Abstract

Today’s interconnected computer network is complex and is constantly growing in size. As per OWASP Top10 list 2013[1] the top vulnerability in web application is listed as injection attack. SQL injection[2] is the most dangerous attack among injection attacks. Most of the available techniques provide an incomplete solution. While attacking using SQL injection attacker probably use space, single quotes or double dashes in his input so as to change the indented meaning of the runtime query generated based on these inputs. Stored procedure based and second order SQL injection are two types of SQL injection that are difficult to detect and hence difficult to prevent. This work concentrates on Stored procedure based and second
A Robust Method for Prevention of Second Order and Stored Procedure based SQL Injections

order SQL injection. It uses a Similarity analysis technique to detect injection. The runtime generated query is checked against a query model for similarity analysis and if both are similar then the runtime query is free from injection else query is vulnerable and the further processing of the query is blocked.

References

- https://www.owasp.org/index.php/What_are_web_applications%3F
- http://www-bcf.usc.edu/~halfond/testbed.html
- Lwin Khin Shar and Hee Beng Kuan Tan, Defeating SQL Injection, IEEE Computer Society, March 2013
- Preventing SQL Injections in Online Applications: Study, Recommendations and Java Solution Prototype Based on the SQL DOM. Etienne Janot, Pavol Zavarsky Concordia University College of Alberta, Department of Information Systems Security
- Buehrer, G., Weide, B. W., and Sivilotti, P. A. G. Using parse tree validation to
prevent sql injection attacks. In SEM (2005)

Index Terms

Computer Science  Databases

Keywords

Sql Injection  Web Application  Stored Procedure  Second Order Injection.