SQL INJECTION PERFORMANCE ANALYSIS

CHAI ROU SIN

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: SQL INJECTION PERFORMANCE ANALYSIS

SESI PENGAJIAN: 2020 / 2021

Saya: CHAI ROU SIN

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

_____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
_____✓_____	TIDAK TERHAD	

(TANDATANGAN PELAJAR)	(TANDATANGAN PENYELIA)
Alamat tetap: 14, Persiaran Sungai Chemor 4, Taman Bunga Raya, 31200 Chemor, Perak.	NUR FADZILAH BINTI OTHMAN Nama Penyelia
Tarikh: 14/09/2021	Tarikh: 14/09/2021

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

SQL INJECTION PERFORMANCE ANALYSIS

CHAI ROU SIN

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Security) with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2021

DECLARATION

I hereby declare that this project report entitled

SQL INJECTION PERFORMANCE ANALYSIS

is written by me and is my own effort and that no part has been plagiarized

without citations.

STUDENT : _____ Date : 14/09/2021

(CHAI ROU SIN)

I hereby declare that I have read this project report and found

this project report is sufficient in term of the scope and quality for the award of

Bachelor of Computer Science (Computer Security) with Honours.

SUPERVISOR : _____ Date : 14/09/2021

(NUR FADZILAH BINTI OTHMAN)

DEDICATION

I would like to dedicate my work to my dearly family, friends, and supervisor. I am very grateful for the spiritual support and motivation from my beloved family when I face all the obstacles.

Besides, I would like to express gratitude to my supervisor, Dr. Nur Fadzilah Binti Othman who has been given fully support throughout this process.

Last, I am deeply indebted to my friends who lend a helping hand to complete this study.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my supervisor, Dr. Nur Fadzilah Binti Othman for the fully support of my final year project within 28 weeks. Without her motivation and enormous knowledge, I could not complete this study during this period.

Besides, I praise and thank my beloved parents, Chai Chuan Sing and Choo Yean Choo, for all of their words of wisdom and mental support. I also would like to appreciate my course mates and friends for their inseparable helping hands.

Last but not least, I offer my acknowledgement to the universal god for listening to my devotions and providing the courage to finish this study on time.

ABSTRACT

Internet technology is a popular information infrastructure in today's business and education worlds. By employing modern science and technology, Web developers produce a variety of web applications or websites for the ease of our everyday lives in numerous fields. However, the ignorance of basic protection and privacy concerns is a critical problem for web developers and causes the attackers grab the opportunity to take malicious actions on these web applications. Thus, SQL injection attack has been identified as one of the most common threats to most web applications today. This attack is a vulnerability to web security that enables an attacker to interact with the requests made to his database by an application. Besides, this kind of hacking technique requires entry point to execute which include Dynamic SQL, modifications of URL Strings, web or application forms, employee abuse of limited access and error messages. The users who lack of acknowledge are easier became the victims of SQL Injection. In this research, it will be mainly focused on the performance of SQL injection on a prototype website and the effectiveness of the prevent approach implemented. There are three ways of SQL injection applied which are Tautologies, Union Queries and SQLMAP while the prevention is inserting mysqli_real_escape_string() function inside the source code of the prototype website. Along this research, these three techniques of SQL injection are success implemented and they are managed to retrieve the data from the hidden database server with bypassing all the authentication on the website. In addition, the prevention utilized is worked on Tautologies and Union queries attack. In short, this research outlines the performance analysis on SQL injection before and after applying the prevention.

