

Dear Members of the Selection Committee,

I am pleased to nominate the paper “RACEDB: Detecting Request Race Vulnerabilities in Database-Backed Web Applications” (IEEE Symposium on Security and Privacy, 2026) for the Best Scientific Cybersecurity Paper Competition. This paper makes a significant and timely contribution to the science of cybersecurity by identifying and systematizing a critical yet underexplored class of vulnerabilities: request race conditions in modern web applications.

Although race conditions have been widely studied, prior research has primarily focused on low-level concurrency within programs. In contrast, this work demonstrates that web applications exhibit a distinct concurrency model in which independent user requests interact through shared database state. This insight reveals a major limitation of existing security tools, which typically analyze requests in isolation and therefore fail to detect vulnerabilities that arise only under concurrent execution.

To address this gap, the authors introduce RACEDB, a principled, concurrency-aware framework that systematically explores interleavings of web requests and detects violations of application-level invariants caused by inconsistent database states. Importantly, the system goes beyond identifying potential issues by validating their exploitability, demonstrating whether the detected races can be triggered in practice. This end-to-end capability significantly enhances both the precision and practical relevance of the approach.

The paper’s empirical evaluation further highlights its impact. By applying RACEDB to real-world applications, the authors uncover previously unknown vulnerabilities, demonstrating that request race conditions are both prevalent and practically exploitable. These findings challenge prevailing assumptions about web application security and expose a critical gap in current defenses.

From a scientific perspective, this work establishes a new foundation for analyzing application-layer concurrency in security contexts. By integrating concepts from database consistency, dynamic analysis, and security testing into a unified framework, it transforms an ad hoc problem into a systematic and rigorously analyzable domain.

In summary, this paper merits strong consideration for the award due to its conceptual clarity, technical innovation, and demonstrated real-world impact. It not only identifies an important

gap in existing security practices but also provides a robust, generalizable solution with the potential to influence future research and practical tools in web application security.

Sincerely,

Chung Hwan Kim  
Assistant Professor  
Department of Computer Science  
Erik Jonsson School of Engineering and Computer Science  
The University of Texas at Dallas