Homework-5

Francesco Penasa

October 17, 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.

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

   Where $x = item\_quantity$ 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 (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.

```c
#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");
    unsigned int item_quantity;
    scanf("%d", &item_quantity);


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

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

    int insurance = 1200;
    if (item_choice == 3)
    {
        int price = 1500*item_quantity + insurance;
        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;
}
```