Wrong Size

Frazew & Archonte

Table des matières

Challenge : Wrong size

On est ici face à une image qui doit cacher le flag dans un élément en rapport avec sa taille (comme le titre du challenge le sous-entend ...).

On va donc chercher à trouver des indices liés à des éléments stockés dans les données mais non visibles immédiatement sur l'image.

Fig. 1: Homer est content

Partie 1 : Récupération des données cachées

On ouvre notre image à l'aide d'un éditeur de texte en hexadécimal (ici bless).

```
bless message.png
```

On obtient une page d'hexadécimal. On s'intéresse aux bordures de l'image et on essaie de voir si en la forçant à s'élargir, on obtient quelque chose d'intéressant.

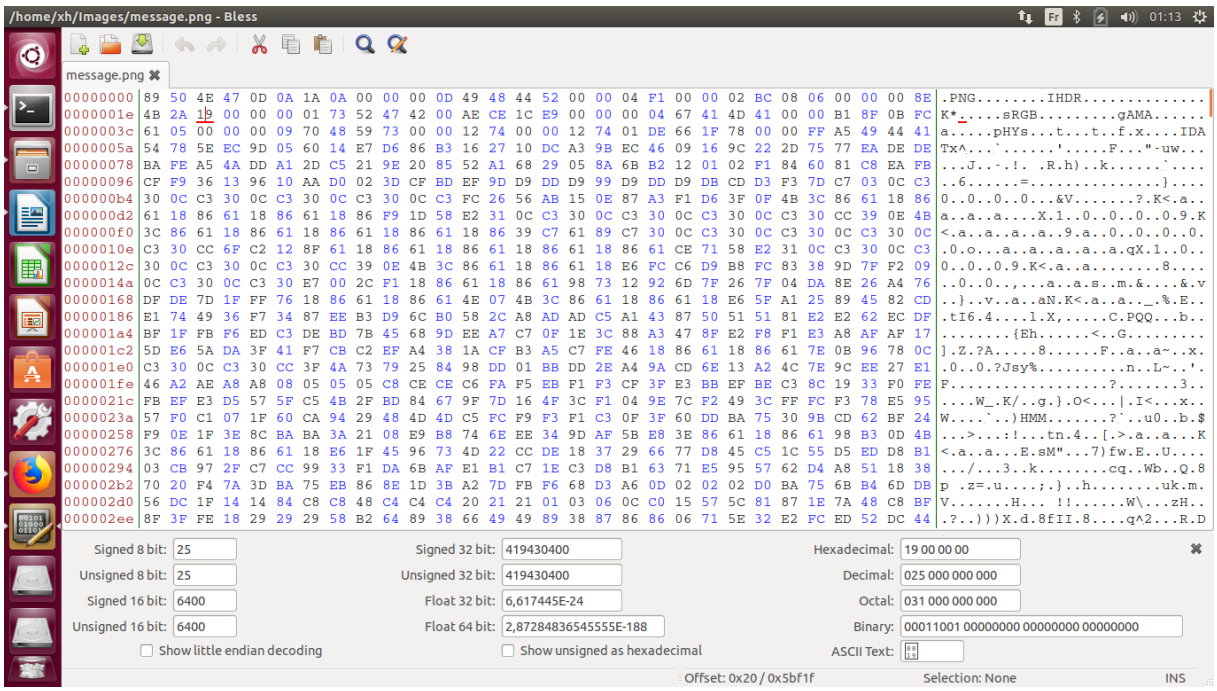

Fig. 2: On modifie la largeur/hauteur de l'image

Cependant, quand on modifie ainsi l'image, elle devient illisible car le « sumcheck » à la fin du fichier hexa n'est plus valide. On doit donc trouver un moyen de la rendre à nouveau utilisable.

Pour ce faire,on utilise pngcsum afin de recalculer cette somme.

```
pngcsum message_modife.png message_recode.png
```

Fig. 3: On obtient ainsi une image avec un flag ! Youpi !

