

Etape 1: Le web

Nous avons 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).

The screenshot shows a login form with the title "Étape 1 : L'Éveil du Phénix". It has two input fields: "Nom d'utilisateur :" containing "admin' --" and "Mot de passe :" containing "*****". Below the fields is a blue button labeled "Connexion".

Etape 2 : Crypto

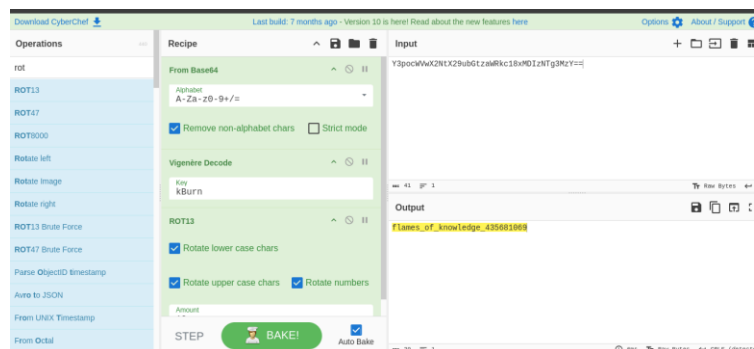
Nous avons deux fichiers : chiffres et , ainsi qu'un deuxième fichier qui n'est rien d'autre que la clé publique RSA. Pour obtenir la clé privée, j'ai utilisé l'outil ****rsactftools****.

Après l'avoir récupérée, j'ai utilisé un outil en ligne pour obtenir la valeur de la ligne 1.

The screenshot shows an online RSA encryption/decryption tool. It has two main sections: "Encrypt" on the left and "Decrypt" on the right. Both sections have input fields for "Enter Plain Text to Encrypt" or "Enter Encrypted Text to Decrypt (base64)", "Enter Public/Private key", and "RSA Key Type" (Public key or Private Key). The "Encrypt" section also has a "Select Encryption Algorithm" dropdown set to "RSA/ECB/PKCS1Padding" and an "Encrypt" button. The "Decrypt" section has a "Select Decryption Algorithm" dropdown set to "RSA/ECB/PKCS1Padding" and a "Decrypt" button. The "Decrypted Output" field shows the result "kBurn". At the bottom, there is a disclaimer: "Any private or public key value that you enter, or we generate is not stored on this site, this tool is provided via an HTTPS URL to ensure that private keys cannot be stolen".

Nous avons 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

Étape 3 : Le Vol Clandestin

Le Phénix prend son envol à travers des cieux dissimulés.

Téléchargez l'image et extrayez le message caché.

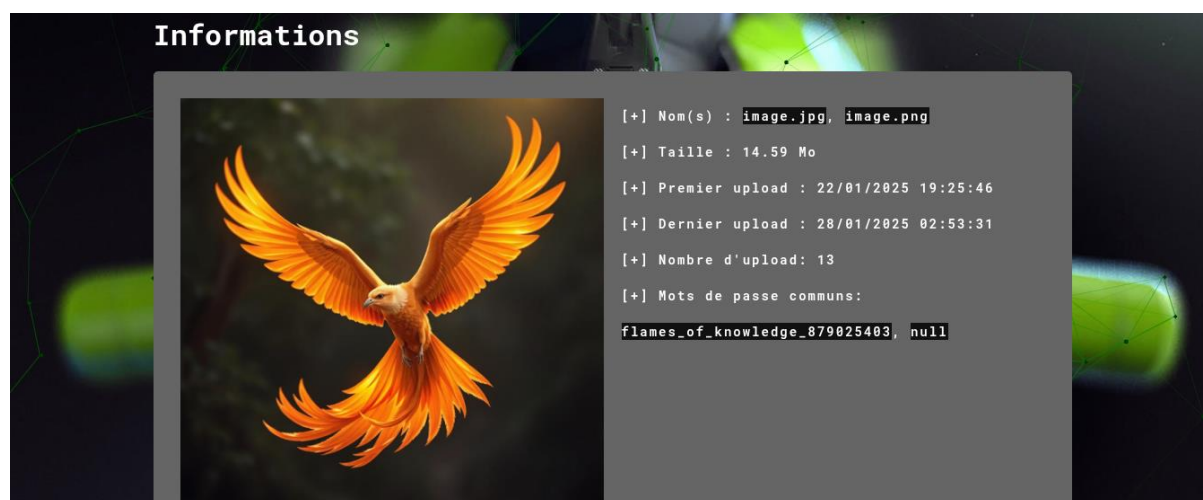
- [Télécharger l'image](#)

Message extrait de l'image :

Vérifier le message

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 avons, 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.

```
"T"[(
%JBj
)BK-
).SQH
nR%v
t&sj
6id b
v))AB
<70ANJ
*T"?;
iulH
'r9S
%JBB
JD"x
5
)P
G:D#b
b\Qt
RkxBR3toahRkZW5fZmxpZ2h0X2Vudw5kXzQ1ODAyNTh9

(kali@kali)-[~/tecd/_image.jpg.extracted/DED22/_phoenix.jpg.extracted]
$ strings 230023.jpg

(kali@kali)-[~/tecd/_image.jpg.extracted/DED22/_phoenix.jpg.extracted]
$ echo "RkxBR3toahRkZW5fZmxpZ2h0X2Vudw5kXzQ1ODAyNTh9" | base64 -d
FLAG{hidden_flight_found_4580258}
```

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

```
STOR file_with_flag.pdf
150 Opening data connection
%PDF-1.4
1 0 obj
<< /Type /Catalog
endobj
2 0 obj
<< /Type /Page /Parent 3 0 R /Resources 4 0 R /Contents 5 0 R
endobj
5 0 obj
<< /Length 56 >>
stream
RkxBR3t0cnV0aF9pb19hc2hlc19maW5hbF84MDI1Njg0MTAyNX0NCg==
endstream
endobj
trailer
<< /Root 1 0 R
%%EOF

(kali@kali)-[~/Documents/Choix/tecd/final]
$ echo "RkxBR3t0cnV0aF9pb19hc2hlc19maW5hbF84MDI1Njg0MTAyNX0NCg==" | base64 -d
FLAG{truth_in_ashes_final_80256841025}

(kali@kali)-[~/Documents/Choix/tecd/final]
$
```

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

