PrintfAttack

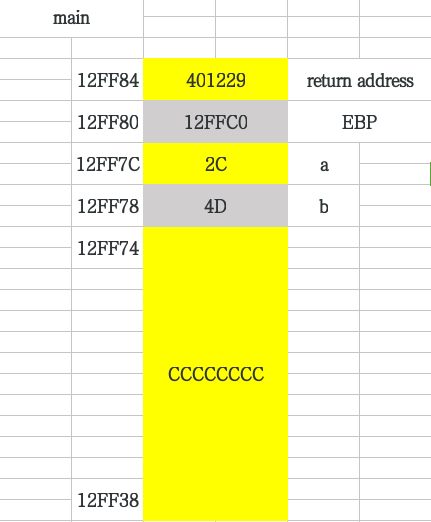
1. printf的缺陷

int a=44,b=77;

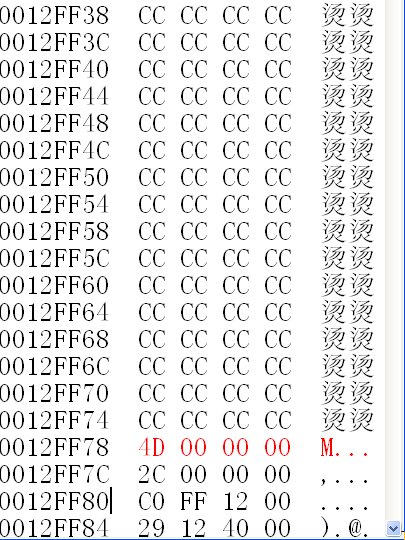
\_\_asm int 3

printf("a=%d,b=%d\n",a,b);

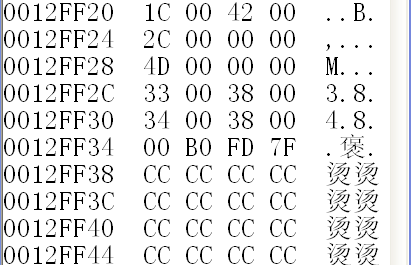
printf("a=%d,b=%d\n");

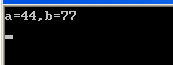


初始化后

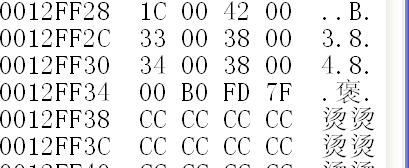


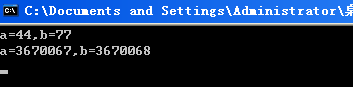
printf("a=%d,b=%d\n",a,b);





printf("a=%d,b=%d\n");





0x380033=3670067

0x380034=3670068

1. 用printf向内存中写数据

int len=0;

\_\_asm int 3

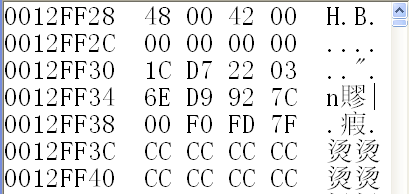
printf("before write:length=%d\n",len);

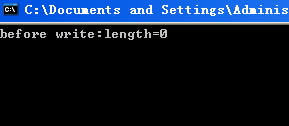
printf("failwest:%d%n",len,&len);

printf("after write:length=%d\n",len);

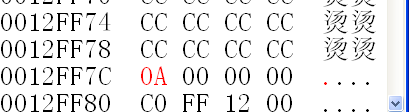
return 0;

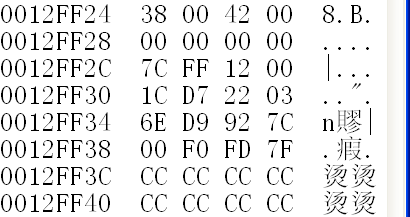
printf("before write:length=%d\n",len);

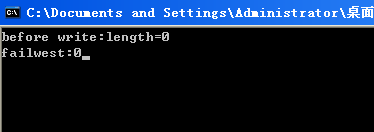




printf("failwest:%d%n",len,&len);







printf("after write:length=%d\n",len);

