ESERCITAZIONE W23D1(2)

Traccia:

Dato il seguente codice assembly, provare a ricostruire le istruzioni originali in C

```
push   %ebp
mov    %esp,%ebp
sub    $0x8,%esp
call   80483e9 <bar>
leave
ret


push   %ebp
mov    %esp,%ebp
sub    $0x8,%esp
call   80483fb <baz>
call   8048400 <quux>
leave
ret
```

Traccia:

```
push   %ebp
mov    %esp,%ebp
pop    %ebp
ret


push   %ebp
mov    %esp,%ebp
mov    $0x0,%eax
movl   $0x1,(%eax)
pop    %ebp
ret


push   %ebp
mov    %esp,%ebp
and    $0xfffffff0,%esp
call   80483dc <foo>
mov    $0x0,%eax
leave
ret
```

Nota:

leave è equivalente a:

mov %ebp, %esp
pop %ebp

SOLUZIONE:

main.c

```c
#include <stdio.h>

void foo();
void bar();
void baz();
void quux();

void foo() {
    bar();
}

void bar() {
    baz();
    quux();
}

void baz() {
    // do nothing
}

void quux() {
    *(int*)(0) = 1; // Provoca un errore di segmentazione
}

int main() {
    foo();
    return 0;
}

```