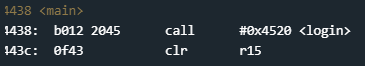
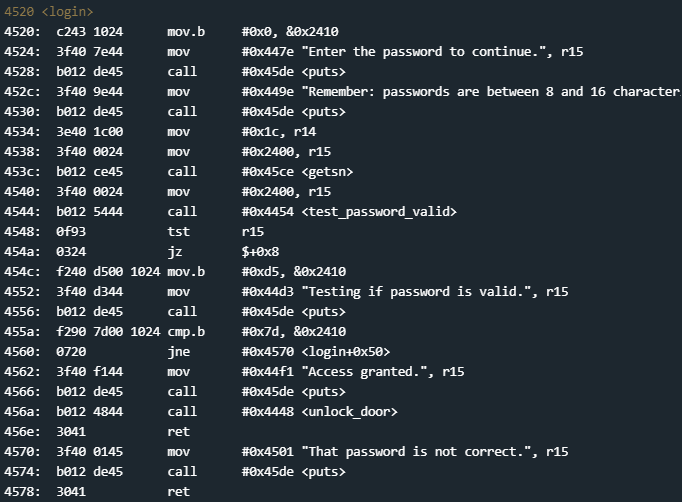
If we look at <main> we can see that it is pretty bare:



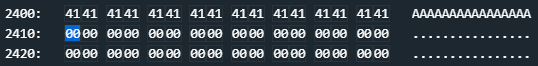
Let’s look at <login>:



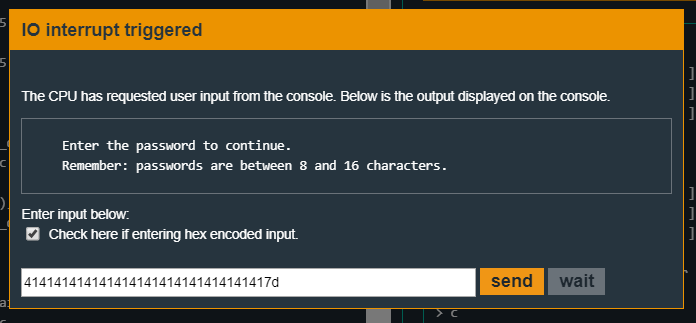
If we think back over the last few challenges, looking for any cmp operations is usually a good place to start. We can see a cmp.b at 455a:

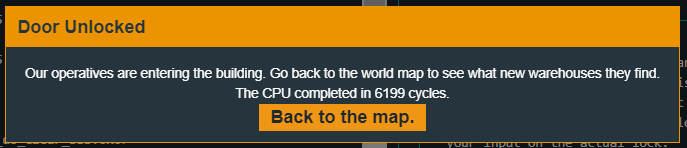


My best guess is that we are comparing the byte located at memory address 2410 to the hex value 7d. Let’s see where the program is placing user input in memory. We can see from one of the output strings that the password is usupposed to be between 8 and 16 characters. As usual, we will use 16 ‘A’s as our character for input:



The highlighted section is the memory location that gets compared before the door unlock is called or jumped over. It doesn’t seem like there is any overflow protection so we should be aple to pass 7d as the 17th hex value, overflowing it into location 2410. This should hopefully unlock the door:





Another challenge solved!