PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

MOHAMED BOUDIAF UNIVERSITY - M'SILA
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

COMPUTER SCIENCE DEPARTMENT

DISSERTATION

Submitted in partial fulfillment of the requirements for the Degree of MASTER

Domain: Mathematics and Computer Science

Branch: Computer Science

Specialty: Information Technology and Communication

By: DRIHEM ABDALLAH

TOPIC

New Detection Method for SQL injection

Publicly defended: 31 / 06 /2016 before a Jury composed of :

Chikouche	**University of M'sila**	**President**
S.Bouhouita	**University of M'sila**	**Supervisor**
M.Kamel	**University of M'sila**	**Examiner**

Academic Year: 2015 /2016

CONTENTS

INTRODUCTION GENERAL

SQL injection is the vulnerability That results when you give an attacker the ability to influence the Structured Query Language (SQL) queries that an application passes to a back-end database. By being able to influence what is passed to the database, the attacker can leverage the syntax and capabilities of SQL itself, as well as the power and flexibility of supporting database functionality and operating system functionality available to the database. SQL injection is not a vulnerability that exclusively affects Web applications; any code that accepts input from an untrusted source and then uses that input to form dynamic SQL statements could be vulnerable (e.g., "fat client" applications in a client/server architecture).

A lot of works have been engaged to remedy to SQL attacks, the goal is to build a scanner that can reveal the vulnerability included in the web sites. Several approaches are proposed; they can be categorized. In our research we focus on the structure of the web page rather than the content, so, we proposed a method based on the variation of the number of the tags between the original page and the resulted one after being injected by an SQL attack.

The experiments realized to evaluate the proposed detection SQL injection method is done on web sites proposed by the researchers' community in the area. Three scanners are considered in order to appreciate the performance of our scanner. The results reveal a better performance.

The dissertation is structured as follow, In the first chapter we have seen a view in web security is presented and the major threats are discussed, In the second chapter a view in SQL injection, what is SQL injection, understanding SQL Injection, how it happens and more things about SQL injection is a full and comprehensive definition, In the third chapter we discuss the proposed approach is motivated and explained and all SQL Injection various types of attacks are explained, and a survey of the famous detection methods are listed, In the last chapter is like a series of experiments are done to evaluate the performance of the method.

CONCLUSION GENERAL

SQL injection is a serious threat with deep dangerous consequences on the integrity and security of web applications. In our work, we proposed a method designed upon the structure of the web page cached by its number of tags. The detection is based on the statement that "the behavior of any SQL attack changes the number of tags from the original page to the injected one".

This statement reveals being a good one, because the detection performance is highly appreciated over the well-known scanners used by the community of researchers and professionals. a series of experiments have shown this fact.

REFERENCES

Books :

[1] Hanqing Wu and Liz Zhao, **Web Security: A WhiteHat Perspective**, by Auerbach Publications, April 6, 2015

[2] John Wiley & Sons, Ltd, **Web Application Security for Dummies**, by Qualys, West Sussex PO19 8SQ England, 2011.

[3] Michael E. Whitman, Herbert J. Mattord, **Principles of Information Security,** Kennesaw State University, 20 Channel Center Boston, MA 02210 USA, 2012.

[4] Justin clarke, **SQL Injection Attacks and Defense**, Rachel Roumelioti , July 2, 2012.

Journals and Survey:

[5] Pushkar Y.Jane , M.S.Chaudhari, SQLIA: Detection And Prevention Techniques: A Survey, iosrjournals, 2, 2013, pp. 56-60.

[6] V. Nithya,R.Regan , J.vijayaraghavan, A Survey on SQL Injection attacks, their Detection and Prevention Techniques, iosrjournals, Volume 2, April, 2013 pp, 886-905

Guide:

[7] **The Ten Most Critical Web Application Security Risks**, OWASP, 2013

[8] **A Guide to Building Secure Web Applications and Web Services**, OWASP.

[9] **Web Application Security a Beginner's guide**, Bryan Sullivan Vincent Liu,

Rapport:

[10] **Application Vulnerability Trends Report**, CENZIC, 2014

Website:

[11] OWASP, www.owasp.org.

BIBLIOGRAPHY

[12] OWASP Zap Scanner, 2015

[13] Netsparker Web Application Security Scanner, Version 3.5.

[14] BTS Pentesting Lab Site.

[15] bWAPP Site.

Abstract

In this work we propose a new algorithm for detecting SQL injections in web applications, which is a serious and dangerous issue. The proposed method considers the structure of the web page and particularly the number of its tags. A series of experimentations are done to valid the performance of "T-Scan" the scanner built upon the proposed method. The results confirm its high detection performance over the famous known scanners.

Résume

Dans ce travail, on propose un nouvel algorithme pour la détection des injections SQL au sein des applications web, qui est un sujet délicat et dangereux. La méthode proposée considère la structure de la page web et particulièrement son nombre de tags. De sérieuses expérimentations sont réalisées afin de valider la performance de « T-Scan » qui est le scanner conçu à partir de la méthode proposée. Les résultats confirment sa performance de détection par rapport aux scanners célèbres connus.

ملخص

في هذا العمل، نقترح خوارزمية جديدة للكشف عن حقن SQL في تطبيقات الويب، والتي هي قضية حساسة وخطيرة. تعتبر الطريقة المقترحة على هيكل صفحة على الوأب، وخاصة في عدد من العلامات. أجريت تجارب للتحقق من أداء "Tscan" الذي هو كاشف يعمل على هذه الخوارزمية المقترحة. النتائج تؤكد أداء الكاشف مقارنة مع الكواشف العالمية المعروفة.