International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.203-212
http://dx.doi.org/10.14257/ijsia.2016.10.7.18

A Study on the Web Services Vulnerability Assessment Plan

Sang-Wook Cha[1], Jong-Suk Park[2], Jangyoun Cho[3], Kyeong-seok Han[4] and Jong-Bae Kim[5*]

[1,2,3,4]Department of IT Policy and Management, Graduate School of Soongsil University, Seoul, 156-743, Korea
[5]Graduate School of Software, Soongsil University, Seoul 156-743,*
[1]icha71@kcue.or.kr, [2]ayman@cgbest.co.kr, [3]chonice@gmail.com,
[4]kshan@ssu.ac.kr, [5]kjb123@ssu.ac.kr*

Abstract

Many companies and governments have been rapidly progressing and expanding their Web services, and have recently invested a lot of time and money for a safer cyber environment to protect implementation and information assets and personal information. However, web hacking techniques to gain knowledge and evolution of web hacking through the web site are still putting a serious threat to Web services. In this paper, OWASP TOP10, NIS 8 vulnerability, Financial Supervisory Service (FSS) designed according to the simulated hacking scenarios 11 vulnerability to attacks based proposes a method for analyzing the vulnerability by check.

Keywords*: Web services, vulnerability, threat, information Assets, simulated hacking*

1. Introduction

Recently, there has been an increase in the possibility for a firm’s information asset and privacy information to be invaded under smart IT environments like SNS (social network services) and cloud service, and there are worries about the occurrence of large-scale damage contrary to the IT damage in the past times.

With cyber attacks now being more sophisticated and highly developed, serious social problems like financial incidents may become more common and can even further intensify into cyber wars between countries. Therefore, each firm and each government should devise highly advanced technological and legal institutional actions against highly complex cyber invasion attacks.

In the age of IoT where everything is connected to each other via the Internet particularly, IT security should be more flexible in dealing with each situation that it faces with the IT & mobile devices used by users to the cloud infrastructure distributing the information on the basis of cloud. Additionally, there should be set flexible security strategies in stage of front-end and back-end depending on the degree of threat under the idea that “there exist different threatening factors depending on what is used and what should be protected.”

Hence, this study intends to suggest a way to analyze the vulnerabilities of a firm’s web-service penetration testing in order to minimize social and economic damages like information leakage by a malicious user, interference of system service, and even data loss by investigating a way to develop the simulated penetration test so as to grasp the IT system asset’s vulnerability specification.

[5*] Corresponding author. Tel. : +82-10-9027-3148.
Email address: kjb123@ssu.ac.kr(Jong-Bae Kim).

2. Concept of Penetration Testing

2.1. Concept of Hacking and Domestic Status of Hacking

Hacking means the act of invading other computers regardless of any intention; that is, a malicious behavior wherein a computer user invades other computer systems without authorization and performs a wrongful action.

Here, the wrongful action means the illegal use of other computer systems, the illegal viewing of someone else's computer data, and the illegal leakage and falsification of data [1]. The number of reports about hacking accidents and privacy leakages are listed in [Table 1], according to Korea Internet and Security Agency's 「Monthly Report of Internet Invasion Accidents and Their Analysis」 and the KISA' Internet Statistical Information Research System.

Also, the number detecting malicious codes was 2,415, 046 in 2013, while its number in present 2015 is 517,701. As seen in [Table 1], the cause in the increase of the number of reported hacking accidents in 2012 might be attributed to a number of personal PCs being misused in performing some port-scan attacks, DDos attacks, and sending spam mails via hackers' remote controls, and it is expected that there will be continued hackers' attacks targeting firms like the web hacking exploiting a web server's vulnerabilities and the DDos attack. Therefore, some comprehensive information-protecting activities for web-services should be required.

Table 1. Font Sizes of Headings. Table captions should always be positioned above the tables.

Classification (year)	Number of Hacking Accidents	Number of Privacy Infringement Counselling
2010	16,295	54,832
2011	11,690	122,215
2012	19,570	166,801
2013	10,600	177,736
First Half of 2014	8,078	103,197

2.2. Penetration Testing

Penetration testing is a simulated penetrating test for grasping the vulnerability specification of targeting an information system's assets.

