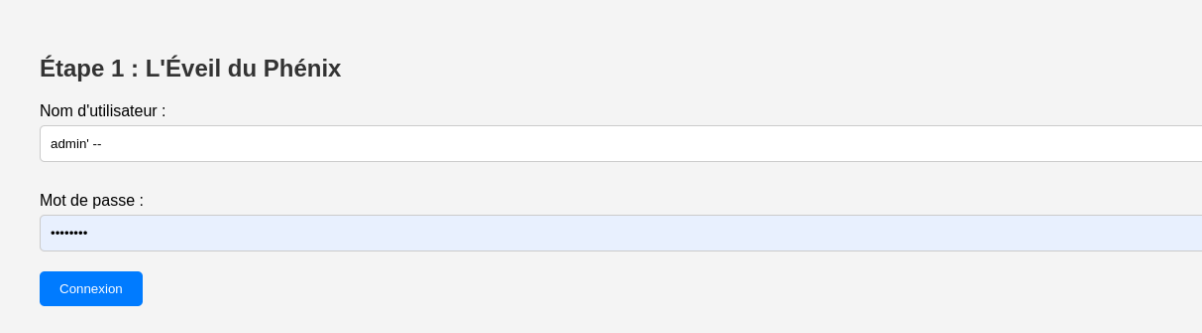
Etape 1: Le web

Nous avions une page de connexion, donc j'ai pensé à une injection SQLi.

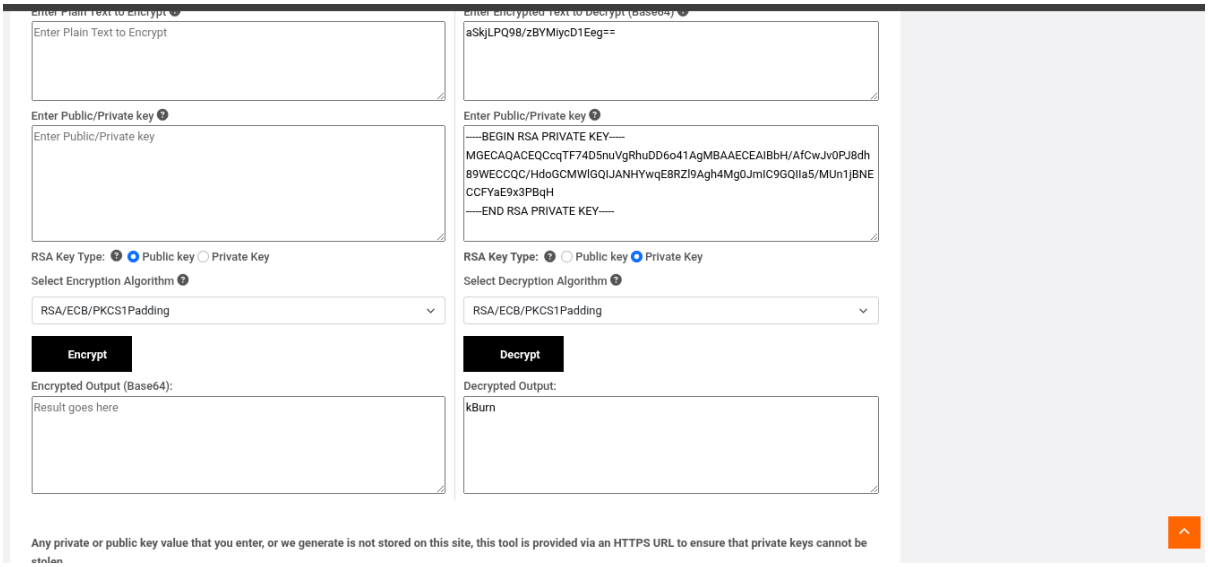
J'ai ensuite trouvé la bonne payload :

admin' -- (au niveau du nom d'utilisateur).



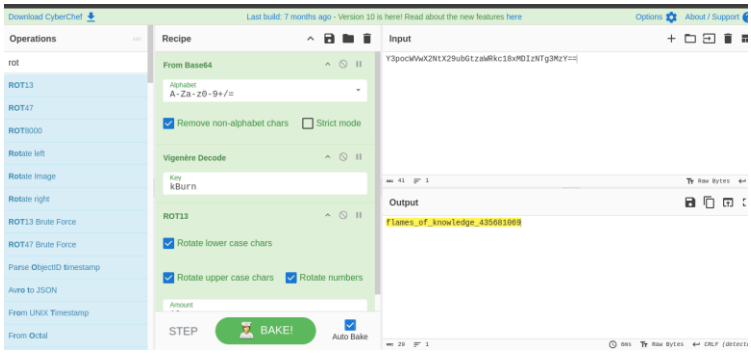
Etape 2 : Crypto

Nous avions deux fichier : chiffres et , ainsi qu'un deuxième fichier qui n'est rien d'autre que la clé publique RSA. Pour obtenir la clé privée, j'ai utilisé l'outil **rsactftools**. Après l'avoir récupérée, j'ai utilisé un outil en ligne pour obtenir la valeur de la ligne 1.

