JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 5 : 945~950 May. 2017

SW 취약점의 보안성 강화를 위한 진단원의 교육 양성 연구

김슬기 · 박대우*

Research on Education and Training of the Analyzer for Security Enhancement of SW Vulnerability

Seul-gi Kim · Dea-woo Park*

Department of Convergence Technology, Hoseo Graduate School of Venture, Seoul 06724, Korea

요 약

소프트웨어의 취약점으로 인하여, 국가의 사이버 인프라와 실물 금융자산 에 대한 해킹 공격이 발생하고 있다. 소프트웨어는 인터넷 정보제공과 사이버 금융결제 및 사이버 인프라를 통제하고 운영하는, 운영체제 및 실행시스템을 구성하는 필수요소이기 때문이다. 이러한 소프트웨어 취약점을 분석하고, 보안성을 강화해야 사이버 인프라의 보안성이 강화되고, 실제 국가와 국민의 실제 생활에 보안성이 강화된다. 소프트웨어 개발보안 제도 분석과 소프트웨어 개발보안 진단 분석 및 소프트웨어 취약점의 보안성 강화를 위한 연구를 한다. 또한 소프트웨어 취약점 진단원 양성 및 보수교육을 위한 교재개발과 진단원 시험문제 개발 및 진단원의 파일럿 테스트, 그리고 진단원의 투입인력・비용기준을 연구한다. 본 논문의 연구는 소프트웨어 취약점 진단원을 양성하는 교육과정과 진단가이드를 제시하여, 국가와 국민 생활의 사이버 인프라의 소프트웨어 보안성을 강화하는 데 목적이 있다.

ABSTRACT

Due to the vulnerability of the software, there is a hacking attack on the country's cyber infrastructure and real financial assets. Software is an integral part of the operating system and execution system that controls and operates Internet information provision, cyber financial settlement and cyber infrastructures. Analyzing these software vulnerabilities and enhancing security will enhance the security of cyber infrastructures and enhance the security of actual life in the actual country and people. Software development security system analysis and software development Security diagnosis analysis and research for enhancing security of software vulnerability. In addition, we will develop a textbook for the training of software vulnerability diagnosis and maintenance education, develop pilot test problems, pilot test of diagnostic staff, The purpose of this study is to enhance the software security of the cyber infrastructures of national and national life by presenting curriculum and diagnosis guide to train the software vulnerability examiner.

키워드 : 취약점, SW보안, SW진단원, 보안성 강화, 시큐어코딩

Key word : vulnerability, software security, software consultant, security enhance, secure coding

Received 30 November 2016, **Revised** 02 December 2016, **Accepted** 26 April 2017

* **Corresponding Author** Dea-woo Park(E-mail:prof_pdw@naver.com, Tel:+82-2-2059-2352)
Department of Convergence Technology, Hoseo Graduate School of Venture, Seoul 06724, South Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.5.945 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/ by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

2016년 6월 대기업의 자료가 유출되었고, 이로 인하여 북한으로부터 사이버테러가 관련되었다는 경찰의 수사결과 발표[1]가 있었다.

2016년 1월부터 마이크로소프트사에서는 자사 웹브라우저 IE(Internet Explorer)의 최신 버전을 제외한 이전버전에 대한 지원을 종료하겠다고 밝혔다. 이러한 것은 최신 버전이 아닌 구 버전의 IE에서 새로운 취약점(vulnerability)이 발견되더라도 지원을 종료한 이후에는 해당 취약점에 대한 패치가 제공되지 않기 때문에 이를 노린 공격이 증가할 것을 예상된다[2].

해킹수법으로는 관리자가 아니어도 인증 없이 접근해 명령을 내릴 수 있는 취약점을 통해 해킹공격을 준비했다. 해당 소프트웨어를 만든 기업도, 사용한 기업도 이러한 취약점을 모르고 있었으며 자칫하면 해당 소프트웨어를 사용하는 160여 개 기관과 기업이 한꺼번에 피해를 볼 수 있는 상황이 있었다[2].

