ANALYSIS OF SQL INJECTION ON VULNERABLE WEBSITE

SITI EZZATUL AIN BINTI YAZID

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

ANALYSIS OF SQL INJECTION ON VULNERABLE WEBSITE

SITI EZZATUL AIN BINTI YAZID

This report is submitted in partial fulfilment of the requirements for the Bachelor of Computer Science (Computer Network)

FACULTY OF INFORMATION ANF COMMUNICATION TECHNOLOGY

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

DECLARATION

I hereby declare that this project report entitled

ANALYSIS OF SQL INJECTION ON VULNERABLE WEBSITE

Is written by me and is my effort and that no part has been plagiarized without citations.

STUDENT : _____ Date:
(SITI EZZATUL AIN BINTI YAZID)

SUPERVISOR : _____ Date:
(EN. ZULKIFLEE BIN MUSLIM)

DEDICATION

For my beloved family

ACKNOWLEDGEMENTS

First and foremost I would like express my gratitude to the Lord Almighty, whom without His guidance, for keeping me in path of righteousness I would not have been able to be as I am today .Next, I would like to express millions of thank you to my supervisor Encik Zulkiflee bin Muslim for guiding me throughout this project, thanks for guided me and give support throughout the entire project and the inspiration for me to keep on going. Also, not forgetting my fellow friends who also went through the Project Sarjana Muda (PSM) with me, always being there for me and give a hand whenever I need it the most and lecturers and staff in UTeM expecially Faculty Information and Communication Technology (FTMK) for supplying me with endless knowledge.

ABSTRACT

SQL Injection is an attack that involves database where it allows attacker to access the database by using an application or using queries. The problem is lack of technical abilities to detect SQL Injection events attacks activities. The purpose of this project are to find classifies the characteristic of SQL Injection. To understand the character of SQL Injection so that, the SQL Injection event can be detect easier. Waterfall Methodology was used to conduct this test bed environment was deploy to faster state instantly. At the end of this project it can be able to detect more effective. For the future, this character will be used to detect an effective SQL Injection detection mechanism.

ABSTRAK

SQL Injection adalah serangan yang melibatkan pangkalan data di mana ia membolehkan penyerang untuk mengakses pangkalan data dengan menggunakan aplikasi atau menggunakan pertanyaan. Masalahnya adalah kekurangan kebolehan teknikal untuk mengesan aktiviti serangan SQL Injection. Tujuan projek ini adalah untuk mencari mengelaskan ciri-ciri SQL Suntikan. Untuk memahami watak SQL Suntikan supaya, acara SQL Injection dapat mengesan lebih mudah. Metodologi Air Terjun digunakan untuk menjalankan persekitaran katil ujian ini digunakan untuk keadaan lebih cepat serta-merta. Pada akhir projek ini, ia dapat mengesan lebih berkesan. Untuk masa depan, watak ini akan digunakan untuk mengesan mekanisme pengesanan Suntikan SQL yang berkesan.

?

TABLE OF CONTENT

CHAPTER	SUBJECT	PAGE
DECLARATION		**iii**
DEDICATION		**iv**
ACKNOWLEDGEMENTS		**v**
ABSTRACT		**vi**
LIST OF TABLE		**xiii**
LIST OF FIGURE		**xiv**
CHAPTER I	**INTRODUCTION**	**1**
	1.1 Introduction	**1**
	1.2 Problem Statement (PS)	**5**
	1.3 Project Question (PQ)	**6**
	1.4 Project Objective (PO)	**6**
	1.5 Project Scope	**7**
	1.6 Project Contribution (PC)	**7**
	1.7 Thesis Organization	**8**
	1.8 Conclusion	**10**
CHAPTER II	**LITERATURE REVIEW**	**11**
	2.1 Introduction	**11**
	2.2 Keyword	**12**
	2.2.1 SQL Injection	**12**
	2.2.2 Vulnerable Website	**13**
	2.3 Related Work	**14**
	2.3.1 SQL Injection	**14**
	2.3.2 Methods	**19**
	2.3.3 SQL Injection Process	**19**
	2.3.4 Types of SQL injection attack	**20**

