INFORMATION SECURITY MANAGEMENT METRICS IN WEB APPLICATION

MOHD HAFIZ BIN ABD RAHIM

UNIVERSITI TEKNOLOGI MALAYSIA

INFORMATION SECURITY MANAGEMENT METRICS IN WEB APPLICATION

MOHD HAFIZ BIN ABD RAHIM

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

This project report is dedicated to my parents; Hj Abd Rahim Bin Talib and Hjh Rosemani Bt Hj Abd Ghani, for their love and prayers, to my brothers and sister; Azmi, Azhar, Izwan and Fazilah, for moral support and to my nephews and nieces; Aizat, Izza, Danial, Sarah, Farizal and Farzana for always being cute.

ACKNOWLEDGEMENT

First of all I would like to give my gratitude and thanks for my GOD, Allah for giving me wisdom and strength and the opportunity to achieve this thesis. I would like to express my deepest appreciation to my sweet supervisor, Dr Norafida Ithnin for her wisdom, patience, understanding, encouragement and for pushing me farther than I thought I could go. Furthermore, I would also like to acknowledge with much appreciation to all amazing Faculty of Computing postgraduate staffs in the front office especially Ms. Lijah for her assistance, patience and suggestions throughout my project. I would also not forget my university, UTM for the excellent facilities and environments.

I thank my wonderful parents, my father Hj Abd Rahim and my mother, Hjh Rosemani for their endless love, support and encouragement and prayers. I also would like to convey much appreciation to an awesome person from USM, Farisya "Fiesya" Azahar for helping me distribute questionnaire and getting respondents for me, without her, I would scarcely have respondents for my project.

I am not forgotten to my best buddies who always with me during the bad and the good times, Mohammed "C. Redfield" Shariff, who had accompanied me all these past two years at UTM, a companion of futsal, football and UEFA Champions League buddy and help me survive all the stress and not letting me give up. I would also like to express my gratitude to Ahmad "Naspi" Nazif for your help in programming and for being one of my respondents. I would like to thank Ahmad Zairi for being such an amazing buddy to me since undergraduate study. You guys are extraordinarily awesome.

ABSTRACT

Nowadays web application becomes an important part of every one’s life to pay bills online, to buy things online and so many more. Despite the rapid growth of web application based software, the vulnerabilities of web application and the attacks also increase rapidly too. Many web developers ignore the importance of developing web application with security in their mind. As a result, many hackers even script kiddies could gain or steal web application user’s sensitive data such as credit card number, user ID and password and so on for their own evil deeds. To evaluate the information security management metrics in web application, the researcher used questionnaire method. The respondents are web application programmer from different level such as experienced, intermediate and novice level. To help developer build web application with security in mind is to create a matrix mapping of information security management metrics in web application to raise awareness of web application vulnerabilities during the web application development. This way, it could help developer to not only raise their awareness regarding security of building a web application, moreover it could help diminished cost of fixing bugs that are found during software development life cycle phase (SDLC).

ABSTRAK

Pada masa kini aplikasi web menjadi semakin penting dalam kehidupan kita seharian untuk membayar bil secara atas talian, membeli barang-barang secara atas talian dan banyak lagi secara atas talian. Dengan pembangunan aplikasi web berasaskan perisian yang semakin pesat membangun ini, ancaman terhadap aplikasi web juga semakin meningkat. Kebanyakan pembangun aplikasi web tidak mengendahkan betapa pentingnya soal keselamatan dalam membangunkan aplikasi web. Akibatnya, para penggodam-penggodam web mengambil kesempatan ini dengan mencuri data-data sensitif pengguna-pengguna aplikasi web seperti nombor kad kredit, nama pengguna dan kata laluan untuk menjalankan niat jahat mereka. Untuk menilai matrik pengurusan keselamatan maklumat dalam aplikasi web, penyelidik menggunakan kaedah soal kaji selidik. Responden adalah terdiri daripada pengaturcara yang berpengalaman, pertengahan dan juga permulaan. Untuk membantu pembangun membina aplikasi web dengan keselamatan di minda mereka adalah dengan mencipta pemetaan matriks berdasarkan pengurusan keselamatan maklumat dalam aplikasi web untuk membangkitkan kesedaran terhadap kelemahan-kelemahan semasa pembangunan aplikasi web. Dengan cara ini, ianya dapat mambantu para pembangun web dengan bukan sahaja membangkitkan kesedaran tentang keselamatan semasa membangunkan perisian, malah dapat mengurangkan kos membaiki ralat-ralat yang dijumpai semasa fasa kitar hayat pembangunan perisian (SDLC).