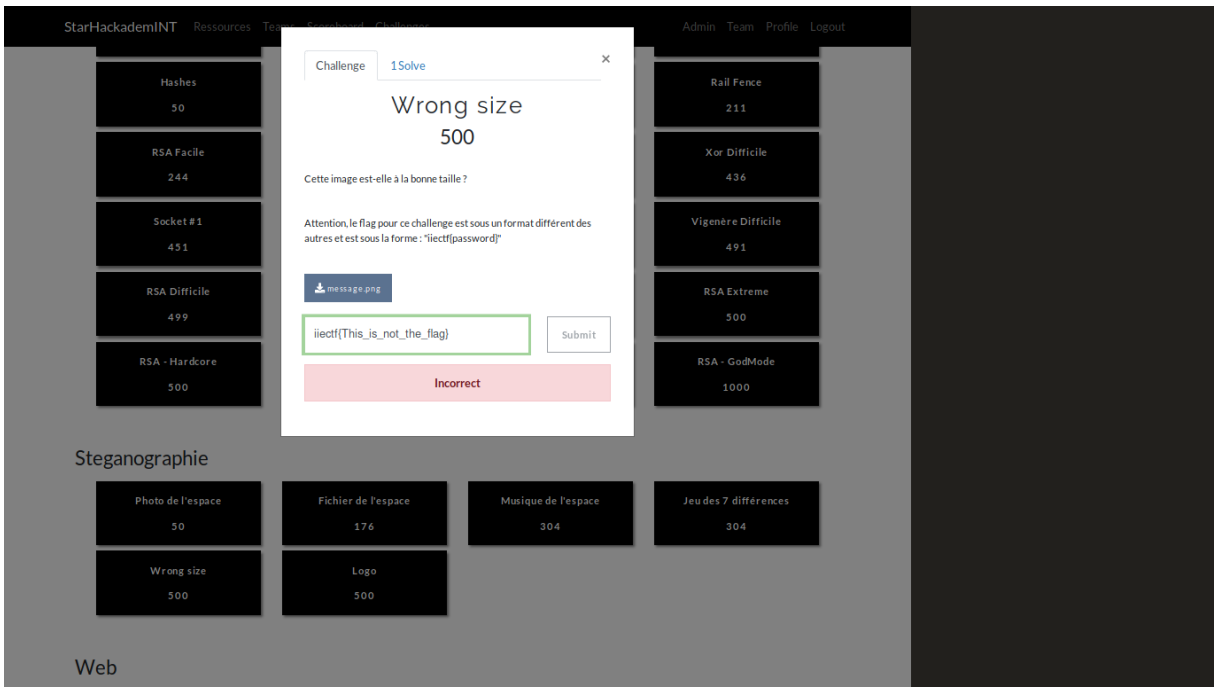

Fig. 4: Ou pas ... En même temps on aurait pu s'en douter

Partie 2 : Chasse au drapeau

Comme on est dans les challenges de « Stéganographie » on va faire de la ... Stéganographie, bravo à ceux qui ont trouvé, pour les autres, il y aura un CF2.

Soit vous aimez la programmation et vous allez chasser tranche de pixel par tranche de pixel avec des programmes Python par exemple, soit vous avez autre chose à faire de votre nuit et on remercie Steven von Acker (haha) pour son outil Java « Stegsolve ». https ://github.com/zardus/ctf-tools/blob/master/stegsolve/install

En utilisant ce superbe outil,on peut récupérer les pixels de chaque couleur et de chaque poids, regarder l'alpha ou même lancer des random color maps. Grâce à celles-ci (ou à une récupération des pixels de poids 0 ou 1), on obtient une version de l'image suivante :

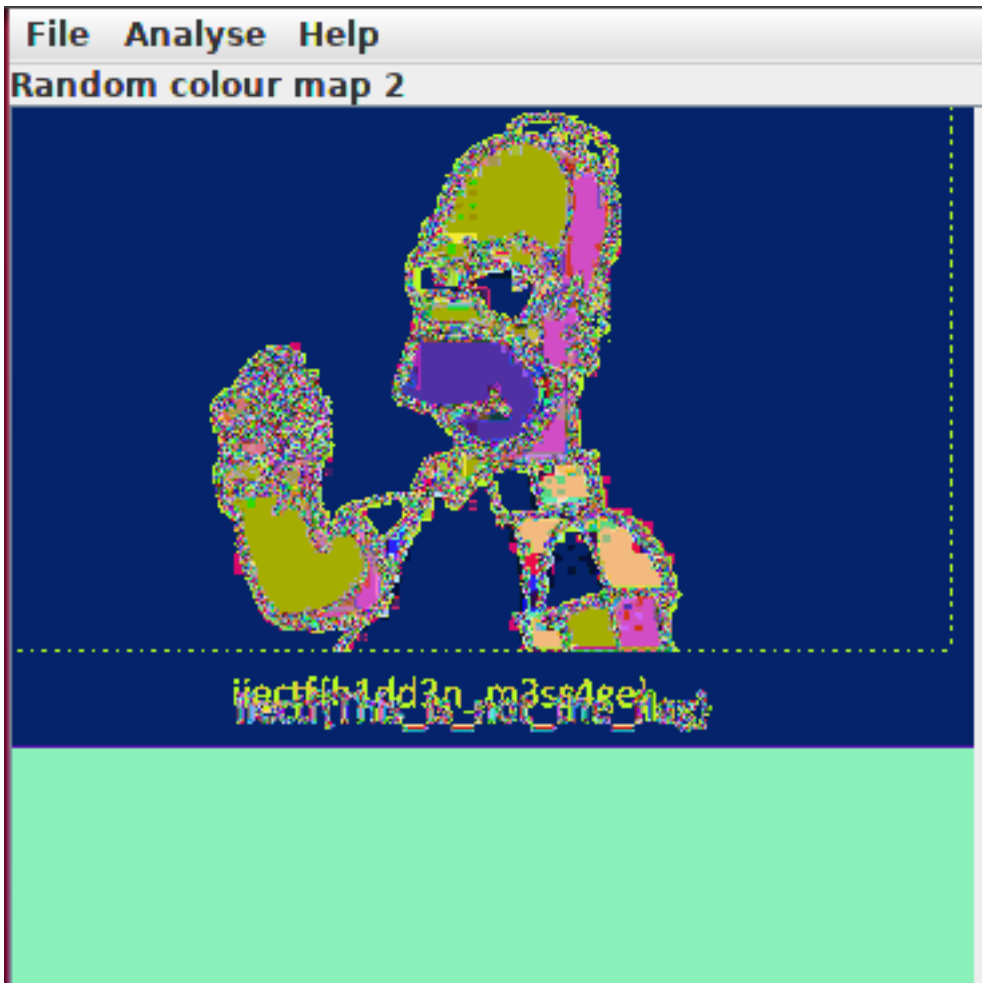

Fig. 5: Sous vos yeux ébahis, le flag !

Le flag est donc iiectf{h1dd3n_m3ss4ge} !