	2.4 Classic Injection	**20**
	2.4.1 Union-Based	**22**
	2.4.2 Error-Based	**23**
	2.5 Blind Injection	**24**
	2.5.1 Time-Based	**25**
	2.5.2 Boolean-Based	**27**
	2.6 Propose Project	**27**
	2.7 Conclusion	**29**
CHAPTER III	**METHODOLOGY**	**30**
	3.1 Introduction	**30**
	3.2 Research Methodology	**31**
	3.2.1 Planning	**32**
	3.2.2 Analysis	**32**
	3.2.3 Design and Development	**33**
	3.2.4 Implementation	**34**
	3.2.5 Testing	**34**
	3.3 Project Milestone	**35**
	3.3.1 Flow Chart of Project	**37**
	3.3.3.1 Stage 1: Planning	**38**
	3.3.3.2 Stage 2: Analysis	**38**
	3.3.3.3 Stage 3: Design and Development	**38**
	3.3.3.4 Stage 4: Implementation	**38**
	3.3.3.5 Stage 5: Testing	**39**
	3.3.3.6 Stage 6: Documentation	**39**
	3.3.2 Gantt Chart of Project	**39**
	3.4 Conclusion	**40**
CHAPTER IV	**DESIGN**	**41**
	4.1 Introduction	**41**
	4.2 Project Requirement and Tools	**42**
	4.2.1 Hardware and Software	**42**

		Requirement	
		4.2.2.1 Ubuntu	**44**
		4.2.2.2 Kali Linux	**44**
		4.2.2.3 SQLMap	**44**
		4.2.2.4 XAMPP	**45**
		4.2.2.5 Burp Suite	**45**
		4.2.2.6 Command Prompt	**46**
	4.3	Flow Chart	**46**
		4.3.1 Flow Chart of Union-Based	**47**
		4.3.2 Flow Chart of Error-Based	**49**
		4.3.3 Flow Chart of Time-Based	**51**
		4.3.4 Flow Chart of Boolean-Based	**53**
	4.4	Network System Architecture	**55**
	4.5	Logical and Physical Design	**56**
		4.4.1 Logical Design	**56**
		4.4.2 Physical Design	**57**
	4.6	Possible Scenarios	**58**
		4.6.1 Scenario of Union-Based	**58**
		4.6.2 Scenario of Error-Based	**59**
		4.6.3 Scenario of Time-Based	**59**
		4.6.4 Scenario of Boolean-Based	**59**
	4.7	Conclusion	**60**
CHAPTER V		**IMPLEMENTATION**	**61**
	5.1	Introduction	**61**
	5.2	Environment Setup	**62**
		5.2.1 Obtain Dataset Phase	**63**
		5.2.2 SQL Injetion Attack Technique and Tools for the	**66**

	Project	
	5.2.3 Operating System Installation	**66**
	5.2.4 XAMPP Activities	**67**
	5.2.5 OWASP Mutillidae	**69**
	5.2.6 Burp Suite Activities	**70**
	5.2.7 Union-Based Injection Attack	**71**
	5.2.8 Error-Based Injection Activities	**72**
	5.2.9 Time-Based Injection Attack	**76**
	5.2.10 Boolean-Based Injection Attack	**81**
	5.3 Conclusion	**86**
CHAPTER VI	**TESTING AND ANALYSIS**	**87**
	6.1 Introduction	**87**
	6.2 Result and Analysis	**88**
	6.2.1 Test Plan	**88**
	6.2.2 Test Organization	**88**
	6.2.3 Test Environment	**88**
	6.2.4 Test Strategy	**89**
	6.2.5 Test Design	**89**
	6.2.6 Test Description	**89**
	6.2.6.1 SQL Injection Attack Report	**90**
	6.3 Conclusion	**92**
CHAPTER VII	**CONCLUSION**	**93**
	7.1 Introduction	**94**
	7.2 Project Summarization	**95**
	7.2.1 Observation on Weakness and Strengths	**95**