TABLE OF CONTENT

CHAPTER **TITLE** **PAGE**

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

OWASP	Open Web Application Security Project
WASC	Web Application Security Consortium
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
SANS	SysAdmin, Audit, Networking and Security
MITRE	Massachusetts Institute of Technology Research and Engineering
PCI DSS	Payment Card Industry Data Security Standard
DISA	Defense Information Systems Agency
FTC	Federal Trade Commission
CIA	Confidential, Integrity and Availability
SQL	Structured Query Language
XSS	Cross Site Scripting
IT	Information Technology
CSRF	Cross Site Request Forgery
OS	Operating System
LDAP	Lightweight Directory Access Protocol
HTTP	Hyper Text Transfer Protocol
SSI	Simple Sensor Interface
XML	Extensible Markup Language
URL	Uniform Resource Locator
DOR	Direct Object Reference
UAT	User Acceptance Testing
SDLC	Software Development Life Cycle
UTM	Universiti Teknologi Malaysia
USM	Universiti Sains Malaysia

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, web application has become very useful for almost every business around the globe. From online banking, pay bills online, online bookstores, e-learning, online auctions; even people love to buy music online. Moreover, with the rapid growth of mobile enabled web application for smart phones or iPhones, now consumer can do their online business anytime and anywhere.

Nevertheless, despite the popularity growth of web based application, many organizations and business owners spend a lot of time encountering web application threats and learning how to mitigate them. Moreover, web application vulnerabilities also become a threat to web applications CIA triangle which is confidentiality, integrity and availability. Many attackers have their own evil deeds to break the confidentiality, integrity and availability of web application. Web application become more vulnerable to a number of malicious attacks led by these kind of internet scum.

Unfortunately, many web application developers simply ignore the importance of building the web application with security in their mind. As a result, the web application becomes more susceptible to a great number of web application attacks such as the most dangerous web application attack, the SQL Injection and

Cross Site Scripting (XSS) attack. These kind of attacks could severe the web application by stealing the important data from the web application's users or customers. The important data are such as username, password, credit card number and other sensitive credentials that should be protected from unauthorized person.

It is imperative for web application developer to integrate security in the very early phase of Software Development Life Cycle (SDLC) to mitigate the risk of web application vulnerabilities and attacks. This is because it could become so expensive to fix the error or security bugs after the web application has been deployed. Nevertheless there are ways to help developer to mitigate the risk of being attack by malicious attackers.

There must have been a security awareness document that could help developers to raise awareness about building web application with security in mind. There are many of security awareness documents out there such as OWASP 2010 Top Ten, WASC Threat Classification or even CWE/SANS 2011 Top 25. Each of these security awareness documents has its own guidelines but there are no standard exist to help developer raise awareness about building web application with security in mind.

1.2 Problem Background

At the moment, security flaws grow almost equally with the growth of web application. There are more than a few security vulnerabilities exist in web application. In addition, most web application developer simply ignores the importance of developing web application that integrated with security in the early phase of SDLC. This is because by following to integrate security in the early phase of SDLC will slower the time of the completion of the web application. In this case, the security once again was being sacrificed for the sake of short dead line.

However, by sacrifice the security in the development of web application, there are high price to pay; the web application now susceptible to a number of web application attacks and vulnerabilities. Moreover, fixing the bugs after the web application has been deployed would cost so expensively. Many researchers stated that web application developer especially programmer need to learn the security coding best practise (Antunes, N., 2012) because they cannot prevent security flaws if they do not know how to use secure coding practises. It is also imperative for web application developer to learn secure coding practise and training. The skills of secure coding practise such as been able to handle error message more robustly and prevent from reveal unsecure error message that could become susceptible to web application attacks and vulnerabilities.

In this study, to help developer build web application with security in mind is to create a matrix mapping of information security management metrics in web application to raise awareness of web application vulnerabilities during the web application development. This way, it could help developer to not only raise their awareness regarding security of building a web application, moreover it could help diminished cost of fixing bugs that are found during software development life cycle phase (SDLC).

1.3 Problem Statement

According to the problem background above, this shows that there is no standards exist to help developer to raise awareness about building web application with security in mind. There are several security awareness documents out there, but each of the security awareness documents has its own guidelines and way to mitigate risk in web application. The problem is, some of the document focused only ten of web application risks, some of them focused only twenty-five the most widespread software error and some focused on both attacks and weaknesses found in web application and has loosely outlined where in software development cycle phase the web application vulnerability could occur. Here, this project to create a matrix mapping that could integrate all the security awareness documents as a list of vulnerabilities that occur in the Software Development Life Cycle (SDLC) phase and also to mapped with web application detection mechanisms; White-box and Black-box Analysis, where in the SDLC phase it should be performed.

1.4 Project Aim

The aim of this project is to recommend metrics in information security management in web application.

1.5 Project Objectives

The objectives of this project are as follows:

i. To study and analyze three security awareness documents; OWASP 2010 Top Ten, WASC Threat Classification and CWE/SANS 2011 Top 25.

ii. To recommend the metrics of information security management in web application.

iii. To validate the recommend matrix mapping of information security management in web application.

