Vulnerable Function A displays the integer overflow vulnerability. This program intends on displaying whatever letter corresponds to the number provided. If you give it a 2 it spits out a B, a 3 is C, and so on. The program relies on the char data type, if passing an extended ascii character with the value above 128 you can pass negative numbers to the function. Since the function uses user input for printing from an array you can then print data from anywhere in the loaded memory, including our secret ????? array.

Sample input: 0  Œ

Vulnerable Function B displays a command injection vulnerability. While it intends to simply echo back the string passed to it, more can be done due to lack of input sanitization. If a && symbol is passed the system will read this as a second command allowing the user to execute any system commands they wish. This could potentially give them complete control over a system.

Sample input: 1 Hello World! && ping 1.1.1.1

Vulnerable Function C display a heap overflow vulnerability. The program allows you to copy your words to the heap but provide your own string length. If you give a string longer than the length you provide you can overflow the heap. This allows you to write to our second secret heap allocation xWxover or even crash the program entirely, undefined behavior.

Sample input: 2 20 askjdnaksjndakjsndkjasndkjansdjknaskjdnkjasndkjanskjdnajksndjkansdjkansjkdnakjsndkjasndkjasndkjansdkjnakjsdnkajsndkjansdkjansjkdnakjsndkjasndkjasndkjansdjknaksjdnaknsdjknakj