

Code 02: Đoạn code sau gặp những lỗi nào? *

```
File: code02.c
1 // gcc -o code02 -zexecstack -no-pie -znorelro -fno-stack-protector code02.c
2 #include <stdio.h>
3 #include <unistd.h>
4 #include <string.h>
5 #include <stdlib.h>
6
7 int main() {
8     char *str = malloc(100);
9     scanf("%s", str);
10    puts("You gave me this?");
11    printf(str);
12    free(str);
13    return 0;
14 }
```

- ☐ Command Injection
- ☐ Buffer Overflow
- ☐ Integer Overflow/Underflow
- ☒ Format String Error
- ☐ Use-After-Free

```
File: code04.c
1 // gcc -o code04 -zexecstack -no-pie -znorelro -fno-stack-protector code04.c
2 #include <stdio.h>
3 #include <stdlib.h>
4 #include <unistd.h>
5 #include <string.h>
6
7 void win() {
8     puts("Bruh!");
9 }
10
11 int main() {
12     char s[100];
13     read(0, s, 100);
14     return 0;
15 }
```

- ☐ Có
- ☒ Không
- ☐ Không biết được

Code 03: Đoạn code sau gặp những lỗi nào? *

0/5

```
File: code03.c
1 // gcc -o code03 -zexecstack -no-pie -znoelro -fno-stack-protector code03.c
2 #include <stdio.h>
3 #include <stdlib.h>
4 #include <unistd.h>
5 #include <string.h>
6
7 int main() {
8     char *m = (char *) malloc(200);
9     fgets(m, 200, stdin);
10    printf("You gave: %s", m);
11    free(m);
12    free(m);
13 }
```

- ☐ Command Injection
- ☒ Buffer Overflow
- ☐ Integer Overflow/Underflow
- ☐ Format String Error
- ☒ Use-After-Free

Code 01: Đoạn code sau gặp những lỗi nào? *

0/5

```
File: code01.c
1 // gcc -o code01 -zexecstack -no-pie -znoelro -fno-stack-protector code01.c
2 #include <stdio.h>
3 #include <unistd.h>
4 #include <string.h>
5 #include <stdlib.h>
6
7 int execute(char *cmd) {
8     char *cpy_cmd = malloc(strlen(cmd));
9     char real_cmd[] = "ping -c 4 ";
10    strcpy(cpy_cmd, real_cmd);
11    strcpy(cpy_cmd + strlen(real_cmd), cmd);
12    printf("Executing %s...", cpy_cmd);
13    return system(cpy_cmd);
14 }
15
16
17 int main() {
18     char cmd[100];
19     fgets(cmd, 100, stdin);
20     execute(cmd);
21     return 0;
22 }
```

- ☒ Command Injection
- ☐ Buffer Overflow
- ☐ Integer Overflow/Underflow
- ☐ Format String Error
- ☐ Use-After-Free

Công cụ đã được giới thiệu, dùng để tương tác với các chương trình khác bằng python là gì? *

1/1

- ☐ gcc
- ☐ gdb
- ☒ pwntools
- ☐ format string