# 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 bertandatangan, memperakukan bahawa
*(I, the undersigned, certifies that)*

**AQEEL 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)* : _____ Tarikh (Date) : 17/10/2010

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

Tandatangan
*(Signature)* : _____ Tarikh (Date) : 17/10/2010

over

## 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

## 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

بسم الله الرحمن الرحيم

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 Abdul 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 (يقين)).

# Table of Contents

# List of Tables

# List of Figures

# 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:

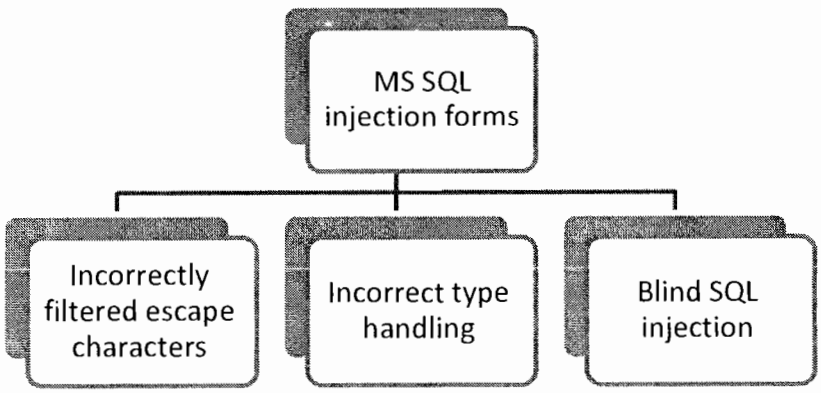


Figure 1.1: MS SQL injection forms

The contents of the thesis is for internal user only

## REFERENCES


Alfantookh, A. (2010). *An automated universal server level solution for SQL injection security flaw.* Paper presented at the Proceedings of the 2004 International Conference on Electrical, Electronic and Computer Engineering (ICEEC'04), Riyadh, Saudi Arabia.

Amirtahmasebi, K., Jalalinia, S. R., & Khadem, S. (2010). *A survey of SQL injection defense mechanisms.* Paper presented at the Internet Technology and Secured Transactions, 2009. ICITST 2009, London, England.

Anchlia, A., & Jain, S. (2010). *A Novel Injection Aware Approach for the Testing of Database Applications.* Paper presented at the Information, Telecommunication and Computing (ITC), 2010, Kochi, Kerala.

Anley, C. (2002). *Advanced SQL injection in SQL Server applications.* Sutton, England: Next Generation Security Software Ltd.

Antunes, N., & Vieira, M. (2009). *Comparing the Effectiveness of Penetration Testing and Static Code Analysis on the Detection of SQL Injection Vulnerabilities in Web Services.* Paper presented at the PRDC '09. 15th IEEE Pacific Rim International Symposium on Dependable Computing, 2009, Shanghai.

Antunes, N., & Vieira, M. (2009). *Detecting SQL Injection Vulnerabilities in Web Services.* Paper presented at the LADC '09. Fourth Latin-American Symposium on Dependable Computing, 2009, Joao Pessoa.

Antunes, N., Laranjeiro, N., Vieira, M., & Madeira, H. (2009). *Effective Detection of SQL/XPath Injection Vulnerabilities in Web Services.* SCC '09. Paper

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

Asmawi, A., Sidek, Z. M., & Razak, S. A. (2008). *System architecture for SQL injection and insider misuse detection system for DBMS.* Paper presented at the ITSim 2008. International Symposium on Information Technology, 2008, Kuala Lumpur, Malaysia.

Bertino, E., Kamra, A., & Early, J. P. (2007). *Profiling Database Application to Detect SQL Injection Attacks.* Paper presented at the IEEE International Performance, Computing, and Communications Conference, 2007. IPCCC 2007, New Orleans, LA, USA.

Buehrer, G., Weide, B. W., & Sivilotti, P. A. G. (2005). Using parse tree validation to prevent SQL injection attacks. *Proceedings of the 5th international workshop on Software engineering and middleware* (pp. 106-113). Lisbon, Portugal: ACM.

Cerrudo, C. (2007). Manipulating microsoft sql server using sql injection. *Application Security Inc*, Retrieved 20-July-2010 from, URL http://www.appsecinc.com/presentations/Manipulating_SQL_Server_Using_SQL_Injection.pdf, Accessed, 7.

Chen, T. M., & Buford, J. (2009). *Design considerations for a honeypot for SQL injection Attacks.* LCN 2009. Paper presented at the IEEE 34th Conference on Local Computer Networks, 2009, Zurich.

