Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.4, Aug. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.4.779

공격 결과 기반의 웹 취약점 위험도 평가 모델 연구: 사이버 킬체인 중심으로

진 희 훈,[1†] 김 휘 강[2‡]
[1,2]고려대학교 (대학원생, 교수)

A Study on Web Vulnerability Risk Assessment Model Based on Attack Results: Focused on Cyber Kill Chain

Hui Hun Jin,[1†] Huy Kang Kim[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

보통의 웹 서비스는 불특정 다수에게 허용을 해야하는 접근 통제 정책으로 인하여, 지속적으로 해커들의 공격 대상이 되어 왔다. 이러한 상황에 대응하고자 기업들은 주기적으로 웹 취약점 점검을 실시하고, 발견된 취약점의 위험도에 따라 조치를 취하고 있다. 이러한 웹 취약점 위험도는 국내외 유관기관의 사전 통계 및 자체적인 평가를 통해 산정되어 있다. 하지만 웹 취약점 점검은 보안설정 및 소스코드 등의 정적 진단과는 달리 동적 진단으로 이루어진다. 동일한 취약점 항목일지라도 다양한 공격 결과를 도출할 수 있으며, 진단 대상 및 환경에 따라 위험도가 달라질 수 있다. 이러한 점에서 사전 정의된 위험도는 실제 존재하는 취약점의 위험도와는 상이할 수 있다. 본 논문에서는 이러한 점을 개선하고자 사이버 킬체인 중심으로 공격 결과 기반의 웹 취약점 위험도 평가 모델을 제시한다.

ABSTRACT

Common web services have been continuously targeted by hackers due to an access control policy that must be allowed to an unspecified number of people. In order to cope with this situation, companies regularly check web vulnerabilities and take measures according to the risk of discovered vulnerabilities. The risk of these web vulnerabilities is calculated through preliminary statistics and self-evaluation of domestic and foreign related organizations. However, unlike static diagnosis such as security setting and source code, web vulnerability check is performed through dynamic diagnosis. Even with the same vulnerability item, various attack results can be derived, and the degree of risk may vary depending on the subject of diagnosis and the environment. In this respect, the predefined risk level may be different from that of the actual vulnerability. In this paper, to improve this point, we present a web vulnerability risk assessment model based on the attack result centering on the cyber kill chain.

Keywords: Web vulnerability, Risk assessment, Cyber Kill Chain

I. 서 론

오늘날 정보통신 기술의 비약적인 발달은 우리에게 다양한 정보 습득 기회의 제공과 생활의 편의성을 제공하게 되었다. 하지만 이와 동시에 여러 정보통신 기술에서 발생하는 취약점을 악용하려는 공격자의 사이버 위협에 대응이라는 과제에 직면하고 있다. 다음 표는 유럽 네트워크 정보보호원(ENISA)에서 2020

Received(04. 22. 2021), Modified(06. 04. 2021), Accepted(06. 04. 2021)

† 주저자, chmod640@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr(Corresponding author)

Table 1. ENISA Threat Landscape 2020

(1) Malware	**(2) Web-based attacks**	(3) Phishing
(4) Web application attacks	(5) Spam	(6) DDoS
(7) Identity theft	(8) Data breach	(9) Insider threat
(10) Botnets	(11) Physical manipulation, damage, theft and loss	(12) Information leakage
(13) Ransomware	(14) Cyber espionage	(15) Cryptojacking

년 발생한 주요 사이버 위협들을 순위별로 통계한 것으로[1], 정보통신 기술의 발전은 사이버 위협이 다양하게 변화해가는 원인을 제공하기도 한다.

다양한 사이버 위협이 발생하고 있지만, 웹 관련 공격이 2위와 4위를 기록하고 있다. 이렇듯 웹 서비스는 오랫동안 공격자들의 주요 대상이 되고 있다. 이러한 현상이 지속되는 원인으로 다음과 같이 3가지를 들 수 있다.

첫째, 불특정 다수에게 허용된 접근통제 정책.

웹 프로토콜은 다른 프로토콜과 달리, 불특정 다수에게 서비스를 제공하는 경우가 일반적이다. 이러한 특징으로 인하여 대부분 기업들의 웹 서비스 관련 정책은 인바운드 트래픽에 대하여 전체 허용 정책으로 운영·관리되고 있다. 공격자들은 이렇게 非신뢰 기반으로 허용된 서비스 포트로 접근하여, 홈페이지에 대한 취약점을 수집 및 공격할 수 있다.

둘째, 신규 취약점에 대한 대응.