7.3	Project Contribution	**95**
7.4	Project Limitation	**95**
7.5	Conclusion	**96**
REFERENCES		**97**

LIST OF TABLE

TABLE	TITLE	PAGE
1.1	Problem Statement	5
1.2	Project Question	6
1.3	Project Contribution	7
2.1	Summary types of SQL Injection	29
3.1	Project Milestone	35
4.1	Hardware Requirement Tools	42
4.2	Software Requirement Tools	43
6.1	Similarity in type of SQL Injection	90
6.2	Differences in type of SQL Injection	91
7.1	Advantages and Disadvantages of project	94

LIST OF FIGURE

DIAGRAM	TITLE	PAGE
1.1	Statistic of SQL Injection on Vulnerabilities of Type	2
1.2	Vulnerability of Websites and Databases detected in United States Universities or Education Department	3
2.1	Taxonomy of Literature Review	14
2.2	SQL Injection in Basic Figure	16
2.3	Distribution of Attack Technique until May 2012	17
2.4	Interaction between user and typical web application	18
2.5	The process of Classic SQL Injection	20
2.6	Union Query	22
2.7	Resulting query generated by web application	23
3.1	Testing Methodology	31
3.2	Flow Chart of Project Activities	37
3.3	Gantt Chart of Project Activities	39
4.6	FlowChart of Union-Based	47
4.7	FlowChart of Error-Based	49
4.8	FlowChart of Time-Based	51
4.9	FlowChart of Boolean-Based	53
4.10	Logical Design	56
4.11	Physical Design	57
5.1	Flow Chart of Obtain the Dataset	63
5.2	Sqlmap captured of Error-Based	65
5.3	SQL Injection Attack Technique and Tools of the Project	66
5.4	Setting on XAMPP for OWASP Mutillidae	67
5.5	Table on OWASP Mutillidae	68
5.6	Login Page on OWASP Mutillidae	69

5.7	Output of HTTP history on Burp Suite	70
5.8	POST Request on OWASP Mutillidae	71
5.9	Command to launch Error-Based Injection attack	72
5.10	Output of the database	73
5.11	Extracting columns in table from nowasp database	73
5.12	Output of columns extraction from the table	74
5.13	Extracting data in the columns	74
5.14	Output extracting data in the columns	75
5.15	Command to extract database using time-based technique	76
5.16	Parameter of the time-based command	76
5.17	Output of the time-based command	77
5.18	Command to extract tables from a database	77
5.19	Output of tables in a nowasp database	78
5.20	Command to extract columns from a table	78
5.21	Output of columns in a accounts table	79
5.22	Command to extract columns from a table	79
5.23	Output of extracting accounts table	80
5.24	Command to extract database from the OWASP Mutillidae	81
5.25	Parameter of the Boolean-based command	82
5.26	Output of extracting database	82
5.27	Command to extract table from the nowasp database	83
5.28	Output of extracting table	83
5.29	Command to extract columns from the accounts table	84
5.30	Output of extracting columns	84
5.31	Command to extract data from the columns	85
5.32	Output of extracting data	85

CHAPTER I

INTRODUCTION

1.1 Introduction

SQL Injection was one of the famous threat to websites and it was publicly disclosed over 15 years. 150,000 people's personal details are being stolen by a hacker that being suspected. Usually, hackers enter malicious commands into forms on a website where this method was easy to make it churn out the data. SQL injection are synonym with stealing the personal details, grab data and hit the sites just to extract huge private data. This threat was the easiest for hacker as it is only take only a few hours.

