World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:09, 2017

# Research on Fuzzy Test Framework Based on Concolic Execution

**Authors :** Xiong Xie, Yuhang Chen

**Abstract :** Vulnerability discovery technology is a significant field of the current. In this paper, a fuzzy framework based on concolic execution has been proposed. Fuzzy test and symbolic execution are widely used in the field of vulnerability discovery technology. But each of them has its own advantages and disadvantages. During the path generation stage, path traversal algorithm based on generation is used to get more accurate path. During the constraint solving stage, dynamic concolic execution is used to avoid the path explosion. If there is external call, the concolic based on function summary is used. Experiments show that the framework can effectively improve the ability of triggering vulnerabilities and code coverage.

**Keywords :** concolic execution, constraint solving, fuzzy test, vulnerability discovery
**Conference Title :** ICCISE 2017 : International Conference on Computational Intelligence and Software Engineering
**Conference Location :** Tokyo, Japan
**Conference Dates :** September 07-08, 2017