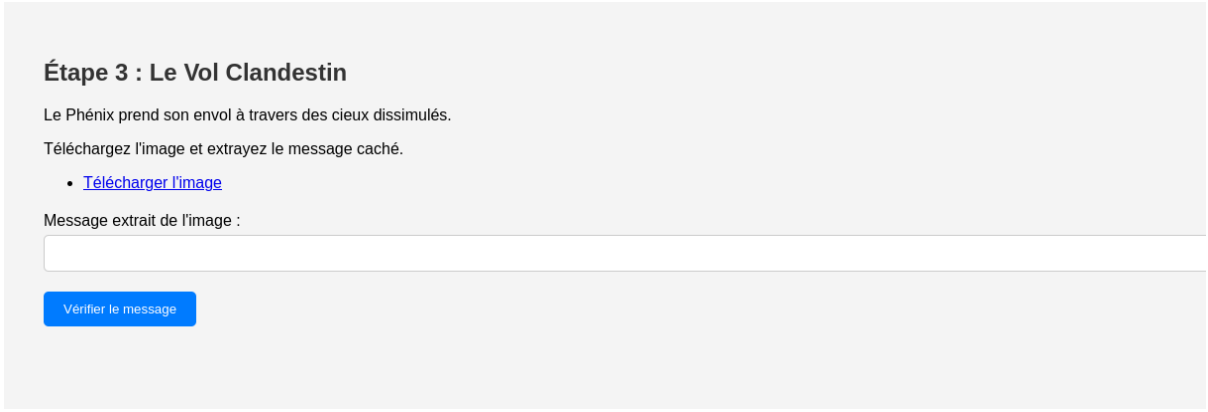


Nous avions un code nommé **kBurn**, et j'avais déjà décodé le code en base64. Voici les étapes : j'ai utilisé le chiffrement de Vigenère, puis un déchiffrement avec ROT13

