DETECTION AND PREVENTION FOR SQL INJECTION ATTACKS IN STORED PROCEDURES USING REAL TIME WEB APPLICATION

NABEEL SALIH ALI

MASTER OF COMPUTER SCIENCE

(INTERNETWORKING TECHNOLOGY)

2015

Faculty of Information and Communication Technology

DETECTION AND PREVENTION FOR SQL INJECTION ATTACKS IN STORED PROCEDURES USING REAL TIME WEB APPLICATION

Nabeel Salih Ali

Master of Computer Science (Internetworking Technology)

2015

DETECTION AND PREVENTION FOR SQL INJECTION ATTACKS IN STORED PROCEDURES USING REAL TIME WEB APPLICATION

NABEEL SALIH ALI

A dissertation submitted
in fulfillment of requirements for the degree of Master of Computer Science
(Internetworking Technology)

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2015

DECLARATION

I declare that this dissertation entitle “Detection and Prevention for SQL Injection Attacks in Stored Procedures Using Real Time Web Application” is the result of my own research except as cited in the references. The dissertation has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ……..……

Name : Nabeel Salih Ali

Date : 02 July, 2015

APPROVAL

I hereby declare that I have read this dissertation and in my opinion this dissertation is sufficient in terms of scope and quality for the award of the degree Master of Computer Science (Internetworking Technology).

Signature	:	…….
Supervisor Name	:	Dr. Abdul Samad Bin Shibghatullah
Date	:	02 July, 2015

DEDICATION

First and foremost, all praises to the Allah the most merciful for the unlimited generosity and guidance to complete this research study. All praises to the prophet Mohammed (S.A.A.W) for whom his life and his track are the perfect guide for our life until the end of the time.

Second, I would like to dedicate my hard work to those who did not stop their daily support since I was born.

To My ***MOTHER…*** my precious diamond

To My ***FATHER…*** who has the big heart

(God's mercy on his soul, and make his lives in his eternal paradise).

To my ***BROTHERS, SISTERS***, I thank them all for their support, and I thank them for being my family.

Third, to the woman who provided all the suitable circumstances for me that lead me to this success that is made by my own hands:

My ***WIFE…*** my soul mate,

To my precious kids **"Ameer & Kawther"**, whose smiles give me passion and strength.

Lastly, I also dedicate my work to my dearest friends with utmost appreciation and gratitude for being there when I needed them.

Nabeel Salih Ali

إهــداء

أولا وقبل كل شيء، كل الثناء إلى الل الرحيم لسخاءه غير المحدود في توفيقي لاكمال هذه الدراسة البحثية. كل المديح للنبي محمد (ﷺ) الذي حياته وانجازاته هي دليل الكمال لحياتنا حتى نهاية العمر

ثانيا أود أن أهدي عملي الشاق لأولئك الذين لم يكفوا عن دعمهم اليومي منذ أن ولدت.

إلى ***أمي*** ... ياجوهرتي الثمينة

إلى ***أبي*** ... ياصاحب القلب الكبير

(رحمه الل.. واسكنه جنة الخلد)

إلى ***أخوتي*** و ***أخواتي***، أنا أشكركم جميعاً لكل الدعم الذي قدمتوه لي.

ثالثا إلى المرأة التي لم تكف عن تهيئة كل الظروف التي قادتني الى هذا النجاح:

زوجتي ... يا توأم روحي

وإلى طفلي الغاليين ***أمير*** و ***كوثر*** اللذان اعطياني بابتسامتهما القوة و الاصرار على مواصلة دراستي.

وأخيرا أود أيضا أن أهدي عملي لأعز أصدقائي بمنتهى التقدير والامتنان ليجري هناك عندما كنت في أمس الحاجة إليها.