Ciampa, A., Visaggio, C. A., & Penta, M. D. (2010). A heuristic-based approach for detecting SQL-injection vulnerabilities in web applications. In *Proceedings of*

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

Desmet, L., Piessens, F., Joosen, W., & Verbaeten, P. (2006). Bridging the gap between web application firewalls and web applications. In *Proceedings of the fourth ACM workshop on Formal methods in security* (pp. 67-77). Alexandria, Virginia, USA: ACM.

Dysart, F., & Sherriff, M. (2008). *Automated Fix Generator for SQL Injection Attacks.* Paper presented at the ISSRE 2008. 19th International Symposium on Software Reliability Engineering, 2008, Seattle, WA.

Ezumalai, R., & Aghila, G. (2009). *Combinatorial Approach for Preventing SQL Injection Attacks.* IACC 2009. Paper presented at the IEEE International Advance Computing Conference, 2009, Patiala.

Ficco, M., Coppolino, L., & Romano, L. (2009). *A Weight-Based Symptom Correlation Approach to SQL Injection Attacks.* Paper presented at the LADC '09. Fourth Latin-American Symposium on Dependable Computing, 2009, Joao Pessoa.

Fonseca, J., Vieira, M., & Madeira, H. (2007). *Testing and Comparing Web Vulnerability Scanning Tools for SQL Injection and XSS Attacks.* PRDC 2007. Paper presented at the 13th Pacific Rim International Symposium on Dependable Computing, 2007, Melbourne, Qld.

Fu, X., Lu, X., Peltsverger, B., Chen, S., Qian, K., & Tao, L. (2007). A Static Analysis Framework For Detecting SQL Injection Vulnerabilities. In

*Proceedings of the 31st Annual International Computer Software and Applications Conference - Volume 01* (pp. 87-96): IEEE Computer Society.

Guimarães, B. (2009). *Advanced SQL injection to operating system full control.* Abu Dhabi: Black hat.

Haixia, Y., & Zhihong, N. (2009). A database security testing scheme of web application. In *ICCSE '09. 4th International Conference on Computer Science & Education, 2009* (pp. 953-955). Nanning.

Halfond, W. G. J., & Orso, A. (2005). Combining static analysis and runtime monitoring to counter SQL-injection attacks. In *Proceedings of the third international workshop on Dynamic analysis* (pp. 1-7). St. Louis, Missouri: ACM.

Halfond, W. G. J., & Orso, A. (2006). Preventing SQL injection attacks using AMNESIA. In *Proceedings of the 28th international conference on Software engineering* (pp. 795-798). Shanghai, China: ACM.

Halfond, W. G. J., Orso, A., & Manolios, P. (2006). Using positive tainting and syntax-aware evaluation to counter SQL injection attacks. In *Proceedings of the 14th ACM SIGSOFT international symposium on Foundations of software engineering* (pp. 175-185). Portland, Oregon, USA: ACM.

Halfond, W., Viegas, J., & Orso, A. (2006). A classification of SQL-injection attacks and countermeasures. In *Int'l Symp. on Secure Software Engineering* (pp. 87-122). New Jersey, USA: Citeseer.

Holz, T., Marechal, S., & Raynal, F. (2006). New threats and attacks on the world wide web. *IEEE Security & Privacy,* 4(2), (pp. 72-75).

Junjin, M. (2009). An Approach for SQL Injection Vulnerability Detection. In *IITNG '09. Sixth International Conference on Information Technology: New Generations, 2009* (pp. 1411-1414). Las Vegas, NV.

Kiani, M., Clark, A., & Mohay, G. (2008). Evaluation of Anomaly Based Character 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.

Kieyzun, A., Guo, P. J., Jayaraman, K., & Ernst, M. D. (2009). Automatic creation of SQL Injection and cross-site scripting attacks. In *ICSE 2009. IEEE 31st International Conference on Software Engineering, 2009* (pp. 199-209). Vancouver, BC.

Kosuga, Y., Kernel, K., Hanaoka, M., Hishiyama, M., & Takahama, Y. (2007). Sania: Syntactic and Semantic Analysis for Automated Testing against SQL Injection. In *ACSAC 2007. Twenty-Third Annual Computer Security Applications Conference, 2007* (pp. 107-117). Miami Beach, FL.

Landsmann, U., & Stromberg, D. (2003). Web Application Security: A Survey of Prevention Techniques Against SQL Injection. *Availability, Reliability and Security,* (pp. 50-59).

Lin, J.-C., & Chen, J.-M. (2006). Protecting Web Sites from Automated and Advanced SQL Injection. In *CIT '06. The Sixth IEEE International Conference on Computer and Information Technology, 2006* (pp. 164). Seoul.

