Oracle Labs, Australia: Research Assistant Position

Test-Case Generation for Node.js Web Applications

Position: 6-month, full-time tenable during June 2018 to May 2019 with the Program Analysis group.

Project Details: This internship will explore test case (e.g. input) generation strategies for Node.js web applications with the goal of improving a dynamic security analysis.

Given an application, test case generation typically aims at automatically generating inputs that will trigger different execution paths (e.g. increase code coverage). In this internship, you will develop a test case generation tool for Node.js web applications to assist an existing dynamic security analysis. While there exists a large body or work on test case generation for web applications, existing work does not address the challenges and particularities of Node.js applications (e.g. dynamically typed, event-driven, prototype-based), and existing work on test case generation for JavaScript focuses on the client-side, not the server-side. During this internship, you will explore a variety of black and grey box techniques like automated crawling, and modelling as well as static analysis, and dynamic analysis to discover the interfaces of Node.js web applications and guide a test case generation strategy. Specifically, you will: 1. familiarise yourself with existing strategies for test case generation (e.g. crawling, modelling, interface discovery, and guided request generation), 2. design and implement a test case generation tool for Node.js web applications, and 3. measure the impact of your tool in terms of improvement to coverage and vulnerability detection, based on an existing security analysis.

Supervisors: François Gauthier, Behnaz Hassanshahi, and Alexander Jordan

François Gauthier has a PhD in Software Engineering from the University of Montreal. His thesis was about static analysis of PHP applications. Since he joined Oracle Labs, he has worked on static security analysis of Java EE applications and is now focusing on dynamic security analysis for Node.js.

Behnaz Hassanshahi has a PhD in Computer Science from the National University of Singapore. Her thesis was about static security analysis for Android. Since she joined Oracle Labs, she has worked on fuzzing and is now focusing on dynamic security analysis for Node.js.

Alexander Jordan has a PhD in Computer Science from the Technical University of Vienna. His thesis was about static analysis of real-time systems. Since he joined Oracle Labs, he has worked on static security analysis of Java EE applications and is now focusing on dynamic security analysis for Node.js.

Oracle Labs, the research arm for Oracle, focuses on applied research that produces new technologies of interest to the company. Oracle Labs Australia, based in Brisbane, focuses on Program Analysis as it applies to a variety of domains, including bug-checking, security analysis, productivity tools, testing, and more. The group is best known for its research on static code analysis that led to scalable and precise bug-checking algorithms embedded in the Oracle Parfait tool. For more information, visit `http://labs.oracle.com/locations/australia` Oracle internships give students valuable industry experience and the chance to work on cutting-edge research projects with real-world applications.

About this position:

Duties You will:

- Work independently to research or develop a state-of-the-art solution to generate test cases for Node.js web applications
- Meet with your supervisor daily for guidance and to discuss ways to solve the problem
- Attend team meetings and give updates on your work
- Present your findings and outcomes to the group.

Prerequisites:

- For students currently enrolled in a PhD or research-based Masters degree in Computer Science or Software Engineering.
- Specific theory and coding skills:
- Knowledge of the Node.js ecosystem is required
- Working knowledge of the web stack and related technologies (e.g. HTML, DOM, AJAX, HTTP, web server, SQL/NoSQL databases) is required
- Knowledge of Linux and a scripting language (e.g. bash or python) is required
- Compiler / Program analysis background is a plus
- Demonstrated ability to work independently and collaboratively.

Benefits:

- These positions are paid at current industry rates.
- Travel & visa costs associated with overseas applicants will be reimbursed.
- Ongoing learning is incorporated into our every week to keep us at the cutting edge.
- International speakers frequently present their research to us.

Contact Paddy Krishnan paddy.krishnan@or acle.com for more details. The position will commence interviewing immediately and remain open until filled.