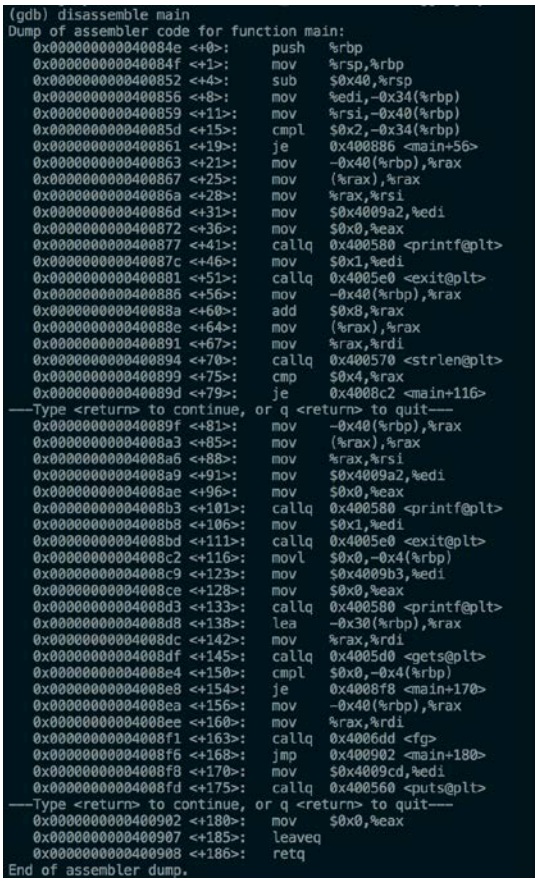
Enumeration and Exploitation

Binary 1 (Medium)

This challenge evaluates the contestant's ability to use a disassembler to exploit a compiled binary. One possible tool to use is the "GDB" Linux program. A Linux binary is provided and the contestant is tasked with extracting the secret flag. This can be solved by disassembling the main function, which reveals a call to "gets".



This is a function that is known to commonly have issues with buffer overflows. The disassembly also reveals the size of the buffer (30 bytes) which can be exploited if more than 30 bytes are inputted. Based on the disassembly, it can be inferred that the original code looks something along these lines:

```
char input[30];
int pass = 0;
printf("Please enter a password: ");
gets(input);
if (pass) {
  // Print out flag
} else {
  printf("Try again.\n");
}
```

Thus, the entering 31 bytes into the password prompt will overflow the buffer, overwriting the value of pass. Any ASCII character for the 31st character would make the pass variable a truthy value and print out the flag.

Question	Answer
What is the flag hidden in the program?	NCL-EZOF-5336