نبيل صالح علي

ABSTRACT

At present, web applications have been used for most of our activities in our life. Web applications are affected by the attacks of SQL injection. SQL injection is a prevalent technique that attackers appoint to impose the database in the most of web applications, by manipulate the SQL queries that send to RDBMS. Hence, change the behavior of the application. Stored procedures SQL injection attack is one of the serious attacks that posed database threats in the underlying database that underlie web applications. Whereas, the attack can be crafted to execute stored procedures that provided by a particular database, encompasses procedures that deal with the operating system. In this research, three major objectives can be organized to direct the work study are: Firstly, to investigate the attacks of SQL injection, and study what has been done to detect and prevent SQLIA in stored procedures in order to, eliminate the lack of their approaches and highlight their weakness, secondly, to identify the various obstacles and factors that would be encountered will be led to be successful to build an appropriate defensive approach to detect and prevent SQLIAs, and the third objective is, to develop WASP tool to build a real-time web application tool (RT-WASP) to detect the SQLIAs, and propose a suitable protective approach to prevent stored procedures SQLIAs. Our methodology encompassed, four phases, primary study or investigation phase, modeling phase, development and proposing phase, evaluations and discussion phase. Investigation phase will study current approaches to counter SQLIAs. Background study, highlight problems and weakness in order to address the gap in detection and prevention SQLIA domain. In modeling phase, evaluate the performance of the existing techniques to identify the factors that would be encountered will be led to get better and efficient results in our work study. In developing and proposing phase, a suitable tool will be developed, and effective preventive approach will be proposed. Evaluations and discussion phase will take a place in order to finalize our work research. The main contributions of this research study are: First, Summarized and analysis of a detailed review of various SQLI attacks and investigation of previous approaches that detected and prevented these attacks in Web applications. Second, developed WASP tool that has been proposed by Halfond.2008 to detect the attacks of SQLI in real-time web applications. Third, proposed a protective approach that includes three preventive mechanisms that are: parameterized stored procedures, customized error messages, and encryption stored procedures in the SQL server. In order to, prevent the danger of SQLIA in stored procedures, and the last contribution is, conducted a comparison analysis of the developed technique and proposed protective approach based on the evaluations respect to efficiency and effectiveness of the technique, and effectiveness of the proposed protective approach. RT-WASP was efficient due to able to stop all SQLIAs and did not generate any false negative, a few false positive values in the results, and pose, low overhead and minimal deploy requirements. Whilst, our protective approach was effectiveness due to, capable to prevent the attacks of stored procedures SQLIAs. Finally, identify and focus on the future scope.

ABSTRAK

Pada masa ini, aplikasi web telah digunakan untuk sebahagian besar aktiviti kita dalam kehidupan kita. Aplikasi web yang terlibat dengan serangan suntikan SQL. Suntikan SQL adalah teknik lazim bahawa penyerang melantik mengenakan pangkalan data dalam sebahagian besar aplikasi web, dengan memanipulasi pertanyaan SQL yang menghantar untuk RDBMS. Oleh yang demikian, mengubah tingkah laku permohonan. Disimpan prosedur SQL serangan suntikan adalah salah satu serangan yang serius yang ditimbulkan ancaman pangkalan data dalam pangkalan data asas yang mendasari permohonan web. Manakala, serangan boleh dibuat untuk melaksanakan prosedur yang disimpan yang disediakan oleh pangkalan data tertentu, merangkumi prosedur yang berurusan dengan sistem operasi. Dalam kajian ini, tiga objektif utama boleh dianjurkan untuk mengarahkan kajian kerja ini adalah: Pertama, untuk menyiasat serangan suntikan SQL, dan belajar apa yang telah dilakukan untuk mengesan dan mencegah SQLIA dalam prosedur yang disimpan untuk, menghapuskan kekurangan mereka pendekatan dan menonjolkan kelemahan mereka, kedua, untuk mengenal pasti pelbagai rintangan dan faktor-faktor yang akan dihadapi akan membawa kepada kejayaan untuk membina pendekatan defensif yang sesuai untuk mengesan dan mencegah SQLIAs, dan objektif ketiga adalah untuk membangunkan alat WASP untuk membina masa nyata alat aplikasi web (RT-WASP) untuk mengesan SQLIAs, dan mencadangkan pendekatan perlindungan yang sesuai untuk mengelakkan disimpan prosedur SQLIAs. Metodologi kami meliputi, empat fasa, kajian utama atau fasa penyiasatan, fasa model, pembangunan dan fasa mencadangkan, penilaian dan fasa perbincangan. Fasa penyiasatan akan mengkaji pendekatan semasa untuk menangani SQLIAs. Kajian latar belakang, masalah kemuncak dan kelemahan dalam usaha menangani jurang dalam pengesanan dan pencegahan domain SQLIA. Dalam fasa pemodelan, menilai prestasi teknik yang sedia ada untuk mengenal pasti faktor-faktor yang akan dihadapi akan membawa untuk mendapatkan keputusan yang lebih baik dan cekap dalam kajian kerja kita. Dalam membangunkan dan mencadangkan fasa, alat yang sesuai akan dibangunkan, dan pendekatan pencegahan yang berkesan akan dicadangkan. Penilaian dan fasa perbincangan akan diadakan dalam rangka untuk menyelesaikan penyelidikan kerja kita. Sumbangan utama kajian penyelidikan ini adalah: Pertama, diringkaskan dan analisis kajian terperinci daripada pelbagai serangan SQLI dan penyiasatan pendekatan sebelumnya yang dikesan dan menghalang serangan ini dalam aplikasi Web. Kedua, yang dibangunkan alat WASP yang telah dicadangkan oleh Halfond.2008 untuk mengesan serangan SQLI dalam aplikasi web masa nyata. Ketiga, mencadangkan satu pendekatan perlindungan yang merangkumi tiga mekanisme pencegahan yang: parameterized prosedur yang disimpan, mesej ralat disesuaikan, dan prosedur penyulitan disimpan di dalam pelayan SQL. Untuk, mencegah bahaya SQLIA dalam prosedur yang disimpan, dan sumbangan terakhir adalah, menjalankan analisis perbandingan teknik maju dan pendekatan perlindungan dicadangkan berdasarkan penilaian berkenaan untuk kecekapan dan keberkesanan teknik, dan keberkesanan yang dicadangkan perlindungan pendekatan. RT-WASP adalah

