Eat the pie

Overview

Type	Contents
Difficulty	Medium
Tags	#Binary #pwn
Author	matta

Description

> I love pecan pie. How about you?
>
> nc eat-the-pie.sstf.site 1337

Solving strategy

When the input buffer is full, the value of the **funcs** array is exposed, where the address of the function can be found, so the binary base can be known.

The return address cannot be altered because there is no BOF, but if you put the address value in the appropriate position of buf and give the index as a negative number, you can jump to an arbitrary address.

There is a system function in plt, so you can jump here. To do that, you need a way to give an arg.

-2xx || system plt || pppr || addr to'sh'

Since buf is near the top of the stack, if you jump to pppr gadget, not jumping to the system, you can call the system function with arguments.

If you look at env, you can see that the path is set, so you can find the string '**sh\x00**' and use the address. (Since libc's fflush function is used, the string'sh\00' exists in the binary.)