또 다른 사례로는 20개월이 넘게 소프트웨어 취약점에 의한 침해사고로 다양한 취약점이 이용되었다. 소셜커머스사이트(Social Commerce Site)는 XSS(Cross Site Scripting)와 Flash취약점을 통해 악성코드 배포 피해를 입었으며, 일일 70만 여명이 감염되는 침해사고가 발생하였다. 또한 증권가 홈페이지에서는 SQL Injection을 통해 개인정보가 유출되어 개인정보 2만 6천 건이 손실되었다. 이러한 사례들은 소프트웨어 취약점에 의한 각종 피해를 발생시킨다[3].

이러한 소프트웨어 취약점으로 인한 사이버 해킹 공격으로 인한 실제사회의 구제척인 피해들이 발생함에 따라, 정부에서는 소프트웨어 개발 시부터 시큐어코딩(secure coding)을 강화하고 있고, 수시로 구축되고 있는 소프트웨어에 대한 취약점 진단과 예방이 필요하며, 따라서 소프트웨어에 취약점 진단원의 양성과 교육에 관한 연구의 필요성이 있다.

본 논문에서는 현재 사이버해킹 동향과 시큐어코딩, 소프트웨어보안 취약점에 대해서 분석하며, 소프트웨어 개발보안 진단가이드 분석에서는 제도분석과 진단가이드를 제안한다. 소프트웨어 취약점의 보안성 강화에서는 진단원 양성 및 보수교육 교재개발과 시험문제를 개발하며, 개발한 시험문제를 기반으로 진단원에게 파일럿 테스트를 진행하며, 투입인력 및 비용기준을 제시한다.

본 논문의 연구는 소프트웨서 취약점 진단원을 양성하는 교육과정과 진단가이드를 제시하여, 국가와 국민생활의 사이버 인프라를 구성하는 스프트웨어 보안성을 강화하는 데 목적이 있다.

Ⅱ. 관련연구

2.1. 시큐어코딩

‘시큐어코딩’이란 소프트웨어 개발과정에서 개발자 실수, 논리적 오류 등으로 인해 소프트웨어에 내재된 보안취약점을 최소화하는 한편, 해킹 등 보안위협에 대응할 수 있는 안전한 소프트웨어를 개발하기 위한 일련의 과정을 의미한다[3].

소프트웨어를 개발하기 위한 과정에서 프로그래머가 코딩한 프로그램에 많은 오류가 발생한다. 이러한 오류는 테스팅에 의해 발견이 되지만, 발견이 되지 않은 오류가 존재하며, 프로그램을 사용하는 중에 발견이 되는 경우가 있어 이러한 경우에는 수정에 많은 시간과 비용이 소모된다. 이러한 오류는 사용 중인 프로그램에 내재된 기능성의 문제를 발생시킬 뿐만이 아닌 보안성에 중요한 문제인 프로그램 취약성을 발생시킨다.

그렇게 때문에 안전한 소프트웨어 개발을 위한 단계별 개발보안으로는 요구사항, 설계 및 디자인, 구현, 테스트 단계로 나눈다. 첫 번째 요구사항 단계에서는 요구사항 중 보안 요구사항 식별을 진행하며, 설계 및 디자인 단계에서는 보안요구사항과 위협에 대한 보안통제를 고려하고 위협원을 도출, 외부인터페이스를 식별, 보안통제 수립단계를 거친다. 구현단계에서는 표준코딩 정의서 및 소프트웨어 개발보안 가이드를 준수하여 개발하며 소스코드 보안약점을 도구를 활용하여 진단을 한다. 마지막 테스트단계에서는 실행코드 보안취약점을 진단하는데 이때 사용되는 진단방식으로는 동적분석인 스캐닝, 모의해킹 테스트 등으로 진행한다[4].

2.2. 사이버해킹 동향

사이버해킹은 보안 패치발표 이전의 제로데이 공격(Zero day Attack), 웹사이트 해킹 등 지능화된 기법을 이용해 지속적으로 공격하는 APT(Advanced Persistent Threat)공격, 모바일 공격 등 사회에 국가 인프라에 대

해 확산되는 추세이다.

