Abstract

This thesis addresses key challenges in **automated software testing** for modern, **distributed software systems**, specifically focusing on applications that rely heavily on **external web services** (e.g., microservices, third-party APIs). The shift from monolithic to complex, interconnected architectures has made comprehensive system-level testing increasingly difficult, particularly when handling external communications.

We present a suite of novel, search-based fuzzing techniques (i.e., white-box and black-box) to reduce manual intervention in testing these systems. Our primary contributions are:

1. **Automated Mocking:** We introduce novel search-based white-box fuzzing techniques for **automatically generating mock external web services** for JVM-based applications, eliminating the need for developers to hand-craft mock services and enabling robust testing of dependency interactions.

2. **Automated Schema Inference:** We solve the challenge of generating well-formed, complex inputs (such as **JSON documents**) for white-box fuzzing by developing techniques to **infer schemas in a fully automated manner**, thus supporting zero manual intervention.

3. **Automated SSRF Detection:** Recognizing that external communications introduce security threats, we present novel techniques to automatically **detect and exploit Server-Side Request Forgery (SSRF)** vulnerabilities in both white-box and black-box fuzzing contexts.

These novel techniques are implemented as an extension to the open-source fuzzer EvoMaster and evaluated using multiple open-source and industrial case studies, including those with known Common Vulnerabilities and Exposures (CVEs). Ultimately, this research provides a significant step toward **fully automated, system-level testing** by generating self-contained test suites with dynamic mocking capabilities and SSRF detection.