Chapter 34
Fuzzy Rule-Based Vulnerability Assessment Framework for Web Applications

Hossain Shahriar
Kennesaw State University, USA

Hisham Haddad
Kennesaw State University, USA

ABSTRACT

This paper addresses the problem of assessing risk in web application due to implementation level vulnerabilities. In particular, the authors address the common research challenge of finding enough historical data to compute the probability of vulnerabilities and exploitations. They develop a Fuzzy Logic based System (FLS)[1] to compute the risk uniformly and to address the diversity of risks. The authors propose a set of crisp metrics that are used to define fuzzy sets. They also develop a set of rule-bases to assess the risk level. The proposed FLS can be a useful tool to aid application developers and industry practitioners to assess the risk and plan ahead for employing necessary mitigation approaches. The authors evaluate their proposed approach using three real-world web applications implemented in PHP, and apply it to four types of common vulnerabilities. The initial results indicate that the proposed FLS approach can effectively discover high risk applications.

INTRODUCTION

Most web applications are found to be vulnerable to code injection attacks. Today's software security practitioners are very much aware of a number of vulnerabilities including SQL Injection (SQLI) (OWASP-SQLI, 2015), Cross-Site Scripting (OWASP-XSS, 2015), Remote File Inclusion (RFI) (WASC-RFI, 2010), and Web session (Evans and Shahriar 2014). These vulnerabilities can be exploited by injecting arbitrary database queries (SQLI), JavaScript code (XSS), server script code (RFI), and stealing of session information (e.g., session id has longer lifetime than necessary). The extent of damage due to various

DOI: 10.4018/978-1-5225-3422-8.ch034

kinds of attacks (code injection, remote file inclusion, session hijacking) depends on the payload and may vary widely (e.g., destroying an entire table in SQLI attack, stealing web session in XSS attack (Session Hijacking 2011)). Thus, it is important to address diverse types of vulnerabilities and their consequences in implemented web applications.

A practical approach to deal with code injection vulnerabilities is to assess the risk level (commonly known as risk analysis or assessment) due to the presence of code level vulnerabilities and their potential impact followed by generating further actions to reduce the risk level such as performing penetration testing and deploying IDS (Schaffer, 2012; May *et al.,* 2004). Thus, risk analysis improves application security for all related stakeholders.

This work is motivated by the observation that traditional risk assessment approaches proposed in the literature do not have the capability to estimate the overall risk due to diverse severity level for a given vulnerability (W3af 2015, Sqlifuzzer 2015, Shar & Tan, 2012; SQL-inject-me, 2015; CVSS Scoring System, 2015). Various vulnerability types and their corresponding attack payload types are not accounted for in most of these assessment approaches. Moreover, most of existing frameworks are quantitative. Thus, risk assessment model related parameters need to be known, which may not be practical to assume in real-world. For example, precise value of assets or resources may not be estimated accurately, the likelihood of vulnerability occurrence may not be computed due to the lack of sufficient historical data, and the severity level due to vulnerability exploitation may not be estimated. Another drawback of existing approaches is considering all types of vulnerabilities equally, and their severity level equally. Thus, a suitable framework is needed to assess the risk of an application due to source code level vulnerability along with the possibility of alternate quantitative values to specify the magnitude of vulnerability and severity levels based on attack payloads.

To address these drawbacks, we propose a Fuzzy Logic-based System (FLS) framework to assess the risk due to code injection vulnerabilities present in an application. Fuzzy logic is a suitable computing technique to deal with the case where quantitative values are not present. It operates on subjective variables (linguistics) and provides a rule-based approach to combine subjective variables (Mamdani, 1974).

We define a set of code level metrics to establish the linguistic terms to relate the subjective magnitude and the corresponding impact due to the actual exploitation of vulnerabilities. We also apply nested FLS to combine diverse types of risk to assess a single value to be useful in practice. The proposed framework provides professionals the flexibility to specify the rules that combine the source of vulnerability and attack payload types to identify the severity level based on knowledge. We evaluate the proposed approach with three real-world web applications implemented in PHP and reported to be vulnerable. The evaluation results indicate that vulnerable versions of the applications are more risky than that of the vulnerability-free version for SQL Injection (SQLI), Cross-Site Scripting (XSS), Remote File Inclusion (RFI), and Web session. The results are more meaningful for software professionals for quality assurance compared to traditional black box level scanner tools which do not have the capability of assessing the overall application's risk level.

The rest of the paper is organized as follows: The next section provides an overview of four common web application vulnerabilities (SQLI, XSS, RFI, Web session); risk analysis steps used in this paper. Then we describe related work on risk assessment. The next section presents the proposed FLS risk assessment framework. We then provide the implementation and experimental results in the subsequent section. Finally, we discuss the conclusion and future work.