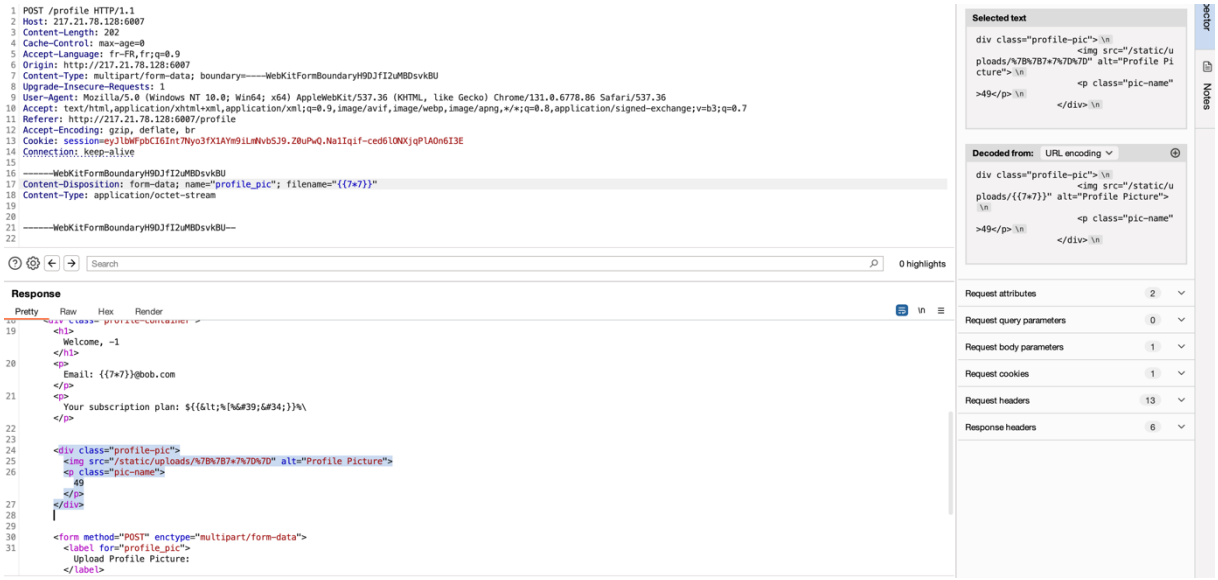
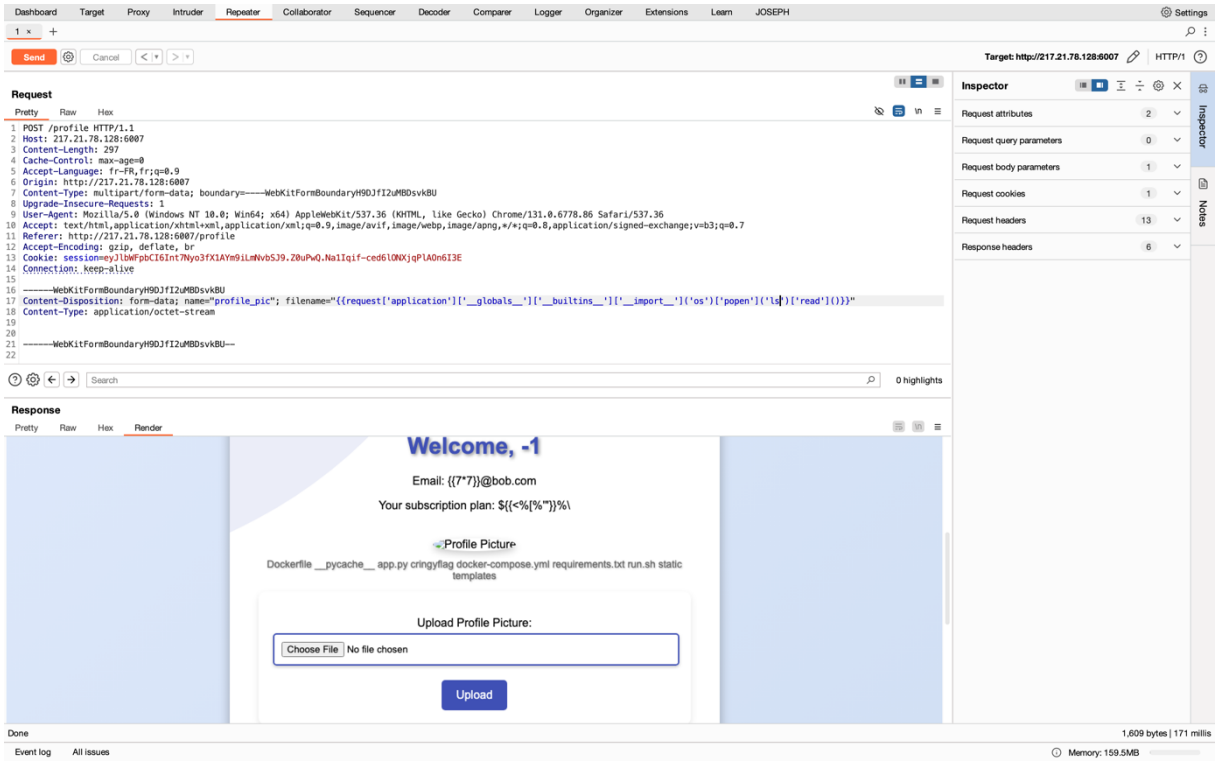
Writeup

1- L’application tourne avec Werkzeug et python

2- Dans l’énoncé du challenge, il est précisé le mot Template. La vulnérabilité courante avec Werkzeug c’est le SSTI (Server Side Template Injection). Encore fallait – il avoir le bon vecteur d’attaque. Le bon vecteur d’attaque est le nom du fichier de la photo de profile. Cela est confirmé par le payload {{7*7}} comme nom du fichier qui donne 49 au reendu sur la page.



3- Une fois le vecteur trouvé, j’ai utilisé le payload suivant pour exécuter des commandes en invoquant les modules nécessaires : {{request['application']['__globals__']['__builtins__']['__import__']('os')['popen']('ls')['read']()}}



Le fichier flag est cringyflag, un cat de ce fichier me donne le flag