ABTRAK

Teknologi internet adalah infrastruktur maklumat yang popular dalam bidang perniagaan dan pendidikan di seluruh dunia pada masa kini. Dengan menggunakan sains dan teknologi moden, terdapat banyak aplikasi web dicipta oleh pembangun web bagi kemudahan dalam kehidupan seharian kita dalam penglibatan pelbagai bidang. Walau bagaimanapun, kekurangan pengetahuan mengenai perlindungan asas dan privasi menyebabkan penyerang berpeluang untuk melakukan tindakan jahat pada aplikasi web. Hal yang demikian, serangan SQL injection telah menjadi satu ancaman yang paling biasa dalam kebanyakan aplikasi web terkini. Serangan ini adalah kerentanan terhadap keselamatan web agar penyerang mampu berinteraksi dengan permintaan yang dilaksanakan dalam pangkalan data. Seterusnya, teknik penggodaman ini memerlukan jalan masuk untuk dilakukan dengan meliputi Dynamic SQL, modifikasi String URL, borang web atau aplikasi, penyalahgunaan pekerja terhadap akses terhad dan mesej ralat. Pengguna yang kurang mengetahui ancaman web mudah menjadi mangsa SQL Injection. Justeru itu, penyelidikan ini akan berfocus terutamanya pada prestasi SQL injection di laman web terdiri dan keberkesanan cara pencegahan yang dilaksanakan. Terdapat tiga cara SQL injection yang diterapkan iaitu Tautologies, Union Queries dan SQLMAP sementara pencegahannya adalah memasukkan fungsi mysqli_real_escape_string () di dalam kod sumber laman web terdiri. Sepanjang penyelidikan ini, ketiga teknik SQL injection berjaya dijalankan dan mereka berjaya mendapat data dari pelayan pangkalan data tersembunyi dengan mengelakkan semua pengesahan di laman web. Seterusnys, pencegahan yang digunakan berjaya pada serangan Tautologies dan Union queries. Ringkasnya, penyelidikan ini menggariskan analisis prestasi pada SQL injection sebelum dan selepas pencegahan diterapkan.

TABLE OF CONTENTS

PAGE

LIST OF TABLES

PAGE

LIST OF FIGURES

PAGE

LIST OF ABBREVIATION

FYP	**-**	**Final Year Project**
SQLI	**-**	**SQL Injection**
SQL	**-**	**Structed Query Language**

LIST OF ATTACHEMNTS

CHAPTER 1: INTRODUCTION

1.1 Introduction

In today's world, the web applications are constructed on *n*-tier architecture which separates the data management, application processing, and presentation tiers logically. Currently, a specific tier is required to added or modified for equipment of design and maintenance rather than revising the whole application. The data management tier comprises of a database server which stores and retrieves the confidential information of the application and users. Besides, the database data is widely used for user authentication, storing the record and its relationship, and presenting the data in a dynamically generated web page (Asish Kumar Dalai and Sanjay Kumar Jena, 2017).

Recently, the general affairs such as banking transaction, shopping, back up data or information are managed by online through web applications. Moreover, these web applications can be found all over the Internet whilst it is crucial to comprehend that they are all databases driven. Database is an important component of web applications as they are capable to store all users' preferences, personally identifying information and sensitive information. To dynamically generate personalized content for each user, web applications interact with the databases by using Structed Query Language (SQL) (Stephanie, 2017). The function of SQL is to manipulate data and relate databases by MySQL, Oracle, MSSQL, etc. These database management systems typically are

implemented on the backend of web applications (Arianit Maraj, Ermir Rogova, Genc Jakupi and Xheladin Grajqevci, 2017).

SQL injection (SQLI) attacks have occurred as the most dangerous forms of web-based device attacks in latest year and ranked as the top among the Open Web Application Security Project's (OWASP) top ten vulnerabilities. SQLI can be launched by inserting malicious characters into the provided input fields of web applications which causes in an updated SQL query. SQL injection attacks do not have a long history. Most content on the Internet in its early days was static and not vulnerable to injection attacks. In Feb 2002, the first scope SQLI attack was happened on Guess.com, more than 200,000 names, credit card numbers and expiration dates of customers had been retrieved by the attackers from the permission of customers' databases (Alenezi, Nadeem and Asif, 2021). According to Akamai, 2017, the numbers of web application attacks increased by 69% compared to Q3 2016 in the 3rd quarter of 2017 while the local File Incorporation and SQL injection attacks reported as hold 85% of these attacks and Cross Site Scripting (XSS) only accounted having 9%. Therefore, SQL injection is getting more widespread on the Internet now (Kausar, Nasar and Moyaid, 2019).

A success performance of SQLI attack must started from the action of searching vulnerability of the users' inputs within a website or web application. Furthermore, the attacker has the ability to generate input material. This type of content is commonly referred to as a malicious payload, and it is the most essential element of the attack. Following the attacker's transmission of this content, malicious SQL commands are executed in the database. Due to the SQL databases store all the data, SQLI attack will bring critical consequences. For the instances, the private information stole by an attacker can be used to impersonate the users or the attacker is going to alter the victim's bank balance with transferring money to others own bank account (Pattewar, Patil and Taneja, 2019).

