Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1217

웹 취약점 스코어링 기법의 advanced 모델 연구

변 으 뜸,† 임 종 인, 이 경 호‡
고려대학교 정보보호대학원

A Study On Advanced Model of Web Vulnerability Scoring Technique

Autumn Byeon,† Jong In Lim, Kyong-Ho Lee‡
Korea University

요 약

웹 취약점 분석은 기업이 웹 애플리케이션의 보안 문제점을 파악하고 개선하는데 도움을 주며 미래창조과학부는 취약점 분석·평가 기준을 배포하여 이를 지원하고 있다. 그러나 기준에서 제시하는 방법으로는 취약 항목에 대한 구분은 가능하지만 취약점 항목의 위험을 분석하기에는 부족하여 효과적인 대응이 어렵다는 문제점이 있다. 본 연구에서는 국내외 취약점 스코어링 기법에 대해 분석하고 올바른 웹 취약점 분석 평가를 위한 스코어링 방법을 제시하고자 한다.

ABSTRACT

Web application security problems are addressed by the web vulnerability analysis which in turn supports companies to understand those problems and to establish their own solutions. Ministry of Science, ICT and Future Planning (MSIP) has released its guidelines for analysis and assessment of the web vulnerability. Although it is possible to distinguish vulnerability items in a manner suggested in the MSIP's guidelines, MSIP's factors and criteria proposed in the guidelines are neither sufficient nor efficient in analyzing specific vulnerability entries' risks. This study discusses analysis of the domestic and international Vulnerability Scoring system and proposes an appropriate evaluating method for web vulnerability analysis.

Keywords: Scoring, Web application, Vulnerability

I. 서 론

기업들은 해킹사고를 방지하고 자사의 보안성을 강화하기 위해 매년 수백~수천만원의 비용을 지불하여 취약점 진단 및 평가를 수행하고 있다.[1] 또한 정보통신기반 보호법, 정보통신망법, 전자금융감독규정 등에는 매년 주기적인 취약점 점검 진행에 관하여 명시하고 있다. 그러나 최근 모 통신사 개인정보 유출이나 아이핀 유출 사건 등 이슈화 되었던 사건들을 분석하여 보면 웹 취약점을 악용한 해킹사건임을 알 수 있다.[2] 웹 서비스는 일반적으로 인터넷을 이용하면 어디에서나 접속할 수 있는 특징을 가지고 있고 내부망과의 접점이 있어, 해킹 공격을 당했을 경우 내부 중요 데이터가 유출되거나, 시스템이 점령당하는 피해를 입을 수 있다. 이러한 환경에서, 발견된 취약점을 신속하게 제거하는 것이 잠재적 위협을 최소화 하는 방법이다. 그러나 발견된 모든 취약점을 한 번에 수정하는 것은 많은 시간과 자원이 소모되며, 따라서 가장 위험하다고 판단되는 취약점을 우선으로 하여 단계적으로 보완하는 것이 중요하다고 볼 수 있다.

현재 웹 취약점 진단 및 평가는 미래창조과학부에서 배포한 주요정보통신기반시설 기술적 취약점 분석 평가기준에서 제시한 방법으로 수행되고 있다. 이 방법은 비밀성,무결성,가용성을 고려하여 위험등급을

접수일(2015년 4월 21일), 수정일(2015년 5월 21일), 게재확정일(2015년 6월 4일)
† 주저자, bet328@korea.ac.kr
‡ 교신저자, kevenlee@korea.ac.kr(Corresponding author)

상,중,하로 구분하고 있다. 그러나 구체적으로 위험 등급 어떻게 구분해야 하는지에 대한 방법은 언급되어 있지 않다. 따로 별첨으로 웹 취약점 항목과 위험 등급이 기술되어있는데, 여기에서는 모든 등급이 "상"으로 제시되어 있다. 웹 서비스 환경은 사용되는 웹 서버나 개발언어가 기업마다 다양하고 웹 서비스 형태도 목적에 따라 구현 언어, 방식, 구성 등이 달라질 수 있다. 이러한 환경에서 같은 취약점이 발견되더라도 해당 사이트에 미치는 영향도 마찬가지로 다양하다. 진단 시 해당 방법만을 가지고 평가할 경우 해당 시스템, 서비스 등의 정량적인 점수의 산출은 가능하지만, 취약점 조치 우선순위를 정하거나, 관련 업종과의 수준 비교 등 의사결정을 위한 방법으로는 한계점이 있다고 볼 수 있다.

