ABSTRACT

The widespread adoption of web applications as an instant means of information broadcasting and various other transactions has essentially made them a key component of today's Internet infrastructure. A critical problem facing today's internet community is the increasing number of attacks exploiting flaws found in web applications. SQL Injection Attacks are a class of web application attack that many of these systems are highly vulnerable to, and there is no known fool-proof defense mechanism against such attacks. In this paper, we propose a *technique* that specifically targets input validation vulnerabilities found in SQL queries that may lead to SQL Injection Attacks (SQLIAs). The deployment of this technique automatically detects runtime SQL queries that are found to contain SQL Injection Vulnerabilities and also eliminates the need to modify source code of application scripts, additionally allowing easy integration with currently-deployed systems.

Keywords : SQL Injection, security, web application, input validation, vulnerability, runtime query.