The purpose of penetration testing is to grasp the vulnerability of targeting information system's assets in terms of the security operation and to suggest which things to be improved in order to prevent any social and economic damages like privacy leakage and data loss by a malicious user. This test is also referred to using other terms like Pen-testing, simulated penetration testing, or the simulation hacking test, and this test is a part of the process for actively evaluating the targeting organization's intelligence security level, so it is performed in a simulation where a real hacking is occurred.

3. Diagnosis Method of Simulation Hacking

3.1. Simulation Hacking Method

In this study, the simulation hacking was conducted under a written penetration testing scenario wherein a virtual hacker invaded the Korean government's major online systems and some portal sites on the Intranet on the basis of the simulation hacking methodology, which was adapted to domestic computation control environment after having referred international/domestic security models and hacking status in use of the 'Online Intelligence vulnerabilities of Top 10 Web Applications' and the '8 Online Intelligence Vulnerabilities' reported by National Intelligence Service and the '11 Online Intelligence Vulnerabilities' reported by Financial Supervisory Service.

The first step was the information-collection step that, as the outside target for this simulation hacking, there were major web services of organizations for the investigator to enable access to on the Internet and their relevant servers, and then collected the information of corresponding systems using of the use service and the vulnerability scanning function toward the servers and the web applications.

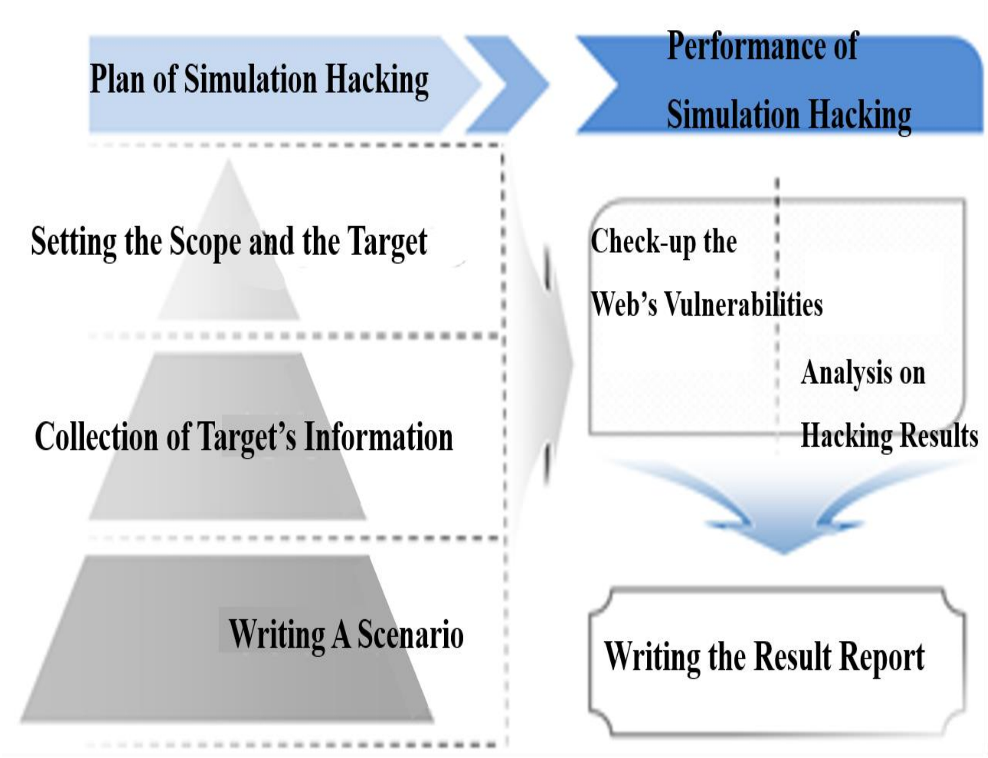
Plan of Simulation Hacking
Performance of Simulation Hacking
Setting the Scope and the Target
Collection of Target's Information
Writing A Scenario
Check-up the Web's Vulnerabilities
Analysis on Hacking Results
Writing the Result Report

Figure 1. One Simulation Hacking's Work Flow

The second step is the vulnerability listing step, which listed the information (the applications use ports and the vulnerability information) having been collected from the information-collection step, and categorized the vulnerability by risk level after analyzing the information.