사이버해킹은 약 75%가 소프트웨어 자체의 보안취약점을 악용하는 것으로 웹 사이트 공격이 대표적이며, 불특정 다수가 쉽게 접근할 수 있고 프로그램의 특성상 외부 공격에 항상 노출되어 있어 사이버 침해사고가 발생될 가능성이 높아지고 있다[4].

최근 국내외에서 발생한 고객정보 유출사고는 XSS 및 SQL Injection공격 등 웹 응용프로그램에 내재된 보안취약점을 주로 악용했는데, 이렇듯 소프트웨어에 내재된 보안취약점은 사이버 침해사고의 주요 원인이 되며, 응용 소프트웨어에 내재된 보안취약점을 악용, 계정탈취・정보유출 등 침해사고를 유발시키지만 관련 보안투자는 미흡한 상황이다.

그림 1에서는 소프트웨어의 취약점을 악용한 현황을 나타낸다.

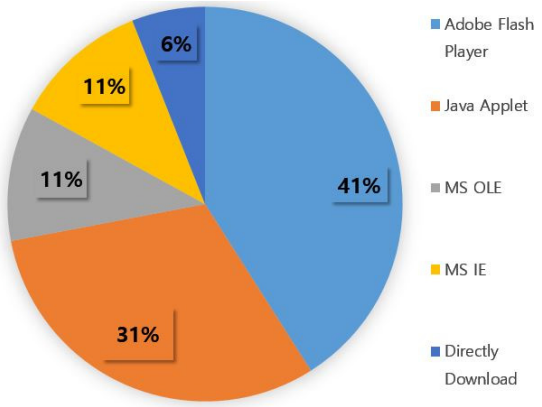

Fig. 1 Software vulnerability abuse status

2.3. 소프트웨어보안 취약점

취약점이란 컴퓨터 시스템의 약점으로 컴퓨터 시스템에 보안상의 문제점이 있는 것을 뜻한다. 소프트웨어 보안에 문제가 발생하는 것은 소프트웨어보안은 소프트웨어 개발과정에서 소스코드를 작성하는 구현단계에서 보안취약점을 배제하기 위한 '시큐어코딩'을 포함하고 있다. 시큐어코딩은 입력데이터의 검증 및 표현, 보안 기능, 시간 및 상태, 오류 처리, 코드 오류, 캡슐화, API오용 등 다양한 취약점에 대응 할 수 있게 되어 있지만, 주로 웹 서버 혹은 웹 애플리케이션이 직접적으로 가지는 취약점에 대해 조치하는 것이 일반적이다[5].

소프트웨어 개발 또는 홈페이지 개발 시, 보안취약점을 이용해 해킹을 시도해 시스템의 내외부적으로 공격을 진행해 악용할 수 있으므로 미국에서는 2002년도부터 시큐어코딩을 의무화 시켰다.

웹 사이트의 경우 불특정 다수가 쉽게 접근할 수 있고, 사용자가 입력한 정보를 처리하는 프로그램의 특성상 외부 공격에 항상 노출되어 있어 사이버 침해사고가 발생할 가능성이 높다.

소프트웨어 보안 취약점의 종류로는 표 1과 같이 메모리보안침입의 버퍼 오버플로(Buffer overflow), 입력확인 오류의 포맷 스트링 버그(Format string bug), SQL 삽입, 코드 인젝션(Code injection), 권한 혼동의 클릭재킹(Click jacking), FTP 바운스 공격(FTP bounce attack) 등이 있다.

특히, 소스코드 보안취약점을 이용한 사이버공격은 침입차단 및 침입방지 시스템 등 일반적인 보안장비로는 대응이 어려운 특징이 있다.

Table. 1 Type of software security vulnerabilities

type	content
Input data verification and expression	For Enter a program value, that can occur due to improper verification of security weaknesses
Security function	Security weaknesses that can occur when improperly implementing authentication, access control, and rights management
Time and state	Security weaknesses in improper time and state management in multi-process operating environments
Error handling	Incomplete error handling can cause security vulnerabilities that can occur because critical information is included in error information
Code error	Security weaknesses caused by coding errors that developers can commit
Encapsulation	Insufficient encapsulation can lead to unauthorized data exposure
API Misuse	Security weaknesses that can result from using inappropriate or insecure API

Ⅲ. 소프트웨어 개발보안 진단가이드 분석

3.1. 소프트웨어 개발보안 제도 분석

행정안전부는 사이버공격의 주요 원인인 소프트웨어 보안약점을 전자정부 서비스 개발단계에서 제거하기 위해 정보시스템 구축 시 '소프트웨어 개발보안(시큐어코딩)'을 그림 2에 따라 의무화하기로 했다.

