Smart Source code Analyzer to Detect Security Vulnerabilities

PCS Gunawardana

(Reg. No.: MS20912048)

MSC in IT

Specialized in Cyber Security

Supervisor: Mr. Udara Samaratunga

November 2021

Department of Information Technology
Faculty of Graduate Studies and Research
Sri Lanka Institute of Information Technology

Table of Contents

List of Figures

List of Tables

Abstract

Web based applications are more vulnerable to unauthorized access. Recently web applications are more important for organizations to implement their business activities and sensitive information sharing among owners. To solve security problems (cyber-attacks, threats) organizations are expending huge money to penetration testing, vulnerability assessments for their IT resources. According to OWASP ratings there are most vulnerable areas in web development. Injection, Broken authentication, Sensitive data exposure, XML external entities (XXE), Broken access control, Security misconfigurations, Cross site scripting (XSS), Insecure deserialization are some top vulnerabilities that can be happened in web application. SQL injection attack can destroy the web application or any online application. SQLI will allow attackers to access, modify, delete sensitive information of application back-end database without authorization. It is possible to run arbitrary commands with using SQL injection which uses high system privileges. Hence effect is high critical. Most of SQL injection attacks are from user inputs dynamically generated. Normally there are several ways to write a code. So those codes can be vulnerable for attacks. Specially SQL injection attacks because of unprepared coding and not follow secure code standards. As example we can write SQL injection prevention code with using prepared statements. In java they have SQL injection safer method which is prepared statement. As example [email: ‘ OR ‘1’ = ‘1 Password: ‘ OR ‘1’ = ‘1] code generate [SELECT userid FROM employee WHERE id = ‘1’ OR ‘1’ = ‘1’ AND password = ‘1’ OR ‘1’ = ‘1’] query. Because this generate WHERE clause always TRUE. [2] So attacker can log into system without valid login id and password. As well as retrieve sensitive information or meta data about database schema such as database names, table names, table field names, table field data types. So this is big issue and harmful for applications. Cross-Site Scripting (XSS) is a most famous attack type by hackers inserting malicious code samples for web application client side (use JavaScript codes for front end not attack host server). These kinds of attacks can be happened mostly because of not proper validation of the content. This is about mostly happened retrieving user sessions, session tokens, sensitive information and cookies, hijack accounts, spread web worms, access browser history and clipboard contents, control web browser remotely, scan and exploit internal network applications. Majority of web sites as example 70% of them are vulnerable to XSS attacks. XSS can be classified into two parts. Those are namely reflected XSS and XSS stored. This is about inserting malicious JavaScript code to web application URL.[3] These are happening due to unsecure software writings. Many software engineers are not aware of security coding standards and they only focus about developing. But the main critical and important thing is security of web application. It should be in developing stage. So this research is to identify security vulnerabilities of software code and future enhancement of this research is to suggest alternative best suitable secure code lines.