Re\_challenge 2

Goal: print “You are great at this:)”

Steps:

1. Open IDA: analyze graph of assembly
2. Create CFD
3. Analyze the assembly/Run
   1. Running it -> does not take any arguments
   2. One password, and only one check for it by using strncmp
   3. Uses gets to retrieve input from user
   4. Strncmp has 3 arguments, and the third is the length
      1. The password is 8 characters long
      2. It compares [ebp-112] and [ebp-376]
         1. [ebp-112] is user input
         2. [ebp-376] is the password made in the program
         3. Only compare the first 8 letters
   5. A bunch of code is letters are generated to make it harder to find the password
   6. The pointer is moved into [ebp-376]
   7. It points to “yagababaZ0ZMQUdmbGF”
4. Run code with “yagababa” and it printed the goal

Answer:

1. ZF = 1 continues
2. puts(“You are great at this :)”)

The password is “yagababa”

> ./re\_challenge2 yagababa

CFD:

