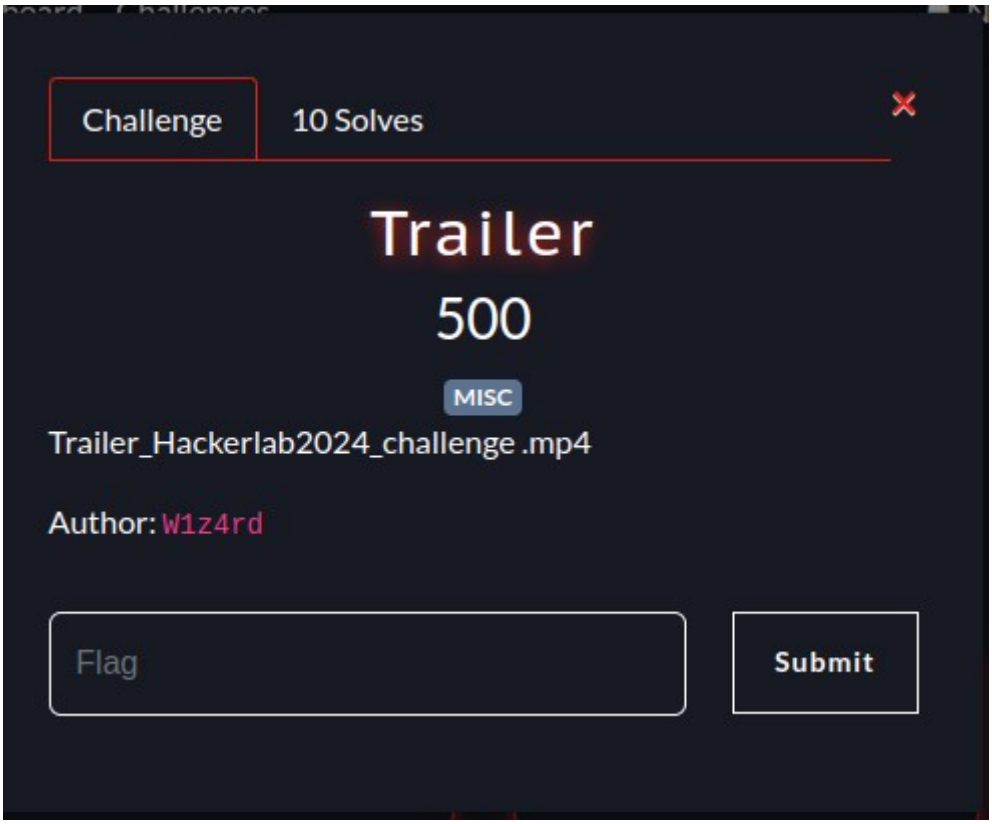
Writeup du challenge Trailer de la phase de qualification pour le HarckerLab 2024

Nom d'utilisateur : takeoff
E-mail : robertohoungbo@gmail.com
Affiliation : IFRI
Pays : Bénin



Le challenge est accompagné d'un fichier mp4 nommé Trailer_Hackerlab2024_challenge.mp4. A l'ouverture du fichier on tombe sur une vidéo un peu bizarre.

J'ai tout d'abord essayé de vérifier les métadonnées de la vidéo avec exiftool mais je n'ai rien obtenu de concluant. J'ai alors continué à regarder la vidéo dans le but de trouver un indice quelconque. Au début je voyais pas grand-chose mais à partir d'un moment je vois dans le coin supérieur droit de la vidéo des petits points blancs qui apparaissent puis disparaissent. N'ayant jamais

été confronté à ce type de challenge, je me suis lancé dans la recherche d'un cas similaire sur internet. Pour ma recherche j'ai utilisé les mots clés suivant : Trailer, vidéo, points blancs coin supérieur droit, challenge, ctf , writeups.

Après près de 45 minutes de recherche je suis finalement tombé sur un article qui détaille très clairement la méthode de résolution du challenge. J'ai alors suivi la même méthode que l'auteur pour résoudre le challenge en adaptant les données au fur et à mesure.

