SQL Injection Attack Mechanisms and Prevention Techniques

Roshni Chandrashekhar, Manoj Mardithaya, Santhi Thilagam, and Dipankar Saha

Computer Engineering Department
National Institute of Technology Karnataka, Surathkal, India - 575 025
roshnic@ieee.org, mmardithaya@acm.org,
santhi@nitk.ac.in, dipankar10@gmail.com

Abstract. SQL Injection Attacks have been around for over a decade and yet most web applications being deployed today are vulnerable to it. The bottom line is that the web has made it easy for new developers to develop web applications without concerning themselves with the security flaws, and that SQL Injection is thought to be a simple problem with a very simple remedy. To truly bring security to the masses, we propose a classification that not only enumerates but also categorizes the various attack methodologies, and also the testing frameworks and prevention mechanisms. We intend our classification to help understand the state of the art on both sides of the fields to lay the groundwork for all future work in this area.

Keywords: SQL injection.

1 Introduction

SQL injection is a method of hacking in which malformed SQL queries are produced through unsanitized user-input. Though an application can easily prevent SQL injection by validating input, too many avenues for data exchange exist in the current web model and the modes of SQL injection vary broadly. In 2002, the Computer Security Institute and the Federal Bureau of Investigation (United States) conducted a survey that discovered that 60% of online databases are subject to security breaches each year [1]. In particular, SQL Injection attacks have featured at the top of OWASPs (Open Web Application Security Project).

Top Ten Most Critical Web Application Security Risks in both 2007 and 2010 [2]. The first in-depth paper documenting SQL Injection methods was published in January 2002, and new methods and prevention techniques have been proposed every year since [3]. Each new research paper contributes a small treatise towards a literature survey, but no significant classification attempts were made until Halfond, Viegas and Orso [4]. While this paper classifies various attack types by injection mechanism, intent of the attacker and the type, it leaves a classification of evasion techniques out. The classification it does make are also very loosely typed and it does not follow a strict structure of categorization. San-Tsai Sun, Ting Han Wei, Stephen Liu, and Sheung Lau try to address this issue by proposing a more concrete classification model that is mutually exclusive and unambiguous [5]. However, its classification methods of SQL injection are based on Threat Modeling, addressing the

P.S. Thilagam et al. (Eds.): ADCONS 2011, LNCS 7135, pp. 524–533, 2012.

larger issue of where and how SQL injection correlates with security systems at large. But its classification of different Attack, Evasion and Countermeasure Techniques are very insufficient, and does not address the various research proposals that have been made. A final consideration is that no significant literature survey has been done in the last three years. To that end, we propose a classification method for SQL Injection Attacks, Prevention Mechanisms, and Vulnerability Testing Suites, and do so by presenting a taxonomy diagram for each.

2 SQL Injection Attacks

First, we propose a classification for SQL Injection Attacks. Such classifications can be found in [4],[5] and [6]. However, we found many injection methodologies missing or misclassified. We also found a difference in classification between academic papers and industrial white papers. To that end, we propose a more complete classification which is in figure 1.

2.1 Injection Avenues

SQL Injection is a type of vulnerability that derives from the larger class of Application Attacks through malicious input. When concerned with web applications with a focus on SQL injection attacks, we find malicious input to be presented through three main avenues. We have also presented a fourth avenue here for the sake of completion to demonstrate that SQL injection is not a vulnerability restricted to just the web application domain.

2.1.1 Injection through Server Variables

This is the most common type of SQL Injection. Server variables are a collection of variables that defines the HTTP Request, environment, and various other network parameters. These include the two most common form submission methods, GET and POST, as well as other more intricate injection avenues such as HTTP header variables and sessions. The bulk of SQL Injection attempts are made through these server variables, either through entering malicious input into the client-end of the application or by crafting their own request to the server.

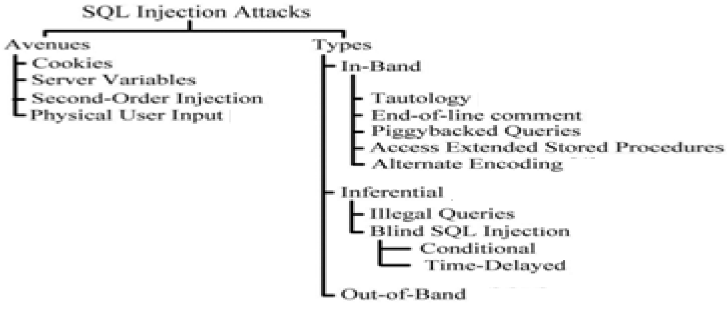

Fig. 1. SQL injection Attack Avenues and Types