What is heap?

Computer programs store data in stacks and in the heap. The stack is usually used for data whose size is known. On the other hand, the heap is used for data whose size is unknown at compilation time.

In the C, the stack is used for variables, and the heap is the result of a dynamic allocation done with malloc.

Within the same thread, programmers must ensure that their functions cannot write down or read out data outside the desired area. If the input can be used in such a way, that sections of the heap not intended for said input are overwritten or read out, we are in a heap exploitation scenario.

From source analyze, we can see that overflowing buffer is the only way to capture flag, which is write 33 byte of string without space, and the flag is ours.

Generated by Notion to PDF