THE KEY RISK INDICATORS OF WEB SITE SECURITY

Lee, SungJoong[1]
Lotte Data Communication Company

Lee, YoungJai[2]
Dongguk University

Keywords: KRI, Risk, Web, Hacking

Abstract

This research is based on IT Security risk assessment on Web Site. It is carried out from 16th JAN 2006 to 24th MAR 2006. The research showed the how much Vulnerability is there through Web Site.To analyze and reduce IT security risks on Web Site, this research used Security Risk on WEB Site by OWASP's TOP 10 Vulnerability.

According to Risk Classification by OWASP's TOP 10 Vulnerability and Tiger Team's[3] own Methodology, the target web sites are selected by a group of web diagnostic specialists. For each web site, the mock diagnosis is implemented for the risk items, and Root causes are analyzed.

Throughout the analysis, we could analyze the vulnerability exist on Web site, find out root causes and classify them, and finally we could find out Key Risk Indicator (KRIs) which needed to make the Risk Assessment Model for the Web sites.

Introduction

It is now a trend that the number of Domestic/International Web sites is continually increasing. Also, the number of corporate business purpose Web sites are also increasing and the amount of information data is exponentially increasing as well.

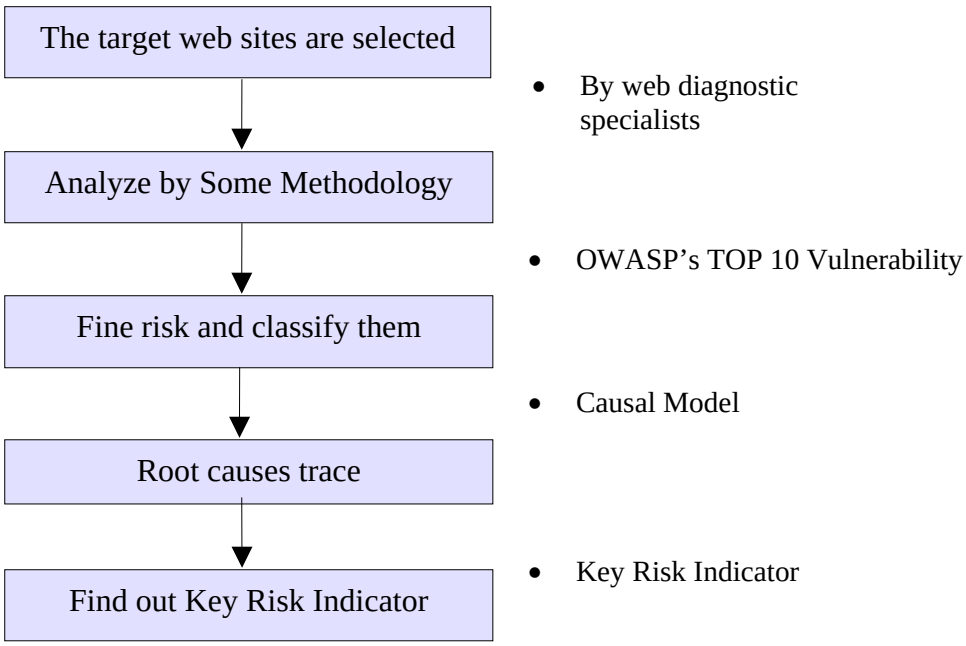
The following table is the statistics of Web site vulnerability which announced by www.scientechsecurity.com (Author: Robert Lemus). It defines the trend that the figures are rapidly increasing.

[1] IT Security Team Manager, Lotte Data Communication Company
Doctoral student of MIS, Graduate School of Dongguk University
Off) 82-2-2102-1021, Cell) 82-11-240-4800, Email: tagging@empal.com
[2] Chairman of TIEMS KOREA Chapter / Chairman of KOREA Business Continuity Plan Associative, 26-3-ga Pil-Dong, Chung-gu, Dongguk University, Seoul, Korea 100-715
Off) 82-2-2260-3297, Cell) 82-18-339-6386, Email: yjlee@dgu.edu
[3] The derivation of the "Tiger Team" is originally come from the military. A Tiger-Team performs a simulated attack on a web site and evaluates their security measures such as web vulnerability.

	2005	2004	2003	2003	2002
CERT/CC	5,990	3,780	3,784	4,129	2,437
NVD	4,584	2,340	1,248	1,943	1,672
OSVDB	7,187	4,629	2,632	2,184	1,656
Symantec	3,766	2,691	2,676	2,604	1,472

[Table 1. Increase of WEB SITE Vulnerability]

However, in this research, with priority given to research and analysis of vulnerability on Web site development, the Key Risk Indicator (KRIs) about building and designing a safe Web Site is studied.