Lien de l'article :
https://github.com/ljx1608/ctf-writeups/blob/main/seetf-2022.md#welcome

J'ai appliqué la même méthode tout en renseignant les données propres à la vidéo qui m'a été fournie.
Dans un premier temps j'ai généré tous les frames de la vidéo à partir du moment où les points blancs ont commencé à apparaître (00:00:20) tout en rognant la vidéo afin qu'elle cadre sur le coin supérieur droit. La commande ffmpeg suivante m'a permis de faire ce traitement sur la vidéo :

```
ffmpeg -ss 00:00:20 -i Trailer_Hackerlab2024_challenge.mp4 -filter:v "crop=200:200:1940:0" processed.mp4
```

J'ai ensuite utilisé le script de résolution de l'article avec la vidéo de sortie processed.mp4. Ce qui m'a permis de retrouver le qr code. Voici le script modifié que j'ai utilisé :

```python
import cv2 as cv
import numpy as np

# Create a blank image of the same size as the input video
output = np.zeros((200, 200), np.uint8)

cap = cv.VideoCapture("processed.mp4")  # Open the video file
while cap.isOpened():  # Loop until the video is over
    # Read the next frame into frame, ret will be `false` if no frame is read
    ret, frame = cap.read()

    # Break if there are no more frames to read
    if not ret:
        break

    # Filter the white (BGR above (200, 200, 200)) pixels from the frame
    mask = cv.inRange(frame, (200, 200, 200), (255, 255, 255))
    # and put them in the output image, using or to combine the different frames
    output = np.bitwise_or(output, mask)

cv.imwrite("output.png", output)  # Save the output image

cap.release()  # Close the video file (er actually unnecessary but i think good habit)
```

L'exécution de ce script m'a permis de reconstituer le qr code comme suit :

En scannant ce code j'obtiens le lien https://justpaste.it/1nhcv.

Je me rends sur l'adresse du lien et je tombe sur un ordre de mission comportant un tas de données. En analysant les données de près, je remarque que c'est en fait les données hexadécimales d'un fichier au format jpg mais il y a un problème avec ces données. Je constate que tous les deux octets les positions sont inversées.

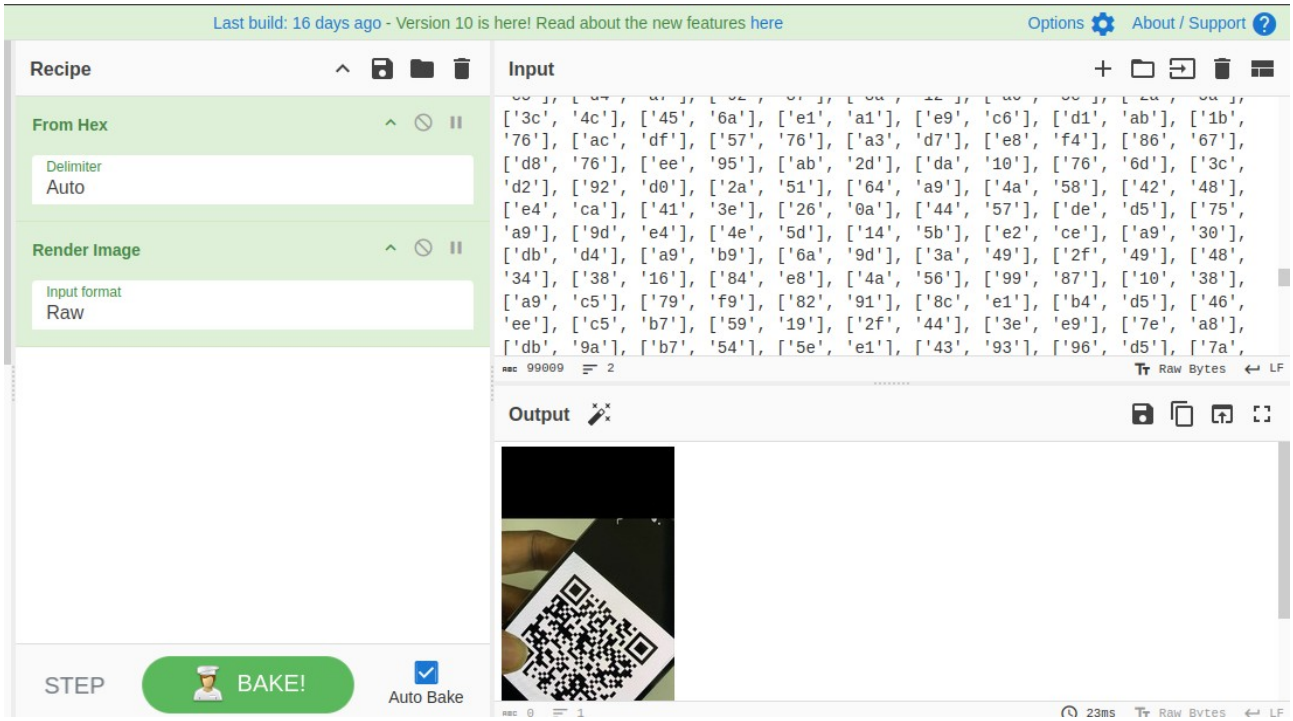
J'ai écrit le script suivant pour reformater les données :

```python
def split_and_reverse_blocks(hex_str):
    return [[block[2:], block[:2]] for block in (hex_str[i:i+4] for i in range(0, len(hex_str), 4)) if len(block) == 4]

def convert_to_ascii(reversed_blocks):
    try:
        return bytearray(int(value, 16) for block in reversed_blocks for value in block).decode('ascii')
    except UnicodeDecodeError:
        return bytearray(int(value, 16) for block in reversed_blocks for value in block).decode('latin-1')

with open("donnes.txt", "r") as fil:
    hex_str = fil.read()
reversed_blocks = split_and_reverse_blocks(hex_str)
print(reversed_blocks)
```

