Tribhuvan University
Institute of Science and Technology

Analysis and Prevention of SQL Injection Attacks

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
Ram Kumar Bhandari
Deccember, 2011

Supervisor
Prof. Dr. Shashidhar Ram Joshi

Department of Electronics and Computer Engineering
Institute of Engineering, Pulchowk, Nepal
(Head)

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Student's Declaration

I hereby declare that I am the only author of this work and that no sources other than the listed here have been used in this work.

……………………………..
Ram Kumar Bhandari
Date: December, 2011

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Supervisor's Recommendation

I hereby recommend that the dissertation prepared under my supervision by **Mr. Ram Kumar Bhandari** entitled **"Analysis and Prevention of SQL Injection Attacks"** be accepted as fulfilling in partial requirements for the degree of M. Sc. in Computer Science and Information Technology.

Prof. Dr. Shashidhar Ram Joshi
Department of Electronics and Computer Engineering,
Institute Of Engineering, Pulchowk, Nepal
(Head)

Tribhuvan University
Institute of Science and Technology

Central Department of Computer Science and Information Technology

LETTER OF APPROVAL

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

____
Dr. Tanka Nath Dhamala
Head, Central Department of Computer
Science and Information Technology
Tribhuvan University

____
Prof. Dr. Shashidhar Ram Joshi
Head,Department of Electronics and Computer
Engineering, Institute of Engineering
Pulchowk, Nepal (Supervisor)

____
(External Examiner)

____
(Internal Examiner)

Date: _____________

Acknowledgement

I would like to express my sincere thanks to my thesis supervisor **Prof. Dr. Shashidhar Ram Joshi** for his valuable suggestions, motivation, support, guidance and care throughout the research and the study.

I would also like to thank all the members of the research committee for their help for the construction of the background ideas required for the research. Special thanks go to **Prof. Dr. Shashidhar Ram Joshi**, **Prof. Dr. Subarna Shakya** and head of the department **Prof. Dr. Tanka Nath Dhamala** for their kind support and encouragement.

Thanks to my classmates of M.SC Computer Science and Information Technology 2006 batch of Central Department of Computer Science and Information Technology and my colleagues **Bikash Balami** and **Shailendra Pradhan** for their encouragements and help in my research work. Last but not the least, I would like to express my deep gratitude to the management and administration committee of CDCSIT, for providing access to the good integration of intellectual properties, technical support and facilities.

ABSTRACT

With the increasing trend of use of web services, the challenges about database security has also been increased consequently. Database security is one of the most essential factors in keeping stored information safe. These days, web applications are used widely as a meddler between computer users. Web applications are also used mostly by e-commerce companies, and these types of applications need a secured database in order to keep sensitive and confidential information. Since SQL injection attacks occurred as a new way of accessing database through the application rather than directly through the database itself, they have become popular among hackers and malicious users.

We focus our research on SQLIA as most web applications are vulnerable to them. A novel technique to counter SQL injection has been proposed, which combines conservative static analysis and runtime monitoring to detect and stop illegal queries before they are executed on the database. In the static part, the technique builds a conservative model of the data structure of the legitimate queries that could be generated by the application. In its dynamic part, the technique inspects the dynamically generated queries for compliance with the statically- build model. Even for fast searching we use the concept of linked list and doubly linked list hash function. If the incoming query resembles with the valid query structures, they should be allowed for execution otherwise they are prevented from execution on the database server

Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ASP	Active Server Pages
CSS	Cross-site Scripting Attack
CVE	Common Vulnerabilities and Exposures
DBMS	Database Management System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
H/W	Hardware
JSP	Java Server Page
OWASP	Open Web Application Security Project
URL	Uniform Resource Locator
SQL	Structured Query language
SQLIA	Structured Query language Injection Attack
RDBMS	Relational Database Management System
IDS	Intrusion Detection System
PL/SQL	Procedural Language/Structured Query Language