<Picture 1> Research and Analysis Model

This Study of Security Risk on Web Site took a part of the project about Information security and cognition raise for a particular corporate. The whole project was implemented as following steps.

The specialist group examined with the Delphi Technique, and selected the preferential observing sites to perform the penetration test, so that the mock hacking and vulnerability analysis are implemented. Finally, the deduced risks are classified, and the root causes are found at last.

It took Two and a half months to analyze a numbers of sample sites' mock hacking and vulnerability analysis, and the scope of this research was limited for a particular corporate Web Site operation.

The Research purpose

Korea is the country that has a various environments for many different Web sites developed, so that on-line commercial transaction and internet information communion culture is highly developed.

Along with such Web site development, the cyber contrary function become a deepen issue. The various types of vulnerability such as degeneration of language, violence, porn and virus diffusion, infringement of copyright, outflow of digital assets and hacking are spreading.

The result that focused on mock hacking and vulnerability analysis is examined as for the basic data to compute KPI and to make propriety Web Site risk avoidance model.

The purpose were to minimize the risk during Web Site and operation, to deduce the risk factors that need to be preferentially managed, and to defined the priority ranks, then deduce Key Risk Indicator, and finally to educate web developers with the guide in future.

Such KRI minimize the risk that caused by the error in designing and developing Web Site and materialize the analysis model for vulnerability with implementing Web Site Development guideline.

Also, the education and examination would be done so that the risk on designing and coding could be minimized, and the ratio of risk and improvement of vulnerability could be measured in the long term of period.

Data Analysis

The risk assessment is examined according to OWASP's TOP 10 Vulnerability (Open Web Application Security Project) Standards and the Tiger Team's self inspection checklist. Security specialists set up the tiger-team, and examined the major sample Sites by mock hacking through the penetrate test.

Also, the risk analysis computed the examination checklist with using OWASP's Top 10 most critical Web application security flaws as a base model.

1. Non-validated input
2. Broken access control
3. Broken authentication and session management
4. Cross site scripting
5. Buffer overflows
6. Injection flaws
7. Improper error handling
8. Insecure storage
9. Denial of service
10. Insecure configuration management

These can be summarized as below 21 items if reclassified with examination actual checklist.

1. XSS (Cross Site Scripting) attack
2. Attack using Vulnerable PC configuration
3. Information outflow by malicious program like key logger
4. Information outflow by vulnerable browser (lack of patch)
5. URL interpretation (vector variable fabrication)
6. Directory Indexing vulnerability attach
7. Absolute path extraction by induction of error
8. Exploiting URL parsing attack
9. XSS (Cross Site Scripting) attack
10. SSL Man-in-middle-Attack
11. Servelet, EJB, Applet vulnerability attack
12. CLASS files decompiling attack
13. Parameter Tampering attack

14. File Upload/Download vulnerability attack
15. SQL Injection attack
16. Path Traversal attack
17. SQL Poisoning attack
18. Outflow of DB Schema
19. System O/S Authorization acquisition through DB
20. Web Command Prompt
21. System/Administrator root account acquisition

We performed the real examination with the experts using the checklist above. And Data is summarized in Table 2 as shown below.

File Upload	File Download	SQL Injection	XSS	Authentication & Session Management	Weak Access Control	Unnecessary Files	Error in O/S environment	Weak error control
19	14	21	23	20	36	34	30	14

[Table 2] The risk of Web Sites Unit = No of count

These vulnerabilities are reclassified to the business impact assessment by classification procedures in different kinds of business impact assessment tables

Business Impact Assessment Table		
Information outflow	Customer	Many registered customer information (Name, Resident number, ID/Password, Address etc.)
	Internal	Many internal employees' information (Name, ID number, Password, Resident number, Address etc.)
System destruction	Possible to delete system files by uploading web shell	
	Possible to delete DB, Table by accessing DBMS through weak access control to DBMS	
	Possible to delete system file by accessing through Telnet/FTP	
System information acquisition	Source Information	Possible to download Source code through file download vulnerability
		In case of existence of Source backup file
		In case of uploading web shell
	Simple Information	Possible to obtain information by exposing system configuration files
		In case that ID/Password in cookie are obtained by snipping and XSS
		In case that Web service sample file is exist
		Possible to expose important information by directory listing vulnerability
		In case that source backup file is exist
Information fabrication	Money fabrication	In case that money related fabrication is possible through accessing DBMS (bid, estimate, sales price etc.)
		In case that buying price in internet shopping mall can be fabricated
	Genuine fabrication	In case of Homepage alteration is possible
		SQL Injection / Replay Attack, Log-in information snipping can fabricate so that the other user's information can be exposed
		In case that DBMS data can be altered.

