

Homework-5

Francesco Penasa

October 26, 2019

1. Exploit Integer Overflow vulnerability.

In order to exploit this vulnerability to get Iphone 11 Pro Max Max for free we have to insert a value in the variable *item_quantity* that makes the following equation true.

$$(x1500 + 1200) - y(2^{32}) = 0 \quad (1)$$

Where $x = \text{item_quantity}$ and $y \in \mathbb{N} > 0$. The main obstacle to resolve this equation is to find x and y as positive integers, for this purpose we developed a simple Python3 script showed below.

```
y = 0
overflow = (2**32) # integer max value + 1 in 32 bits.
while (True):
    y = y+1
    x = (y*overflow - 1200) / 1500
    if x == int(x):
        print("Found: " + str(x))
        break
```

This script tries all possible natural number greater than zero for the value y and check if the resultant x is an integer or a float/double number, if it is an integer print the x and stop the cycle.

The result is: **214748364.0**

Inserting such result during the execution of the C code as input for the question "*Great device, how many?*" will give us the following response: *You solved the problem The Iphone Max Max is yours.*

2. Fix Integer Overflow vulnerability.

To fix this vulnerabilities we check if *item_quantity* is greater than 10^6 .

```
if (item_quantity >= 1000000){
    printf("Overflow_Risk!\n");
    return -1;
}
```

This operation will grant us that the *item_quantity* variable will not reach the value **1431655** making it impossible for the *price* variable ($\text{item_quantity} * 1500 + 1200$) to exceed the $2^{32} - 1$ value and go in overflow.

In the following page the screenshot of its implementation in the C code is showed.

```

1  #include <stdio.h>
2  #include <stdlib.h>
3
4  int main()
5  {
6      printf("Hello, which product do you want to buy?\n");
7      printf("1) iPhone 11\n");
8      printf("2) iPhone 11 Pro\n");
9      printf("3) iPhone 11 Pro Max\n");
10
11     // Get item
12     int item_choice;
13     scanf("%d", &item_choice);
14
15     printf("Great device, how many?\n");
16     unsigned int item_quantity;
17     scanf("%d", &item_quantity);
18
19
20     if (item_quantity >= 1000000){
21         printf("Overflow Risk!\n");
22         return -1;
23     }
24
25     if (item_quantity <= 0) {
26         printf("You should buy at least one Iphone!\n");
27         return -1;
28     }
29
30     int insurance = 1200;
31     if (item_choice == 3)
32     {
33         int price = 1500*item_quantity + insurance;
34         if (price == 0) {
35             printf("You solved the problem\n");
36             printf("The Iphone Max Max is yours\n");
37             return 1;
38         }
39         printf("You have to pay €%d\n", price);
40     }
41     else
42     {
43         if (item_quantity > 3) {
44             printf("You can buy maximum 3\n");
45             return -1;
46         }
47         int price = 1000*item_quantity;
48         printf("You have to pay €%d\n", price);
49     }
50     return 0;
51 }

```