TECHNIQUES FOR PREVENTING SQL ATTACKS AGAINST WEB APPLICATIONS

Dhori Beta

[1"]Fan S. Noli" University of Vlora, Albania, Email: dhoribeta@yahoo.com

Abstract

The SQL thread to the web applications is one of the most crucial and more important problems nowadays. Web application programmers can obviously use different languages of programming in order to create various web applications which interact with one another and are based on a series of data. It is a known fact that most of today's Web applications keep data in databases, since they allow the creation of dynamic websites. Web application accepts input from the user which later are processed by different applications or scripts to generate a Query to the database. Generated query in SQL Language are often not processed correctly as a result of irregular data provided by users and therefore attackers can modify these requests to the database, creating the opportunity to get private and confidential data from the database. Although programmers have different tools to enhance applications security and defense from SQL injection attacks, none of them is perfect and these attacks are still numerous and getting more sophisticated. Between programmers and attackers developed a constant battle. the aim of this article is to mention and describe some of the techniques used in order to provide the privacy of the users' application data making it possible to avoid the possibility of injecting the SQL code in these applicationsin. This article gives some simple and advanced techniques that can be used to give access to important data from database, DoS attacks and get maximum privileges on the database. Also this article give some methods to detect and prevent these attacks on more used databases, SQL Server, Oracle and MySQL.

***Keywords*:** *SQL injection, database, security, web Aplication, attack*