그 동안은 소스코드 취약점 자동진단도구, 소스코드 취약점 DB구축, 소스코드 자동진단도구 개발, 자동진단도구 시험적용, 안전한 시스템개발 방안마련, 국외 SW 등 시스템 개발체계 분석, 안전한 시스템 개발방안 등 악성코드를 개별적으로 분석해 대응할 수 있는 패턴을 개발하고 적용하는 방식으로 보안위협에 대응해 왔으나, 하루에 분석할 수 있는 악성코드 수가 한계가 있고 투자에도 제한이 있어 보다 근본적인 해결책이 필요하다.

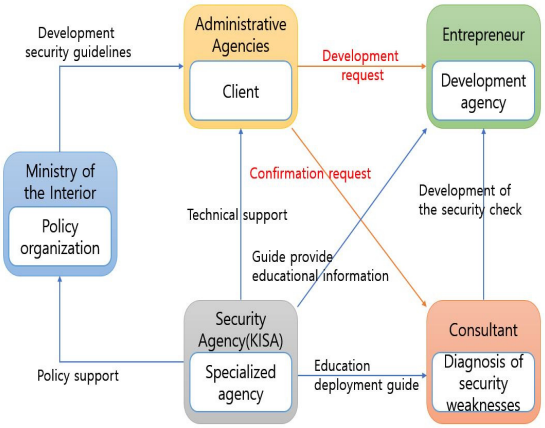

Fig. 2 Secure coding system

3.2. 소프트웨어 개발보안 진단 분석

자산정보화사업 수행 시 시큐어코딩을 준수하여 소프트웨어를 개발했는지, 여부를 진단하기 위해 소프트웨어 보안약점 진단기법을 제시한다.

대상은 전자정부 소프트웨어 보안약점 진단원이며 범위는 행정기관 등이 추진하는 정보화사업으로 유지보수로 변경되거나 신규로 개발되는 소스코드 전체로 한다.

발주자 입장에서는 소프트웨어의 보안약점 진단, 제거 요구사항 도출시 활용 할 수 있으며 사업자 입장에서는 자체적으로 소프트웨어 보안약점을 진단, 제거 시 활용할 수 있다.

진단원 입장에서는 사업자가 수행한 소프트웨어 보안약점 제거 결과 진단 시 활용할 수 있으며, 일반적으로는 소프트웨어 개발보안체계 및 보안약점 진단 및 제거 방법에 대한 이해하는데 활용한다.

Ⅳ. 소프트웨어 취약점의 보안성 강화

4.1. 진단원 양성 및 보수교육 교재개발

현재 소프트웨어 진단원 양성을 위한 보수교육과 교재개발은 부족한상황이다. 소프트웨어 보안은 웹 서버, 웹 응용프로그램 서버 등 웹 관련 자체의 보안취약점을 이용한 공격은 침입차단시스템 등 보안장비로 대응하기 쉽지 않다. 그렇기 때문에 실제 소프트웨어 보안약점 진단을 통해 적절히 대응하고 예방할 수 있는 소프트웨어 보안진단 인력 및 양성에 필요한 교육 보조재 등이 필요한 상황이다.

교재의 구성으로는 기본교육으로 소프트웨어 개발보안 제도・기준, 소프트웨어 보안약점 진단・제거기술, 진단 수행능력의 배양을 위한 교육을 진행하며, 소프트웨어 개발보안 의무화 대상, 범위, 기준과 정보화사업 단계별, 기관별, 주체별 개발보안활동을 교육한다. 또한 소프트웨어 보안약점에 대한 설명 및 보안대책과 JAVA 언어로 작성된 시큐어코딩 예제 기반의 구체적인 진단방법을 소개하며 용어정리와 소프트웨어 보안약점 항목으로 구성한다.

