

# Question Set 0x06

HQS Challenge

January 20, 2016

***The following questions are in 64-bit architecture.***

*To answer the following questions download this binary: `chal0x01` or `https://goo.gl/ItW840`*

1. What command would you use to display the disassembly of this program (with Intel syntax)?
2. What is the address of the main function?
3. List a few of the high-level C library functions that this program calls?

*For the following questions download this binary: `chal0x02` or `https://goo.gl/PW5Nnc`*

1. What instruction is located at address 0x400664
2. Under which function is this instruction found?
3. Forward thinking: What might this instruction do, by itself?
4. Forward thinking: Which address range appears to do *something* of interest to a hacker/malicious user and why?

## Solutions

1. `objdump -d -Mintel chal0x01`
2. `000000000040069d`
3. `scanf()` or `_isoc99_scanf()`, `printf()`, `puts()`, `strcmp()`
1. `xor ebx,ebx`
2. `__libc_csu_init`
3. Zeroes out the register `ebx`
4. `0x4005bb - 0x40060f`