Chapter 63
A Simple Solution to Prevent Parameter Tampering in Web Applications

Oğuzhan Menemencioğlu
Karabük University, Turkey

İlhami Muharrem Orak
Karabük University, Turkey

ABSTRACT

Business over the internet such as banking and several online services are growing rapidly. Similarly, social media web portals are also getting more and more involved in our daily life. Since these applications are popular and consist of personal and valuable data, they attract malicious attacks to their vulnerable points. The weakness can also be faced in all businesses and institutions that do not care the necessary security steps. The web parameter tampering is one of the major attacks which is based on the modification of parameters. In order to prevent the parameter tampering, a novel and simple mechanism is implemented by verifying the validity. The mechanism is based on a deterministic finite state machine. Beside this static method, the system also has run time validation which leads for the usage of hybrid analysis approach. As an evaluation, performance assessment of the algorithm is done for real time attacks targeting a web site.

INTRODUCTION

Internet becomes essential for connecting companies, service providers and users online to each other. In spite of their wide usage, the web applications have some vulnerabilities. Scripting languages such as PHP, communicate with database using low-level queries as strings API. These languages represent data and code with the strings instead of more sophisticated APIs. Therefore application code can include database queries which takes unchecked user inputs (Wassermann & Su, 2007). Although the most common vulnerability is related to database implementation, there are also some other weak points of

DOI: 10.4018/978-1-5225-3422-8.ch063

the web applications such as cross-site scripting. It will be useful to understand the vulnerabilities and to introduce reliable and effective solution for preventing the attacks.

There are different approaches to detect and prevent tampering attacks. For Structured Query Language Injection Attacks (SQLIAs), a taxonomy was provided by Chung et al. (Chung, Wu, Chen, & Chang, 2012). Figure 1 illustrates their taxonomy. Details of taxonomy and concerned concepts are provided in below. This taxonomy can be considered as general classification of all types of vulnerabilities.

First approach stated in the taxonomy is static analysis. Zhang et al. proposed a method which can be classified as static analysis, to eliminate integrity problems by trying to detect absence of integrity constraint enforcement (Zhang et al., 2011).

Dynamic analysis is another widely proposed approach. Ogheneovo and Asagba used a dynamic method comparing real time user queries with syntactic structure of the queries defined by parse tree (query modification) (Ogheneovo & Asagba, 2013). Chan et al. introduced a dynamic method using machine learning. They discovered associative patterns by using fuzzy logic. They generated and pruned the rules by using Apriori algorithm for validating input values, input field lengths, and SOAP size (Chan, Lee, & Heng, 2013, 2014). On the one hand, Chung et al. proposed a method that checks the queries whether they are legitimate. If queries are not legitimated, then they are processed with vulnerability detectors. They integrated their algorithm with the well-known three vulnerability detectors instead of developing a new detector (Chung et al., 2012). Jang and Choi used regular expression and size of user query result to control inputs (Jang & Choi, 2014). Kim and Lee used support vector machines to classify SQLIAs (Kim & Lee, 2014).

On the other hand, in some studies hybrid methods were proposed by using static analysis and providing dynamic approach with runtime detector. In this respect, Lee et al. decreased the complexity of the algorithm from $O(n^3)$ to $O(n)$ by comparing static SQL queries with dynamically generated queries after removing the attribute values (Lee, Jeong, Yeo, & Moon, 2012). The AMNESIA method proposed

Figure 1. Taxonomy of approaches