The third step is the invasion step wherein in cases of existence of high-risk vulnerabilities having been detected from the vulnerability list, the investigator tried an attack toward the web or the server in order to seize the web manager's authority and server's authority in exploiting vulnerability or using a certain web hacking skill.

Table 2. Attack Types at the Simulation Hacking Trial

Classific ation	Attack type	Explanation
Server System	Password Guessing	Method wherein a hacker randomly enters a user′s account and password and connect to the target server
	Detecting Files Containi ng Sensitive Information	Attack the target server after acquiring some files incl uding the user′s account file and password file.
	Password Crack	Method acquiring the chance to access to the root wit h /etc/password file′s reading authority.
	Exploiting vulnerable Se rvices	Attack the server system in case the vulnerability patc h is not appropriately performed.
WEB/W AS Server	Password Guessing	Method wherein an attacker randomly enters a user′s account and password and connect to the target server
	Directory Listing)	Method accessing the web browser in case that the dir ectory listing is allowed.
	Detecting Files/Pages Co ntaining Sensitive Inform ation	Method attacking the target server after acquiring some files including the user′s account and password files.
Applicat ion System	Password Guessing	Method wherein an attacker randomly enters a user′s account and password and connect to the application system.
	Authentication Routing	When there is no authentication like the manager funct ion or such function is not appropriate.
	XSS Attack (CrossSite Scripting)	Method wherein an attacker maliciously enters the java script in the targeting application system and makes t he user execute the system.
	SQL Injection	Method wherein an attacker approaches to the data in DB or the store procedure via the web′s application.

DB MS	Password Guessing	Method wherein an attacker randomly enters a user′s account and password and connect to the DB
Network	Routing of Invasion-Shutting System	Method wherein an attacker installs the back door inside the target system and connect it to the outside of invasion-shutting system.

3.2. Simulation Hacking Scenario

For the inside simulation hacking, it is the method wherein an attacker tries to access the inside of the target system not having any security settings from outside via a remote router. With this method, an attacker can access the target system’s inside network through wireless hacking, and also attacks the system network after collecting important information by scanning the system’s inside network.

Also, an attacker can do a hacking trial by scanning the system’s important servers, DBMS, and personal PCs in using a vulnerable service that is open for the work purpose, or any share folder wherein the security option is not applied in order to identify whether there exists important information and the server’s account information, and to seize them.

In another method, an attacker can identify whether the firm’s information and the user’s privacy information are leaked by approaching the target system’s network, its important servers and DBMS in exploiting the web Vulnerabilities existing in the operating server.

