PrimeVUL was previously introduced as a dataset for training and evaluating large language models (LLMs) for vulnerability detection (VD), but research revealed the considerable gap between capabilities and practical requirements for deploying code LLMs in security roles. This project aims to enhance the detection and fixing of security vulnerabilities in open-source codebases through stub testing. By focusing on a sample of vulnerabilities from the TensorFlow codebase, this research implements stub tests to recreate vulnerabilities and validate fixes. Key findings highlight the effectiveness of stub testing in improving software reliability, proving the value of automated test generation for training LLMs in VD as stub tests provide modality of information, allowing for dynamic vulnerability tracing during development. When implemented, automated stub test generation ensures detected vulnerabilities are addressed, while data augmentation techniques simulate edge cases likely to cause vulnerabilities, both of which provide comprehensive detection and fixing solutions to enhance software robustness and reliability.