

I debugged the program with GDB, and found a segment fault occurred in XRef::getNumEntry.



The fault occurred when the program executed the instruction on the .text 0x0011872e. Because, at that time, the value stored by the register “ebp” is 0 at that time, and the address “0x14” is obviously invalid.

I got the source code segment corresponding to the disassemble instructions.



I think the register ecx on the .text 0x0011872 stored the variable “size” which is a private member of Class XRef defined in XRef.h.

Maybe at that time, the instance of the class XRef has been destructed. As a result, when the program executed the instruction on the .text 0x00118717, the register ebp will be overwritten by 0.