贪吃蛇
反汇编代码分析报告

THINCT

2023 年 12 月 9 日

SnakeGame::update

EBX 代替当前的函数栈底

```
.text:004079C0   push    ebx
.text:004079C1   mov     ebx, esp
.text:004079C3   sub     esp, 8
.text:004079C6   and     esp, -8
.text:004079C9   add     esp, 4
.text:004079CC   push    ebp
.text:004079CD   mov     ebp, [ebx+4]
.text:004079D0   mov     [esp+4], ebp
.text:004079D4   mov     ebp, esp
```

1. 当eip在.text:004079C0处，esp所指向的是ret addr.
2. 当eip在.text:004079C1处，ebx 所指向的是esp-4.此时:
   - ebx+4指向的是ret addr
   - ebx+8 指向的是第一个参数

EBX 代替当前的函数栈底

```
.text:004079C3   sub      esp, 8
.text:004079C6   and      esp, 0FFFFFFF8h
.text:004079C9   add      esp, 4
.text:004079CC   push     ebp
```

esp实现了向下最近的8的倍数取证。比如12取整就是8，16取整就是16，18取整就是16.因为是针对栈结构地址取整，所以越是往小的方向越安全，因为对于栈结构来讲，越小的地址是没有用过的地址。所以后面的ebp,esp, ebp只能作为局部变量的索引，而对于参数的索引，用ebx比较合适。

总结:

对于这个函数来讲，并不是按照套路*ebp*作为局部变量和函数参数的唯一参考. *Italic*测试