본 연구에서는 국내외 취약점 스코어링 방법들을 분석하고 적합한 스코어링 기법을 제시한다. 산업별 취약점 비교와 취약점간 비교로 담당자가 올바른 의사 결정을 내릴 수 있도록 취약점들을 스코어링 기법을 적용하고 산업군별로 분류하여 정리한다. 각 산업군별 취약점 항목들의 제시한 스코어링 기법에 적용하여 우선순위를 도출하고 타 업종과의 수준비교 결과를 제시하였다.

II. 관련 연구

기존 문제점에 대하여 분석하거나, 웹 애플리케이션의 중요성 및 평가의 필요성 및 적용 연구 등에 대하여 조사하였다. 노회관은 주요정보통신기반시설 취약점 관리체계의 문제점이 있음을 지적하고 추가 대응을 제시하였지만, 웹 취약점 항목에 관련한 내용은 기술하지 않았다.[3] 이재현은 웹 취약점 대응의 중요성에 대하여 언급하였고 효과적인 대응을 위한 OWASP 및 WASC 분석의 필요성을 언급하였다.[4] 문재찬 등은 OWASP 산정방법의 문제점을 제기하면서, 안전한 웹 애플리케이션 개발을 위한 취약점 순위화를 시도하였으며, 기존 항목에 대한 매칭을 통하여 순위를 설정하였다.[5][6] 평가 관련된 부분에서는 김동진 등이 국내외 보안 취약점 관리체계를 소개 및 분석하면서 국내에도 국내 사정에 맞는 취약점 관리체계를 도입 및 운영해야 한다고 언급하고 있다.[7] 안준선 등은 CWSS의 평가 척도 중에 소프트웨어 보안약점에 관련된 평가 항목을 도출하여 적용하는 방법을 제시하였다.[8] 또한 여러 환경에서의 취약점 평가 연구도 이루어졌는데, 이강재는 마이크로 환경의 전력망에서 보안 위협을 정량적으로 평가하기 위해서 CVSS,CWSS 등을 분석하였고,[9] 김지홍은 공격 침투 경로를 예측을 위해 시스템 운영체제 점수 부여를 위해 CVSS 방법을 이용하기도 하였다.[10]

Table 1. precedent research

no	author	Contents
1	H.K.Noh	A Study on the Improvement of the Vulnerability Management System in the Information and Communications Infrastructure(Vulnerability analysis and evaluation for Major Information and Communications Infrastructure)
2	J.H.Lee	Study on the OWASP and WASC-oriented Web Application Security
3	J.C.Moon	Vulnerability Analysis and Threat Mitigation for Secure Web Application Development
4	D.J.Kim	An Analysis of Domestic and Foreign Security Vulnerability Management Systems based on a National Vulnerability Database
5	K.J.Lee	Study of quantitative evaluation method for the microgrid security threat
6	J.H.Kim	Automated attack path enumeration method based on system vulnerabilities analysis
7	J.S.Ahn	Quantitative Scoring Criteria on the Importance of Software Weaknesses

선행 연구들은 기존의 문제점을 지적하고, 웹 취약점 대응의 중요성에 대하여 언급하고 있지만 발견된 웹 취약점 대응에 대한 우선순위 도출 방법 등에 대해서는 언급되어 있지 않았지만, 평가 방법에 대해서는 여러 분야에서 다양한 평가 시도가 이루어지고 있다.