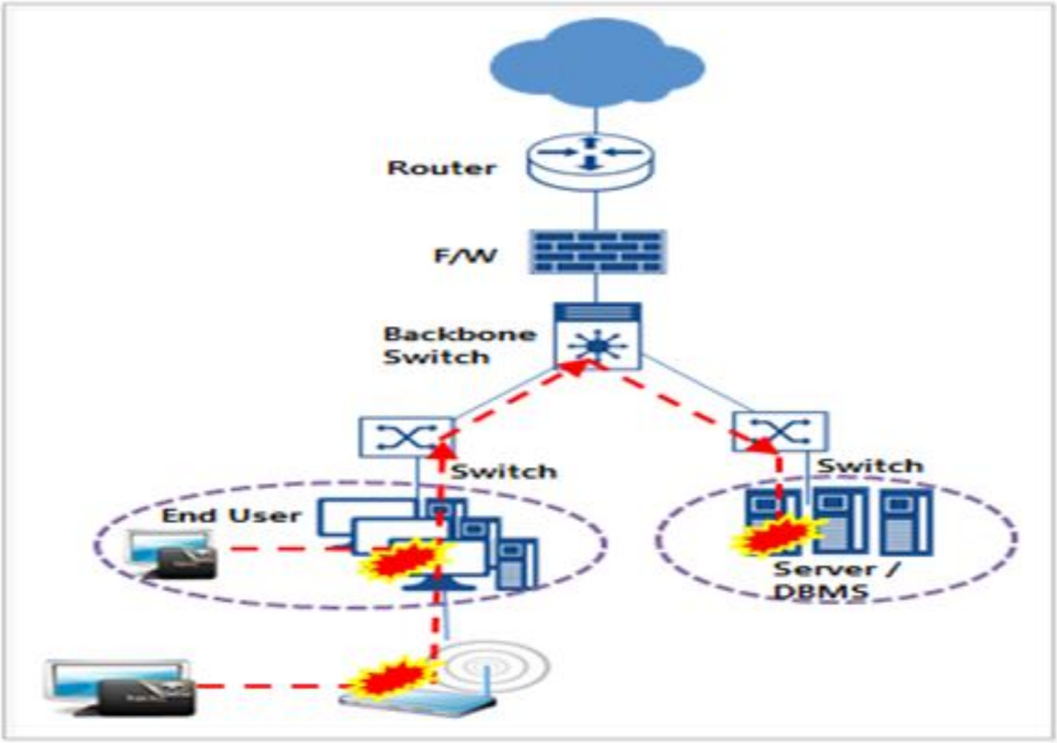

Figure 2. Inside Simulation Hacking’s Flow Chart

For the outside simulation hacking, an attacker attacks a web application (homepage) which can be accessed from the outside and checks whether privacy information and important files in the server were leaked in using the exposed vulnerabilities, and in case the invasion into the web’s operation server in utilizing the web application’s certain

Vulnerabilities is enabled, the attacker tries to access its inside network and its major server systems or tries to access to the systems, and then identify whether any information leakage was indeed leaked or not.

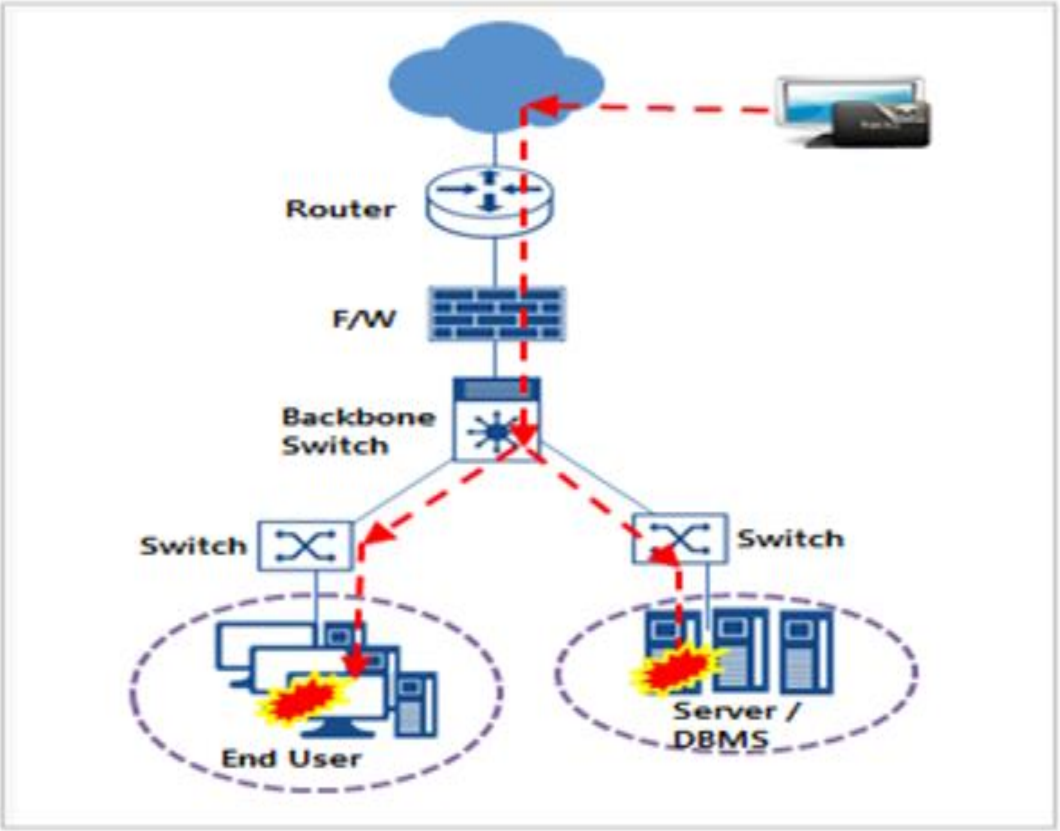

Figure 3. Outside Simulation Hacking's Flow Chart

4. Check Items in the Simulation Hacking

4.1. Check Items in the Simulation Hacking

In order to evaluate the reliability of the simulation hacking's check-up and the safe diagnosis against hacking trials, this study made a check list about the check items in the National Intelligence Service's 8 online Vulnerabilities and the Financial Supervisory Service's 11 online Vulnerabilities. This list is seen in [Table 3].