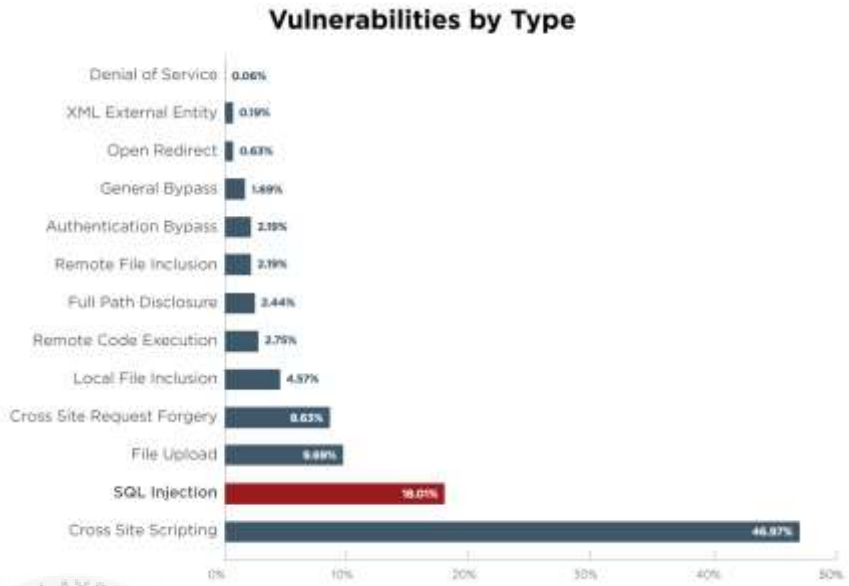

Figure 1.1: Statistic of SQL Injection on Vulnerabilities by Type(Wordpress, Learning, Security, Never, & This, 2017)

Figure 1.1 shows the statistic of SQL Injection on Vulnerable by type. Based on the figure above it is proven that SQL Injection is among of the top vulnerable compared to others. SQL Injection was second most vulnerable leading by vulnerabilities types as it is become more trending today.

Growing fast technology and internet will also increase the number of hacking by day. SQL Injection was increased annually. Hacking was causes by the lack of security and privacy issues. An enormous private data was usually attract attackers to steal it. Most infamous attacks in 15 years through e-commerce or any web applications such as university, online shopping, bank, hospital and more. Attacker to uses SQL Injections to Target Universities or Education Departments which hacker gains access through the system and attempted to steal and sell the data to third parties. Commonly, uses variety free tools to identify the vulnerability of the websites and databases. This will

Figure 1.2: Vulnerability of Websites and Databases detected in United States Universities or Education Department(Election et al., 2017)

SQL Injection campaign which was able to successfully manipulate from the user input. SQL injection was rely on database applications and protocols which have not been well secured. Traditionally point of attack for an SQL Injection is query string, which web developers may provide to users or administrators.

Today, SQL injection was repeatedly sits at first spots of vulnerabilities in OWASP Top 10 report. Troy Hunt said, due too many incidents, it must be other factor that keep it very high up there as always the number one risk. Parsing is one of the data in the request back to server but attacker take this with SQL injection attack to do something is not mean to do which return them a piece of private data. This will attract them to repeat it over and over again to grab each piece of data.

Rogue SQL statements will allow the attacker to access, modify or delete data stored on the database that it is not available normally to do. It will become extreme if attacker can gain control over the server. If the

websites application was not well secured, then it is possible to inject the code fragments.

Any retails and other industry that accept payment cards for transactions, SQL injection was the infamous attack. 53% from the owner retails trust that sensitive and confidential customer information was stolen because it was a high-profile breaches elements.

Hacker usually use tools that automates the process instead. SQLMap is a piece of software which it explore the pages on the website, similar on how search engine explore. However it is also looks for input forms on the websites, then the submit forms with inputs might be easy for attacker to launch the attacks. When attacker looking for a target, they can go through the scripts in all URLs and test them automatically to see if the websites are vulnerable.

