Abstract

Software security vulnerability is a flaw in a software product that could compromise the integrity, availability, or confidentiality of a software system. The growth and development of software have brought about a corresponding increase in vulnerabilities, which has necessitated the need to develop software security assurance tool that can detect and prevent these vulnerabilities. Previous studies have suggested both commercial and open source tools such as Ashcan, Web Inspect, Web King, Skipfish, and OWASP ZAP just to mention but a few to help mitigate against this security gaps. However, each of this approach has its merits and demerits in detecting vulnerabilities. As a result, this paper seeks to develop a more proactive approach which is a merger or integration of the strength of existing techniques into one system: An integrated web vulnerability detector scanner: which is a software assurance tool for
detecting vulnerabilities in web application. The analysis involves presenting a general overview of web application, web application scanners and web application vulnerabilities. Lastly, we present the theoretical framework for detecting web application vulnerabilities based on the proposed model. The preliminary findings show that the concept is feasible within the domain of vulnerability detection.

References

An Integrated Approach for Detecting Security Vulnerabilities in Web Applications: A Theoretical Perspective


28. A. Makkar and K. Jain, "


Index Terms

Computer Science Security
Keywords

Software Vulnerability, Static Analysis, Web Application