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

Ala’ Yaseen Ibrahim Shakhatreh, 2010. All rights reserved ©.
KOLEJ SASTERA DAN SAANS  
(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  
(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): [Signature]

Tarikh  
(Date): 11/05/2010

PROF. MADA YABDUL BASHAH MAT ALI  
Pensyarah  
Bidang Sains Gunean  
Kolej Sastera Sains  
Universiti Utara Malaysia
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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERMISSION TO USE</td>
<td>I</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>II</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>III</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td>IV</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>VII</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>VIII</td>
</tr>
</tbody>
</table>

## 1.0 INTRODUCTION

1.1 Introduction                               | 1    |
1.2 Problem Statement                          | 6    |
1.3 Research Questions                         | 7    |
1.4 Research Objectives                        | 8    |
1.5 Significance of Study                      | 8    |
1.6 Scope of the Study                        | 9    |

## 2.0 LITERATURE REVIEW

2.1 Overview                                   | 11   |
2.2 SecuBat Scanning Tool                      | 11   |
2.3 SQL-IDS Intrusion Detection System         | 12   |
2.4 SAFEI-I Intrusion Detection System          | 13   |
2.5 ARDILLA Scanning Tool                      | 14   |
2.6 AMNESIA Intrusion Detection System         | 15   |
2.7 MySqlInjector Scanning Tool ...........................................16

3.0 METHODOLOGY.................................................................20
3.1 Overview .................................................................20
3.2 Information Gathering ..................................................20
3.3 Design .................................................................22
3.4 Development ...........................................................24
3.5 Evaluation ...............................................................27

4.0 SYSTEM ANALYSIS & DESIGN...........................................33
4.1 Overview ...............................................................33
4.2 Use Case Diagram .....................................................33
4.3 Collecting System Requirements .....................................34
4.4 Activity Diagram .......................................................35
4.5 Use Case Specifications ...............................................36
4.6 Sequence Diagram .....................................................45
4.7 Collaboration Diagram ...............................................47
4.8 Class Diagram ........................................................52

5.0 PROTOTYPE TESTING & RESULTS DISCUSSION...............54
5.1 Overview ...............................................................54
5.2 Test Case 1 ...............................................................54
5.3 Test Case 2 ...............................................................64
5.4 Test Case 3 ...............................................................72
5.5 Test Case 4 ................................................................. 75
5.6 Results Discussion .................................................... 79

6.0 CONCLUSION AND RECOMMENDATION ..................... 81
   6.1 Contributions ....................................................... 81
   6.2 Conclusion .......................................................... 82
   6.3 Limitations .......................................................... 82
   6.4 Recommendation .................................................. 82

REFERENCES .................................................................. 83

APPENDIX A ................................................................. 87
LIST OF TABLES

Table 2.1: Scanning tools with their features .......................... 19

Table 3.1: Applying MySqlInjector on 50 websites for evaluation...... 30

Table 4.1: Functional and non-Functional Requirements............... 34
LIST OF FIGURES

Figure 1.1: Apache Server percentage .................................................6
Figure 3.1: MysqlInjector flow of events .............................................23
Figure 3.2: RUP Diagram ................................................................25
Figure 3.3: Appending Attacking Pattern ..............................................28
Figure 4.1: Use Case Diagram .................................................................33
Figure 4.2: Activity Diagram ..................................................................36
Figure 4.3: Use Case Injec Attacks .........................................................37
Figure 4.4: Use case Extract Website Info ..............................................39
Figure 4.5: Use case Check Protections ..................................................41
Figure 4.6: Use case Form Exploit ...........................................................43
Figure 4.7: Sequence Diagram for Inject Attacks ....................................45
Figure 4.8: Sequence Diagram for Extract Website Info .........................46
Figure 4.9: Sequence Diagram for Check Protections .............................46
Figure 4.10: Sequence Diagram for Form Exploit ..................................47
Figure 4.11: Collaboration Diagram for Inject Attacks .........................48
Figure 4.12: Collaboration Diagram for Extract Website .......................49
Figure 4.13: Collaboration Diagram for Check Protections ....................50
Figure 4.14: Collaboration Diagram for Form Exploit ............................51
Figure 4.15: Class Diagram 1 .................................................................52
Figure 4.16: Class Diagram 2 .................................................................52
Figure 4.17: Class Diagram 3 .................................................................53
Figure 4.18: Class Diagram 4 .................................................................53
Figure 5.1: A Website in Normal Situation ............................................55
Figure 5.2: Website Displaying Error Notifications ...............................56
Figure 5.3: Website's Page Loads Normally ..........................................56
Figure 5.4: Applying Order By Attack ....................................................57
Figure 5.5: Generating Error .................................................................58
Figure 5.6: Applying Union & Select Statements ....................................58
Figure 5.7: Exposing the Defected Columns .........................................59
Figure 5.8: Shows the Database Version ..............................................60
Figure 5.9: Revealing the System User ..................................................61
Figure 5.10: Revealing the Structure of Tables ......................................61
Figure 5.11: Executing MysqlInjector ....................................................62
Figure 5.12: Penetration Test Using MysqlInjector .................................63
Figure 5.13: Web Page Loads Normally ...............................................64
Figure 5.14: Website Displays Error after Injecting Attack ....................65
Figure 5.15: Appending Order By 3 .......................................................66
Figure 5.16: Returning Error With Value 4 ............................................67
Figure 5.17: Column 2 Is the Mirror of the Database .............................68
Figure 5.18: Exposing the Database Version ........................................69
Figure 5.19: Revealing Website Structure and Data .............................70
Figure 5.20: Security Assessment Using MysqlInjector .......................71
Figure 5.21: A Website in Normal Request ............................................72
Figure 5.22: Page Loads Normally After Attacking ...............................73
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.23</td>
<td>Injection Ten Attacking Patterns</td>
<td>74</td>
</tr>
<tr>
<td>5.24</td>
<td>Page Loads Normally</td>
<td>75</td>
</tr>
<tr>
<td>5.25</td>
<td>Displaying Error After Attacking</td>
<td>75</td>
</tr>
<tr>
<td>5.26</td>
<td>Page Loads Normally When Order By 1</td>
<td>76</td>
</tr>
<tr>
<td>5.27</td>
<td>The Database Entry Through Column 1</td>
<td>76</td>
</tr>
<tr>
<td>5.28</td>
<td>Obtaining Database Version</td>
<td>77</td>
</tr>
<tr>
<td>5.29</td>
<td>Information About Tables</td>
<td>77</td>
</tr>
<tr>
<td>5.30</td>
<td>MySqlInjector in Penetration Test</td>
<td>78</td>
</tr>
</tbody>
</table>
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
The contents of the thesis is for internal user only
REFERENCES