보수교육으로는 지침・기준 등, 제도 변경사항, 최신보안약점, 진단・제거기술, 소프트웨어 개발보안 지식의 지속적인 습득 및 기술능력 유지를 위한 교육을 진행한다[6].

4.2. 진단원 시험문제 개발

최근 소프트웨어보안 트렌드를 반영하여, 구현단계 직무분석 내용을 보완하며 설계 및 운영단계에서 보안약점 기준 및 보안진단 방법 등에 관한 문제를 개발한다.

소스코드 보안약점 진단문제로는 파일명과 소스 행번호로 취약지점을 제시하며, 분석결과 리포트 자동작성 및 시큐어코딩 예제 등 관련된 문제를 개발한다.

진단원 선발을 위한 1차 필기 기본지식 확인(4지선다형, 단답형)문제와 현장실무 지식을 테스트하는 2차 실기(서술식, 논술식 등)에 활용할 문제유형을 개발한다.

시험문제가 필기로만 진행될 뿐만 아니라 실습 테스트인 모의해킹형식으로 가상프로그램을 사용하여, 프로그램의 코딩단계에서 취약점을 찾아내는 환경을 마련한다.

표 2에서는 진단원 시험문제 개발예제로 4지선다형, 단답형, 논술형식의 예제를 나타내었다.

Table. 2 A diagnostic test sample problem

• Matter of example
Problem type detection and cases of mismatched items are? ① Inappropriate input detection≦Session Cookie ② SQL Injection Detection≦Hibernate ③ XSS≦JSP ④ Vulnerable URL Redirection≦SHA-1
• Short-answer questions
1) Explain and the case of Vulnerable URL Redirection 2) Explain and the case of SQL Injection Detection 3) Explain and the case of Cross Site Scripting
• Essay type questions
Many breach was triggered across the application software source code, depending on governments to remove potential security vulnerabilities that may exist. The guidelines for software security weaknesses. Describe the types of typical security weaknesses, and the targets and scope of software development security coverage, standards, and how to diagnose software vulnerabilities during software development?

4.3. 소프트웨어 취약점에 대한 보안정책

프로그램을 코딩할 때 최초의 단계부터 소프트웨어 개발보안정책을 세워 코딩을 진행한다.

시큐어코딩 단계인 요구사항 분석부터 개발필요사항 분석까지 보안정책을 적용해 코딩을 하게 되면 소프트웨어 취약점에 대한 오류를 찾게 되는 시점이 빨라지며, 빠를수록 결함에 대한 수정비용이 줄어들고 시간을 단축시킬 수 있다. 또한 소프트웨어 디자인, 코딩 작성, 지정된 Unit 단위의 테스트, 소프트웨어 통합 테스트과정에서는 주기적인 점검을 진행하여 시제품 테스트단계를 거치기 전에 소프트웨어의 결함을 찾아내는 것이 중요하다.

국가 및 정부에서는 개발보안 정책으로는 일회성 가이드가 아닌 취약점이 발견될 때마다 DB가 업데이트 된 세부 가이드방안을 제시하며, 보안 가이드를 실시한다.

국가 및 정부에서 발주한 공공사업에는 보안정책 가이드를 적용하며, 소프트웨어의 취약점을 진단하는 진단원의 교육 및 가이드에 대한 교육을 진행한다.

기업의 입장에서는 지정된 보안정책가이드에 대한 지침을 적용시키며, 정보시스템 감리 시 검사항목을 세분화 시켜 오류를 최소화 시킨다. 이때는 보안약점 제거여부를 포함시켜 개발단계에서 적용하여 활성화한다.

개발자는 보안정책 가이드에 맞는 프로세스를 적용시키며, 개발 생명주기에서 각 단계가 끝날 때마다 가이드 내용에 관한 적용여부를 확인하고 점검한다. 개발자는 기본적으로 시큐어코딩의 교육을 의무화해야하며, 취약점을 발견했을 시 취약점에 대한 이해도와 오류수정에 대한 교육을 거친다.