III. 국내·국외 현황

3.1 국내 현황

3.1.1 주요정보통신기반시설 취약점 분석 · 평가기준

국내 대부분의 업체들이 미래창조과학부에서 제시한 "주요정보통신기반시설 취약점 분석·평가 기준"은에 따라 취약점 진단을 수행하고 있으며, 현재 최신 버전은 2014년 1월 버전이다. 이 기준에서는 "기술

적 취약점 점수계산" 항목에서 다음과 같이 취약점 점수 산출식을 제시하고 있다.[11] 이 계산법은 웹 취약점 항목에 대해서도 동일하게 적용하도록 기술되어 있다. 취약점 점수는 점검항목 등급을 반영하여 계산하도록 제시되어 있으며 위험등급은 상,중,하로 나누어 정의하고 등급을 나누는 기준은 비밀성,무결성,가용성을 고려하여 정의하고 구분해야 한다고 되어 있다. 다만 취약점 분석·평가 결과에 대해 정량적인 점수(100점 만점)로 산출·관리를 희망하는 경우 Fig. 1의 산출식을 활용한다. 식별된 취약점을 전체 취약점 개수로 나누고 100을 곱하여 백분율 형태로 결과가 도출되게 되며, 자산이 여러개일 경우 Fig. 2. 처럼 모든 자산의 점수를 더하여 전체 자산 개수로 나누는 계산 방법을 이용하고 있다.

Score sum, if all vulnerabilities are identified : A
Score sum of identified vulnerability: B

$$\text{(Calculation)}: \frac{A-B}{A}\times 100$$

Fig. 1. vulnerabilities calculation method 1

Number of asset: N
Score by asset: S1, S2, ..., Sn

$$\text{(Calculation)}: \sum_{n=1}^{N} S_n \div N$$

Fig. 2. vulnerabilities calculation method 2

3.2 국외현황

3.2.1 OWASP Risk Rating Methodology

OWASP(Open Web application security project)는 웹 애플리케이션의 주요 취약점 목록인 OWASP top 10을 발행하고 있으며 2004년 발행 이후 3마다 업데이트를 수행하여 현재 3회 갱신, 최신 버전은 2013년도에 발행하고 있다. OWASP는 top 10 선정 시 6단계로 이루어져 있는 OWASP Risk Rating Methodology.[12]를 이용한다. OWASP는 Likelihood와 Impact로 RISK를 계산하고 있으며, Likelihood는 Threat Agent Factor와 Vulnerability factor로 도출하고 Impact는 Technical Impact와 Business Impact로 도출하며, 최종적으로 Fig. 3. 과 같이

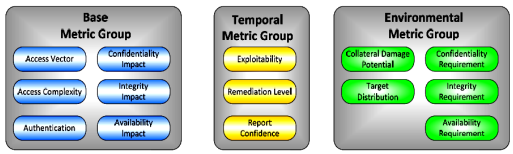

Fig. 3. CVSS Metric Group

Risk를 계산한다.

3.2.2 CVSS

CVSS(Common Vulnerability Scoring System)은 다양한 기종의 하드웨어와 소프트웨어의 실제 발생한 보안 취약점의 중요성을 평가하고 확인하기 위해 만들어 졌으며, 현재 버전은 3까지 나와 있으나 정착단계인 2버전이 주로 활용되고 있다. CVSSv2의 평가항목은 Fig. 4.와 같이 세가지 메트릭 그룹으로 구성된다.[13]

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Fig. 4. OWASP Risk Calculation

3.2.3 CWSS

CWSS(Common Weakness Scoring System)는 보안약점의 중요도를 평가하는 방법이며, 소프트웨어에서 발생하는 약점 제거에 대한 우선순위를 줄 수 있는 정량적 기준을 제시한다. CVSS와는 유사하지만 기존에 이미 확인(발견)된 취약점을 평가하는 CVSS와는 다르게 CWSS는 취약점이 발견되기 전 프로세스에 적용할 수 있다. CWSS는

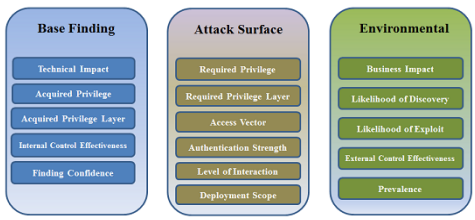

Fig. 5. CWSS Metric Group

CVSS와 같이 3가지 매트릭스 그룹을 가지고 평가를 진행하며, 각각 Base Finding, Attack Surface, Environmental이다.[14] 현재 버전 1.0.1이 2014년 9월에 발표되었고, SANS Top 25에 일부 평가 척도가 활용되었다. 다음의 Fig. 5. 에서 CWSS의 Metric Group을 확인할 수 있다.

