Homework_5

To exploit the integer overflow on this program you have to find the right integer to put in the **item_quantity** input. This happens because there is a product operation between the price of the product and the quantity of the item the user wants to buy. This kind of operation can really easy lead to integer overflow. You can use a simple brute force algorithm to find the number (The following code has this goal).

```
#include <stdio.h>

int main(){

    int  a = 1500;

    int b = 0;
    int res;


    do{
        res+=a;
        b++;
    }
    while (res!= -1200);

    printf("b=%d\n", b );

    return 0;
}
```

The output of this algorithm is: **214748364**. So you can just input this number in the program, and you will obtain the solution.

Fix

To fix the problem you can limit the number of iPhone an user can buy, with the price capped with the max integer value. This program finds integer overflow and handle it with an error, preventing the user to buy iPhones with a non positive price.

```
#include <stdio.h>
#include <stdlib.h>
```

```
int main()
{
        printf("Hello, which product do you want to buy?\n");
        printf("1) IPhone 11\n");
        printf("2) IPhone 11 Pro\n");
        printf("3) IPhone 11 Pro Max Max\n");

        // Get item
        int item_choice;
        scanf("%d", &item_choice);

        printf("Great device, how many?\n");
        int item_quantity;
        scanf("%d", &item_quantity);

        if (item_quantity <= 0) {
                printf("You should buy at least one Iphone!\n
                return -1;
        }

        int insurance = 1200;
        if (item_choice == 3)
        {
                int price_no_insurance = 1500 * item_quantity

                printf("item_quantity: %d\n", item_quantity);
                printf("item_quantity: %d\n", price_no_insura

                if(item_quantity != price_no_insurance/1500){
                        printf("Integer overflow!!: %d\n", pr
                        return -1;
                }

                int price = price = price_no_insurance + insu

                if(price < 0){
                        printf("Integer overflow!!: %d\n", pr
                        return -1;
                }
                if (price == 0) {
                        printf("You solved the problem\n");
                        printf("The Iphone Max Max is yours\n
                        return 1;
                }
                printf("You have to pay €%d\n", price);
        }
        else
        {
```

```
                  if (item_quantity > 3) {
                          printf("You can buy maximum 3\n");
                          return -1;
                  }
                  int price = 1000*item_quantity;
                  printf("You have to pay €%d\n", price);
          }
          return 0;
  }
```

The **price_no_insurance** contains the product of the operation. This variable is then checked for integer overflow, using the inverse operation (You make the division and you control that you obtain a coherent solution).

The maximum number of iPhone that an user can buy is **1431654**.