An Approach to Detection of SQL Injection Vulnerabilities Based on Dynamic Query Matching

Abstract

Web is one of the most popular internet services in today’s world. In today’s world, web servers and web based applications are the popular corporate applications and become the targets of the attackers. A Large number of Web applications, especially those deployed for companies to ebusiness operation involve high reliability, efficiency and confidentiality. Such applications are written in script languages like PHP embedded in HTML allowing establish the connection to databases, retrieving data and putting them in WWW site. In order to detect known attacks, misuse detection of web based attacks consists of attack rules and descriptions. Misuse detection considers predefined signatures for intrusion detection. One of the most common in web application attack is SQL Injections. Here an attacker exploits with faulty input strings so that the dynamic queries generate by the web application changes the structure designed by the developer. Thus, the SQL injected query generated becomes maliciously crafted queries. In this paper we have tried to classify the SQL Injection attack based on their vulnerabilities in web applications. We have also reported the approaches and how implemented in recent years by some of the researcher’s in their methodologies for detection and protection of SQL Injection attacks. Our technique of classification has avoided
An Approach to Detection of SQL Injection Vulnerabilities Based on Dynamic Query Matching

the developer’s dependent approaches adopted by the researchers such as – initialization of syntactical rule, valid trusted string database, static or pre generated program code checking etc. Our approach based on dynamic query matching with SQL signature, successfully detected SQL injection vulnerabilities with a very low false positive rate. It is also easy to implement in real-world scenario. SQL signature updates adaptively.

Reference


Index Terms

Computer Science Security
Key words

web  php  sql
injection
classification
DTD