

Universiti Teknologi MARA

**SQL INJECTION: COMPARISON OF
PREVENTION STRATEGIES FOR PHP**

MOHD FAIRUZ BIN ABDUL JALIL

2005616484

Thesis submitted in fulfillment of the requirements for
Bachelor of Science (Hons) Information System Engineering
Faculty of Information Technology And
Quantitative Science

MAY 2008

ACKNOWLEDGEMENT

In the name of Allah, the Most Merciful and the Most Compassionate.

Alhamdulillah and peace upon Prophet Muhammad S.A.W., this thesis is finally finished according to time and objectives required.

This study would not have been possible without the assistance and support from those who guided the author in his course of graduate work. First, the author would like to thank Allah SWT for His grace and mercy throughout this research. It is by His hands and wisdom in guiding the author to finish his work within the study.

The author would like to extend his thanks to honorable supervisor, Cik Ruhaila Bte Maskat, for academic guidance, support, encouragement, and help during the study. Furthermore, the author would like to specially thank her for patience and tolerance, in which her diligence, dedication and working attitudes are good examples to the author.

And the most thanks to my family for their encouragement in finishing this course gloriously. Last but not least, for my friends who have given advices and suggestions to make this thesis achieves it goals.

Thanks.

TABLE OF CONTENTS

<i>CONTENT</i>	<i>PAGE</i>
DECLARATION	ii
APPROVAL	iii
ACKNOWLEDGEMENT	iv
TABLE OF CONTENTS	v
LIST OF FIGURES	viii
ABSTRACT	ix
CHAPTER ONE: INTRODUCTION	1
1.1 Background	1
1.2 Problem Statements	2
1.3 Research Objectives	4
1.4 Research Scope	3
1.5 Research Significance	4
CHAPTER TWO: Literature Review	6
2.1 Introduction	6
2.2 Threats vulnerabilities and attacks	6
2.3 Application Vulnerability Categories	7
2.4 Core Security Principles	8
2.5 SQL injection	10
2.5.1 Objectives of SQL injection	12
2.5.2 Steps in executing SQL Injection	12
2.5.3 Impacts of SQL injections	14
2.5.4 Avoiding SQL injection from occurring	14
2.6 PHP (Hypertext Processor)	16

2.6.1	A built -in function in PHP	17
2.6.1.1	Magic Quotes	17
2.6.1.2	SQL Error Handling	19
2.7	MySQL	20
CHAPTER THREE:		
RESEARCH APPROACH AND METHODOLOGY		24
3.1	Introduction	24
3.2	Research Approach	24
3.3	Problem Assessment & Research Study	25
3.4	Knowledge Acquisition	25
3.5	Data Analysis	25
3.6	Determine frameworks	25
3.7	Frameworks analysis	27
3.8	Finding	27
CHAPTER FOUR: RESULTS AND FINDINGS		28
4.1	The weakness of website which lead SQL injection Vulnerable	28
4.2	SQL Prevention Strategies	30
4.3	Applying selected malicious code into framework been chosen	36
4.4	Identify which framework have applied SQL injections prevention strategies.	48
4.4.1	Input Validation	48
4.4.2	Minimal error message	50

ABSTRACT

Since 2002, over 10% of total cyber vulnerabilities were SQL injection vulnerabilities. Since most developers are not experienced software security practitioners, a solution for correctly fixing SQL injection vulnerabilities that does not require security expertise is desirable. By using SQL injection attacks, an attacker could thus obtain and/or modify confidential/sensitive information. SQL injection attacks take advantage of code that does not filter input that is being entered directly into a form. Susceptible applications are applications that take direct user input and then generate dynamic SQL that is executed via back-end code. Objectives of the research are to identify weakness in current website, identify the prevention strategies, applying malicious code to PHP framework which is Joomla 1.0.15 and eZ Publish 4.0.0 and finally identify whether SQL prevention strategies have been applied. As for the results, both framework have applied the SQL injections prevention strategies and not allowing SQL injection to occur.