IV. 문제점

4.1 취약점 조치 우선순위 제시의 어려움

주요정보통신기반시설 취약점 분석·평가 기준에서 제시한 웹 취약점 항목들의 등급은 Table 1. 과 같이 모두 "상"으로 되어 있다.

이러한 경우 취약점이 발견되고 정리된다 하더라도, 모든 취약점 등급이 "상" 이기 때문에 취약점을 제거하기 위한 우선순위를 정하기가 어렵다는 문제가 발생한다. 다음은 A site에서 발견되었던 취약점 간의 비교표이다.

먼저 SQL Injection 취약점을 살펴보면, Blind SQL Injection에 의해 내부 DB정보가 탈취당하는 결과를 얻을 수 있었다. 이는 중대한 취약점으로 해당 취약점으로 인하여 내부 중요 정보가 유출될 수 있는 취약점이다. 두 번째로 정보 누출 취약점을 보면 이메일 정보가 소스코드에 포함되어 보이는 문제점이었다. 해당 정보로 특별하게 2차 공격에 이어지지는 않았으므로 그 위험성이 앞서 발견된 SQL Injection에 비해 낮다고 볼 수 있으나 기존 기준에 의하면 둘 다 등급이 "상"이다. 결과적으로 취약점 간의 중요도 평가가 어렵다는 것을 나타내고 있다.

Table 2. Web application Vulnerabilities of MSIP's guidelines

Item	Degree	Item	Degree
Buffer over flow	H	Cross Site request Forgery	H
Format string	H	Prediction of session	H
LDAP Injection	H	Inadequate approval	H
Running OS command	H	Insufficient session ends	H
SQL Injection	H	Fixed session	H
SSI Injection	H	Automatic attack	H
XPath Injection	H	Omission of verification process	H
Directory Listing	H	File Upload	H
Information break	H	File Download	H
Malicious content	H	Manager page exposure	H
XSS	H	Path tracing	H
Minor string Strength	H	Public position	H
lack of authentication	H	Plain text data transmission	H
Weak password recovery	H	Cookies modulation	H

Table 3. Comparison of Vulnerabilities

Name	SQL Injection	information break
Cause	Absence of input value verification	Lack of proper security settings
Method	Attack by SQL Injection tool	Information view by reading source-code
Damage	Internal Privacy information loss(Residence Numner)	E-mail information loss
Influence	Second attack possibility	N/A
Risk	H	H

4.2 사이트와의 수준 비교의 어려움

사이트마다 환경이 다양하기 때문에 동일한 취약점이 발견된다 하더라도 해당 취약점에 대한 해석은 달라져야 한다. 다음은 동일한 취약점이 발견된 두 개의 사이트를 비교하여 보았다.

같은 취약점이지만 A사이트의 파일 업로드 성공 이후 웹쉘 접근이 가능하였지만 실제 커멘드 명령에

Table 4. Comparison of Sites

Site	A Site	B Site
Cause	Absence of input value verification	Absence of input value verification
Method	Upload or authentication detouring by code modification	Upload without filtering
Damage	Possibility of running web-shell, but not right to running command	Possibility of running weg-shell, and command
Influence	N/A	Second attack possibility
Risk	H	H

대한 권한이 없었으므로 더 이상의 공격이 이루어지지 않았다. 그러나 B사이트의 경우 웹쉘 접근 뿐 아니라 커멘드 명령의 실행이 가능함을 확인하여 2차 공격까지 이루어 질 수 있었음을 보였다. 같은 취약점이라도 다른 형태로 분석이 되어야 하지만, 현재 고정된 기준으로 적용된 항목을 이용할 경우엔 제대로 된 평가가 어렵다.

V. 개선방안

5.1 기준 제시

CVSS는 발견된 취약점에 대한 스코어링을 하기 위한 기준을 제시하고 있으며, 다양한 전문가들에 의해서 검증된 방법이다. 평가하고자 하는 취약점은 진단 시 발견된 항목에 대한 평가이기 때문에 평가 방법으로 적절하다고 볼 수 있다. 국내 연구에서도 취약점 관리를 위해 이용되기도 하였다.[15] 본 연구에서도 스코어링을 위해 활용할 것이다. 평가항목 매트릭스 중 Temporal metrics와 Environmental Metrics는 제외한다. Temporal metrics의 경우는 기존의 발견된 취약점에 관련된 내용(패치가능여부, 공격코드 공개여부, 취약점신뢰도)을 담고 있어 실제 진단 시 발견된 다양한 취약점에 적용하기에는 맞지 않고 Environmental Metrics의 경우는 주변 환경에 관련된 내용으로 취약점 자체에 대한 평가로는 적합하지 않아 제외하였다. 따라서 남은 Base Metrics를 기준으로 스코어링 및 분류를 수행할 것이다.