1.2 Problem Statement

In most cases, most of users did not notice about security and privacy, also less awareness about using internet or sharing information and others.

Any activities that involved online and not well secures allow attackers to access unauthorized private data. Security and privacy issues have been an ignorant to any e-commerce websites or any web applications such as hospital, bank and online shop. Thus, a huge private data can be vulnerable to the attackers where it can be used in future without any individual notice about it. Table 1.1 shows the summary of problem in this project.

Table 1.1: Summary of Problem Statement

PS	Problem Statement
PS1	Lack of understanding in SQL Injection causes detection of intrusion activity cannot be detected easily.

PS1: Lack of understanding in SQL Injection causes detection of intrusion activity cannot be detected easily.

The attacker will easily access the database of a web application as user are not aware of security of web applications. As web applications security remains unknown variety type of attack SQL Injection attack can be test to perform an attack to steal huge amount of private data. Due to this problem, intrusion activity cannot be detected easily.

1.3 Project Question

In fact, the best design produce the most secured and privacy for the web application is preliminary study of the injection architecture needed in the web programming before any customize work will represent. Once, SQL injection is understood then implement this variety type and testing the attacks are propose. Table 1.2 below shows the project question that this project will embark upon.

Table 1.2 Summary of Project Question

PS	PQ	Project Question
PS1	**PQ1**	What is the difference between each types of attacks?
	PQ2	How to retrieve the data from the database?
	PQ3	How to know the classified SQL Injection attacks base on it types?

1.4 Project Objective

In order to solve the problem identified as Section 1.2, three objectives are derived,

1. **To find the difference between the types of SQL Injection attack.**
   Each types of SQL Injection attack has its own behaviour and pattern, so that there are differences among the types of the attack.

2. **To steal the data from the database which the data should not normally be available.**
   Stealing private data from a database by extracting the database as it is not well-secured.

3. **To characterized the SQL Injection attacks**
   Differentiation on its behaviour and pattern on SQL Injection, this will leads to classification each types of SQL Injection

1.5 Project Scope

The Scope of this research paper will be focusing on the issue below:

1. Define differences for each type SQL injection attacks by scanning and testing the SQL statements on the sqlmap.
2. Characterized the type of SQL Injection type based on the test has been done about it behaviour and pattern.

1.6 Project Contribution

Project contribution are shown in the Table 1.4

PS	PQ	PO	PC	Project Contribution
PQ1	**PQ1**	**PO1**	**PC1**	Taxonomy a better way to study about SQL injection attack such as character each type of it.
PQ2	**PQ2**	**PO2**	**PC2**	Comparative analysis between SQL Injection types
PQ3	**PQ3**	**PO3**	**PC3**	Synthesize characteristics of SQL Injeciton type.

The expectation by end of this project is to able to detect SQL Injection more efficient.

1.7 Thesis Organization

This report consist of seven chapters which is Chapter 1: Introduction, Chapter 2: Literature Review, Chapter 3: Methodology, Chapter 4: Design, Chapter 5: Implementation, Chapter 6: Testing and Analysis and lastly Chapter 7: Conclusion.

Chapter 1: Introduction

This chapter explain about the definition, background study, problem statement, objective, scope and expected output related to the SQL Injection on Vulnerable Website.

Chapter 2: Literature Review

This chapter elaborated about SQL Injection, types of SQL injection attacks and the technique for each type of SQL injection attacks. It will help to more understanding about what is SQL Injection on Vulnerable Websites.

Chapter 3: Methodology

This chapter provide a decision of the method of development that will be carry out to develop thus project. With certain method of analysis will help to analyse the attacks in less time required and easy for system testing and correction.

Chapter 4: SQL Attack Analysis and Design

This chapter will explained in detail the design scenarios of the attack such as:

1. Specifies the types of SQL injection
2. Specifies the characteristics on SQL injection