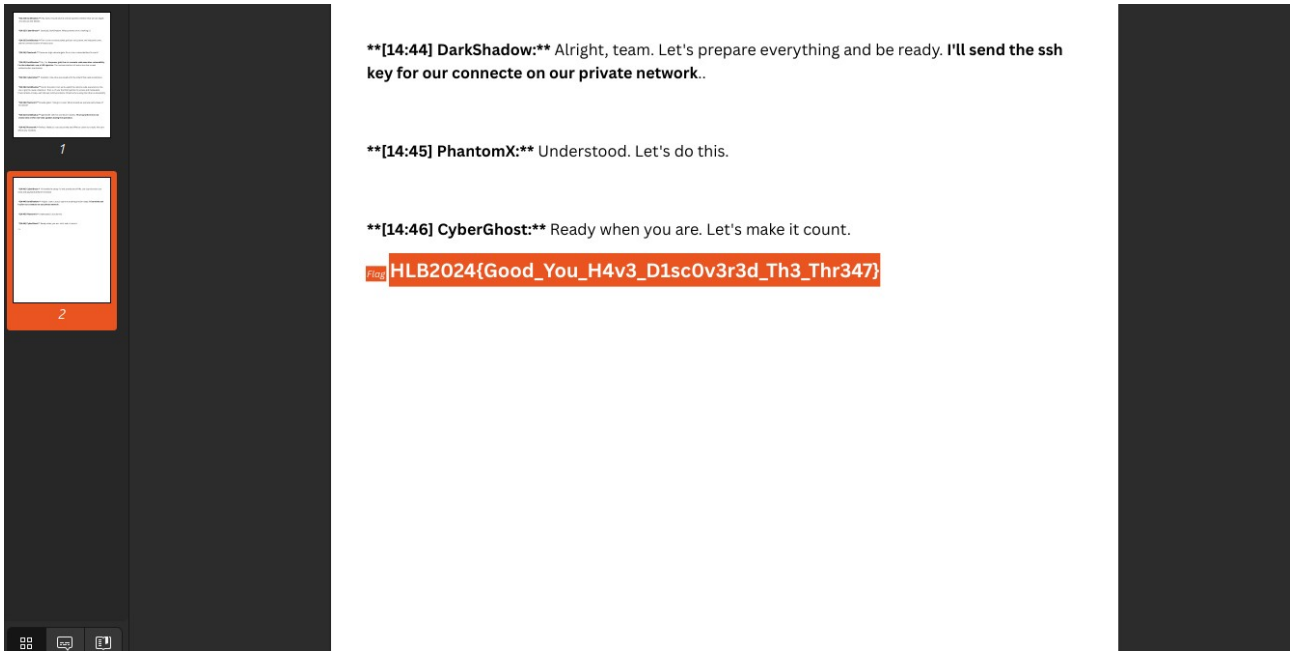
En mettant la sortie du script dans un fichier puis en chargeant le fichier sur Cyberchef, les fonctionnalités from_hex et render_image de cyberchef me permettent d'obtenir l'image jpeg comme suit :



Après scannage du qrcode sur l'image j'obtiens un nouveau lien : https://mega.nz/file/dtcG1Y4Y#KEtRvI2HZJAEIIcNepAVdKr2QI7bRNwCC1SuqL4w9EI

A partir du lien je télécharge le fichier pdf nommé ics_discussion.pdf. A l'ouverture du fichier, je tombe sur une discussion sur l'attaque d'infrastructures critiques du Bénin. Je défile vers la fin du ficher et je vois l'indicateur flag mais sans le

flag. J’ai essayé de sélectionner les espaces vides et le flag est apparu.



Flag : HLB2024{Good_You_H4v3_D1sc0v3r3d_Th3_Thr347}

Merci !