c_c 语言实现堆栈修改,通过ret跳转到自定义函数 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/285/2021_2022_c_c___E8_AF_AD_E8_A8_c97_285147.htm 好处是,编译后没有jmp指令,通过ret 跳转到需要的代码,另外在调试时,某些代码会被当作数据,可以增加调试难度. 缺点,需要调用函数的堆栈有至少4个字节的空间,否则堆栈返回出错. 但是这四个字节空间不会被摧毁. 可能我有些东西还没有照顾到,如果有错误,大家告诉我.) 编译环境: vc6 vc7 #include int somefunc(void *ptr) ...{ printf("in somefunc... "). return 0. } void stackbuild(void *ptr) ...{ printf("in stackbuild... "). *(unsigned int*)(amp.ptr. *(unsigned int*)amp.ptr-1). //注意此处对堆栈操作 *(unsigned int*)(amp.ptr. } int main(int argc, char *argv[]) ...{ // 还是嵌入了一句汇编，平衡堆栈.)哪位高人改改，看能不能把嵌入汇编去掉 __asm...{push 0} //预留4字节空间,平衡堆栈，注意此句和下面的句子要一起用，没有下面的调用，必须没有该语句 stackbuild(somefunc). printf("exit main... "). return 0. } 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com