Bài tập 1 – buffer1

```c
#include <stdio.h>
#include <stdlib.h>
void get_shell(){
    printf("Yay! You've called get_shell function\n");
    system("/bin/sh");
    exit(0);
}
void buf_overflow(){
    int a = 0;
    char buf[25];
    gets(buf);
    puts(buf);
    if (a == 0xdeadbeef){
       printf("Return to my caller...\n");
       return;
    }
    else exit(0);
}
int main(){
    buf_overflow();
}
```

Yêu cầu: khai thác hàm **buf_overflow()** để gọi được hàm **get_shell()** và truyền lệnh

Bài tập 1 – buffer2

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>
void shell() {
    printf("Yay! You've called shell\n");
    system("/bin/bash");
    exit(0);
}
void sup() {
    printf("Hey dude ! Waaaaazzaaaaaaaa ?!\n");
    exit(0);
}
void main()
{
    int var;
    void (*func)()=sup;
    char buf[128];
    fgets(buf,133,stdin);
    func();
}
```

Yêu cầu: khai thác hàm **main()** để gọi được hàm **shell()** và truyền lệnh.