TESTING PROGRAMS FOR VULNERABILITIES

DOTA_Group3: Hong Yun Qin Jianxing
Qu Shaobo Zhang Shuhao

SYMBOLIC EXECUTION

PYCPARSER

Z3(SMT SOLVER)

GUI

INTRODUCTION:

Buffer overflow is a common vulnerability in programs. Many attacks on Microsoft systems are based on various buffer overflow problems. However, in some commonly used languages like C or Java, these problems won't be pointed out by the compiler and it's easy to be unaware of them.

In this project, we will use symbolic execution to discover buffer overflow problems in small programs which are written in the subset of C and develop an analyzing application with a GUI. Our approach is shown to capture all overflows of the source code written in our object language.

GUI OUTPUT: