



BOSTON APPLICATION SECURITY CONFERENCE

The bearer of this certificate attended the following presentation on **Saturday, April 5, 2025, from 10:00 AM to 11:00 AM** at the Microsoft Technology Center, 5 Wayside Road, Burlington, MA 01803.

TALK -No Laughing Matter: The OWASP Top 10 for LLMs in Code Examples – Jacob Berry

Agenda: With artificial intelligence (AI) and Large Language Models (LLMs) taking the world by storm, promising to revolutionize everything from customer service to code generation, you better hold onto your keyboards—because when your AI starts hallucinating, it's no laughing matter! Join us as we dive into the OWASP Top 10 AI & ML security risks, and some of the hilarious and not so funny things you need to be wary of when leveraging these tools for your engineering organizations. We'll cover everything from prompt injection attacks to model hallucination (think AI on a bad trip), and more. We'll share real-world code examples that highlight these risks in a way that may make you laugh, and possibly cry, but we will definitely keep it entertaining. Discover how to leverage the power of AI, while still keeping in mind its quirks and security risks, as the use of AI in our systems will only grow, and security is best integrated from as early as possible. Whether you're a developer, business leader, or just an AI enthusiast, join this talk to gain some insights into the evolving threats.

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.

