Homework #1

The homework is composed of three main steps. In each step, you are not allowed to modify any function except a specified section of entrance function. In the entrance function, it is forbidden to call any function/Jump (e.g., secret functions, printf, etc.), but other operations are permitted. Extract the hw1.tar file and modify each step’s c file. The c files are going to be compiled in docker containers with the following commands. It is recommended to use gdb (debugger) and disassemble the compiled code to understand what to do.

* docker build -t hw1 .

**Step 1) 30 points**

Build: docker build -t hw1 .

Run: docker run -it --rm --name hw1-running hw1

Output: now inside entrance()!

now inside secret()!

The process must return successfully. Getting segmentation fault leads to getting 0 from this step.

**Step 2) 30 points**

Build: docker build -t hw1 .

Run: docker run -it --rm --name hw1-running hw1

Output: now inside entrance()!

now inside first secret()!

now inside second secret()!

The process must return successfully. Getting segmentation fault leads to getting 0 from this step.

**Step 3) 40 points**

Build: docker build -t hw1 .

Run: docker run -it --rm --name hw1-running hw1

Output: now inside entrance()!

now inside secret()!

If we see “KABOOM!\nYou failed!\n” on the screen, you get 0 from this step. Getting segmentation fault leads to getting 0 from this step.

Violations of scholastic honesty include, but are not limited to cheating, plagiarizing, fabricating information or citations, facilitating acts of dishonesty by others, having unauthorized possession of examinations, submitting work of another person or work previously used without informing the instructor, or tampering with the academic work of other students. Any of scholastic dishonesty is a serious academic violation and will result in a disciplinary action.