

Sanitizer validation using symbolic execution and library cross-checking

Abstract

The goal of this project is to analyze sanitization libraries in seek of vulnerabilities. More specifically, we want to find inputs that reveal vulnerabilities in existing sanitization functions. Our contribution is twofold: (1) we want to find spec-violating inputs for the sanitization function and (2) report vulnerabilities not covered by the current library.

Contact

student: Mateus Araujo Borges <MateusAraujoBorges AT gmail.com>

mentor: Marcelo d'Amorim

co-mentor: Corina Pasareanu

Repository

The sources for this project are available from a Mercurial repository at TBD

Description

Project documentation/wiki/blog are available at TBD