Sanan Hasanov

sanan.hasanov@ucf.edu
s4nsec.github.io

Education

2022 - **Ph.D., Computer Science**, *University of Central Florida*, Orlando, FL, USA
Advisor: Prof. Paul Gazzillo
Interests: Systems Security, Fuzzing

2022 - 2025 **M.Sc., Computer Science**, *University of Central Florida*, Orlando, FL, USA
Relevant Coursework: Advanced Data Structures and Algorithms, Software Engineering, Computer Communication Networks

2017 - 2022 **B.Eng., Computer Engineering**, *Baku Higher Oil School*, Baku, Azerbaijan
GPA: 3.8/4.0

Work Experience

Aug 2022-Current **University of Central Florida**, *Graduate Research Assistant*, Orlando, FL, USA
- Led the design, development, and evaluation of *KonfFuzz*, a configuration-aware kernel fuzzing tool, resulting in the discovery of *41* new kernel bugs and a *9%* increase in basic block coverage for fuzzers like syzkaller.
- Contributed to Linux kernel security by performing root cause analysis of configuration-dependent bugs, reporting them to maintainers, leading to *5* patches and a *CVE* designation (CVE-2023-3161).
- Streamlined bug reporting workflow by creating automation scripts to test bug reproducers and automatically notify relevant subsystem maintainers.

Jun-Aug 2024 **Trail of Bits**, *Summer Intern*, New York, NY, USA
- Designed and implemented a tracer for the Medusa smart contract fuzzer in *Go*, enhancing vulnerability detection capability and code coverage of the fuzzer up to *18%* and *32%*, respectively.
- Developed and executed benchmarks for Medusa's value generation feature, demonstrating improved runtime performance and bug detection compared to featureless Medusa and Echidna.
- Communicated findings effectively with team members to refactor tools and optimize workflows, improving system efficiency.

Jun-Aug 2023 **Margin Research**, *Security Research Intern*, New York, NY, USA
- Automated smart contract vulnerability analysis by building a Python tool integrating OpenAI and Google APIs, enabling efficient scraping, root cause analysis, and vulnerable code tracing, and successfully mapping over 200 incident cases.
- Authored a comprehensive guide on smart contract security for interns of the company, compiling and presenting information on prevalent real-world vulnerabilities and mitigation strategies.

Publications

IEEE/ACM ICSE, 2025 A Little Goes a Long Way: Tuning Configuration Selection for Continuous Kernel Fuzzing
Sanan Hasanov, Stefan Nagy, Paul Gazzillo

arXiv, 2024 Can You Fuzz Me Now? Overcoming Configuration Blind Spots via Configuration-aware Kernel Fuzzing
Sanan Hasanov, Stefan Nagy, Paul Gazzillo

Projects

Jan 2024 - Current **KonfSetup**
- Implemented KonfSetup, a Python-based platform that provides experimental setup environment for configuration-aware fuzzing experiments using kmax, QEMU, Google Drive and OpenAI APIs.
- Conducted benchmarking using KonfSetup, to compare KonfFuzz and syzkaller, leading to discovery of 41 novel bugs in the kernel.

Skills

Languages Bash, Python, Go, C

Tools syzkaller, QEMU, SQL, CodeQL, Git, Docker, Kubernetes, ollama, GCP, AWS, Azure, CI/CD, Jenkins, Ansible