특정 제조사에 의해서 생산되는 하드웨어 제품과는 달리, 홈페이지는 소프트웨어로 구성된 애플리케이션으로 누구나 쉽게 제작할 수 있는 생산성을 갖고 있다. 다음 통계는 2010년부터 2018년까지 국내에 서비스 되고 있는 홈페이지 운영 현황을 나타내고 있으며, 사업자보다 홈페이지 증가율이 지속적으로 높아지고 있음을 알 수 있다[2]. 특정 제조사의 애플리케이션이나, 하드웨어 장비라면 제조사를 통한 취약점 조치가 가능하지만, 개별적으로 대량 생산된 홈페이

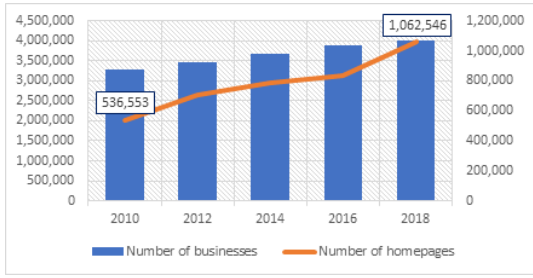

Fig. 1. Current status of Korean website

지는 다양한 취약점을 內在하고 있을 수 있다. 하지만 취약점 진단이나 침해사고가 발생하기 전까지는 이러한 취약점을 인지할 수 없기에, 운영자 미발견 또는 미조치 취약점을 대상으로 공격이 감행된다.

셋째, 웹 서비스를 통하여, 추가 공격 가능.

앞서 사이버 공격 통계를 통하여 다양한 사이버 위협이 발생하고 있음을 확인하였다. 이러한 공격들은 홈페이지 취약점 공격 성공시, 내부망 침투, 중요자료 유출, 악성코드 유포, 디페이스 공격 등이 가능하다.

이러한 이유로 해커들은 지속적으로 웹 서비스를 대상으로 공격을 수행하고 있다. 이에 대응하기 위하여, 국내·외 기관은 관련 기준과 법령을 제정하고 있으며, 가이드 제작 및 배포를 통하여 웹서비스 침해사고 예방을 위한 다양한 노력을 하고 있다.

다양한 예방 노력 중의 하나로 공격자의 입장에서 웹 취약점 점검·모의해킹과 같은 침투 테스트를 통하여 서비스의 보안 수준을 평가한다. 발견된 취약점은 위험도에 기반하여, 조치 우선순위를 정하게 된다. 하지만 이러한 취약점들의 위험도는 유관 기관의 통계 또는 전문업체의 자체적인 평가로 사전에 정의된 위험도이다. 웹 취약점 점검은 동적으로 이루어지기 때문에 사전에 평가된 위험도와 실제 점검 대상에서 발견된 취약점의 위험도는 점검 대상, 환경 등에 따라 상이할 수 있다. 이러한 점을 개선하고자 사이버 킬체인 모델과 함께 웹 취약점을 분석하고, 점검 결과 기반으로 현실적인 위험도를 평가할 수 있는 모델을 제안한다.

II. 관련 연구

2.1 웹 취약점 점검 현황 및 특성

여러 기업들은 운영 중인 정보시스템에 대한 취약

점 점검을 주기적으로 수행한다. 대표적인 취약점 점검 대상으로는 서버·단말 운영체제, 네트워크 장비, 데이터베이스, 보안장비, 응용 프로그램 등으로 구분지을 수 있다. 이중 응용 프로그램을 제외한 서버, 네트워크·보안 장비, 데이터베이스의 경우에는 보안 설정 값에 대한 적정성 유무만을 판단하기에, 정적·자동 점검이 가능하다. 하지만 이와 달리 응용 프로그램의 경우 소스 코드 수준의 점검만이 아닌, 응용 프로그램이 운영되고 있는 정보통신기술(ICT) 전반의 운영 환경에서 발생 가능한 취약점 점검을 동적으로 수행한다.

웹 취약점 점검은 홈페이지 규모, 점검 수행 인력의 전문성, 수행 기간 등 다양한 부분에서 간접적으로 영향을 받게 된다. 점검 형태 또한 지정된 보안 설정을 정적 점검하는 방식과 달리, 공격 가능한 부분에서 취약점을 찾아내는 방식으로 진행되기 때문에 취약점 점검을 완료하였어도, 운영시 소스코드의 수정, 환경의 변화, 발견하지 못한 內在 취약점 등으로 인하여 취약점은 지속적으로 발견 될 수 밖에 없다. 이러한 어려움을 개선하고자 시중에는 상시적 웹 취약점 점검이 가능한 자동화 도구가 다양하게 존재하지만, 자동화 도구만으로 해결하지 못하는 논리적 프로세스 결함까지 점검하는 것은 무리가 있다.

이러한 이유로 주로 전문 인력과 자동화 도구를 혼합·활용하여 주기적인 점검을 수행하고 있다. 하지만 위험 평가에 한해서는 관련 가이드나 자동화 도구에서 정의한 사전 위험도로만 평가되고 있는 상황이다. 취약점을 찾는 행위가 중요하듯이, 위험도에 따른 조치 우선 순위를 가이드하는 것 또한 중요하다.