5.2 기준 항목 설명

CVSS의 Base Metrics 평가기준 항목은 공격수행 위치, 공격 복잡도, 인증필요여부, 기밀성, 무결성 가용성을 포함한다.

Table 5. Attack Vector

Value	Score	Standard
Local(L)	0.395	Vulnerability attack by local access
Adjacent Network (AN)	0.646	Vulnerability attack by neighboring network access
Network (N)	1.0	Vulnerability attack by network access (Remote)

공격수행 위치(AV) : 공격이 성공하기 위한 위치를 나타낸다 .

공격 복잡도(AC) : 취약점 공격을 성공하기 위한 복잡도의 정도를 나타낸다.

인증 필요여부(AU) : 공격자가 취약점을 공격하기 위해서 필요한 인증의 수를 나타낸다.

기밀성(C)/가용성(I)/무결성(A) : 공격 성공 시 기밀성/가용성/무결성에 미치는 영향을 나타낸다.

Table 6. Attack Complexity

Value	Score	Standard
High(H)	0.35	Many conditions for attack
Medium(M)	0.61	Skill-need
Low(L)	0.71	Access condition-no reference

Table 7. Authentication

Value	Score	Standard
Multiple(M)	0.45	Multi-factor
Single(S)	0.56	Single-factor
None(N)	0.704	No factor

Table 8. Confidentiality/Integrity/Availability Impact

Value	Score	Standard
complete(C)	0.660	Big Impact
partial(P)	0.275	Common
None(N)	0.0	No Impact

5.3 점수 계산식

점수계산식은 CVSS의 매트릭스 계산식을 따르며, 계산식은 CVSS v2이다. 현재 v3도 있으나 아직 완전한 버전이 나오지 않은 상태이기 때문에 v2의 계산 방식을 따라 수행한다. 점수는 Impact(Im, 영향도) Exploitability(EX,악용가능성)을 계산하고 이후에 점수(Score)를 계산한다. 단 Impact가 0인 경우는 $f(Im)=0$ 이고, 그렇지 않은 경우는 1.176 값을 가진다.

$$Impact(Im) = 10.41 \times (1(1-C) \times (1-I) \times (1-A))$$
$$\text{Exploitability}(EX) = 20 \times AV \times AU \times AC$$
$$Score = ((0.6 \times Im) + (0.4 \times EX) - 1.5) \times f(Im))$$

다음은 A사의 SQL Injection 취약점을 위의 계

Table 9. Vulnerability assessment of site A (SQL Injection)

NO	Assessment factor	Result	Basis
1	Attack Vector	N	Possible attack from outside
2	Attack complexity(AC)	L	Possible attack by Automatic tool
2	Authentication(AU)	N	No need
3	Confidentiality(C)	C	Big Impact
4	Integrity(I)	C	Big Impact
5	Availability(A)	N	No Impact
Score		9.4	

산식을 적용하여 점수를 평가한 결과이다.

5.4 적용 및 평가

5.4.1 업종별 취약점 점수 도출

적용 및 평가를 위하여 2011~2015년도에 수행한 기술 취약점 진단 프로젝트 에서 진단 대상이었던 사이트 약100여개를 대상으로 하였다. 발견된 취약점을 주요정보통신기반시설 기술적 취약점 평가 기준에 맞추어 재 정렬하고, 사이트를 업종별로 나누어 계산하였다. 진단 시 발견되지 않은 취약점은 제외하였다.