1.2 Problem Statement

SQLI is a kind of an injection attack that allows malicious SQL statements to be executed. These statements manage a database server that is hidden behind a web application. SQL injection bugs may be exploited by attackers to circumvent device protection measures. In addition, they are able to bypass authentication and authorization of a website or web application and the entire SQL database's content can be retrieved.

Once SQLI attack is successful toward a victim's database system, the records in the database would be added, modified, and deleted. Sometimes, they will hold the stolen data for ransom for example especially the credential data for example credit number or identification number from the financial application.

Besides, an attacker can gain a permanent backdoor into an organization's infrastructure, resulting in a long-term monitor that can go undetected for a long time. Moreover, this kind of attack is leading to the penetration on an organization operation hence became a threat. Hence, this study is important to be conducted to provide more clearly definition on SQL injection and its prevention.

1.3 Research Questions

According to the problem statement above, there are three research questions are shown as the Table 1.1.

Table 1.1: Research Questions

No.	Research Questions
1.	How the SQL injection affects the website?
2.	Which technique of SQL injection to be analyzed?
3.	What is the prevent approach against SQL injection attack?

1.4 Research Objectives

To solve the research questions above, three research objectives are composed in the Table 1.2 below.

Table 1.2: Research Objectives

No.	Research Objectives
1.	To develop a prototype website and conduct SQL injection attacks on it
2.	To propose Tautologies, Union Queries, and SQLMAP as SQLI attacks
3.	To identify the prevention on SQL Injection

:

1.5 Research Summary Matrix

The summary of research questions and research objectives of this project are listed in the Table 1.3 below.

Table 1.3: Summary of Research Questions and Research Objectives

Research Questions	Research Objectives
How the SQL injection affects the website?	To develop a prototype website and conduct SQL injection attacks on it
Which technique of SQL injection to be analyzed?	To propose Tautologies, Union Queries, and SQLMAP as SQLI attacks
What is the prevent approach against SQL injection attack?	To identify the prevention on SQL Injection.

1.6 Scope of the Research

The scope of this research is determined based on the research objectives. The list of the research scope is shown as below:

1. The project will cover the performance of SQL injection on a website or web application by using techniques of Tautologies, Union Queries, and SQLMAP.

2. The project is focus on the performance of the website or web application investigated with and without the prevention approaches.

1.7 Research Contribution

The contribution of this research is to figure out the way how the SQL injection attack emerged and the prevention approaches on web applications. Online developers can test this attack on their web application to discover the existence of the hidden vulnerability. Meanwhile, they can ensure the safety of users and safeguard the users' credential data stored in the database. Furthermore, users can provide comments or report any insecure online applications to the web developer if they discover any SQL injection vulnerabilities. As a result, the expected outcome provides users with a clear picture of how to define SQL injection attacks based on the implications.

Besides, this research is presented the brute force attack of SQLMAP to retrieve the data from the database hidden. From the previous research, the developers are focus on vulnerability analysis according to the risk level. However, this research is focused on the brute force attack of SQLMAP to retrieve the data from the database hidden. It presents its high efficiency on SQLI attack for the users from the comparison in term of time consuming to other techniques.

1.8 Research Organization

In this research, there are six chapters are included and summarized in the following description.

1.8.1 Chapter 1: Introduction

This chapter will introduce the performance analysis of SQL injection on database system. At the same time, the introduction is separated into several parts which consist of problem statement, research questions, research objectives, research summary matrix, research scopes and keywords about this study.

1.8.2 Chapter 2: Literature Review

This chapter is going to explain a few of reviewed research about the techniques on detection and prevention of SQL Injection.

1.8.3 Chapter 3: Project Methodology

This chapter proposes all the methodology and steps will be taken to finish this study. To ensure this research is completed on time, milestones and Gantt chart are included in this chapter.

1.8.4 Chapter 4: Implementation

This chapter illustrates the embedded coding of SQL injection attack on one website to show its effects on the database system. Next, the expected outcome from the attack is going to be examined in the following chapter.

1.8.5 Chapter 5: Testing and Analysis

This chapter tests and analyzes the consequence when some prevention is implemented before working with SQL injection attack. The result in this chapter will compare with the results from previous chapter and explained in more details.