Prevention of Web Application Against SQL-Injection Attack

Dissertation

Submitted To

Central Department of Computer Science and Information Technology

Institute of Science and Technology

Tribhuvan University

In Partial Fulfillment of the Requirements for the Degree of

Master of Science

In

Computer Science and Information Technology

By

Madhav Dhakal

March, 2008

Kirtipur, Nepal

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Date:

LETTER OF RECOMMENDATION

Mr. ***Madhav Dhakal*** has carried out this thesis work entitle **“PREVENTION OF WEB APPLICATION AGAINST SQL-INJECTION ATTACK”** under my supervision and guidance. In my best knowledge this thesis successfully completed which fulfills the requirements for the aware of the Degree of Master’s in Computer Science and Information Technology, therefore I recommended for further evaluation.

. . . . .

Asso. Prof .Dr. Subarna Shakya
Department of Electronics and Computer Engineering
Pulchowk Campus, Pulchowk
(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 as the partial fulfillment of the requirement of Master of Computer Science and Information Technology from Tribhuvan University, Nepal.

Evaluation Committee

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

Asso. Prof. Dr. Subarna Shakya
Department of Electronics and
Computer Engineering
Pulchowk Campus, Pulchowk
(Supervisor)

(External Examiner)

(Internal Examiner)

Date:

Acknowledgements

This thesis work would not exist without help, advice and encouragement of many people. I thank my supervisor, Associate Professor Dr. Subarna Shakya, who taught me much about teaching and research methodology. His broad theoretical knowledge and idea has always brought a breath of fresh air during the most challenging of time.

I am grateful to the professors and lecturer, Prof. Dr. Devi Dutta Paudyal, Prof. Dr. Shashidhar Ram Joshi, Prof. Dr. Onkar Pd. Sharma, Mr. Arun Timilsina, Mr. Sudarshan Karanjit, Mr. Min Bhadur Khati, Mr. Samujjwal Bhandari, Mr. Bishnu Gautam and Mr. Hemanta B.C of Central Department of Computer Science and Information Technology who, while not being directly involved in my thesis work, nevertheless influenced me greatly. I want to thank my co-supervisor Mr. Dinesh Bajracharya for giving me continuous support, inspiration and guidance throughout the study period of my thesis work.

Many thanks go to my colleagues, who helped me directly or indirectly to accomplish my work. I am especially grateful to Dr. Tanka Nath Dhamala, Head, Central Department of Computer Science and Information Technology, has also been a positive and encouraging influence on my research efforts.

I am also indebted to my friends Mr. Nischal Regmi, Mr. Sanu Manandhar, Mr. Bishnu Pd. Pandey, Mr. Kamal Raj Sharma, Mr. Rabin Shrestha and brother Mr. Prakash Dhakal for their interest, cooperation, worries and complain.

Finally, I thank to my parents, who were ultimately the people, who prepared me for this endeavour. I own you all my success.

Madhav Dhakal

madhavdhakal25@gmail.com

Abstract

Web applications are accessed using internet and so face risks associated with usage of internet. There are numerous attacking techniques in the database of web applications, one of them simplest technique is the SQL Injection technique. SQL Injection is an attacking method used by the hackers to retrieve, manipulation, fabricate or delete information in organization's relational database through web applications. Information in the database mainly constitutes an organization's most important information and attacks on it could threaten the organization's confidentiality, availability, integrity and so on. It is a simple and required database and server- script language knowledge but no special tool or experience

In this thesis work, we study the different attacking techniques through SQL Injection and it applies to popular Internet Information Server Page/ASP.NET/SQL Server Platform. We discuss some ways in which attacker can inject the SQL-code in to the database of web application and then addresses some of the prevention techniques with our own prevention method i.e. transition table validation method, which is related to them with the validation. Similarly, we also found that execution time taken by guarded statement is comparatively greater than the execution time taken by normal statement.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

SQL	Structured Query Language
SQLIAs	SQL –Injection Attacks
RDBMS	Relational Database Management System
SSL	Secure Socket Layer
IDS	Intrusion Detection System
AMNESIA	Analysis and Monitoring for NEutralizing SQL-Injection Attacks
WebSSARI	Web application Security by Static Analysis and Runtime Inspection
DFA	Deterministic Finite Automata
ASP	Active Server Page