Abstract

SQL injection attacks are often found within the dynamic pages of a web application that exploit the security vulnerability of the database layers of an application. In this attack category a specifically crafted SQL command is entered in the form field of a web application instead of the expected information. SQL injection takes advantages of the design flaws in poorly designed web applications to poison SQL statements and bypass the normal methods of accessing the database content. In these types of Injection attempt the database server execute undesirable SQL Code to steal, manipulate or delete the content of a database. The proposed algorithm is implemented on an application which is placed on a proxy server kept between the Database server and a web server. It is working on multi-level template based approach, which is a model based approach to detect the illegal queries before they are executed on the database server. With the support of the query evaluation engine it can detect and block the injected query. Only the benign query is allowed to get the access to the back end database server. An alert message is generated if there is an Injection.
References

4. Ruse, Michelle, Tanmoy Sarkar, and Samik Basu."Analysis & detection of SQL injection Vulnerabilities via automatic test case generation of programs." Applications and the Internet

Index Terms

Computer Science Information Sciences

Keywords
Vulnerability, Exploit, injection, Benign Query, Detection, Prevention