Ⅴ. 결 론

본 연구에서는 소프트웨어의 개발보안 제도와 진단을 분석하였으며, 취약점의 보안성 강화를 위한 진단원 양성과 교재, 시험문제 개발에 대해 연구하였다.

소프트웨어의 취약점의 보안성 강화를 위해 진단원 양성 및 보수교육과 교재개발을 제시하였는데, 이때 진단원 양성하는데 필요한 커리큘럼에 대하여 미흡한 교육부분에 대해서는 교육방식을 추가시켜 진단원 양성에 대한 효과를 극대화시키도록 할 것이다. 또한 취약점을 진단하여 패치가 이루어져 보안성을 강화시키는데, 이때 진단하는 진단원의 기준을 제시하여, 진단원 양성을 하여 더 많은 취약점을 찾아내는 것이 보안성을 강화시키는 방법 중 하나이므로 제시한 방법을 통해 진단원이 현재보다 많이 양성될 수 있도록 보안성 강화를 향상시킬 것이다.

소프트웨어 개발보안정책을 통해 시큐어코딩의 보안성 문제와 가이드라인을 제시함에 따라 소프트웨어의 취약점을 최소화시켜 피해를 줄일 수 있다고 생각한다.

보안정책 가이드가 공공사업 및 개인사업에 적용됨에 따라 소프트웨어상의 취약점을 줄일 수 있으며, 소프트웨어의 오류를 최대한 빨리 찾아내고, 오류를 수정함으로써 시간적 피해와 금전적 피해를 최소한으로 줄이는데 목적을 두고 있다.

또한 소프트웨어의 취약점을 찾아낼 때마다 취약점 DB를 업데이트를 하고, 구축을 하여 적용하게 된다면 소프트웨어 개발단계별 적용정책인 5단계 중 3단계인 테스트 요구사항단계에서 취약점 검출에 대한 효과가 나타날 것이라고 예상된다.

소프트웨어의 취약점을 통해 물질적, 금전적 피해가 많이 발생함에 따라, 향후 논문에서는 소프트웨어보안의 취약점을 진단하는 방식에 대하여 연구할 예정이다.

REFERENCES

[1] K. B. Kim, “Cyber Attack using Software Vulnerability,” inews24, [Internet]. Available: http://news.inews24.com/php/news_view.php?g_serial=963171&g_menu=020200, 2016. 06. 16.

[2] 2015REVIEWS & 2016PREDICTIONS, AhnLab Clinic Center, “The Top 5 Security Threats that Swept 2015,” [Internet]. Available: http://acc.giro.or.kr/secu_view.asp?seq=24474, 2016.1.4.

[3] “Software Development Security Guide,” Ministry of the Interior, Korea Internet & Security Agency(KISA), Nov. 2013.

[4] “Software Development Security Guide,” Ministry of the Interior, Korea Internet & Security Agency(KISA), Nov. 2013.

[5] S. M. Cho, H. Lee, “A Countermeasure against the Abatement Attack to the Security Server,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 20, no. 1, pp. 94-102, Jan. 2016.

[6] S. G. Kim, D. W. Park, “Research for Enhancing Security of Software Vulnerability,” in *Proceeding of Conference on Korea Institute of Information and Communication Engineering*, KOREA, vol. 20, no. 2, pp. 182, Oct. 2016.

김슬기(Seul-gi Kim)

2016 2월 : 호서대학교 디지털디스플레이공학과 졸업(학사)
2016년 ~ 현재 : 호서대학교 벤처대학원 융합공학과 석사과정(석사)
※관심분야 : 사이버보안, Forensic

박대우(Dea-woo Park)

1998년 : 숭실대학교 컴퓨터학과 (공학석사)
2004년 : 숭실대학교 컴퓨터학과 (공학박사)
2004년 : 숭실대학교 겸임교수
2006년 : 정보보호진흥원(KISA) 선임연구원
2007년 ~ 현 재 : 호서대학교 벤처대학원 교수
※관심분야 : Hacking, Forensic, CERT/CC, 침해사고 대응, e-Discoverty, 사이버안보, 네트워크 보안, 스마트폰 보안