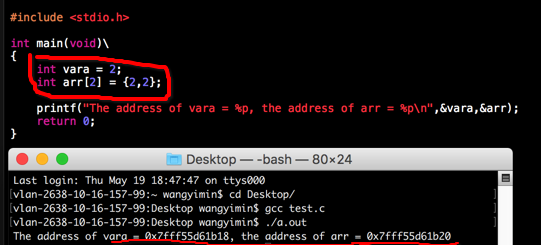
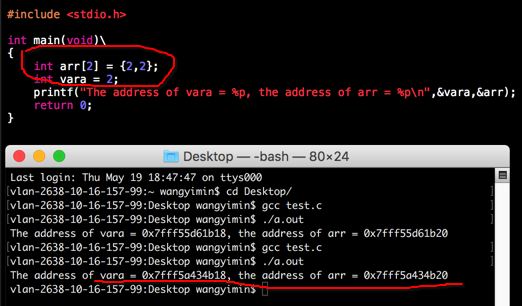
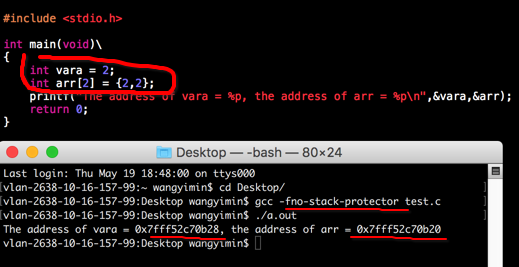
1.3.1. If we do not provide ‘-fno-stack-protector’ to GCC, the GCC would re-layout the sequence of local variables to avoid the changes resulting of buffer overflow. The picture 1 and 2 show that the memory address of ‘arr[]’ is always higher than the memory address of ‘vara’, because in default without ‘-fno-stack-protector’, the GCC will re-layout the array to memory address. However, in Picture 3, when we provide the ‘-fno-stack-protector’, and define ‘arr[]’ after ‘vara’, the memory address of ‘vara’ is always higher than the memory address of ‘arr[]’. In this situation, the overflow of array will change the value of integer. Therefore, it is necessary for us to provide the flag –fno-stack-protector.



Picture1 Picture 2

 Picture 3

Canary refers to a method that is used to detect a buffer overflow before the running of malicious code. The principle is that, it puts a small integer, which is randomly generated at the begging of the program, before the array or stack pointer. When buffer overflow happens, it will overwrite the memory from low addresses to high addresses, so the overwriting of the point will cover the small integer. Therefore, the value of the small integer can be used to detect the buffer overflow.

1.3.2. No, it would not still be exploitable, because Java has a machine to automatically check the bounds of a buffer to avoid the buffer overflow.

1.3.3.Imagine you were exploiting a program that was running with escalated privileges (i.e. could read sensitive files, modify other users settings and so on) is it possible to obtain a BASH shell using buffer overflows? Be sure to explain what shellcode is and how the shellcode is executed.

2.1After entering any username, we entry the password as following: “string + ‘or’ + identical [equation](link:equation)”. In this situation, the conditional branch of SQL is changed to: ((username = ‘any username’) && (password= ‘any password’)) || identical equation. The identical equation is always right, so the conditional branch is always right. Therefore, we can log in as any user.

2.2 Yes, we can work out the password of Bobby by entering the status query like this: ‘UNION SELECT password FROM User where username =’Bobby. In this way, the query will return the password of Bobby. The ‘UNION’ is used to combine the results of more than 2 SELECT queries. The different SELECT queries’ results of UNION must have the same number of columns and the types of the columns must be similar. In this program, the types of ‘status’ and ‘password’ are TEXT, so the query is changed to: SELECT status FROM Users WHERE username = ‘‘UNION SELECT password FROM User where username=’Bobby’. The result of SELECT status is null and the result of SELECT password is the password of Bobby. Therefore, we work out the password of Bobby.

2.3 Firstly, program need to use a variable to save the string entered by users. Then program detect the variable to filtrate the special characters, such as quotation (‘), semicolon (;) and annotation symbol (--). Finally, program uses operates the query language without the special characters. It is not a difficult security problem to fix. The reason of the problem is that SQL operates a whole query language, so if we do not deal with the special characters, we cannot avoid it.