在看雪上看到backer出的一道测试c语言的题.

iteye_10465 于 2008-05-05 16:55:00 发布 27 收藏
文章标签： c/c++
测试你的C语言功底

在实际的教学中，我们发现很少有真正精通了C语言编程的学员，一般都有或多或少概念不是完全清楚的问题，特别是一些需要丰富的实战经验才能体会和明白的问题，如字符串，指针，类型转换，定义指向函数的指针类型，这也是导致学习VC++困难的一个原因。下面有几个简单测试将能发现你对C语言的掌握情况。

1、如何在下面的test函数里加入代码可以使程序运行起来输入和输出的相等？
(环境是vc6Debug方式下)

```
#include<stdio.h>
voidtest()
{
intt;
scanf("%d",&t);
在这里加入代码
}
voidmain()
{
intm;
test();
printf("m=%d",m);
}
```

不知道应该如何写这段代码,最后用嵌套汇编的方式编写代码.

```
#include<stdio.h>
void test()
{
int t;
scanf("%d",&t);
//在这里加入代码
_asm
{
mov esi,t
pop edi
mov [edi-4],esi
push edi
}
}
void main()
{
int m;
test();
printf("m=%d",m);
}
```

不知道方法是否正确,有高手知道的话,请指教.

还是看看backer给出的答案吧!

这一题需要去了解在函数体中栈内存的分配情况。

```
#include<stdio.h>
void  test()
{
//当程序流程进入test函数入口的时候也会对变量作一些寄存器的保护和预留空间
//push     ebp
//mov      ebp,esp
//sub      esp,48h
//push     ebx
//push     esi
//push     edi
//lea      edi,[ebp-48h]
//mov      ecx,12h
//mov      eax,0CCCCCCCCh
//rep  stos     dword  ptr  [edi]
//      预留了0x12*sizeof(DWORD)个字节空间
//      变量t的地址为ebp-4
    int  t;
    scanf("%d",&t);//?请在以下添加代码,使用main函数中的变量m输出值等test函数中的变量t;
//计算变量t在内存中的位置和上一层函数中变量m在内存中位置的差
//先写到这一句用反汇编看一下
//变量t和m都在预留空间的最下端(堆栈是向上长的，变量是按定义先后也是从下向上放的)
//push     edi(main).....0x1
//push     esi(main).....0x2
//push     ebx(main).....0x3
//push     ebp(自己).....0x4
//返回地址.....0x5
//0x10*sizeof(DWORD)的空间.....0x15
//空间最下面的DWORD字节存放变量m.....0x16
//我们把t向下偏移0x16的位置(存放着变量m)上把t的内容写进去即可。
//也可以看一下OD里图：
```

```
    *( &t + 0x16) = t;
//这样整型指针pos就指到了变量m我们把t的值直接赋给*p(就是m)即可。
}
int main()
{
//当程序进入main函数的时候，会对一些局部变量作一些预留空间
//    push    ebp
//    mov     ebp,esp
//    sub     esp,44h
//    push    ebx
//    push    esi
//    push    edi
//    lea     edi,[ebp-44h]
//    mov     ecx,11h
//    mov     eax,0CCCCCCCCh
//    rep stos    dword ptr [edi]
//    预留了0x11*sizeof(DWORD)个字节空间
//    m的变量地址是ebp-4
    int m;
    test();
    printf("m=%d",m);
    return 0;
}
```