BOSTON APPLICATION SECURITY CONFERENCE

The bearer of this certificate attended the following presentation on **Saturday, April 5, 2025, from 3:00 PM to 3:50 PM** at the Microsoft Technology Center, 5 Wayside Road, Burlington, MA 01803.

TALK: API Fuzzing in the SSDLC. Problems and possible solutions – Arseniy Sitnikov

Agenda: In my talk I would like to discuss the need for securing API endpoints. 73% of the companies have encountered a vulnerability in their api handle at least once in the last three years. And the list for possible vulnerabilities is so large and unique to API, that any other practice (SAST, SS, SCA, even DAST) is not obligated to find them. As a solution there is a practice of API Fuzzing - sending misconfigured or primarily vulnerable payloads to endpoints and checking if the response matches the expected. And in theory it works as a charm - by studying a specific app, understanding its business logic and workflow its facile to create a list of suitable payloads and the triage process is also pretty easy, because the engineer mostly understand the expected results and can match it with the received one. And that's how usually many companies work that provide testing API as a service. But everything becomes more complex when you try to implement API Fuzzing in the SSDLC. To begin with picking out a perfect tool for the job (or coding your own) and finally with trying to automate the process and integrate it in the companies life. I went through all this and haven't found any papers or talks beforehand had to solve all the problems with solely my team and me. The problems ranged from working with legacy applications that don't have any documentation on their API configuration and ending with working out a way to work in different physical(and logical) networks without being banned by the internal company security for DoSing companies servers. In my talk I want to talk about my experience, several important issues that may be overlooked but extremely important and talk about possible ways to develop the tool and the practice.

Please retain this certificate as evidence of your attendance at this presentation and submit a claim for **ONE CPE CREDIT** in accordance with the guidelines of your certifying organization.