Table 10. Industry-specific vulnerability score

no	Name	Existence	Public	Game	Service	Finance	Construction
1	File Upload	H	8	6.66	10	7.5	10
2	File Download	H	0	0	7.5	5	0
3	SQL injection	H	5.7	5.7	5.7	5.7	5.7
4	Minor string Strength	H	5	5	5	5	5
5	Inadequate approval	H	6.8	0	7	6.81	6.1
6	Plain text data transmission	H	7.5	0	0	7.5	0
7	Manager page exposure	H	0	0	0	5	5
8	Directory Listing	H	5.1	5	5	5	6.6
9	Public position	H	4.3	4.3	4.3	4.3	4.3
10	Information break	H	7.8	0	7.5	7.8	6.4

방법을 적용한 결과 업종별로 사이트 취약점에 대한 점수가 다르게 나온 것을 알 수 있으며 이는 실제 진단 시 고객에게 현재 고객 사이트에 대한 취약점 척도를 제시해 줄 수 있다.

5.4.2 진단 결과 적용

최근 진단한 금융관련 사이트 B의 취약점을 적용하여 다음의 결과를 얻을 수 있었다.
적용 결과 사이트 B에서 발견된 취약점의 점수가 계산되어 나온 것을 알 수 있으며 해당 점수를 비교하여 어떤 취약점 항목을 우선적으로 해결해야 할지에 대한 척도도 제공해 줄 수 있음을 확인할 수 있었다. 또한 관련 업계 점수와의 비교를 통해 현재 B사이트의 취약점 현황에 대한 파악을 할 수 있었다.

Table 11. Vulnerability assessment of Site B

no	Name	Existence	SiteB	Finance Ave.	Rank
1	SQL Injection	H	10	7.5	1
2	Information break	H	5	5.3	4
3	XSS	H	4.3	4.3	5
4	Inadequate approval	H	6.4	6.8	2
5	File Upload	H	10	10	1
6	Plain text data transmission	H	5.7	5.7	3
Average		-	6.9	6.6	

5.4.3 개선 방법 적용 프로세스

앞서 제시한 방법을 적용한 프로세스이며 해당 프로세스를 따를 경우 취약점에 대한 평가와 보완해야 할 취약점의 우선순위를 얻어낼 수 있다.

① 웹 취약점에 대한 분석을 수행하여 취약점을 찾아낸다. 취약점 항목 기준은 미래창조과학부의 취약점 분석 평가 항목에 따른다.

② 찾아낸 취약점들을 스코어링 한다. 평가항목에 맞추어 점수를 계산한다.

③ 취약점 진단 결과 통계 DB에 진단 결과를 업데이트한다. 진단 대상 사이트의 산업군을 파악하여 해당 산업군에 업데이트한다.

④ 진단 결과를 분석한다. 2가지 작업을 수행하며, 첫 번째로는 산업별 수준을 비교하며, 두 번째로

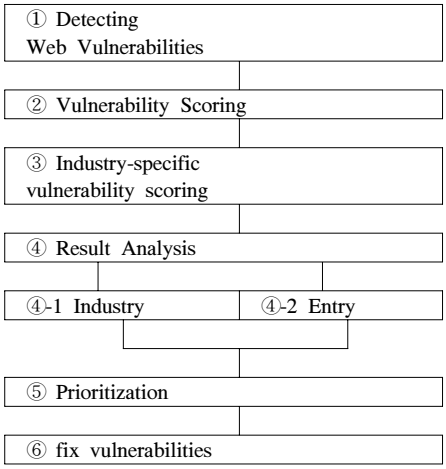

Fig. 6. Advanced Web Vulnerability Scoring and Fix process

는 취약점 항목간의 비교를 수행한다.

⑤ 우선순위를 정한다. 우선순위는 비교 결과를 토대로 하여 가장 긴급하게 수정해야 할 취약점을 선별할 수 있다.

⑥ 우선순위에 맞게 취약점을 수정한다.

VI. 결 론

웹 취약점에 대한 정확한 평가는, 기업이 보안수준에 대해 인지하고 문제점을 해결하기 위한 중요한 자료가 된다. 그러나 국내에서 사용되는 방법으로는 정확한 평가가 어려워 동종 업계와의 비교나, 발견된 취약점간의 비교가 어려워 적절한 대응을 하기 어려운 점이 있다. 본 논문에서는 국내의 웹 취약분석 평가 방법의 문제점을 알아보고 해외의 취약점 분석 평가 방법을 분석하여 웹 취약점에 대한 평가를 올바르게 수행할 수 있도록 방법을 제시했다. 이 방법은 실제 취약점 진단을 수행하는 인력이 발견된 취약점에 대한 올바른 평가를 할 수 있게 도와주고 기업이 웹 취약점 현황에 대해 정확하게 인지하고, 대응 시 우선순위를 정하는데 도움이 될 것이다.

