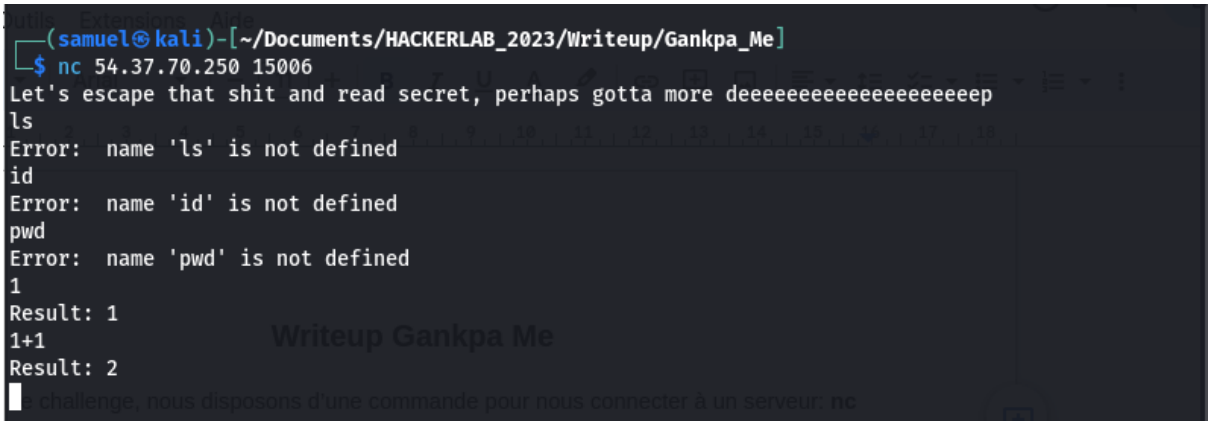
Writeup Gankpa Me N4t10n

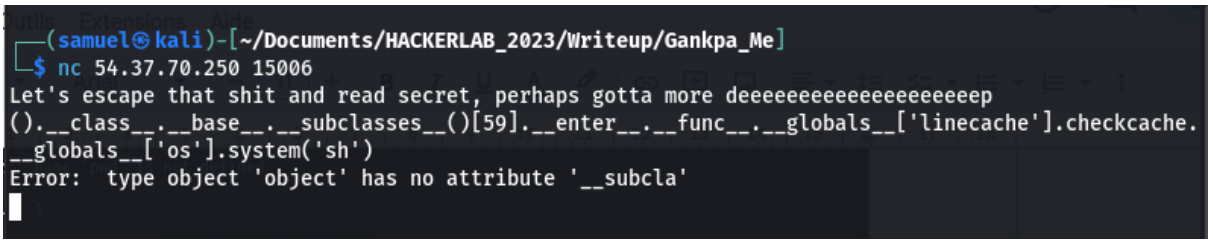
Pour ce challenge, nous disposons d'une commande pour nous connecter à un serveur: **nc 54.37.70.250 15006.** Le contexte est celui: **Aide-moi à m'échapper d'ici, stp !!!.** Cela fait penser à challenge de type **jail break**



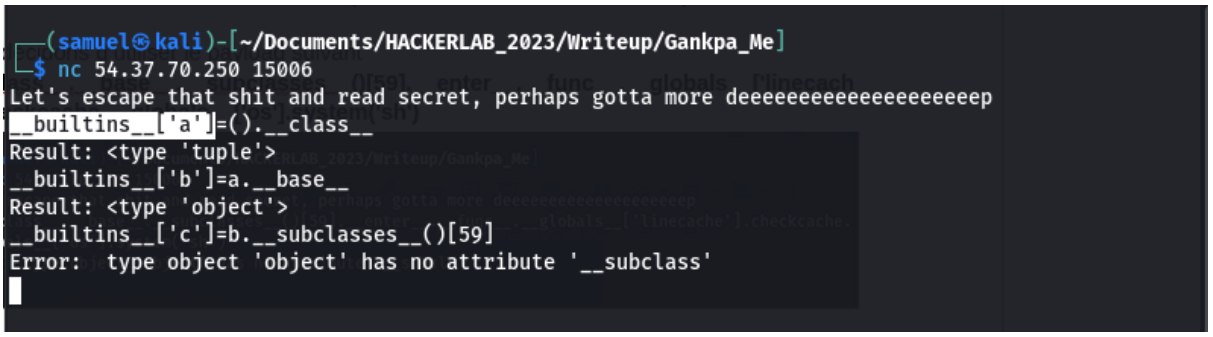
On constate que nous avons des restrictions sur le serveur (On s'y attendait). En faisant des recherches sur les erreurs générées, on se rend compte que nous sommes en face d'un terminal python. Nous avons la possibilité de faire des calculs simples. Il s'agit donc d'un **python jail break**

Après quelques recherches on tombe sur ce site qui parle du sujet https://zolmeister.com/2013/05/escaping-python-sandbox.html. Ensuite nous avons ce site https://blog.pepsipu.com/posts/albatross-redpwnctf qui explique clairement la vulnérabilité à exploiter. Il s'agit de partir des classes, objets et modules auxquels nous avons accès dans ce jail et de remonter, en nous basant sur leur hiérarchie, vers des modules qui nous permettront d'exécuter des commandes système sur le serveur et sortir du jail.

