SQL-injection vulnerability scanner using automatic creation of SQL-injection attacks (MySqlInjector)

A Thesis submitted to Faculty of Information Technology in partial
Fulfillment of the requirements for Master Degree
(Information Technology),
University Utara Malaysia

By
Ala' Yaseen Ibrahim Shakhatreh

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

ALA' YASEEN IBRAHIM SHAKHATREH
(802322)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/ her project paper of the following title)

SQL-INJECTION VULNERABILITY SCANNER USING AUTOMATIC CREATION OF SQL-INJECTION ATTACKS (MYSQLINJECTOR)

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **ASSOC. PROF. ABDUL BASHAH MAT ALI**

Tandatangan
(Signature) :

PROF. MADYA ABDUL BASHAH MAT ALI
Pensyarah
Bidang Sains Gunaan
Kolej Sastera & Sains
Universiti Utara Malaysia

Tarikh
(Date) : 11/05/2010

PERMISSION TO USE

In presenting this thesis of the requirements for a Master of Science in Information Technology (MSc. IT) from Universiti Utara Malaysia, I agree that the University Library may take it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or in their absence, by the Dean of the Graduate School. It is understood that any copying or publishing or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Graduate School
Universiti Utara Malaysia
06010 Sintok
Kedah Darul Aman

ABSTRACT

Securing the web against frequent cyber attacks is a big concern, attackers usually intend to snitch private info, deface, and damage websites, to prove their identities, this kind of vandalism may drive many corporations which conduct their business through the web to fall down. One of the most dangerous cyber attacks is SQL-injection attack, this kind of attack can be launched through the web browsers. The vulnerability of SQL injection can be resulted from inappropriate programming practice, which leaves a lot of doors wide opened to the attackers to exploit them, and to gain the access to confidential info. In order to get rid of this vulnerability, it is feasible to detect it and enhance the coding structure of the system to avoid being an easy victim to this kind of cyber attacks, this kind of detection requires a powerful tool that can automatically create SQL-injection attacks using efficient features to detect the vulnerability. This study introduces a new web scanning tool (MySqlInjector) with enhanced features that will be able to conduct efficient penetration test on PHP based websites to detect SQL injection vulnerabilities. This tool will automate the penetration test process, to make it easy even for those who are not aware about hacking techniques.

ACKNOWLEDGEMENT

By the name of Allah, the Most Compassionate Most Merciful

I would like to express my gratitude to **Allah** for providing me the blessing to complete this work. Hence, I deeply gratefulness to my supportive and helpful supervisor, **Prof. Madya Abdul Bashah** for assisting and guiding me in the completion of this research. With all truthfulness, without Allah then his support, the project would not have been a complete one. **Prof. Madya Abdul Bashah** has always been my source of motivation and guidance. For that, I am truly grateful for him continual support and cooperation in assisting me all the way through the semester. In addition, I am grateful to **Prof. Dr. Zulikha** for her help to make my project successful.

I would like to present my thanks and appreciations to my mother Amal Mohammad, my father Yaseen Ibrahim, and all my family who has always been there for me. Finally, I would like to express my appreciations to my friends, colleagues, other staff, and everyone who has helped me in this journey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Penetration testing or web auditing is one of the most important topics that security researchers concern about. It aims to prove the effectiveness of the security system of such a website, because application level attacks rank at the top of nowadays cyber attacks as they are preferred by nowadays attackers. The philosophy behind web auditing is to ensure one entry point to web applications by conducting penetration tests represented by conducting sophisticated attacks on websites. Rather than one entry point to the system, it will be considered as a security flaw that attracts potential hackers to exploit it. Moreover, penetration testing covers checking against a wide range of web vulnerabilities which are related to web application level vulnerabilities such as cross-site-scripting XSS, SQL injection, IFRAME flaws, DNS attacks, web authentication flaws, remote code execution, and remote file inclusion. Exploiting any one of these vulnerabilities may enable remote attacker to gain administrative access to the infected website which gives him/her the control to deface, damage and snitch credentials (Wright, Freedman, & Liu, 2008).

Penetration testing is recommended for those critical or popular websites. It is trying to break into the organization's IT system. It aims to demonstrate the robustness of the security system, that in order to expose the vulnerabilities and giving advice on how to recover these flaws (Midian, 2003). Penetration testing is an essential requirement for

REFERENCES

Anley, C. (2002). Advanced SQL Injection In SQL Server Applications. *An NGSSoftware Insight Security Research (NISR) Publication.* Retrieved from http://www.ngssoftware.com

Basta, A., & Halton, W. (2008). *Computer Security and Penetration Testing.* USA: Thomson Course Technology.

