bubbly

by itsecgary / UMDCSEC

Tags: ghidra rev sorting pwn

Rating: 5.0

bubbly

Category: Rev

Points: 395

Description:

> It never ends
> `nc 2020.redpwnc.tf 31039`
> **Author:** dns
> **Given:** bubbly

Writeup

The first thing I did here was run the program. Seems like we have to do some kind of sorting.

```
$ ./bubbly
I hate my data structures class! Why can't I just sort by hand?
1
2
32
Try again!
```

After playing with it for a minute or so, I decided to open it up in **Ghidra**. Looks like we have the methods **main**, **check**, and **print_flag**:

main:

```
int main(void) {
  uint32_t i;
  int unused;
  _Bool pass;

  setbuf(stdout,(char *)0x0);
  setbuf(stdin,(char *)0x0);
  setbuf(stderr,(char *)0x0);
  puts("I hate my data structures class! Why can\'t I just sort by hand?");
  pass = false;
  while( true ) {
    __isoc99_scanf(&DAT_00102058);
    if (8 < i) break;
    nums[i] = nums[i] ^ nums[i + 1];
    nums[i + 1] = nums[i + 1] ^ nums[i];
```

```
    nums[i] = nums[i] ^ nums[i + 1];
    pass = check();
  }
  if (pass == false) {
    puts("Try again!");
  }
  else {
    puts("Well done!");
    print_flag();
  }
  return 0;
}
```

check:

```
_Bool check(void) {
  uint32_t i;
  _Bool pass;

  i = 0;
  while( true ) {
    if (8 < i) {
      return true;
    }
    if (nums[i + 1] < nums[i]) break;
    i = i + 1;
  }
  return false;
}
```

print_flag:

```
void print_flag(void) {
  int unused;

  system("cat flag.txt");
  return;
}
```

Seems like the goal here is to reach this **print_flag** method, but we have to find out how. The while loop in the **main** method seems to be taking an already-defined array and swapping two of the values.

```
while( true ) {
  __isoc99_scanf(&DAT_00102058);
  if (8 < i) break;
  nums[i] = nums[i] ^ nums[i + 1];
  nums[i + 1] = nums[i + 1] ^ nums[i];
  nums[i] = nums[i] ^ nums[i + 1];
  pass = check();
}
```

The check method being called at the end of the while loop pretty much just makes sure this array is *sorted*. It looks like the only way to break out of this loop is to enter a number greater than 8. Let's take a look at our array:

```
nums
00104060 [0]    1h,   Ah,   3h,   2h
00104070 [4]    5h,   9h,   8h,   7h
00104080 [8]    4h,   6h
```

nums = [1, 10, 3, 2, 5, 9, 8, 7, 4, 6]

Now, our job here is to sort the array by calling an index of the array for the program to swap that index with the index (i) with the index after it (i+1). There are many routes to take for sorting this, but here is mine (the bold values are the *swapped* values):

0 1 2 3 4 5 6 7 8 9 --- index values

[1, 10, 3, 2, 5, 9, 8, 7, 4, 6] --- original

[1, **3**, **10**, 2, 5, 9, 8, 7, 4, 6] --- (enter "1")

[1, 3, **2**, **10**, 5, 9, 8, 7, 4, 6] --- (enter "2")

[1, 3, 2, **5**, **10**, 9, 8, 7, 4, 6] --- (enter "3")

[1, 3, 2, 5, **9**, **10**, 8, 7, 4, 6] --- (enter "4")

[1, 3, 2, 5, 9, **8**, **10**, 7, 4, 6] --- (enter "5")

[1, 3, 2, 5, 9, 8, **7**, **10**, 4, 6] --- (enter "6")

[1, 3, 2, 5, 9, 8, 7, **4**, **10**, 6] --- (enter "7")

[1, 3, 2, 5, 9, 8, 7, 4, **6**, **10**] --- (enter "8")

[1, **2**, **3**, 5, 9, 8, 7, 4, 6, 10] --- (enter "1")

[1, 2, 3, 5, 9, 8, **4**, **7**, 6, 10] --- (enter "6")

[1, 2, 3, 5, 9, **4**, **8**, 7, 6, 10] --- (enter "5")

[1, 2, 3, 5, **4**, **9**, 8, 7, 6, 10] --- (enter "4")

[1, 2, 3, **4**, **5**, 9, 8, 7, 6, 10] --- (enter "3")

[1, 2, 3, 4, 5, 9, 8, **6**, **7**, 10] --- (enter "7")

[1, 2, 3, 4, 5, 9, **6**, **8**, 7, 10] --- (enter "6")

[1, 2, 3, 4, 5, **6**, **9**, 8, 7, 10] --- (enter "5")

[1, 2, 3, 4, 5, 6, 9, **7**, **8**, 10] --- (enter "7")

[1, 2, 3, 4, 5, 6, **7**, **9**, 8, 10] --- (enter "6")

[1, 2, 3, 4, 5, 6, 7, **8**, **9**, 10] --- (enter "6")

nums = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]

And now it's sorted! Let's get the flag:

```
$ nc 2020.redpwnc.tf 31039
I hate my data structures class! Why can't I just sort by hand?
1
2
3
4
5
6
7
8
1
6
5
4
3
7
6
5
7
6
7
999999
```

```
Well done!
flag{4ft3r_y0u_put_u54c0_0n_y0ur_c011ege_4pp5_y0u_5t1ll_h4ve_t0_d0_th15_57uff}
```

Flag

flag{4ft3r_y0u_put_u54c0_0n_y0ur_c011ege_4pp5_y0u_5t1ll_h4ve_t0_d0_th15_57uff}

Resources

Ghidra

Original writeup (https://github.com/itsecgary/CTFs/tree/master/redpwnCTF%202020/bubbly).

Comments