
# Software Engineering II: EvoGFuzz

*SoSe 23 Group 08*

**Viet Cuong Ngo (621349)**
**Angelina Teodoridis (599563)**
**Kai Werk (584214)**
**Wei Jin (620999)**

Module supervised by:
Prof. Dr. Lars Grunske
Dr. Thomas Vogel

Institute for Computer Science
Humboldt-University at Berlin

June 21, 2023

# 1 Topic

Evolutionary Grammar-based fuzzing. (EvoGFuzz)

# 2 Tool

EvoGFuzzPlusPlus by Martin Eberlein and Eik Reichmann.
Website: https://github.com/martineberlein/evogfuzzplusplus
ISLa : https://github.com/rindPHI/isla

# 3 Research question

Usage of ISLa to expand EvoGFuzz via (maybe ISLearn and) semantic constraints.

# 4 Motivation

Adding semantic constraints to evolutionary grammar-based fuzzing in order to test improvements in precision and recall.
We will compare runtime, precision, and recall, with and without usage of ISLa.

# 5 Suggested Solution

While generating the input files, use iSLA constraints to generate semantically correct inputs. We hope the implementation of ISLa will increase precision/recall, and thus enhance the performance of EvoGFuzz.