

Jules Hauchecorne
HAUJ21049307

Poney

Comme les informations du poney sont conservées après la fermeture de l'exécutable et qu'il n'y a pas d'autre répertoire on peut assumer que les informations sont conservées dans le flag.txt et que poney fait une lecture/écriture de flag.txt. J'ai très rapidement tenté de voir ce qu'il y avait de visible depuis l'exécutable que ce soit avec juste ouvrir le fichier avec un éditeur texte ou en le lançant avec strace.

Cela m'a permis de déterminer en premier que le fichier source était écrit en c, et qu'il y avait des fread fopen etc d'employés pour lire flag.txt. De plus, il y avait une ligne dans le binaire qui laissait supposer que l'action Gueuler traiter d'une certaine façon était la solution pour interagir avec flag.txt.

Par la suite, j'ai essayé à plusieurs reprises d'utiliser l'option changer le nom pour modifier la valeur de Gueuler. Avec par exemple un nom suivi d'un point virgule puis tenter de modifier la valeur de Gueuler comme on le ferait en C.

J'ai de même tenté de faire des printf pour obtenir de l'information sur le code source mais sans succès. Possiblement que j'aurais pu éventuellement réussir à obtenir de quoi mais avant d'en arriver là j'ai voulu regarder le fichier mentionné dans l'exécutable , .mon_petit_poney.cfg supposé être dans HOME/

C'était finalement juste un fichier texte contenant les attributs du poney, avec les permissions d'écriture. Donc évidemment j'ai mis Gueuler à true et lancer le binaire en choisissant

l'action 3 Gueuler qui a afficher le contenu du flag.txt

FLAG

Je_pourrais_gueuler_dans_le_cul_dun_poney

CWE

- CW-732

Incorrect Permission Assignment for Critical Resource

Le fichier .mon_petit_poney.cfg aurait dû être protégé d'accès.

Correction

Retirer la permission de lecture et d'écriture aux utilisateurs non root sur le fichier .mon_petit_poney.cfg

