SpiderSapien: Client-Centric Crawler and Security Scanner

Eric Olsson[1], Benjamin Eriksson[1], Adam Doupé[2] , Andrei Sabelfeld[1]

[1] Chalmers University of Technology and University of Gothenburg
[2] Arizona State University

Black-box web application crawling and scanning plays an important role for security testing of web applications. Yet state-of-the-art scanners fall short of addressing key characteristics of a modern web application: its extreme dynamism and interactivity on the client side. This paper identifies immersive interaction as a key ingredient for scanners to deeply explore modern web applications. We propose SpiderSapien, a client-centric crawler and security scanner. Driven by immersive interaction, SpiderSapien incorporates novel methods to detect interactable elements, order UI interactions, and use LLMs to solve forms. In doing so, we demonstrate how to reliably discover and test deep states of modern web applications. The evaluation of our approach shows substantial improvements in both code coverage and vulnerability detection over previous work, with an average increase in code coverage of 21.5% compared to the *union* of the other scanners and a total of 36 XSS vulnerabilities, across 6 of the 8 web applications, compared to the 4 XSS others find. In addition, a separate empirical evaluation of SpiderSapien's LLM-powered form solving capabilities on diverse *real forms* on the open web demonstrates superiority over the previous approaches in generating desired input on the client side, solving at least 23.3% more of the non-trivial forms compared.