CS 395

G01167216

Nghi Vi

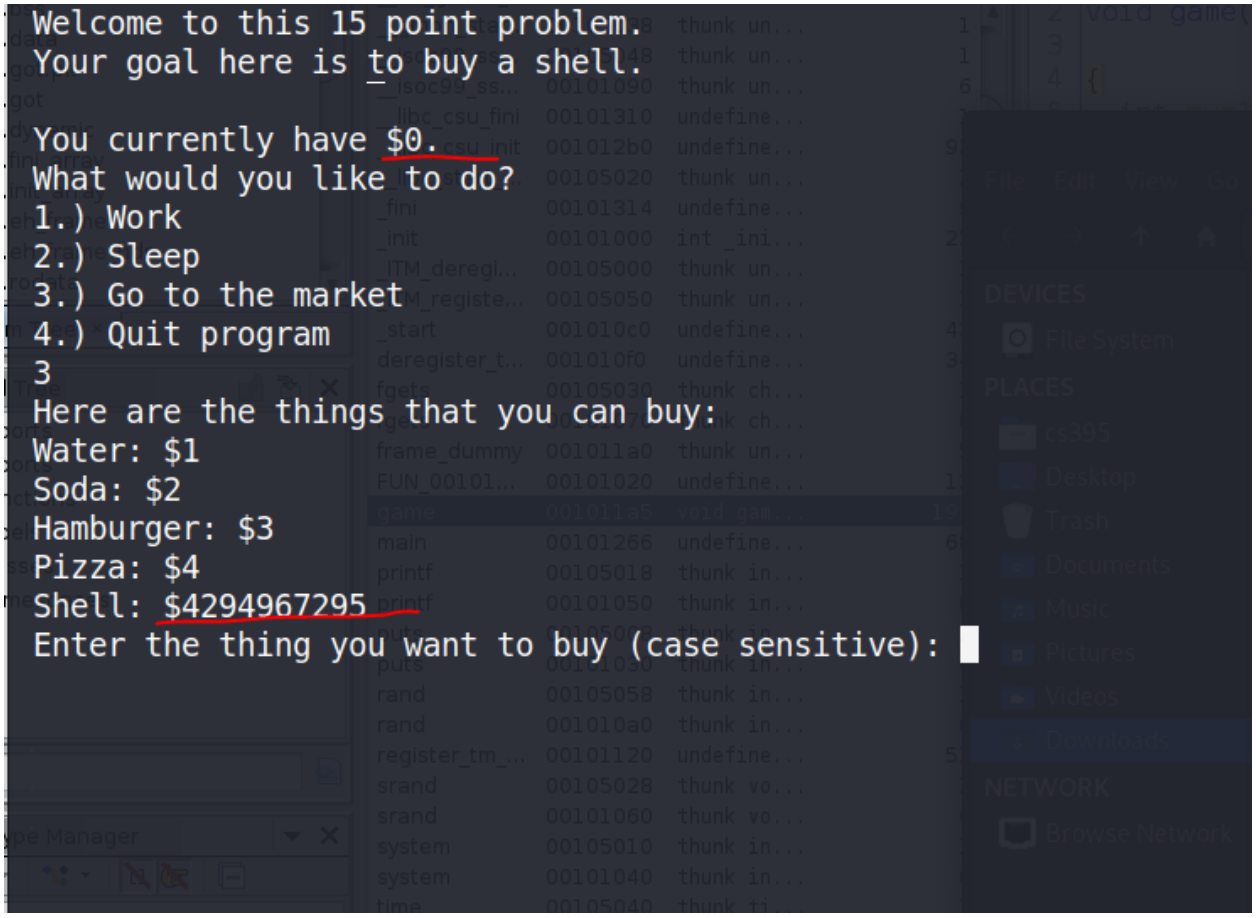
Final Project Writeup

Buy Shell

I. Reconnaissance

The goal of this binary is to get the variable money to be the maximum value of an unsigned int to buy a shell. Each time you work, you get 1 dollar, and you can accumulate all the points. Obviously, the honest and righteous way to buy a shell is to work every day until you accumulate enough wealth to get a nice shell. However, since the integer is stored as unsigned, it might be vulnerable to int overflow attack where it would wrap around to the other end of the spectrum once it gets smaller than 0. Let's test this theory

II. Crafting Exploit



After buying a water when we have 0$, the amount next is $4294967295, which is enough for a shell.

III. Result

After that we only need to go ahead and buy a shell to finish the challenge.

```
You currently have $4294967295.
What would you like to do?
1.) Work
2.) Sleep
3.) Go to the market
4.) Quit program
3
Here are the things that you can buy:
Water: $1
Soda: $2
Hamburger: $3
Pizza: $4
Shell: $4294967295
Enter the thing you want to buy (case sensitive): Shell
You bought a shell!
$ ls
buyshell  buyshell.c
$ pwd
/home/cs395/Desktop/CS395_Final_Challenges/BuyShell
$ whoami
cs395
$
```