An Agent Based Intelligent Dynamic Vulnerability Analysis Framework for Critical SQLIA Attacks: Intelligent SQLIA Vulnerability Analyzer Agent

Jeya Mala Dharmalingam, Thiagarajar College of Engineering, Madurai, India
M Eswaran, Zoho Corporation, Chennai, India

ABSTRACT

This article describes how software vulnerability analysis and testing for web applications should detect not only the common attacks but also dynamic vulnerability attacks. These are the attacks such as structured query language injection attacks (SQLIAs) which will extract the most crucial user information from the targeted database. In this proposed approach, an intelligent agent namely intelligent vulnerability analyzer agent (IVA) is proposed in which the external attacks due to dynamic user inputs are identified using a heuristic-guided intelligent graph searching and then a pre and post condition based analysis is performed to identify the dynamic vulnerabilities. Further, the proposed approach is compared with some of the existing works based on the number of false positives and false negatives of attacks detection and confirmed that the proposed work is a novel and effective one in finding out SQLIAs.

KEYWORDS
Intelligent Vulnerability Analyzer Agent (IVA), Software Testing, Software Vulnerability Testing, Structured Query Language Injection Attack (SQLIA), Web Applications

INTRODUCTION

In general, web applications are real-time applications that include online sales, online auctions, online banking, online stock forecasting and so on. These applications have to be deployed with higher degree of reliability, confidentiality and efficiency. As these applications are vulnerable to various kinds of attack, protecting such applications from them is essential (Balasundaram and Ramaraj, 2012). The OWASP’s Top 10 most critical web application security risks are: Injection, Broken Authentication and Session Management, Cross-Site Scripting (XSS), Insecure Direct Object References, Security misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, etc. (OWASP Report, 2017)

Many of the web based applications are two-tier or three-tier architecture ones, in which the business information or customer related crucial information will be stored in back-end databases. The Structured Query Language (SQL) is used to communicate with such back-end databases to store, process and update the information.

DOI: 10.4018/IJIIT.2018070104

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
The attackers or intruders generally use these SQL statements present in the server-side code of the web application and inject them with malicious input along with the dynamic user input. This helps them to access and retrieve the crucial information stored in these databases without the knowledge of the users of the websites and even the administrators of the website. This type of attack which is called as SQL Injection Attack (SQLIA) allows the intruders to retrieve information from the backend databases directly. Depending on the security measures of the application, the risk of SQL Injection attack can vary from remote code execution and total system compromise to basic information disclosure (Tajpour et al., 2011).

According to Teska Labs report (2016), today’s malicious hackers have an average of 312 days to exploit “zero-day” computer software flaws before human cyber security experts can find and fix these flaws. Due to the severity level of such attacks, several researchers’ have proposed different approaches to reduce their impact for secured online transactions. Based on the literature reviews, it has been identified that, most of the existing works are using static code analysis techniques with some persistent storage to store different attack types to evaluate the vulnerabilities of user inputs. But, as these will cause second order attacks by the intruders on these backend tables again by means of SQL injection attacks, the existing works are proven to be error-prone. Some of the dynamic execution based analysis techniques depend on mutation based analysis which requires huge amount of storage space to store different versions of the queries for each kind of attack and also higher execution time is required to execute both mutated queries and actual queries to compare their results.

The vulnerability and severity level of SQLIA s and the insights gained over the problems in the existing works have been the motivation behind this research work to find an alternative mechanism that will prevent SQLIA s and also does not have any second order attacks with less time consumption.

Hence, the objective of this research work is twofold: (1) to identify the potential SQL queries that are vulnerable to attack and (2) to provide an alternate mechanism to rewrite them in order to prevent SQLIA type of attacks using an intelligent agent with heuristic guided graph searching technique.

In this research work, a novel intelligent vulnerability analysis framework is developed to monitor the source code for any SQLIA type of vulnerabilities. As a first step, it extracts all the SQL queries from the given web application. Once all the SQL queries are extracted, the intelligent agent filters out only the dynamic user input based queries for vulnerability evaluation. These queries are then constructed as graphs and are compared with their corresponding SQL master graphs (SQLMG). If there is a mismatch in the nodes, the agent will generate a ‘First Alert’. Then that query will be analyzed for a second level analysis, in which each node in the current graph has been compared with SQLMG for a pre or post condition violation. This is done by analyzing the pre and post conditions during the path exploration process from one node to another. This comparison of each node in the current graph will identify any pre or post condition violations. The accumulated result of pre and post condition violations helps the agent to classify the dynamically submitted queries as either vulnerable or non-vulnerable. If a query is identified as vulnerable during this subsequent analysis, the agent will term it as the ‘Final Alert’ and the query is treated as a ‘Malformed Query’ and will be logged for further action taken by the administrator. Due to the double folded rigorous check on the SQL queries, the proposed approach achieves an accuracy of 99% to 100% in SQLIA detection.

Further, the proposed approach has been compared with some of the existing dynamic vulnerability analysis based research works such as Mutation Based and XML SQL Tree based approaches and identified that, the proposed work has less number of false positives and false negatives count. Also, the total time taken is very less when compared to the other approaches. In addition to that, as there is no secondary storage being used to store attack types for comparison, the proposed approach completely avoids second order attacks. As there is no secondary storage used, the storage consumption for the processing of the proposed approach is very less.

Hence, a novel Intelligence based vulnerability analysis framework has been developed and is implemented as a tool. This provides a complete automation to prevent the web applications from security threats. It is also confirmed that, this tool will help the web developers as well as the website
Related Content

Semiotic Evaluation of Product Ontologies
[www.igi-global.com/chapter/semiotic-evaluation-product-ontologies/54425?camid=4v1a](www.igi-global.com/chapter/semiotic-evaluation-product-ontologies/54425?camid=4v1a)

Simulation of Temperature and Precipitation under the Climate Change Scenarios: Integration of a GCM and Machine Learning Approaches
[www.igi-global.com/chapter/simulation-of-temperature-and-precipitation-under-the-climate-change-scenarios/173372?camid=4v1a](www.igi-global.com/chapter/simulation-of-temperature-and-precipitation-under-the-climate-change-scenarios/173372?camid=4v1a)
Collusion-Free Privacy Preserving Data Mining
www.igi-global.com/article/collusion-free-privacy-preserving-data/46962?camid=4v1a

The Satiation of Natural Curiosity
www.igi-global.com/article/the-satiation-of-natural-curiosity/185499?camid=4v1a