Abstract

Software vulnerability remains a serious problem among industry players in the world today because of the numerous security related challenges it possess to end-users and stakeholders. Although previous studies have proposed various methods and tools that can be used in reducing or eliminating software vulnerability, those studies, however, raised several additional questions that need be addressed: (1) Can all the tools be used in curbing software vulnerabilities. (2) Can a specific tool detect all software vulnerabilities? To address these questions, we performed a detailed evaluation of the various software vulnerability detection methods and tools to find out their differences and similarities. Our studies also seeks to investigate the most efficient approach for detecting vulnerabilities based on previously proposed benchmarks and present some recommendations for future studies.
Evaluation of Software Vulnerability Detection Methods and Tools: A Review

Names," Common Vulnerabilities and Exposures: The Standard for Information Security

21. N. Dor, M. Rodeh, and M. Sagiv, "CSSV: Towards a realistic tool for statically detecting

22. B. Hackett, M. Das, D. Wang, and Z. Yang, "Modular checking for buffer overflows in the
232-241.

security problems," ACM Transactions on Information and System Security (TISSEC), vol. 5,

24. N. Nethercote and J. Seward, "Valgrind: a framework for heavyweight dynamic binary


26. J. Gray, Benchmark handbook: for database and transaction processing systems:

27. P. E. Black and E. Fong, "Proceedings of Defining the State of the Art in Software

Index Terms

Computer Science

Security

Keywords

Benchmarks; Software Vulnerability; Vulnerability Detection