代码

```c
#include <signal.h>
#include <setjmp.h>
#include <stdio.h>
#include <unistd.h>
#include <string.h>

sigjmp_buf buf;

void handler_segv(int sig){
    siglongjmp(buf, 1);
}
/* 有时会出现bus error,和segv同样处理 */
void handler_bus(int sig){
    siglongjmp(buf, 1);
}

int main(){
    printf("main enter\n");
    if(signal(SIGSEGV, handler_segv) == SIG_ERR){
        printf("signal error\n");
    }
    if(signal(SIGBUS, handler_bus) == SIG_ERR){
        printf("signal error\n");
    }
    unsigned long tmp = 0;
    /* 代码段开始 */

    unsigned long i = 0x400000 - 0x1000;
    long cnt = 0x400 - 1;
    /* 虚拟地址有48位,页号有36位 */
    while(cnt != ((long)1 << 36) - 1){
        /* 不能访问的话回到这里遍历下一页 */
        sigsetjmp(buf, 1);
        i += 1 << 12;
        cnt += 1;
        tmp = *(unsigned long* )i;
        /* 下面一句可能不会被执行 */
        printf("pagenum: %lx\n", i);
    }
    return 0;
}

```

不处理 SIG_BUS 的话有时候不能访问栈的高位地址

(Ubuntu 16.04 64 位, 48 位虚拟地址)

输出结果是能访问的虚拟页的首地址,省略掉后三个 0 是能访问的虚拟页号
(省略了栈的一部分)

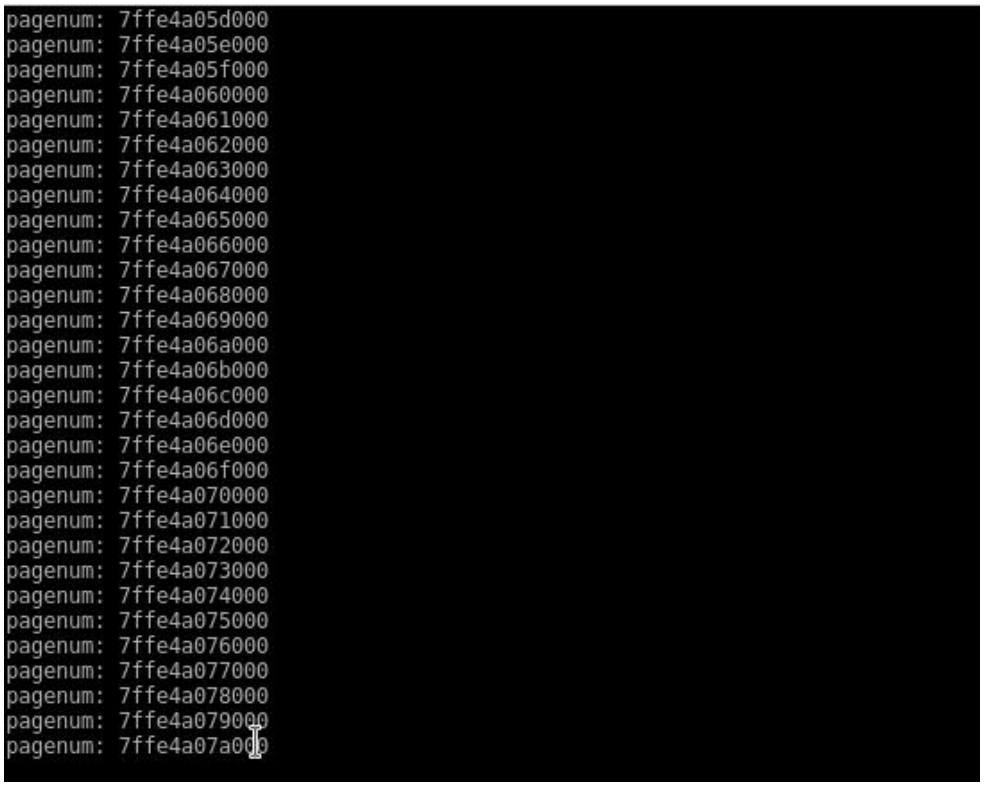
```
dand@iZ2ze936cp0odzkhse20okZ:~/Desktop$ gcc test_.c
dand@iZ2ze936cp0odzkhse20okZ:~/Desktop$ ./a.out
main enter
pagenum: 400000
pagenum: 600000
pagenum: 601000
pagenum: 1efb000
pagenum: 1efc000
pagenum: 1efd000
pagenum: 1efe000
pagenum: 1eff000
pagenum: 1f00000
pagenum: 1f01000
pagenum: 1f02000
pagenum: 1f03000
pagenum: 1f04000
pagenum: 1f05000
pagenum: 1f06000
pagenum: 1f07000
pagenum: 1f08000
pagenum: 1f09000
pagenum: 1f0a000
pagenum: 1f0b000
pagenum: 1f0c000
pagenum: 1f0d000
pagenum: 1f0e000
pagenum: 1f0f000
pagenum: 1f10000
pagenum: 1f11000
```

```
pagenum: 1f16000
pagenum: 1f17000
pagenum: 1f18000
pagenum: 1f19000
pagenum: 1f1a000
pagenum: 1f1b000
pagenum: 7f0785852000
pagenum: 7f0785853000
pagenum: 7f0785854000
pagenum: 7f0785855000
pagenum: 7f0785856000
pagenum: 7f0785857000
pagenum: 7f0785858000
pagenum: 7f0785859000
pagenum: 7f078585a000
pagenum: 7f078585b000
pagenum: 7f078585c000
pagenum: 7f078585d000
pagenum: 7f078585e000
pagenum: 7f078585f000
pagenum: 7f0785860000
pagenum: 7f0785861000
pagenum: 7f0785862000
pagenum: 7f0785863000
pagenum: 7f0785864000
pagenum: 7f0785865000
pagenum: 7f0785866000
pagenum: 7f0785867000
pagenum: 7f0785868000
pagenum: 7f0785869000
```

