Gabriel Sherman

Salt Lake City, UT | gabesherman6@gmail.com | +1 207-307-1490

linkedin.com/in/gabe-sherman | gabe-sherman.github.io

Research Interests

My research focuses on fuzz testing, with a strong passion for proactively securing widely used software. I am particularly interested in extending fuzz testing to previously unexplored areas. My current work centers on automating harness generation for security critical software libraries.

Education

Ph.D., Computer Science	University of Utah	2024-*current*
B.S., Computer Science	University of Utah	2020-2024

Publications

1. **No Harness, No Problem: Oracle-guided Harnessing for Auto-generating C API Fuzzing Harnesses**
   Gabriel Sherman, Stefan Nagy
   International Conference on Software Engineering **(ICSE '25)**

Research Experience

Ph.D. Research Assistant, University of Utah – Salt Lake City, UT — August 2024 – *current*

- Currently conducting research under Dr. Stefan Nagy to expand the capabilities of automatic harness generation through testing, development, and evaluation.
- Developed a novel automatic harness generation technique and published a top-tier conference paper detailing the approach.
- Uncovered and reported over 60 bugs across a wide range of software libraries, with over 40 confirmed. Some of the bugs I have found can be found here: futures.cs.utah.edu/bugs/?search=gabe+sherman

Summer Research Intern, Trail of Bits – Salt Lake City, UT — 2024, 2025

- Performed research and developed tooling for various security goals for two consecutive summers.
- *Summer 2025* — Built a browser-based checksec tool for cross-platform security analysis of ELF, PE, and Mach-O binaries, with a Rust backend for security checks and a client-side JavaScript interface to display results.
- *Summer 2024* — Developed and advanced an automatic harness generation approach for C-based libraries, integrating Trail of Bits' Multiplier tool for static analysis, generating harnesses for widely-used open-source libraries, and performing fuzzing and bug triage that led to the identification and reporting of 6 confirmed bugs.

Invited Talks & Articles

Checksec Anywhere – Trail of Bits Intern Showcase.	07/2025
Introduction to Fuzzing – University of Utah Cybersecurity Club.	03/2025
Automated Bug Finding – Guest Lecture at Kahlert School of Computing.	09/2024
Automatic Harness Generation for C-based Libraries – Empire Hacking NYC.	08/2024
Automated Harness Generation – Mountain West Undergraduate Research Showcase.	11/2023

Technical Skills

Build Systems: Make, CMake, Autotools, Ninja, Meson

Debugging and Profiling: GDB, perf, strace, ASan/UBSan

Software testing: Fuzzing, Static & Dynamic Testing, Crash Triage

Languages: Python, C, C++, Bash/Shell, Java, Rust

Projects & Activities

Market Simulation Game

- Designed and implemented a browser-based market simulation game where users buy and sell products to maximize profits.
- Developed the backend using Spring Boot and MongoDB, exposing core functionalities through a REST API for seamless integration.
- Built a responsive and interactive frontend using React, leveraging the REST API to display real-time market data in a user-friendly interface.

University of Utah CTF Team

- Competed in cybersecurity competitions, solving challenges in binary exploitation, digital forensics, reverse engineering, and web security.
- Specialized in identifying and exploiting vulnerabilities in binaries and analyzing digital artifacts for forensic investigations.
- Collaborated with team members to develop creative solutions and improve overall performance in competitions.

Operating System Fundamentals

- Built an early prototype of a kernel based on the xv6 architecture. This prototype included booting, interrupt handling, and running processes in user space.
- Implemented a reduced linker program. Parsed the ELF file to perform relocation on all entries in the relocation table.