Benini, M., & Sicari, S. (2008). Risk assessment in practice: A real case study. *Computer Communications.* 31(2008), 3691-3699.

Cardellini, V., Casalicchio, E., Colajanni, M., & Yu, P., S. (2002). The State of the Art in Locally Distributed Web-Server Systems. *ACM Computing Surveys*, 34(2). 263-311.

Danan, V. (2006, Jun 12). Use THTTPD as your Web server when Apache is overkill. *TechRepublic.* Retrieved from http://articles.techrepublic.com.com/5100-10878

Failed firm banned from selling customers' personal data. (2009, September). *Network Security*, 1-1.

Fu, X., & Qian, K. (2008, July 21). SAFELI-SQL Injection Scanner Using Symbolic Execution. *TAV-WEB- Workshop on Testing, Analysis and Verification of Web Software*, 34-39. Americus, Georgia USA.

Ghezzi, C., Jazayeri, M., & Mandrioli, D. (1994). *Fundamental of software engineering.* Upper Saddle River, NJ, USA: Prentice Hall.

Halfond, W. G. J., & Orso, A. (2005, Nov 7). EMNESIA: Analysis and Monitoring for Neutralizing SQL-Injection Attacks. *ASE '05*, 174-183. doi: 1-58113-993-4/05/0011/ACM. Long Beach, California, USA.

Heijstek, W., & Chaudron, M. R. V., (2008). Evaluation RUP Software Development Process Through Visualization of Effort Distribution. EuroMicro Conference Software Engineering and Advanced Applications, 34, 266-273. Doi: 10.1109/SEAA.

Jaferian, P., Elahi, G., Shirazi, M., & Sadeghian, B. (2005). RUPSec: Extending Business Modeling and Requirements Disciplines of RUP of Developing Secure Systems. *Proceeding of the 2005 EUROMICRO Conference on Software Engineering and Advanced Applications*, 31, IEE Computer Society.

Kals, S., Kirda, E., Kruegel, C., & Jovanovic, N. (2006). SecuBat: A Web Vulnerability Scanner. International World Wide Web Conference Committee IW3C2, 2, 247-256, Edinburgh, Scotland.

Kemalis, K., & Tzouramanis, T. (2008). SQL-IDS: A Specification-based Approach for SQL-Injection Detection. SAC '08. 2153-2158. Fertaleza, Ceara, Brazil.

Kiezun, A., Guo, P. J., Jayaraman, K., & Ernst, M. D. (2009, May 16). Automatic Creation of SQL Injection and Cross-Site Scripting Attacks. *ICSE '09*. 199-209. Vancouver, Canada.

Kruchten, P., (2002). Tutorial: Introduction to the Rational Unified Process. *ICSE '02*. 703-703. Orlando, Florida, USA.

Lemos, R. (2005). Flawed USC admissions site allowed access to application data. *SecurityFocus*. Retrieved from http://www.securityfocus.com/news/11239

Midian, P. (2003). How to ensure effective penetration test. *Information Security Technical Report*, 8(4), 65-77.

Mattsson, U. (2007, July). Defending the Database. *Network Security*, 14-17.

Newson, A. (2005, Dec). Network Threats and Vulnerability Scanner, *Network Security*, 13-15.

Roichman, A., & Gudes, E. (2007, June 22). Fine-grained Access Control to Web Database. *SACMAT '07*, 31-40, Sophia, Antipolis, France.

Su, Z., & Wassermann, G. (2006, January 11). The Essence of Command Injection Attack in Web Applications. *POPL '06*, 372-382, Charleston, South California, USA.

Tonella, P., & Ricca, F. (2004). A 2-Layer Model for the White-Box Testing of Web Applications, *6th IEEE International Workshop on Web Site Evolution WSE'04 6*, 100-107, DOI: 10.1109/WSE.2004.10012.

Tudoroiu, R., Cretu, V., & Paquet, J. (2009). Investigation using Rational Unified Process (RUP) Diagrams for Software Process Modeling. *Proceeding of the International Multi-conference on Computer Science and Information Technology*, 4, 19-26.

Whittaker, A., & Newman, D. (2006). *Penetration Testing Network Defense.* Indianapolis, USA: Cisco Press.

Wright, C., Freedman, B., & Liu, D. (2008). *The IT Regulatory and Standards Compliance Handbook.* Burlington, MA, USA: Syngress Publishing.