...


pagenum: 7ffe08fe8000
pagenum: 7ffe08fe9000
pagenum: 7ffe08fea000
pagenum: 7ffe08feb000
pagenum: 7ffe08fec000
pagenum: 7ffe08fed000
pagenum: 7ffe08fee000
pagenum: 7ffe08fef000
pagenum: 7ffe08ff0000
pagenum: 7ffe08ff1000
pagenum: 7ffe08ff2000
pagenum: 7ffe08ff3000
pagenum: 7ffe08ff4000
pagenum: 7ffe08ff5000
pagenum: 7ffe08ff6000
pagenum: 7ffe08ff7000
pagenum: 7ffe08ff8000
pagenum: 7ffe08ff9000
pagenum: 7ffe08ffa000
pagenum: 7ffe08ffb000
pagenum: 7ffe08ffc000
pagenum: 7ffe08ffd000
pagenum: 7ffe08ffe000
pagenum: 7ffe08fff000
pagenum: 7ffe09000000
pagenum: 7ffe09001000
pagenum: 7ffe09002000
pagenum: 7ffe0909f000

...


pagenum: 7ffe4a05d000
pagenum: 7ffe4a05e000
pagenum: 7ffe4a05f000
pagenum: 7ffe4a060000
pagenum: 7ffe4a061000
pagenum: 7ffe4a062000
pagenum: 7ffe4a063000
pagenum: 7ffe4a064000
pagenum: 7ffe4a065000
pagenum: 7ffe4a066000
pagenum: 7ffe4a067000
pagenum: 7ffe4a068000
pagenum: 7ffe4a069000
pagenum: 7ffe4a06a000
pagenum: 7ffe4a06b000
pagenum: 7ffe4a06c000
pagenum: 7ffe4a06d000
pagenum: 7ffe4a06e000
pagenum: 7ffe4a06f000
pagenum: 7ffe4a070000
pagenum: 7ffe4a071000
pagenum: 7ffe4a072000
pagenum: 7ffe4a073000
pagenum: 7ffe4a074000
pagenum: 7ffe4a075000
pagenum: 7ffe4a076000
pagenum: 7ffe4a077000
pagenum: 7ffe4a078000
pagenum: 7ffe4a079000
pagenum: 7ffe4a07a000

...