Table 3. List Mapping for Checking Items in Simulation Hacking and Its Vulnerabilities

Check Items in the Simulation Hacking		Risk Level	Vulnerability List
No Verification Method for Entered value	Diagnose whether SQL phrase can be inserted.	H	OWASP TOP 10 Injection Vulnerability Cross Site Scripting Unsecure Authentication and Unsecure Session Management Reference of Unsecure Direct Objective Cross Site Request Forgery(CSRF) Wrong Security Setting Store of Unsecure Encryption Poor URL Connection Control Protection of Insufficient Transport Layer Unverified Redirect and Forward
	Diagnose whether the XSS/CSF attack is possible.	H	
	Diagnose the reference possibility of Unsecure, direct objective.	M	
	Diagnose the possibility manipulating the hidden field.	M	
Treatment of Vulnerable Files	Diagnose the possibility to upload and remote execute malicious files.	H	
	Diagnose the vulnerabilities at downloading important information files.	H	
Vulnerable Access Control	Diagnose the possibility that the manager pager is exposed and guessed.	M	
	Diagnose the possibility that the backup file and the text file are existed.	L	Financial Supervisory Service′s 11 Online Vulnerabilities SQL Injection Vulnerability XSS Vulnerability Directory List Exposure Vulnerability Manager Page Exposure Vulnerability File Upload Vulnerability File Download Vulnerability Parameter Falsification Vulnerability Vulnerable Authentication Vulner
Vulnerable Authentication Session and Management	Diagnose the possibilities to manipulate the cookie file and to seize the session.	H	
	Diagnose the possibility that any redirect and forward not being verified are existed.	M	
	Diagnose whether the user′s browser is authenticated.	M	
	Diagnose whether there is any coding which is vulnerable in terms of authentication information	M	

Poor Management and Control of Vulnerable Account	Diagnose whether the authentication and privacy information can be transmitted in form of plain language.	M	ability Unnecessary File Exposure Vulnerability Vulnerability Not-Verified Redirect and Forward Vulnerability
	Diagnose whether the vulnerable account and the default account can be used.	H	
	Diagnose whether there is any password policy or not and (if existed) the policy is applied to the password control.	L	
Wrong Security Setting	Diagnose whether the command injection is possible.	H	
	Diagnose whether the directory list is exposed.	M	
	Diagnose whether any information is exposed through the error page.	L	National Intelligence Service's 8 Online Vulnerabilities
	Diagnose whether any information is exposed by unnecessary note.	L	
	Diagnose whether there is any wrong security construction	M	SQL Injection Vulnerability XSS Vulnerability Directory LIsting File Download Vulnerability File Upload Vulnerability Technote Vulnerability Zeroboard Vulnerability WEBDAV Vulnerability
Vulnerable S/W Use	Diagnose the security construction's state resulting from the use of open S/W	M	
	Diagnose the security construction of bulletin board S/W	H	
Other Security Actions	Diagnose whether any research engine is exposed.	L	

4.2. Risk Levels of Check Items in the Simulation Hacking

The vulnerabilities found in conducting the simulation hacking trial could be divided into three categorizes of high risk, medium risk, and low risk, according to each vulnerability's risk level to influence the web application.

Here, high risk means the risk level wherein the web application can be directly influenced, like authority acquisition and service interference, but also to extract privacy information and then manipulate the information like data forging and falsification. Medium risk implies the risk level wherein some important information like the authentication information, the user's privacy information, the web application's inside information, and the application's execution information can be exposed. Finally, low risk means the risk level wherein the information to be rarely exploited directly in any invasion can be exposed.

5. Conclusion

This study described the system checking the vulnerabilities known about web services through simulation hacking. The Korean IT system environment is represented as the world-best Internet environment.