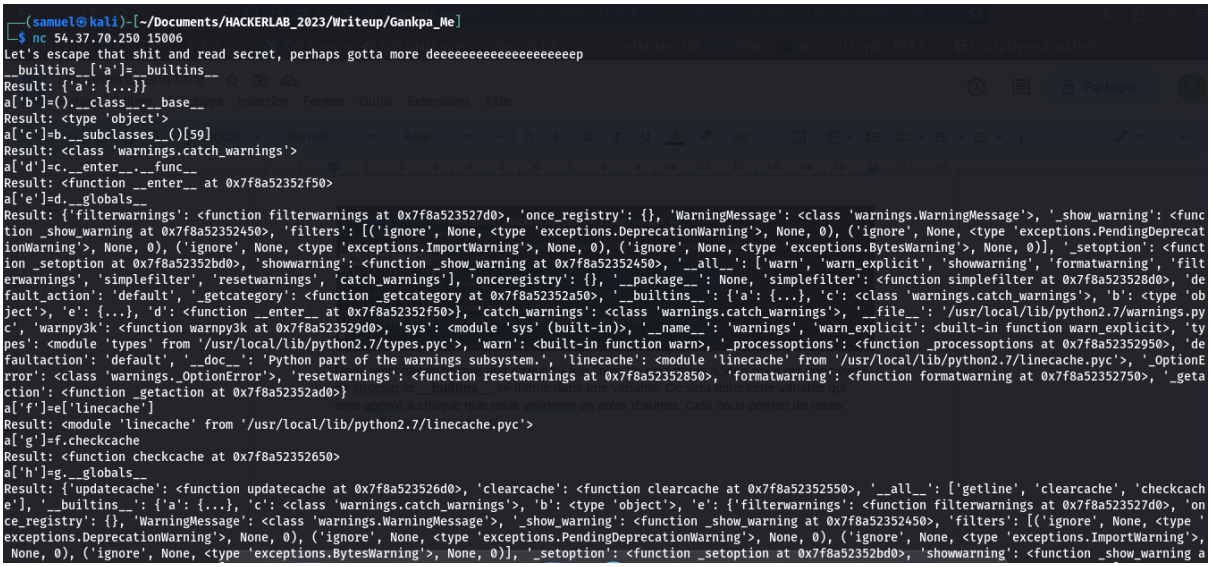
Nous décidons d'utiliser le payload suivant
().__class__.__base__.__subclasses__()[59].__enter__.__func__.__globals__['linecache'].checkcache.__globals__['os'].system('sh')

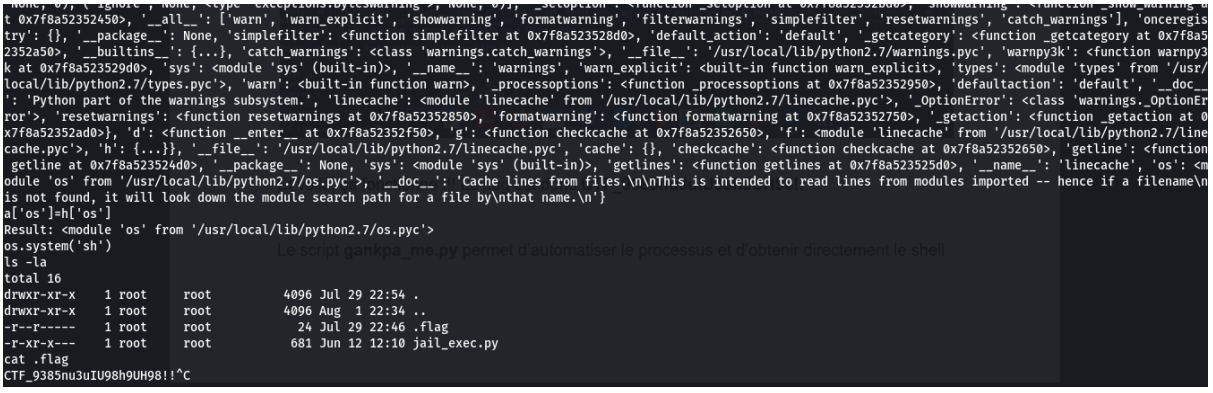


A notre grande surprise il ne fonctionne pas. Nous avons une limite de 30 caractères. Après quelques recherches, notre meilleure option serait de stocker le payload partie par partie dans des variables en tenant compte de la limite. Nous décidons donc d'utiliser **__builtins__** pour le faire



Nous rencontrons encore une erreur dû à la limite de caractères. L'idée nous est donc venu de stocker le **__builtins__** lui-même dans une variable. Ce sera donc cette variable qui sera appelée à chaque fois que nous voudrons en créer d'autres. Cela nous permet de rester dans la limite des 30 caractères.





Et voilà, ça fonctionne !!! Le flag est donc **CTF_9385nu3uIU98h9UH98!!**

Le script **gankpa_me.py** permet d'automatiser le processus et d'obtenir directement le shell.