Automated Whitebox Fuzz Testing

Description
Fuzz testing is an effective technique for finding security vulnerabilities in software [1, 2, 3]. The idea is to combine symbolic execution and dynamic test generation to provide a suitable coverage of the code to detect problematic code fragments.

The student is supposed to focus on automated whitebox fuzz testing and investigate the state of the art (approaches that also go beyond [1, 2, 3]).

Prerequisites
A basic knowledge of Software Engineering I/II.

References


Contacts
Lars Grunske (grunske@informatik.hu-berlin.de)
Software Engineering Group
Institut für Informatik
Humboldt-Universität zu Berlin