pour obtenir le flag final

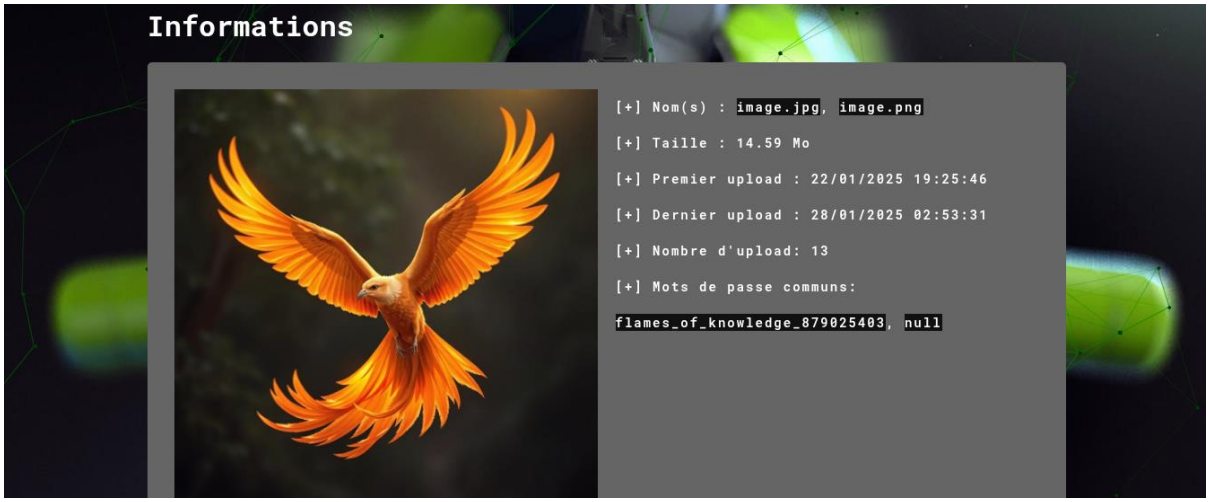


Etape3 :Stegano



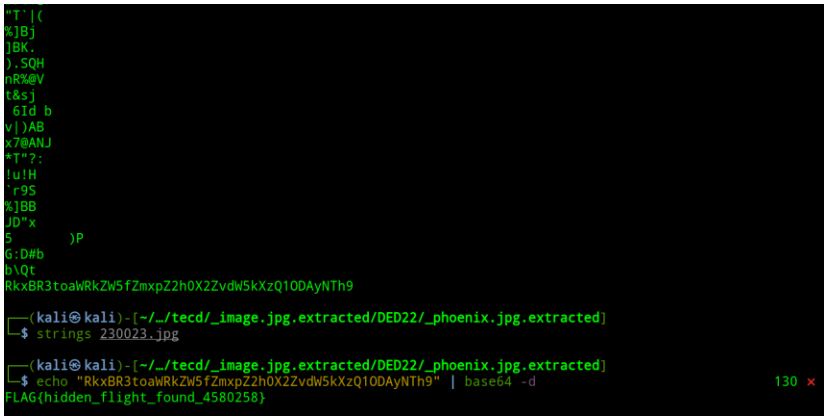
Après l'avoir téléchargée, j'ai utilisé **binwalk** pour extraire les informations de l'image. Nous avons découvert un fichier **.rar**. À ma grande surprise, ce fichier me demandait un mot de passe. J'ai beaucoup réfléchi à différentes approches, puis je me suis souvenu de mon précieux outil, que j'utilise souvent dans les challenges stéganographiques : [AperiSolve](https://aperisolve.com/).

J'ai donc uploadé l'image du challenge directement sur cet outil.



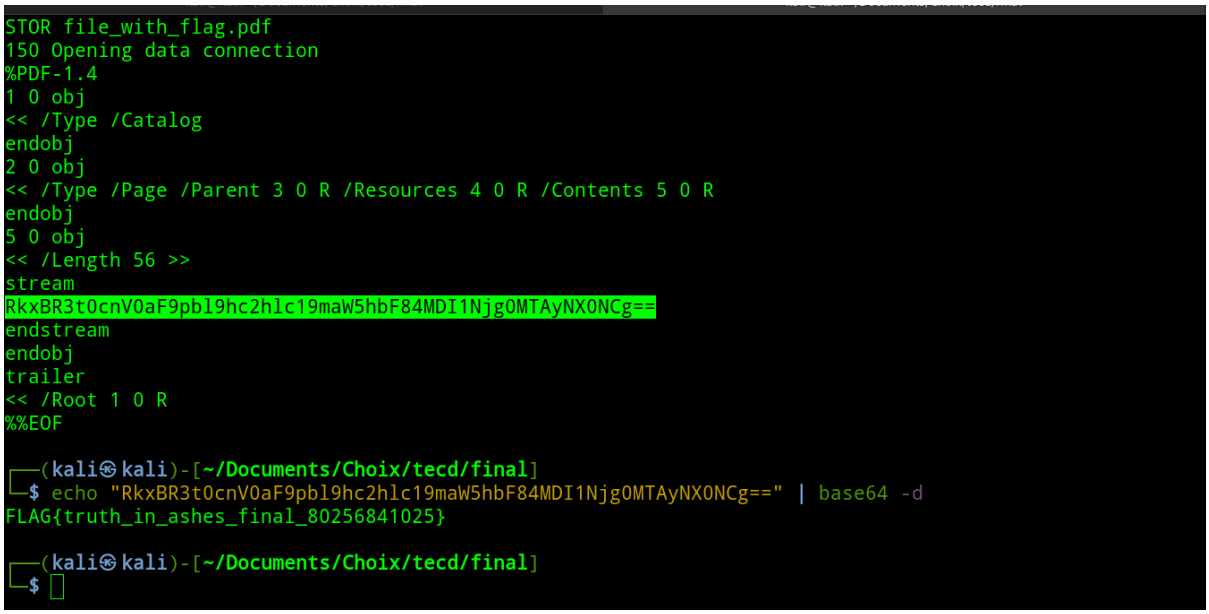
J'ai obtenu le mot de passe de mon fichier **.rar**, puis j'ai extrait tout le contenu. Nous avions, au total, 6 images. J'ai alors commencé à analyser chacune d'elles avec la commande **strings**.

Sur la première image, en utilisant **strings**, j'ai trouvé un code en base64. Je l'ai décodé et obtenu le mot "flag". Je me suis dit que c'était le flag, mais non. J'ai donc répété la même démarche pour les autres images, et bingo ! Le flag se trouvait dans la troisième image.



Petit discrément, la commande `strings` que j'ai mise en bas avant de décoder le flag final, c'est juste pour vous montrer le nom de la commande hein, le nom du fichier de l'image, et j'ai fait `Ctrl+C` pour avoir une nouvelle ligne

Etape 4: Forensics



J'ai téléchargé le fichier, j'ai utilisé la commande **strings** et, à ma grande surprise, j'ai trouvé le flag qui était encodé en **base64**. Je l'ai rapidement décodé (*chap chap chap*) et voilà, j'ai obtenu le flag ! 🎉 🚀 💻

🥳 **Quand la chance te sourit, ça va vite hein ! 😎 ✨**

Auteur:foundhack

CHAMSS-DINE ADEDOYI AGBIZOUNON