PREVENTING MS SQL INJECTION IN WEB APPLICATION

Aqeel Sahi Khader

Universiti Utara Malaysia 2010
PREVENTING MS SQL INJECTION IN WEB APPLICATION

A project submitted to Dean of Postgraduate Studies and Research in partial
Fulfillment of the requirement for the degree
Master of Science of Information Technology
University Utara Malaysia

By
Aqeel Sahi Khader
KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertanda tangan, memperakuan bahawa
(I, the undersigned, certifies that)

AQEEQ SAHI KHADER
(802802)

calon untuk ijazah
(candidate for the degree of) MSc. [Information Technology]

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project of the following title)

PREVENTING MS SQL INJECTION IN WEB APPLICATION

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan
dan meliputi bidang ilmu dengan memuaskan.
(that this project is in acceptable form and content, and that a satisfactory
knowledge of the field is covered by the project).

Nama Penyelia
(Name of Supervisor) : ASSOC. PROF. ABDUL BASHAH MAT ALI

Tandatangan
(Signature) : [Signature] Tarikh (Date) : 17/10/2010

Nama Penilai
(Name of Evaluator) : MR. MOHD TARMIZI MUSA

Tandatangan
(Signature) : [Signature] Tarikh (Date) : 17/10/2010
PERMISSION TO USE

In presenting this project in partial fulfillment of the requirements for a postgraduate degree from University Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this project in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of Postgraduate Studies and Research. It is understood that any copying or publication or use of this project or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to University Utara Malaysia for any scholarly use which may be made of any material from my project.

Requests for permission to copy or to make other use of materials in this project, in whole or in part, should be addressed to

Dean of Postgraduate Studies and Research

College of Arts and Sciences

Universiti Utara Malaysia

06010 UUM Sintok

Kedah Darul Aman

Malaysia

ii
ABSTRACT

A security threat on the Internet is one of the biggest challenges in this time with the great advances in techniques used for attacks. One of the easiest and most serious of these attacks is the MS SQL injection attacks that have come to represent a serious threat to any site or application that contains a database. These attacks could allow an attacker to obtain sensitive information and the value of databases. A method of this attack is easy to learn and the damage caused ranging from reasonable to the detriment of the whole system. Regardless of the damage there are a lot of applications on the Internet vulnerable to this attack. Using some ways can prevent such attacks completely. In this research I will focus on the coding to protect the website from the MS SQL injection attacks by design system to give some information about how to attack using SQL injection and also given the solution for this attack by giving a secure login codes.
ACKNOWLEDGEMENT

By the Name of Allah, the Most Gracious and the Most Merciful

First of all, I would like to thank Allah, for having made everything possible by giving me strength and courage to do this work.

First, I would like to thank to my supervisor of this project, Assoc Prof. Madya Abdal Bashah Mat Ali for the valuable guidance and advice. He inspired me greatly to work in this project. His willingness to motivate me contributed tremendously to my project.

Besides, I would like to thank the authority of University Utara Malaysia (UUM) for providing me with a good environment and facilities to complete this project.

An honorable mention goes to my family, especially my mother and friends for their understandings and supports on me in completing this project, as well as all lecturers at the faculty of Information Technology, that they gave me all the information for completing the requirements of this study, especially my evaluator Mr. Mohd Tarmizi Musa is due to his advice. Without helps of the particular that mentioned above, I would face many difficulties while doing this project. Finally, I want to dedicate this research to my mother in the first and also to my niece (Yaqeen (يقيقه)).
# Table of Contents

PERMISSION TO USE ........................................................................................................... ii
ABSTRACT ............................................................................................................................. iii
ACKNOWLEDGEMENT........................................................................................................ iv
Table of Contents ...................................................................................................................... v
LIST OF TABLES ..................................................................................................................... vii
LIST OF FIGURES ................................................................................................................... viii

CHAPTER ONE: INTRODUCTION

1.1 INTRODUCTION ................................................................................................................ 1
1.2 PROBLEM STATEMENT .................................................................................................... 6
1.3 RESEARCH QUESTIONS .................................................................................................... 7
1.4 RESEARCH OBJECTIVES ............................................................................................... 7
1.5 SCOPE AND CONSTRAINT .............................................................................................. 8
1.6 RESEARCH SIGNIFICANCE .............................................................................................. 8
1.8 SUMMARY ....................................................................................................................... 9

CHAPTER TWO: LITERATURE REVIEW

2.1 MS SQL INJECTION ......................................................................................................... 10
2.2 DATABASE SECURITY ..................................................................................................... 15
2.3 WEB SECURITY ............................................................................................................... 17
2.4 SOFTWARE GAPS .......................................................................................................... 21
2.5 SUMMARY ....................................................................................................................... 24

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 DESIGN RESEARCH METHODOLOGY ......................................................................... 25
3.1.1 Awareness of Problem ............................................................................................... 27
3.1.2 Suggestion .................................................................................................................. 28
3.1.3 Development ............................................................................................................. 28
3.1.4 Evaluation .................................................................................................................. 28
3.1.5 Conclusion ............................................................................................................... 29
List of Tables

