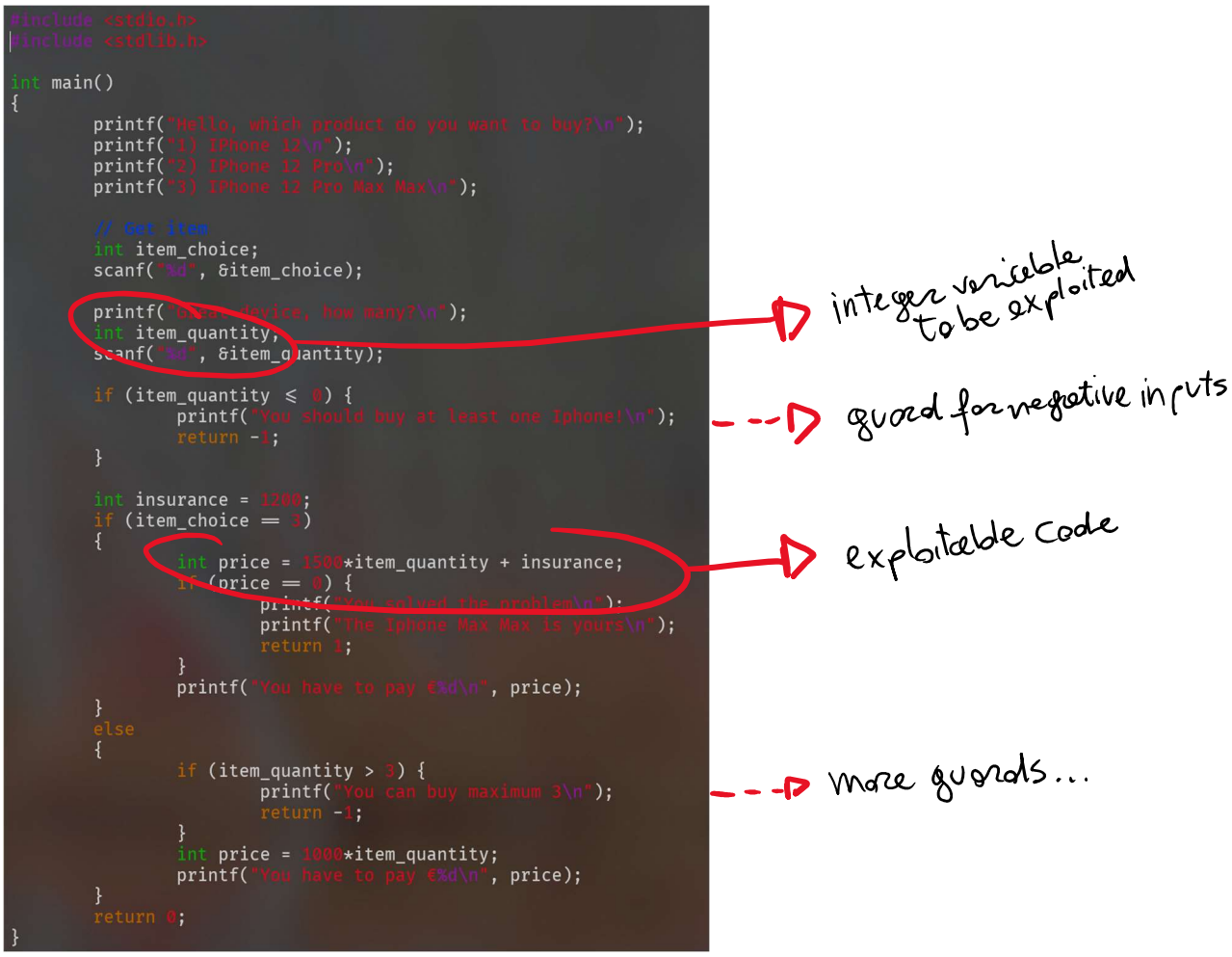
In order to exploit the exercise, we first take a look of the source code.

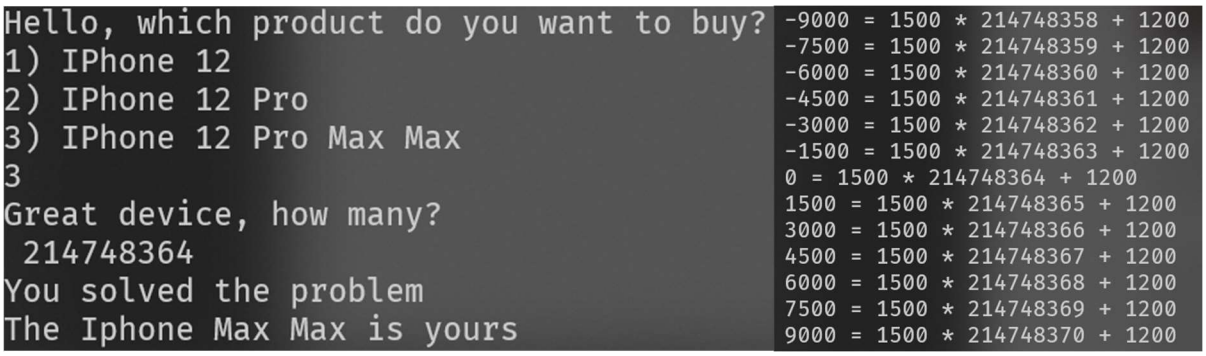


This code has an evident flaw in the `int price = 1500 * ….` line. An arbitrarily large item_quantity variable, which is also an int, can cause the price variable to overflow easily due to the multiplication with 1500.

In order to exploit the code, we can follow two paths. Both are equally easy. The first would not need even the knowledge of the source code: we can just brute force our way by repeatedly running the program and trying increasing values of item_quantity until the exploit is performed. The second way is described here.

```
int i = 0;
int tmp;
while(1) {
  tmp = 1500 * i + 1200;
  if (tmp == 0)  {
    printf("%d\n", i);
    return 12;
  }
  i++;
}
```

This short code snippet brute forces the formula used in the source code of the program, in order to find a suitable i that when substituted makes price equal to 0. Running it eventually finds an i value of 214748364.



Plugging this value in the program completes the exploit and the exercise.