		In case that writing can be done on administrator only bulletin(notice) board
		Possible to alter and delete the other person's writings

[Table 4] Business Impact Assessment of Web Site Vulnerability

Such results of business impact analysis which based on assessment table above are requested to fix according to Quick_Fix Management procedure. 44 Information outflows, 22 System destruction errors, 66 system information acquisitions, 39 Information fabrications are summarized and fixed.

Unit = No of count

Execution result	Information outflow		System destruction error	System information acquisition error		Information fabrication error	
Company & SITE	Customer	Internal		Source information	Simple Information	Money fabrication	Genuine fabrication
TOTAL	19	24	22	22	44	6	33

[Table 4] Results of business impact assessment on Web site vulnerability.

According to [Table 5] The RISK and Vulnerability Causal Model, the causes of such risks can be defined as below.

1. Absence of education for developers (Web hacking/Safe coding style training)
2. Absence of Developer training (Web hacking/Safe coding style training) and Source code examination solution
3. Absence of Network operator targeted training
4. Absence of System operator targeted training/periodic examination on configuration file
5. Absence of Periodic examination on source file backup
6. Absence of DBMS access control solution and Network segmentation

Level 1	Level 2	Cause	a reform measure
Information spillage	Customer's Information	developers coding style problems	Absence of Developer training (Web hacking/Safe coding style training) and Source code examination solution
		developers configuration problems	Absence of DBMS access control solution and Network segmentation
	Private Information	developers coding style problems	Absence of education for developers (Web hacking/Safe coding style training)
		developers configuration problems	Absence of DBMS access control solution and Network segmentation
System demonstration	OS,DBMS	developers coding style problems	Absence of education for developers (Web hacking/Safe coding style training) and Source code examination solution
		developers configuration problems	Absence of DBMS access control solution and Network segmentation
		firewall rule configuration problems	Absence of Network operator targeted training
System Information	Source Code	developers coding style problems	Absence of education for developers (Web hacking/Safe coding style training) and Source code examination solution
		developers configuration problems	Absence of Periodic examination on source file backup

	Simple System Information	developers configuration problems	Absence of System operator targeted training and Periodic examination on source file backup
		developers coding style problems	Absence of education for developers (Web hacking/Safe coding style training) and Source code examination solution
Information falsification	Money falsification	developers configuration problems	Absence of DBMS access control solution and Network segmentation
		developers coding style problems	Absence of education for developers (Web hacking/Safe coding style training) and Source code examination solution
	Data falsification	coding style and configuration problems	Absence of education for developers (Web hacking/Safe coding style training) and Source code examination solution
		developers coding style problems	Absence of education for developers (Web hacking/Safe coding style training) and Source code examination solution
		developers configuration problems	DBMS access control solution and Network segmentation
		developers coding style problems	Absence of education for developers (Web hacking/Safe coding style training) and Source code examination solution
		developers coding style problems	Absence of education for developers (Web hacking/Safe coding style training) and Source code examination solution

[Table 5] The RISK and Vulnerability Causal Model

Summary and Conclusion

This research has eagerly watching results in two main focuses. Firstly, Web-business is rapidly growing in Korea at present, Web site risk analysis is tried comparatively in practice, and throughout the Key Risk Indicator (KRIs) analysis, Web site security risks are defined as indicators even though they were restrictive.

Secondly, the basic indication to bring up the training on developers and management objects could be found by analysis on web site risk, defining and classifying root causes and defining priority ranks for KRI.

However, suggestion for future research to complement and improve is, to be able to minimize the risk efficiently, the Risk Avoidance Model regarding on the Key Risk Indicator which measured in this research is needed to be studied and verified research model.

Also, the priority rank for measured KRI is needed to be done, Training on developers and management object are needed to be indicated, and finally, the results from them are needed to be indexed for the future.

Throughout such research, Web site security GUIDE which is based on Risk Avoidance Model can be established, so that it can be set up and apply to the developers who are participated on the particular projects.

Reference

National Computerization Agency, Guideline for Incident & Problem Management of Information System, October, 2004.

Youn, Ju-Yong, “A Study on Crisis Management System for Information Technology,”Doctoral Dissertation, 1999.

Lee Young-Jai, "Critical Issue for Business Area Impact Analysis in Business Crisis Management," TIEMS Conference, 1999.

M.Hondo , "Securing Web Service" IBM System Journal Vol 41, NO 2 , 2004.

Jahan Moreh "Profiles of Web Services Security", CSI , November 14, 2005

Yen-Ming Chen "Web Application Security Scorecard" , CSI , November 14, 2005

John Weinschenk "The Web ApplicationSecurity Crisis" CSI , November 14th, 2005