Table 3.1: Mapping between research objects and research methods ........................................ 27
Table 4.1: Functional requirements ......................................................................................... 31
Table 4.2: Nonfunctional requirements ................................................................................... 33
Table 4.3: Manager Table ....................................................................................................... 49
Table 4.4: Book Table ........................................................................................................... 50
Table 4.5: Discussion Table .................................................................................................... 50
Table 4.6: development environment ....................................................................................... 51
Table 4.7: Secure login test case ............................................................................................ 66
Table 4.8: Insecure login test case .......................................................................................... 69
List of Figures

Figure 1.1 MS SQL injection forms ................................................................. 1
Figure 1.2 Normal accesses to the web application (Cerrudo, 2007) .................. 3
Figure 1.3 SQL injection access the server (Cerrudo, 2007) ........................ 5

Figure 2.1 High-level overview of AMNESIA (Halfond, W., & Orso, A. 2006) .... 12
Figure 2.2 High-level overview of the approach and tool (Halfond, W., Orso, A., & Manolios, P. 2006) .......................................................... 13
Figure 2.3: Augmented Attack Tree Modeling of SQL Injection Attacks (Wang, J., Raphael, C., Whitley, J., & Parish, D, 2010) .......................... 14
Figure 2.4 AOP Based mechanism (Anchlia, A., & Jain, S. 2010) .................. 15
Figure 2.5: Testing model (Haixia, Y., & Zhihong, 2009) .............................. 17
Figure 2.6: Example of interaction between user and a typical web application (Halfond, W., & Orso, A. 2005) ......................................................... 18
Figure 2.7: Combinatorial Approach for Preventing SQL Injection Attacks (Ezumalai, R., & Aghila, G, 2009) ......................................................... 20
Figure 2.8: Correlation process (Ficco, M., Coppolino, L., Romano, L., Detection, K., Attacks, K., & Detection, K. 2009) ................................. 21
Figure 2.9: Experimental tested (Chen, T., & Buford, J. 2009) ..................... 23
Figure 2.10: Populating and loading the SQL injection honeypot (Chen, T., & Buford, J. 2009) ................................................................. 24
Figure 3.1: The General methodology of design research (Vaishnavi & Kuechler, 2006) ................................................................. 26

Figure 4.1: Use case diagram for SQLIPS ..................................................... 35
Figure 4.2: Home page sequence diagram .................................................. 36
Figure 4.3: Home page collaboration diagram ............................................ 36
Figure 4.4: Secure login sequence diagram ................................................ 37
Figure 4.5: Secure login collaboration diagram ......................................... 38
Figure 4.6: Insecure login sequence diagram ................................................. 39
Figure 4.7: Insecure login collaboration diagram .......................................... 40
Figure 4.8: Manage sensitive data sequence diagram .................................... 41
Figure 4.9: Manage sensitive data collaboration diagram ............................. 42
Figure 4.10: Service page sequence diagram ............................................... 43
Figure 4.11: Service page collaboration diagram .......................................... 43
Figure 4.12: Discussion page sequence diagram ........................................... 44
Figure 4.13: Discussion page collaboration diagram ...................................... 45
Figure 4.14: About page sequence diagram .................................................. 45
Figure 4.15: About page collaboration diagram ............................................. 46
Figure 4.16: Logout sequence diagram ......................................................... 46
Figure 4.17: Logout collaboration diagram .................................................... 47
Figure 4.18: Class diagram ........................................................................... 48
Figure 4.19: Home page .............................................................................. 52
Figure 4.20: Login page ............................................................................... 53
Figure 4.21: Add new connection ................................................................. 54
Figure 4.22: Insecure login page ................................................................. 56
Figure 4.23: Secure login page ..................................................................... 60
Figure 4.24: Secure login message .............................................................. 60
Figure 4.25: Manage sensitive data page ...................................................... 61
Figure 4.26: Service page ........................................................................... 62
Figure 4.27: Discussion page ....................................................................... 63
Figure 4.28: About and contact page ............................................................ 64
CHAPTER ONE

INTRODUCTION

This chapter presents the introduction of the study, the problem statement, the research question, the objective of study, the significance of study, and scope of the study.

1.1 INTRODUCTION

Today, most web application provides with high security technology. Unfortunately, this web application can be attacked by hackers whom try to disturb their organization. From the literature review that we find, SQL injection is types of security attack, which attack web applications that are using database services. There are three forms of MS SQL injection as shown below:

![MS SQL injection forms]

Figure 1.1: MS SQL injection forms
The contents of the thesis is for internal user only
REFERENCES


presented at the IEEE International Conference on Services Computing, 2009, Bangalore.


the 2010 ICSE Workshop on Software Engineering for Secure Systems (pp. 43-49). Cape Town, South Africa: ACM.


IIITNG '09. Sixth International Conference on Information Technology: New
Generations, 2009 (pp. 1411-1414). Las Vegas, NV.

Distribution Models in the Detection of SQL Injection Attacks. In ARES 08.
Third International Conference on Availability, Reliability and Security, 2008
(pp. 47-55). Barcelona.

of SQL Injection and cross-site scripting attacks. In ICSE 2009. IEEE 31st
International Conference on Software Engineering, 2009 (pp. 199-209).
Vancouver, BC.

Sania: Syntactic and Semantic Analysis for Automated Testing against SQL
Applications Conference, 2007 (pp. 107-117). Miami Beach, Fl.

Prevention Techniques Against SQL Injection. Availability, Reliability and
Security, (pp. 50-59).

Advanced SQL Injection. In CIT '06. The Sixth IEEE International Conference

architecture towards preventing SQL injection attacks. In Proceedings of the