berkesan kerana dapat menghentikan semua SQLIAs dan tidak menghasilkan apa-apa negatif palsu, beberapa nilai-nilai positif palsu dalam keputusan dan menimbulkan, overhead rendah dan keperluan Menempatkan minimum. Walaupun, pendekatan pelindung kami adalah keberkesanan kerana, mampu untuk mencegah serangan disimpan prosedur SQLIAs yang disimpan. Akhir sekali, mengenal pasti dan memberi tumpuan kepada skop masa depan.

ACKNOWLEDGEMENT

First and foremost, praise be to Allah, for giving me this opportunity, the strength and the patience to complete my thesis finally, after all the challenges and difficulties. I would like to thank my supervisor, ***Dr. Abdul Samad Bin Shibghatullah*** for his high motivation and most significant contribution in this thesis.

I would also like to thank Ministry of Higher Education and Scientific Research of IRAQ, all UTeM staff and Malaysian people and ***Dr. Abd Samad Bin Hasan Basari*** and ***Dr. Mohd Sanusi bin Azmi.*** Furthermore, I want to thank my friends who have helped and motivated me throughout. May Allah reward them all abundantly, Sincere thanks to all.

Nabeel Salih Ali

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

HTML	-	Hyper Text Markup Language.
SQL	-	Structure Query Language.
SQLI	-	Structure Query Language Injection.
SQLIV	-	Structure Query Language Injection Vulnerabilities.
SQLIAs	-	Structure Query Language Injection Attacks.
WASP	-	Web Application SQLI Protector.
XSS	-	Cross Site Scripting.
IP	-	Internet Protocol.
DBMS	-	Data Base management System.
RDBMS	-	Relational Data Base management System.
RT-WASP	-	Real Time Web Application SQLI Preventer.
OWASP	-	Open Web Application Security Project.
OS	-	Operating System.
UI	-	User Interface.
ID	-	Identification.
VoIP	-	Voice over IP.
CSRF	-	Cross Site Request Forgery.
RFI	-	Remote File Inclusion.
LFI	-	Local File Inclusion.

RFI	-	Remote File Inclusion.
FPD	-	File Path Disclosure.
RCE	-	Remote Code Execution.
DDL	-	Data definition Language.
DML	-	Data manipulation language.
MySQL	-	Structure Query language.
ASCII	-	American Standard Code for Information Interchange.
VNC	-	Virtual Network Computing.

LIST OF PUBLICATIONS

i. NABEEL SALIH ALI, ABDUL SAMAD SHIBGHATULLAH, MUNQATH H. AlATTAR,2015. Review Of The Defensive Approaches For Structured Query Language Injection Attacks And Their Countermeasures, Journal of Theoretical and Applied Information Technology, pp.258-269, Vol 67, no 2.

ii. NABEEL SALIH ALI, ABDUL SAMAD SHIBGHATULLAH, 2015. Protected Web Applications Using Real-Time Technique To Detect SQL Injection Attacks, Jurnal Teknologi (Sciences and Engineering).

CHAPTER 1

INTRODUCTION

1.0 Background

Describes In this chapter, a clear picture about the research study by present and explain clearly: introduction, research problem, research objectives, research questions, and so on.

