CTF-CHALLENGE Report

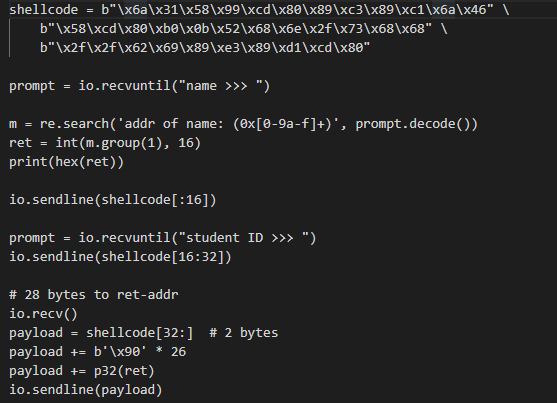
2017314712 김우진

1) your-first-bof

Addr of name 0xffffd5a0

Addr of comment 0xffffd5c0

We can know that name and student course of 16bytes string



So we input 16byte codes 2times for not making segmentation faults

After inputing the comment the code returns so we have to make it not to return

So we overwrite a code to not finish which is the information of payload

So after inputing dummy codes we input the return address for name address not to finish the code then io.interactive and find the flag

2) Cheat the game

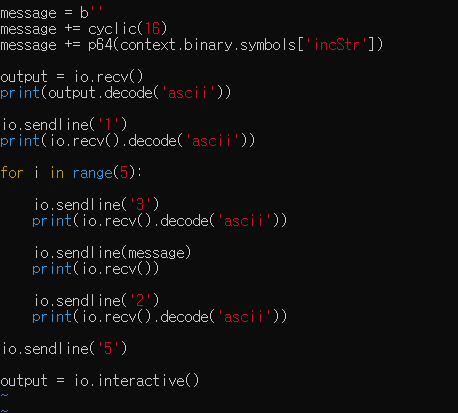
Item Object 0x406ae0

When we bought object and don’t use message buffer is 0x406b00

When we use object it frees 0x406ae0

So when there’s nothing to free it goes an error.

To solve this we should return to have an object when send a message



incStr is a function which increases the str

after repeating this int Int we can get the flag

for the above code I hust increased str so I cant get the flag

3) Ghost student

When we go to print individual grade and enter 7 strange values comes out.

So we can know that there is the problem.

Looking at gdb we get there is a fuction print\_flag() so by inputting return value of this fuction we can get the function.

By overlapping data after student6 in changing the grade we can solve the problem

But we shouldn’t change the canary part which is the value that we can when we input 7 so we send the buffer than value , buffer and the return address.

