**一 造成segment fault，产生core dump的可能原因**

1.内存访问越界

 a) 由于使用错误的下标，导致数组访问越界

 b) 搜索字符串时，依靠字符串结束符来判断字符串是否结束，但是字符串没有正常的使用结束符

 c) 使用strcpy, strcat, sprintf, strcmp, strcasecmp等字符串操作函数，将目标字符串读/写爆。应该使用strncpy, strlcpy, strncat, strlcat, snprintf, strncmp, strncasecmp等函数防止读写越界。

2 多线程程序使用了线程不安全的函数。

3 多线程读写的数据未加锁保护。对于会被多个线程同时访问的全局数据，应该注意加锁保护，否则很容易造成core dump

4 非法指针

a) 使用空指针

b) 随意使用指针转换。一个指向一段内存的指针，除非确定这段内存原先就分配为某种结构或类型，或者这种结构或类型的数组，否则不要将它转换为这种结构或类型的指针，而应该将这段内存拷贝到一个这种结构或类型中，再访问这个结构或类型。这是因为如果这段内存的开始地址不是按照这种结构或类型对齐的，那么访问它时就很容易因为bus error而core dump.

5 堆栈溢出.不要使用大的局部变量（因为局部变量都分配在栈上），这样容易造成堆栈溢出，破坏系统的栈和堆结构，导致出现莫名其妙的错误。