1.1 Introduction

Nowadays, the Internet becomes a widely significant adoption gate for information dissemination and various other online transactions through inventing the wheel for the revolution of informatics in the recent years. We are using the Internet or web applications for most of the activities in our animation. Thereby, the Internet is becoming widespread information infrastructures. Since the emergence of web programming, web applications have become the most adequate way to offer access to online services via the Internet. It led to gain applications a huge popularity in the world due to; they are achieved enterprise integration through; they allowed of its numerous Internet-enabled applications (Shrivastava et al, 2012).

The web application can be widely classified into two classes: static web applications and dynamic web applications. When the information displayed to the user via HTML web pages called static web applications. When the user input data to the web

applications and they have done actions based on the user input called dynamic web applications. Nevertheless, web applications are typically interact with backend underlying database, whereby, the data underlie web applications is often has sensitive information and confidential. As we see Figure1.1. If an unauthorized user can gain the information by send malicious code, Thereby, an attacker can get illegal access and thefts to the trusted users sensitive data and cause totally destroy or damage to the system (Kindy & Pathan, 2012).

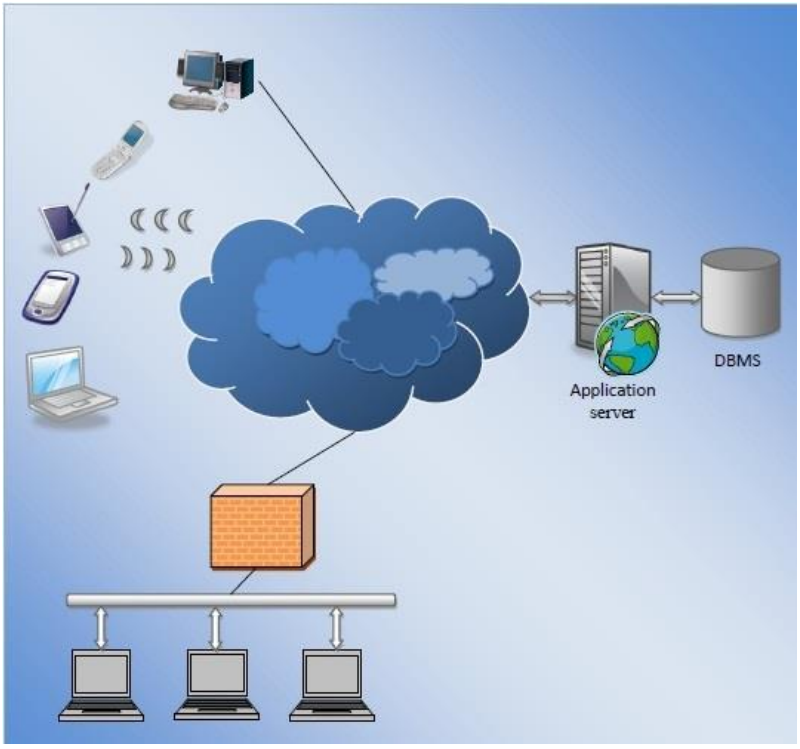

Figure 1.1: Typical Internet World Wide (Aich,2009)

Web applications are frequently vulnerable to attacks due to poor in design, configuration faults, or weakness written code of the web applications. Since web applications are utilized by thousands of users and almost all the web applications are predicated on the using of the Internet. Example: online shopping, e-banking, admission portals, and various government activities like online electricity bill's payment, etc. (Kindy & Pathan, 2012).

There is one kind of attack that is most common and damaging for online services via web applications is Structured Query Language Injection (SQLI) attacks. This attack takes the benefit of trust existing between the users and the server as well as a take feature of absence of input/output validation on the server to reject malicious codes (Baranwal 2012).

With increasing the use of the Internet in the era, most of the web applications developers are not aware of privacy and security issues. Whereby many kinds of attacks against web applications making web applications attractive targets of security attacks. SQLIAs are one of the serious security threats of web applications nowadays. The destination from our research, to develop WASP tool in real-time web application in order to detect the attacks of SQLI and propose a preventive approach to prevent stored procedures SQLI attacks.

1.2 Research background

As the Internet increasing recently, Corporations and organizations are constantly striving to improve their communication capabilities by provide secure application level, that allowing more sensitive and confidential information exchange between organizations via using the web applications. Thereby, Companies are started putting their databases on the Internet for public access. Web applications and are often stored valuable and confidential information, which making them a good target for penetration threats that may be achieved by database injection. The potential downtime and damages for the services if any could loss amount to millions of dollars as we notice in Figure1.2. As well, It was led to prevented many applications that have been critical-mission from going online (Halfond et al. 2011).