A Study on Dynamic Analysis and Penetration Testing Tools for Web Applications

Behnaz Hassanshahi
Oracle Labs Australia

Abstract

JavaScript has become the most popular language for web application development in recent years. It provides features to build complex and powerful applications that our society is highly dependent on. However, such complexity makes it more cumbersome for developers to write secure programs. In fact, recent studies show that code injection vulnerabilities is prevalent in these applications. Attackers may compromise these vulnerabilities to launch devastating attacks.

Even though researchers have proposed various tools and techniques to test web applications, few of these tools are tailored for finding security-critical vulnerabilities. The exiting research-based test generation techniques mostly report the code coverage of the analysis for finding programming errors. On the other hand, there are plenty of free and commercial tools available which are leveraged by penetration testers and hackers to find serious vulnerabilities. While the results and reports show the effectiveness of these penetration testing tools in practice, they are highly dependent on domain-specific knowledge. Usually, the analyst has to put a lot of manual effort to use these tools to find zero-day security vulnerabilities in large applications. This gets even harder if the analyst is not familiar with the code-base under test.

Our goal is to understand the implications of the existing gap between academic research techniques and penetration testing tools for finding security vulnerabilities in web applications developed in JavaScript. For this purpose, first we conduct a literature survey of the dynamic analysis and test generation techniques for JavaScript applications. Next, we study the widely used penetration testing tools and contrast their goals with the research-based tools. We present our observations on how these two directions may benefit from each other in order to tackle serious security issues in web applications.

About the Author

Behnaz Hassanshahi has received her PhD in Computer Science from National University of Singapore under supervision of Dr Roland Yap. Her research interests include program analysis and its intersection with computer security. Her PhD thesis topic was “Characterization, Detection and Exploitation of Data Injection Vulnerabilities in Android”. She is currently undertaking research work in the area of dynamic testing and fuzzing at Oracle Labs Australia.