1.6 Project Scope

The scopes of this project are:

1. The research focused on security awareness documents only, not standard.
2. The research is not generalized, only specific and focused on web application vulnerabilities only.
3. The experts are web application developer including programmer, system analyst and IT officer. They come from experienced, intermediate and novice level.

1.7 Organization of Report

This report comprises of six chapters. The chapters are organized with different works that involved in this study. The details on each chapter are described in the following paragraphs. Chapter 1 consists of overview the project, problem background, problem statement, objectives and scope of this project. Chapter 2 of this report presents the literature review of web application vulnerabilities' security awareness documents. It discussed about the related information about OWASP 2010, WASC Threat Classification and CWE/SANS 2011 Top 25, methods for detecting web application vulnerability and why information security metrics is needed in building web application. Chapter 3 of this report discussed about the research methodology used. Chapter 4 of this report explained about list of vulnerabilities and recommended metrics in information security management in web application. Chapter 5 of this report is about the discussion of analysis, results and the experts' feedback. Chapter 6 is the concluding chapter which discussed of achievements, challenges and constraints of this project.

REFERENCES

Antunes, N., Vieira, M.(2011). *Defending Against Web Application Vulnerabilities*. University of Coimbra, Portugal.

Antunes, N.; Vieira, M.; , "*The Devils Behind Web Application Vulnerabilities*," Computer , vol.PP, no.99, pp.1, 0 doi: 10.1109/MC.2011.259 2011 URL: *http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5999632&isnumber=5306045*

Alshammari, B.; Fidge, C.; Corney, D.; , "*Security Metrics for Object-Oriented Designs*," Software Engineering Conference (ASWEC), 2010 21st Australian , vol., no., pp.55-64, 6-9 April 2010 doi: 10.1109/ASWEC.2010.34

Abdulrazeg, Ala A.; Norwawi, Norita Md; Basir, Nurlida; , "*Security metrics to improve misuse case model*," Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on , vol., no., pp.94-99, 26-28 June 2012 doi: 10.1109/CyberSec.2012.6246129

B. Arkin, S. Stender, and G. McGraw, "*Software Penetration Testing*," IEEE Security & Privacy, Jan.-Feb. 2005, pp. 84-87.

Shao, S. Khurshid, and D. E. Perry, "*A Case for White-box Testing Using Declarative Specifications Poster Abstract*," in Testing: Academic and Industrial Conference Practice and Research Techniques - MUTATION, 2007. TAICPART-MUTATION 2007, 2007, p. 137.

DD.P. Freedman and G.M. Weinberg, *Handbook of Walkthroughs, Inspections, and Technical Reviews: Evaluating Programs, Projects, and Products, Dorset House*, 2000.

D. Stuttard and M. Pinto, *The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws*, John Wiley & Sons, 2007.

F. Saglietti, N. Oster, and F. Pinte, "*White and grey-box verification and validation approaches for safety- and security-critical software systems*," Information Security Technical Report, vol. 13, no. 1, pp. 10–16, 2008.

Herrera, S.O.S.; , "*Information security management metrics development*," Security Technology, 2005. CCST '05. 39th Annual 2005 International Carnahan Conference on , vol., no., pp. 51- 56, 11-14 Oct. 2005 doi: 10.1109/CCST.2005.1594818

N. Ayewah and W. Pugh, "*A Report on a Survey and Study of Static Analysis Users*," Proc. Workshop Defects in Large Software Systems (DEFECTS 08) ACM, 2008, pp. 1-5.

OWASP Foundation. (2010). “*Top 10 2010 – OWASP*.” Accessed at: *https://www.owasp.org/index.php/Main_Page*

Shar, Lwin Khin (2012). *Defending Against Cross-Site*. Nanyang Technol. Univ., Singapore, Singapore.

T. Murnane and K. Reed, “*On the effectiveness of mutation analysis as a black box testing technique*,” in Software Engineering Conference, 2001. Proceedings. 2001 Australian, 2001, pp. 12 –20.

Wei Qu; De-Zheng Zhang; , "*Security Metrics Models and Application with SVM in Information Security Management*," Machine Learning and Cybernetics, 2007 International Conference on , vol.6, no., pp.3234-3238, 19-22 Aug. 2007 doi: 10.1109/ICMLC.2007.4370705

Wong, Caroline (2012). *A Beginner’s Guide: Security Metrics*. McGraw Hill.

Yu, W.D.; Le, K.; , "*Towards a Secure Software Development Lifecycle with SQUARE+R*," Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE 36th Annual , vol., no., pp.565-570, 16-20 July 2012 doi: 10.1109/COMPSACW.2012.104