Grenoble INP **UGA**
Ensimag **UFR IM2AG**

M2 CySeC
Advanced Security

Dynamic-Symbolic Execution (DSE) with Angr

This lab requires the use of the CySeC virtual machine, now avalaible from the Ensimag computers :

1. You can start it by typing /matieres/supplements/lance-vm-WMM9SY07.sh
2. The cysec password is cysec2020

Beware : do not try to **enlarge the VM window** (otherwise its execution will become **dramatically slow!**)

The purpose of this lab is to follow part of the Angr tutorial described on the provided set of slides (starting from slide 29).

Part 1 – Discovering some Angr DSE features

1) Do the first 4 exercises (from slides xx to yy), knowing that the objective is to feed the target program with a good password in order to obtain the string « Good Job ! » on the screen. Angr will help to do that (almost) in an automated way !

To do so you simply to complete the python script provided and run it with python ; it will tell you the truth !

Hints : you can use either objdump or ghidra to disassemble/decompile the target binary in order to find the few information you need.

2) Read the slides describing the following exercises (up to exercise 14), of course you can also do some of these exercises if you want …

Part 2 – Using Angr to (automatically!) trigger and exploit a buffer overflow …

We now focus on exercise 15 (arbitrary read). The purpose here is to enter a password allowing to over-read past a buffer in order to print the secret string « Good Jobs ! » (not supposed to be accessed during a regular execution).

Once you succeed with exercise 15 you can finish with exercise 17 ...