Liu, A., Yuan, Y., Wijesekera, D., & Stavrou, A. (2009). SQLProb: a proxy-based architecture towards preventing SQL injection attacks. In *Proceedings of the*

*2009 ACM symposium on Applied Computing* (pp. 2054-2061). Honolulu, Hawaii: ACM.

Madan, S. (2009). Shielding against SQL Injection Attacks Using ADMIRE Model. In *CICSYN '09. First International Conference on Computational Intelligence, Communication Systems and Networks, 2009* (pp. 314-320). Indore.

Madan, S. (2010). Security Standards Perspective to Fortify Web Database Applications from Code Injection Attacks. In *ISMS, 2010 International Conference on Intelligent Systems, Modelling and Simulation* (pp. 226-230). Liverpool.

Maor, O., & Shulman, A. (2009). Blindfolded SQL injection. *Imperva*. Retrieved on 9 July 2010, from http://www. imperva. com/download. asp.

Maor, O., & Shulman, A. (2009). Top Ten Database Security Threats. *Imperva*. Retrieved on 9 July 2010, from http://www. imperva. com/download. asp.

Mattsson, U., & Green, O. (2008). Enterprise Application Security-How to Balance the Use of Code Reviews and Web Application Firewalls for PCI Compliance. *Availability, Reliability and Security,* (pp. 67-75).

Merlo, E., Letarte, D., & Antoniol, G. (2006). Insider and Ousider Threat-Sensitive SQL Injection Vulnerability Analysis in PHP. In *WCRE '06. 13th Working Conference on Reverse Engineering, 2006* (pp. 147-156). Benevento.

Merlo, E., Letarte, D., & Antoniol, G. (2007). Automated Protection of PHP Applications Against SQL-injection Attacks. In *CSMR '07. 11th European Conference on Software Maintenance and Reengineering, 2007* (pp. 191-202). Amsterdam.

Merlo, E., Letarte, D., & Antoniol, G. (2007). SQL-Injection Security Evolution Analysis in PHP. In *WSE 2007. 9th IEEE International Workshop on Web Site Evolution, 2007* (pp. 45-49). Paris.

Metatron security services Ltd. (2009). *Imperva SecureSphere 6 Security Target.* Modiin, Canda: Imperva Inc.

Muthuprasanna, M., Wei, K., & Kothari, S. (2006). Eliminating SQL Injection Attacks - A Transparent Defense Mechanism. In *WSE '06. Eighth IEEE International Symposium on Web Site Evolution, 2006* (pp. 22-32). Philadelphia, PA.

Rietta, F. S. (2006). Application layer intrusion detection for SQL injection. In *Proceedings of the 44th annual Southeast regional conference* (pp. 531-536). Melbourne, Florida: ACM.

Schwartau, W. (2001). *The History and Evolution of Intrusion Detection.* New York, USA: SANS

Shahriar, H., & Zulkernine, M. (2008). MUSIC: Mutation-based SQL Injection Vulnerability Checking. In *Proceedings of the 2008 The Eighth International Conference on Quality Software* (pp. 77-86): IEEE Computer Society.

Shanmughaneethi, S. V., Shyni, S. C. E., & Swamynathan, S. (2009). SBSQLID: Securing Web Applications with Service Based SQL Injection Detection. In *Proceedings of the 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies* (pp. 702-704): IEEE Computer Society.

Su, Z., & Wassermann, G. (2006). *The essence of command injection attacks in web applications.* Paper presented at the ACM SIGPLAN-SIGACT symposium on Principles of programming languages, Charleston, South Carolina, USA.

Vaishnavi V & Kuechler B (2004). Design Research in information system . *Auerbach Publication.* Retrieved 7-July-2010, from http://www.isworld.org/Researchdesign/drisISworld.htm.

Valli, C. (2006). SQL Injection-Threats to Medical Systems; Issues and Countermeasures. *Paper presented at the 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing-SAM.*

Wang, J., Phan, R. C.-W., Whitley, J. N., & Parish, D. J. (2010). Augmented attack tree modeling of SQL injection attacks. In *ICIME, 2010 The 2nd IEEE International Conference on Information Management and Engineering* (pp. 182-186). Chengdu.

Wei, K., Muthuprasanna, M., & Kothari, S. (2006). Preventing SQL injection attacks in stored procedures. In *Software Engineering Conference, 2006. Australian* (pp. 8).

Zhang, Q., & Wang, X. (2009). SQL Injections through Back-End of RFID System. In *CNMT 2009. International Symposium on Computer Network and Multimedia Technology, 2009* (pp. 1-4). Wuhan.