향후 연구로는 제시한 평가 기준이 좀 더 높은 수준의 객관성을 가질 수 있도록 연구할 필요가 있으며, 추가적인 항목 등의 관한 부분의 연구도 필요해 보인다. 이러한 연구는 웹 취약점 진단 및 평가의 수준을 높여 줄 수 있을 것이다.

References

[1] Young-Tek Jo, "Study on Improving the information protection level by Integrated Evaluation Items(IEI)," The Korea Institute information and communications university, pp. 54, May. 2011

[2] Money Today broadcast, "Government hacked, 750000 of i-pin illegal issued by system hacking" http://news.mtn.co.kr/v/201503051821335248 8, Mar, 2015

[3] Jin-Young Lee, Dong-Jin Kim, Min-Jae-Kim, "Taxonomy Comparison of CWE and 7PK vulnerabilities," Proceedings of KISS, 36(D), pp. 26, Nov. 2009

[4] Dong-Jin Kim, "An Anaysis of Domestic and Foreign Security Vulnerability Management Systems based on a National Vulnerability Database," Internet and Information Security, 1(2), pp. 140-145, Nov. 2010

[5] Jae-Hyun Lee, "Study on the OWASP and WASC-oriented Web Application Security," Journal of Advanced Navigation Technology, 15(3), pp. 376, Jun. 2011

[6] Jae-Chan Moon, "Vulnerability Analysis and Threat Mitigation for Secure Web Application Development," Journal of the Korea Society of Computer and Information, 17(2), pp 133, Feb. 2012

[7] Jae-Chan Moon, "Selection and Ranking of Common Attack Patterns for Developing Secure Web Applications," Proceedings of KIISE, 39(B), pp 226-228, Jun. 2012

[8] Sooho Lee, "Researching Information System Security Survey," Graduate Schoolof Konkuk Information and Communications, pp. 35-43, Feb. 2013

[9] Joonseon Ahn and Ji-ho Bang, "Quantitative Scoring Criteria on the Importance of Software Weaknesses,"

Journal of KIISC, 22(6), pp. 1408-1417, Dec. 2012
〔10〕 Hee-gwan Noh, "A Study on the Improvement of the Vulnerability Management System in the Information and Communications Infrastructure(Vulnerability analysis and evaluation for Major Information and Communications Infrastructure)," Department of Information Security Graduate School Soongsil University, pp. 19-20, Dec. 2012
〔11〕 Ministry of Science, ICT and Future Planning, "Vulnerability analysis and evaluation criteria for Major Information and Communications Infrastructure(Vulnerability analysis and evaluation calculation)," pp. 1-5, Aug. 2013
〔12〕 OWASP, "OWASP Risk Rating Methodology," OWASP(https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology), Feb. 2015
〔13〕 Peter Mell, Karen Scarfone, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0, ", CVSS, p. 2-23, Jun. 2007
〔14〕 Bob Martin, Steve Christey Coley, "Common Weakness Scoring System," CWE(http://cwe.mitre.org/cwss/cwss_v1.0.1.html) Sep. 2014
〔15〕 Kyoung-Ki Kim, "Research of improved CVSS vulnerability management in Financial ISAC," Department of Information Security Graduate School of Information Communication Sungkyunkwan University, 37-52, Aug. 2008

〈저자소개〉

변 으 뜸 (Autumn Byeon) 정회원
2008년 2월: 성결대학교 정보통신공학 졸업
2007년 12월 ~ 현재 : 한국정보보호교육센트, 씨드젠 근무
2009년 ~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호 정책, 취약점 진단, 디지털포렌식 등

임 종 인 (Jong In Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월:고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 원장, 고려대학교 사이버국방학과 교수,
개인정보보호 위원회 위원, 대검찰청 디지털수사자문위원회 위원장,
금융보안 연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원,
국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버 국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월~현재: 삼성그룹, nhn, 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책