Also, due to the occurrence of large-scale privacy-leakage accidents, there have been recently emerging matters regarding privacy protection in cyber space. Therefore, each firm should regularly conduct an analysis on the vulnerabilities of its server, network, DBMS, application systems, and WEB/WAS server, etc. around the OWASP Top 10, the Financial Supervisory Service's 11 Online Vulnerabilities, which were described in this study, and the National Intelligence Service's 8 Vulnerabilities, and remedy any discovered vulnerabilities. Also, as being investigated in this study, simulation hacking can be classified into inside simulation hacking and outside simulation hacking.

Simulation hacking is the method of checking practical security vulnerabilities by checking a firm's security level from the 3rd perspective in using some hacking techniques being used the most in real world, and it is judged that the method being suggested by this study will be helpful in preventing any real security accidents by finding any hole within a firm's security system from a virtual hacker, and checking and analyzing the firm's security problems.

Moreover, as the matter of hacking threats by an outside user is well known, each firm and each organization should make various investments in protecting their security systems from any outsider attack, and although the accident rate of inside user's hacking threat is higher and its damage is very serious, they devaluate its seriousness and then most firms and organizations insufficiently prepare against inside user's hacking accidents.

Hence, it is the perfect time to set a system for controlling important information's life cycles as well as building physical, managerial and technological security systems for information security while monitoring the information's flow based on people's actions.

References

[1] http://ko.wikipedia.org

[2] KISIA, "Survey for Information Security Industry in Korea: Year 2013", **(2013)** December.

[3] K. Kiyeon, "Vulnerability Detection and Mitigation of Web Application based on SW Security Testing", PhD Diss., Dankook University, **(2012)** Febuary.

[4] KISA, "Recent Major Hacking Incidents and Response Strategies", INTERNET & SECURITY FOCUS, **(2014)**, pp. 24-47.

[5] K. Jingu, "A Study on The Verification of Improved Security Vulnerability when Building Website", PhD Diss., Namseoul University, **(2014)** August.

[6] KISA, "Major Hacking Techniques and Response Strategies", Internet & Security Focus 2013, vol. 4, **(2015)**.

[7] T. Wilhelm, "Professional Penetration Testing, Second Edition: Creating and Learning in a Hacking Lab", **(2015)**, ISBN-13: 978-1597499934, ISBN-10: 1597499935

[8] Owasp Korea Chapter, "OWASP Top10-2013: The Ten Most Critical Web Application Security Risks", http://www.owasp.or.kr

[9] S.-H. Kwon and D.-W. Park, "Hacking and Security of Encrypted Access Points in Wireless Network", Journal of Information and Communication Convergence Engineering, Korea, **(2012)**, pp.156-161

[10] D.-W. Park, "A Study on Real-time Cooperation Protect System Against Hacking Attacks of WiBro Service", Journal of Information and Communication Convergence Engineering, Korea, vol. 9, no.4, **(2011)**.

Authors

Sang-Wook Cha, received his bachelor's degree of public administration in Kookmin University, Seoul (2004) and Incheon Univ.public dministrationmaster's degree, Incheon (2009). His research interests focus on Public utilization and sharing the data, etc

Jong-Suk Park, received his master's degree of Public Administration in Sungkyunkwan University, Korea(2004). He worked in the IT field as a system engineer over 20 years. Now, he is CEO of S3I Co., LTD. since 2004. His current research interests include ITO, IT-governance, IT audit.

Jangyoun Cho, received his master's degree on Business Management from Aju University in 2004, performing his business in legal IT fields at Open SNS since 2005 with his main interests on electronic filing, information protection, anonymous and project management.

Kyeong-Seok Han, received his bachelor's degree of Education (1979) and master's degree of Management (1984) in Seoul National University, doctor's degree of MIS in Purdue University, USA (1989). Now he is a professor in the Dept. of Management, Soongsil University, Seoul, Korea. His research interests focus on Technical MIS, Digital Economy, Agent-Eased Simulation, Web Programming, ERP.

Jong-Bae Kim, received his bachelor's degree of Business Administration in University of Seoul, Seoul (1995) and master's degree (2002), doctor's degree of Computer Science in Soongsil University, Seoul (2006). Now he is a professor in the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.