OJMAS
Offa Journal of Multidisciplinary and Advanced Studies
P-ISSN: 3121-7506
E-ISSN: 3156-5182

ADOPTION OF INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL) FRAMEWORK TO MITIGATE VULNERABILITIES IN A CLOUD-BASED PLATFORM

Author: Jimoh Hammed. O

Published: -

Issue: Issue 1

Volume: Volume No 1

Abstract

This paper discusses how integrating the Information Technology Infrastructure Library (ITIL) governance framework with Open Web Application Security Project (OWASP) techniques can enhance vulnerability management in cloud environments. The framework will be used on one of the cloud technologies called “Docker.” On this cloud platform, OWASP Juice Shop, which is a vulnerable website, will be installed to demonstrate a hands-on exploitation of critical vulnerabilities, such as broken access control, security misconfiguration, and injection, among other vulnerabilities. This will be executed in a virtualization environment with the use of Kali Linux embedded in the virtual machine and a tool called Burp Suite as a proxy for interception. Each vulnerability triggered formal ITIL processes: Incident Management for containment, Problem Management for root-cause analysis, Change Control for secure code deployment (e.g., parameterized queries, CSP headers), and CSI for knowledge retention. The work proves that embedding defensive coding practices and automated scanning within governed workflows transforms reactive patching into an actionable intelligent approach to improve the security posture of the cloud environment and ensure best practices are strictly adhered to within an organization.

Keywords

docker, burp suite, ITIL, incident management and problem management