SLAIT - Secure Language Assembly Inspector Tool

Michael Bratcher and Maria Linkins-Nielsen

Faculty Advisor(s): Dr. Marius Silaghi, Dept. of Electrical Engineering and Computer Science, Florida Institute of Technology

Motivation

- Students executing low-level language code may need to place their systems into a vulnerable state
- Faulty low-level code can lead to unintentional system damage and security risks
- Inspecting register and flag behavior during execution is often a tedious process for beginners
- Existing workflows can require lowering device security level

SLAIT provides secure sandboxed execution with breakpoint-level register visibility and no local setup required.

Objective

Develop a secure web-based platform that enables users to:

➔**Upload** assembly programs through a browser
➔**Select** instruction inspection points
➔**Execute** code inside an isolated sandbox
➔**Capture** register and flag state changes
➔**Visualize** execution behavior step-by-step

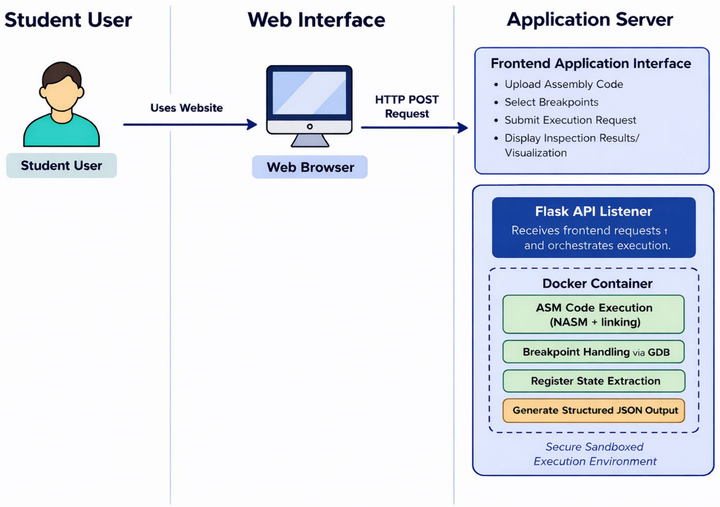
Key Features

- Secure Docker-based execution sandbox
- Register & Flag inspection at user-selected lines
- No local installation required
- Platform-independent debugging workflow

Educational Applications

- Supports computer architecture instruction
- Enables safe instruction-level experimentation
- Shows step-by-step register and flag changes
- Removes assembly debugging setup barriers

Architecture Diagram



Software Stack:

GDB
The GNU Project Debugger

Flask

Application