Write Up HELP.

On a basiquement 4 fonctions.

Une fonction win() qui ouvre le fichier flag.txt et le lis puis l'affiche.

Une fonction handler() qui appelle la fonction win

Une fonction set_handler() qui met un handler sur le signal SIGSEGV (-11). En case de segfault, le handler sera appele et donc notre fonction win par consequent.

On devine qu'il faut faire segfault le programme.

On voit dans la fonction main() que la fonction set_handler est appelee. On a egalement un buffer de 0x1000 bytes (4096 bytes). Et qu'un input utilisateur est pris avec la fonction scanf. Cette fonction est vulnerable car elle ne controle pas la taille de l'input.

On peut donc declencher un segfault en faisant un buffer overflow. Pour cela il suffit d'envoyer 0x1010 bytes. car il faut remplir le buffer, reecrire sRBP puis sRIP.

Commande: python -c "print('A'*0x1010)" | nc chall 7000