

Lab 3: Symbolic Execution Using Angr

Preparation

Download a tarball from <http://www.cs.ucr.edu/~heng/teaching/cs260-winter19/lab3.tgz>. It contains two binaries: `re` and `afl_strcmp`.

Install Angr by following the instructions in <http://angr.io>.

Objective

Problem 1: The first binary “`re`”, when given a correct input, it will print out “right”. Please write an Angr script to find this correct input.

Problem 2: The second binary “`afl_strcmp`” has a vulnerability. When given a right input, it will crash. Please write an Angr script to trigger the crash.

Submission

You need to write a report. For each problem, you need to display your script and explain each line of your script, attach important screenshots, and explain the output.