Daniel Quiroga

QUIZ3

1

Since the comparison is between an unsigned and signed variable. The b is converted into a signed integer variable and since the representation of the negative in binary has the leftmost binary bit equal to 1 when converted to sign, the b will be much bigger than any other positive number and hence the comparison would yield a false since b would be much larger than a when unsigned.

2

a

the allocated memory for kbuf is max 800 so anything higher would cause an overflow

b

if we choose values of len and n that equal exactly 800, we would be able to get an extra index of memory since kbuf has indices up to 799 and would expect a terminated string as the final character but instead would be able to have a character hence causing a vulnerability when using the memcpy function.

c

if we make the if statement a greater than or equal to comparison than we would avoid the overflow from happening another way would be to avoid manual memory allocation and use say malloc instead

3

a. No, the way that printf may cause some issues depending on what is passed in by the user
b. I see a buffer overrun vulnerability with how the lack of formatting used in printf
c. S/he will be able to see some contents of the stack and will be able to overwrite or write into memory which can lead to various of security and functionality issues.
d. You would avoid this by using the modifier of "%s" to assure that it will print out what we expect and avoid this vulnerability.
e. "\xde\xoc\xad\xde%x%x%x%x%s" would allow us to read the memory at address 0xdeadcode