

Bachelor-/Masterarbeit

LLM-basierte Konfiguration von Fuzzern

Ziel

Fuzzing zählt zu den effektivsten Methoden, um Sicherheitslücken in Software automatisiert aufzuspüren. Den größten manuellen Aufwand verursachen dabei zwei Schritte: das Schreiben geeigneter Fuzzing-Targets (Harnesses), die die Schnittstellen einer Bibliothek sinnvoll ansprechen, und die Auswertung von Coverage und Crashes. Aktuelle Ansätze wie PromptFuzz¹ und CKGFuzzer² zeigen, dass Large Language Models (LLMs) Harnesses automatisch erzeugen können.

Ziel dieser Arbeit ist es, Fuzzing-Targets mit **lokal betriebenen LLMs** (z. B. über Ollama³) zu erstellen. So lässt sich der Ansatz auch bei vertraulichem Quellcode einsetzen. Als Einstieg dienen PromptFuzz oder CKGFuzzer; alternativ werden Harnesses direkt mit dem LLM generiert. Anschließend werten **LLM-Agenten** Coverage-Berichte und Crashes aus. Sie identifizieren nicht erreichte Code-Bereiche, verbessern Harnesses iterativ und bewerten gefundene Crashes.

Das genaue Thema und der Umfang werden nach Absprache festgelegt. Mögliche Schwerpunkte:

- Anbindung lokaler LLMs an PromptFuzz/CKGFuzzer und Vergleich mit Cloud-Modellen
- Direkte, agentenbasierte Harness-Generierung mit Feedback aus Build und Fuzzing
- Agentenbasierte Coverage-Analyse zur gezielten Verbesserung der Harnesses
- Automatische Crash-Triage: Deduplizierung, Ursachenanalyse, Unterscheidung echter Bugs von Harness-Fehlern

Anforderungen und Voraussetzungen

- Einarbeitung in Fuzzing (AFL++/libFuzzer) und LLM-basierte Harness-Generierung
- Einordnung in verwandte Arbeiten (PromptFuzz, CKGFuzzer, OSS-Fuzz-gen)
- Konzeption und Implementierung einer Pipeline aus lokalem LLM und Agenten

¹Lyu et al.: <https://dl.acm.org/doi/10.1145/3658644.3670396>

²Xu et al.: <https://dl.acm.org/doi/pdf/10.1109/ICSE-Companion66252.2025.00079>

³<https://ollama.com>

- Evaluation auf Open-Source-Bibliotheken, z. B. anhand von Coverage, gefundenen Crashes und dem Anteil kompilierbarer Harnesses
- Kenntnisse in C/C++ und Python sowie Erfahrung mit Linux
- Interesse an IT-Sicherheit, Softwaretests und LLMs

Ansprechpartner

Prof. Dr. Lothar Braun | ✉ lothar.braun@tha.de | ☎ +49 821 5586-3378

THA_innos

Das Institut für innovative Sicherheit (THA_innos) bietet eine Vielzahl von Abschluss- und Projektarbeiten im Themenfeld der Cyber Security an. Unser Team unterstützt Studierende dabei mit Know-How und Praxiserfahrung und ist zudem offen für eigene Themenvorschläge. Durch die enge Zusammenarbeit mit der Forschungsgruppe vor Ort im MRM-Gebäude lernen Studierende sowohl das Institutsleben, als auch die aktuelle Forschung von THA_innos kennen.

Weitere Informationen auch unter <https://innos.tha.de>