Tribhuvan University

Institute of Science and Technology

Blocking SQL Injection in Database Stored Procedures

Dissertation

Submitted to

Central Department of Computer Science and Information Technology

Kirtipur, Kathmandu, Nepal

In partial fulfillment of the requirements

for the Master's Degree in Computer Science and Information Technology

by

Sanu Manandhar

(December, 2010)

Supervisor

Dr. Subarna Shakya

(Associate Professor)

Department of Electronics and

Computer Engineering,

Pulchowk Campus

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Date:___________

Recommendation

I hereby recommend that the dissertation prepared under my supervision by **Mr. Sanu Manandhar** entitled **"Blocking SQL Injection in Database Stored Procedures"** be accepted as fulfilling in part requirements for the degree of masters of science. In my best knowledge this is an original work in computer science.

Dr. Subarna Shakya

Associate Professor
Department of Electronics and Computer Engineering,
Pulchowk Campus,
Institute of Engineering
(Supervisor)

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

We certify that we have read this dissertation work and in our opinion it is satisfactory in the scope and quality as a dissertation in the partial fulfillment for the requirement of Master of Science in Computer Science and Information Technology.

Evaluation Committee

Prof. Dr. Jeevan Jyoti Nakarmi
Act. Head, Central Department of Computer Science and Information Technology
Tribhuvan University

Dr. Subarna Shakya
Associate Professor
Department of Electronics and Computer Engineering,
Pulchowk Campus, IOE
(Supervisor)

(External Examiner)

(Internal Examiner)

Date: _______________

ABSTRACT

Web application is described as an application accessible by the web through a network. SQL injection is an attack method used by hackers to retrieve, manipulate, fabricate or delete information in organizations' relational databases through web applications. Information processed by web applications has become critical to corporations, customers, organizations, and countries.

Several research papers in literature have proposed ways to prevent SQL injection attacks in the application layer by examining dynamic SQL query semantics at runtime. However, very little emphasis is laid on securing stored procedures which could also suffer from SQL injection attacks. Some research papers in literature even refer to stored procedures as a remedy against SQL injection attacks. As stored procedures reside on the database front, the methods proposed by them cannot be applied to secure stored procedures themselves.

In this research paper, we propose a technique to defend against the attacks targeted at stored procedures.

ACKNOWLEDGEMENT

This dissertation would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this study.

I am heartily thankful to my supervisor, **Associate Professor Dr. Subarna Shakya** , whose encouragement, guidance and support from the initial to the final level enabled me to develop and understanding of the subject. I want to thank my co-supervisor **Mr. Jagdish Bhatta** for giving me continuous support, inspiration and guidance throughout the study period of my thesis work. I am grateful to Dr. Shashidhar Ram Joshi, Mr. Min Bahadur Khati of Central Department of Computer Science and Information Technology who, while not being directly involved in my thesis work, nevertheless influenced me greatly.

Many thanks go to my friends Mr. Madhav Dhakal, Mr. Sachin Kumar Shrestha and Mr. Rajesh Gurubacharya for their interest, cooperation, worries and complain.

Lastly, I offer my regards and blessings to all of those who supported me in any respect during the completion of the project.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

SQL	Structured Query Language
SQLIA’s	SQL-Injection Attacks
SP	Stored Procedure
API	Application Program Interfaces
RDBMS	Relational Database Management System
DML	Data Manipulation Language
DDL	Data Definition Language
HTML	HyperText Markup Language
ID	Intrusion Detection