I Believe You Can’t Fly

Enoncé :

In the world of Featherstone Airways, where airships dominate the skies and steam-powered engines hum in harmony with the winds, disaster strikes aboard Flight 404. A cacophony of alarms blares through the cabin, and an automated voice pierces the tension:
"Alert: Navigation systems compromised. Manual override unavailable."

The captain, drenched in sweat, confesses that the ship’s intricate steam-core systems have been infiltrated by rogue machinists. The autopilot is spewing erratic commands, and the controls have been rendered useless. Amid the chaos, your gaze falls upon a forgotten device—a mechanical tablet left behind by the ship’s chief engineer. Its dimly glowing screen is your only hope to uncover the secrets of this sabotage and reclaim control of the vessel.

The tablet appears to hold critical files containing traces of the hackers’ interference. To restore the autopilot and prevent the airship from plunging into the abyss, you must uncover the password hidden within these files.
As the last passenger with a keen mind for cyber-steam security, it falls to you to analyze these files, piece together the password, and save the airship before it’s too late. Time is of the essence, and the lives of everyone aboard rest in your hands. Will you rise to the challenge and prove yourself the hero of the skies?

Solution :

Le flag est décomposé en 2 parties.

- Analyse des logs :

- Fausses réponses :
  ercbafr : ROT13 (reponse).
  c29sdXRpb24= : Base64 (solution).
  636c6566 : Hexadécimal (clef).
  0110001011111011011000110110100001100101 : Binaire (bûche).

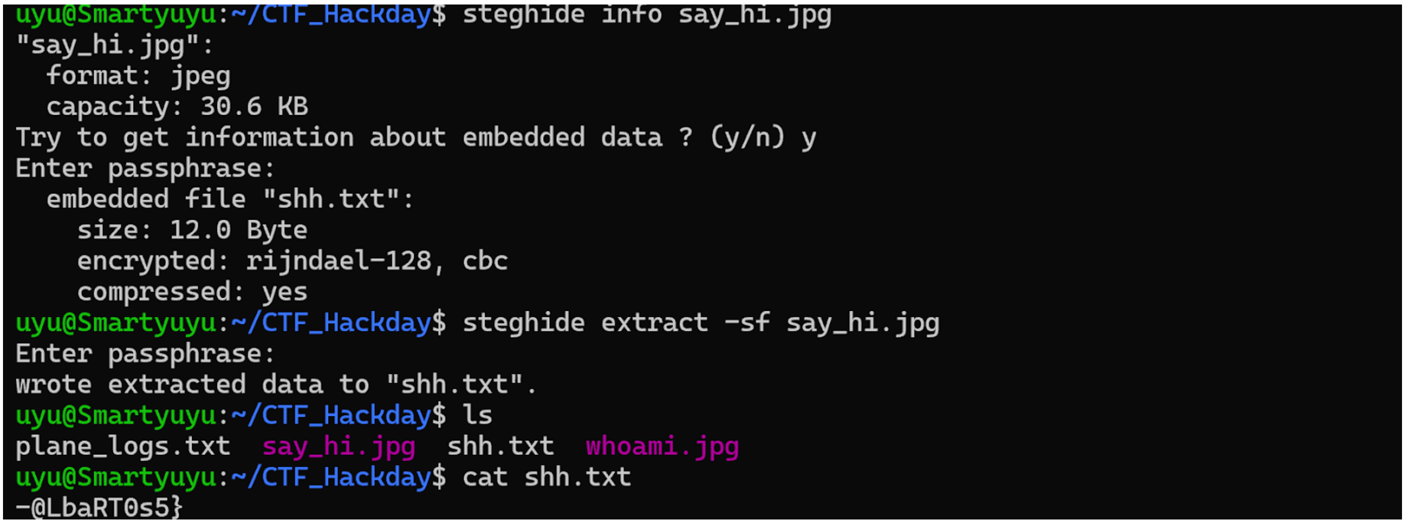
- Bonne réponse :
  KDFNGD\~dPbCbiU6H: Décalage ASCII (+3 sur chaque caractère) -> Indice donné dans les logs pour savoir que c’est un décalage de 3 : *“[2025-01-22 14:08:50] INFO: Sometimes the answer is just three steps ahead.”*

=> La première partie du flag est : **HACKDAY{aM_@_fR3E**

(voir suite page suivante)

- Analyse des images :

Seule l’image say_hi.jpg nous intéresse. Voici le procédé afin de trouver la suite du flag :



```
uyu@Smartyuyu:~/CTF_Hackday$ steghide info say_hi.jpg
"say_hi.jpg":
  format: jpeg
  capacity: 30.6 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "shh.txt":
    size: 12.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
uyu@Smartyuyu:~/CTF_Hackday$ steghide extract -sf say_hi.jpg
Enter passphrase:
wrote extracted data to "shh.txt".
uyu@Smartyuyu:~/CTF_Hackday$ ls
plane_logs.txt  say_hi.jpg  shh.txt  whoami.jpg
uyu@Smartyuyu:~/CTF_Hackday$ cat shh.txt
-@LbaRT0s5}
```

L’indice pour savoir que le passphrase était “securepassword” se trouve dans les logs sous forme *“[2025-01-22 14:03:25] INFO: The most secure password is often the simplest one.”*

La 2e partie du flag est : **-@LbaRT0s5}**

Pour valider ce challenge, on combine les deux réponses qui forment : **HACKDAY{aM_@_fR3E-@LbaRT0s5}**