WU méthode 1 de xenomorph :

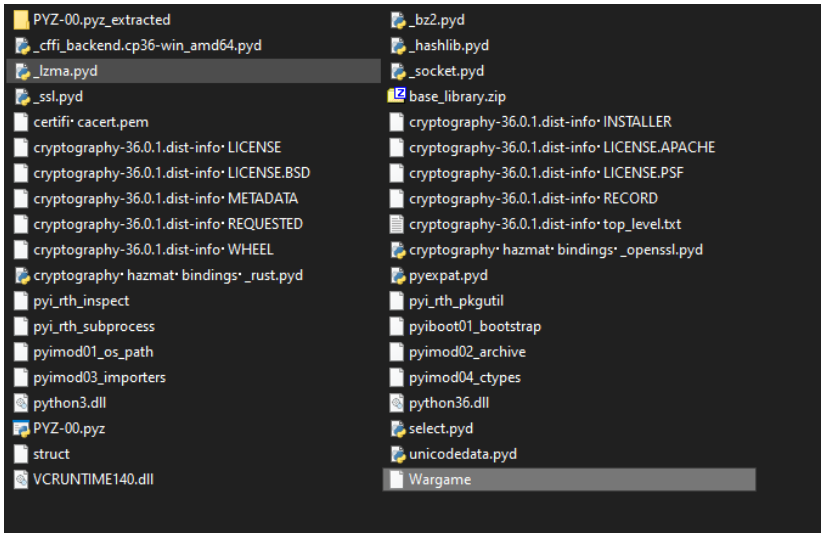
Unpack :

https://github.com/countercept/python-exe-unpacker

```
┌──(root DESKTOP-F0G8TIA)-[/mnt/c/Users/MAEL/Desktop/xeno/python-exe-unpacker]
└─# python2.7 python_exe_unpack.py -i ../ESD_Update.exe -o unpacked
[*] On Python 2.7
[*] Processing ../ESD_Update.exe
[*] Pyinstaller version: 2.1+
[*] This exe is packed using pyinstaller
[*] Unpacking the binary now
[*] Python version: 306
[*] Length of package: 7828656 bytes
[*] Found 37 files in CArchive
[*] Beginning extraction...please standby
[!] Warning: The script is running in a different python version than the one used to build the executable
    Run this script in Python306 to prevent extraction errors(if any) during unmarshalling
[!] Unmarshalling FAILED. Cannot extract PYZ-00.pyz. Extracting remaining files.
[*] Successfully extracted pyinstaller exe.
```

python3 python_exe_unpack.py -i ../ESD_Update.exe -o unpacked

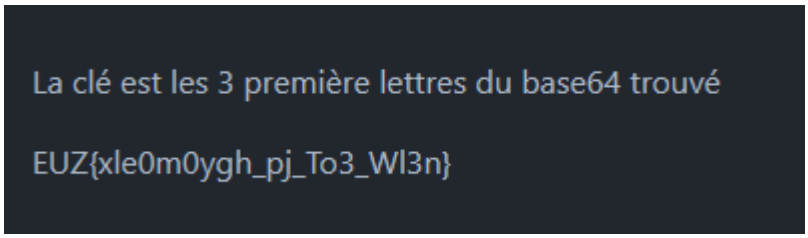
On récupère un tas de fichiers



Je fais un strings sur le fichier **Wargame** je trouve une base64 que je decode

aHR0cHM6Ly9naXRodWIuY29tL3hlbmEyMi9SZWRUZWFtU2NyaXB0L3Jhdy9tYWluL0VTRF9FR0dTLmV4ZQ

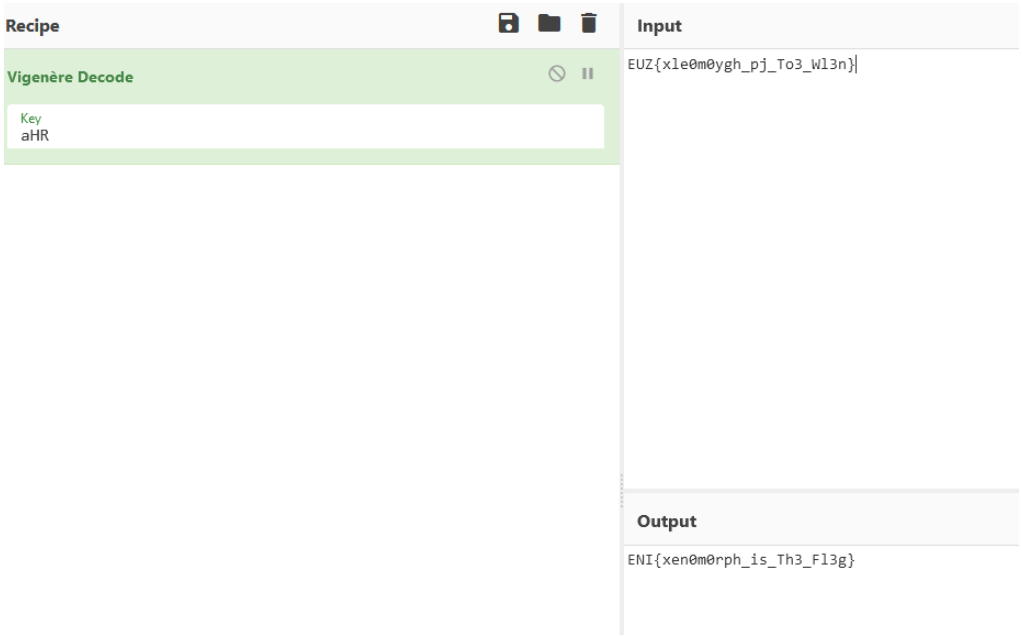
https://github.com/xena22/RedTeamScript/raw/main/ESD_EGGS.exe



Dans le **Github** on trouve un fichier **Flag.md**

Simple Vigenère avec la clef les 3 premières lettres

Et voilà flag (:




```
```