IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Application Security and Secure Coding Practices

Nilam Nagesh Lokhande
Student, Department of Masters of Computer Applications
Late Bhausaheb Hiray S. S. Trust's Hiray Institute of Computer Application, Mumbai, India
nilamlokhande2303@gmail.com

Abstract: *The concept of security in web applications is not new. However, it is often ignored in the development stages of the applications. Moreover, developers are more inclined to implement features and often do not practice secure coding. Therefore, countless web applications are launched with security vulnerabilities like cross-site scripting, injection attacks and resource alterations. As software applications are used more often across a range of industries, maintaining their security has grown to be a top priority. Web applications comprise a large proportion of the contemporary Internet with many of them dealing with sensitive information and handling critical operations whose compromise could result in large monetary and privacy costs. Naturally, the security of web applications has become an increasingly important issue as web technologies are utilized more and more. Without practicing secure coding and having an integrity verification system in place, it is difficult to defend security attacks. To that end, the incorporation of security controls throughout the software development lifecycle (SDLC) has emerged as the most prominent solution for detecting security defects early and fixing them with minimal cost and overhead. This research paper gives an in-depth analysis of secure coding techniques and application security. The study finishes by summarizing the main conclusions and highlighting the value of application security and secure encryption procedures to lower risk and safeguard sensitive data*

Keywords: Vulnerabilities, Security, guidelines, confidentiality, mitigate, SDLC

REFERENCES

[1]. Secure Programming Cookbook for C and C++ by John Viega and Matt Messier
[2]. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities by Mark Dowd, John McDonald, and Justin Schuh
[3]. Secure Coding in Java: Best Practices for Secure Java Development by Robert C. Seacord
[4]. Threat Modeling: Designing for Security by Adam Shostack
[5]. Secure Development for Mobile Apps: How to Design and Code Secure Mobile Applications with PHP and JavaScript by J.D. Glaser
[6]. Secure Coding Guidelines for the Java Programming Language by Oracle
[7]. Common Weakness Enumeration (CWE) - MITRE Corporation
[8]. The Building Security In Maturity Model (BSIMM) by Cigital, Inc.
[9]. Security Development Lifecycle (SDL) Implementation Guide by Microsoft
[10]. ISO/IEC 27034: Application Security
[11]. NIST SP 800-64: Security Considerations in the System Development Life Cycle
[12]. CWE (Common Weakness Enumeration) and CERT Secure Coding Standards
[13]. www.sans.org/reading-room/topics/secure-coding
[14]. www.nist.gov/topics/software-assurance
[15]. www.computer.org/technical-committees/center-for-secure-design