

# Software-Tests automatisch erzeugen – Frische Ansätze für Forschung, Praxis und Lehre

Andreas Zeller  
CISPA Helmholtz-Zentrum für Informationssicherheit, Saarbrücken  
zeller@cs.uni-saarland.de

## Zusammenfassung

Automatisch erzeugte Softwaretests können mit wenig menschlichem Aufwand viele Fehler finden. In diesem Vortrag stelle ich aktuelle Techniken zur Testerzeugung vor, die für ein gegebenes Programm vollautomatisch dessen Eingabesprache ableiten und aus den so entstehenden Grammatiken große Mengen gültiger Testeingaben ableiten. Unser grammatikbasierter LangFuzz-Testgenerator hat so in den JavaScript-Interpretern von Firefox, Chrome und Edge tausende Fehler gefunden. Die Techniken sind in dem interaktiven Buch "Generating Software Tests" ([www.fuzzingbook.org](http://www.fuzzingbook.org)) zusammengefasst. In einer Mischung von Text und Programmcode können Leser im Browser direkt mit den Programmen experimentieren und ihren Code live ergänzen und erweitern.

## Abstract

Automatically generated software tests can find many errors with little human effort. In this talk I will introduce current test generation techniques that automatically derive the input language of a given program and derive large amounts of valid test inputs from the resulting grammars. Our grammar-based LangFuzz test generator has found thousands of errors in the JavaScript interpreters of Firefox, Chrome and Edge. The techniques are summarized in the interactive book "Generating Software Tests" ([www.fuzzingbook.org](http://www.fuzzingbook.org)). In a mixture of text and program code, readers can directly experiment with the programs in their browsers and supplement and extend their code live.