2.2 국내·외 취약점 점검 가이드

웹 애플리케이션을 비롯한 소프트웨어 취약점 및 보안 약점 점검을 위한 가이드 라인이 국내·외에는 다양하게 존재한다. 이 중 웹 분야에서 대표적인 취약점 항목은 OWASP Top 10(2017), 과학기술정보통신부 주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드(2017), 한국인터넷진흥원 홈페이지 취약점 진단·제거 가이드(2013), 국정원 8대 취약점(2005) 등이 있다. 또한 특정 소프트웨어의 알려진 취약점을 위한 CVE/CVSS가 존재한다. 국내 정보보호 전문업체는 웹 모의해킹과 같은 취약점 점검시 이와 같은 취약점 항목을 적절히 혼합하여 사용하고 있다. 또한 소프트웨어 보안 약점 정적 점검을 위한 CWE/CWSS, 행정안전부 소프트웨어 보안 약점 진단 가이드가 있다. 본 절에서는 동적 환경에서 실시되는 웹 취약점 점검 가이드를 분석하고, 각각의 차이를 알아보고 웹 취약점 항목 통합시 적절히 활용한다.

2.2.1 OWASP Top 10(2017)

국제적으로 웹 취약점 평가의 척도가 되고 있는 OWASP Top 10은 웹 애플리케이션에서 발생 가능한 취약점 중에서 공격 가능성(E) 및 취약점 분포(P), 탐지 용이성(D), 기술적 영향(T)을 주기적으로 평가하여, 웹 취약점 공격 상위 10개를 발표하는 통계적 지표이다.

OWASP Top 10 지표는 국내와 달리 위험도를 정의하고 있다. 이를 통해 우리는 웹 애플리케이션 운영시 주의해야 할 취약점을 인지할 수 있다. 하지만 이는 사전에 정의된 평가 기준으로 위험도를 측정한 것으로, 실제 운영 환경에서 발생하는 취약점의 위험도를 표현하기에는 한계가 있다. 또한 광범위한 기준으로 취약점을 제시하고 있기에 해당 항목만으로 웹 취약점 점검을 수행하고, 평가하기에는 어려움이 존재한다.

Table 2. OWASP Top 10 - 2017 Details About Risk Factors

RISK	E	P	D	T	S
A1: Injection	③	②	③	③	8
A2: Authentication	③	②	②	③	7
A3: Sensitive Data Exposure	②	③	②	③	7
A4: XML External Entities (XXE)	②	②	③	③	7
A5: Broken Access Control	②	②	②	③	6
A6: Security Misconfiguration	③	③	③	②	6
A7: Cross-Site Scripting (XSS)	③	③	③	②	6
A8: Insecure Deserialization	①	②	②	③	5
A9: Vulnerable Components	②	③	②	②	4.7
A10: Insufficient Logging&Monitoring	②	③	①	②	4

본 논문에서는 OWASP Top 10의 각 항목을 국내 가이드의 통합된 웹 취약점의 상위 개념으로 구분할 것이며, OWASP Top 10 항목별 위험 산정치 점수[3]를 사전 위험도로 활용할 것이다.

2.2.2 주요정보통신기반시설 웹 취약점(2021)

과학기술정보통신부는 주요정보통신기반시설을 구성하고 있는 정보시스템에 대한 기술적 취약점 점검을 위한 가이드를 제작하였다[4]. 해당 가이드는 유닉스 서버, 윈도우즈 서버, 네트워크·보안 장비, 제어시스템, 개인용 컴퓨터, 데이터 베이스, 웹 분야로 구분되어 있으며, 중요도를 상·중·하로 평가하고 있다.

Table 3. Major information and communication infrastructure

Check List	Importance
Buffer overflow	High
Format string	High
LDAP injection	High
OS command injection	High
SQL injection	High
SSI injection	High
XPath injection	High
Directory indexing	High
Information leak	High
Malicious content	High
Cross-site scripting	High
Weak string strength	High
Insufficient authentication	High
Weak password recovery	High
Cross-site request forgery	High
Session prediction	High
Insufficient authorization	High
Insufficient session expiration	High
Session pinning	High
Automated attack	High
Missing process validation	High
File upload	High
File download	High
Admin page exposure	High
Path trace	High
Location disclosure	High
Data plain text transmission	High
Cookie tampering	High

웹을 제외한 다른 평가 항목들은 보안설정의 적정성에 대한 정적 점검이 가능한 반면, 웹의 경우에는 애플리케이션에서 발생 가능한 취약점을 동적으로 점검해야 한다. 점검 항목이 OWASP Top 10보다 세분화 되어 있는 특징이 있다. 앞서 설명하였듯이 웹 분야는 취약점 점검 방식이 다르기에 인력·시간 등 보다 많은 자원을 필요로 한다.

또한 정적 점검이 가능한 분야는 상·중·하로 중요도가 구분되어 있으나, 웹의 경우에는 모든 항목이 상으로 평가되어 있다. 이러한 이유는 기반시설을 대상으로 만들어진 점검 항목이므로 웹 애플리케이션을 통하여, 직접적인 접근과 공격이 가능하므로, 미약한 취약점일지라도 기반시설의 기밀성·가용성·무결성이 심각하게 위협받을 수 있기 때문이다. 이렇게 상으로 분류된 취약점에 대해서는 기간 내에 조치할 것을 정보통신기반 보호법에서는 규정하고 있다. 하지만 일반적인 환경에서 운영되는 웹 애플리케이션의 경우에는 소스 코드 수정만이 아닌, 보안장비, 보안패치 등으로 보안대책을 유연하게 수립할 수 있다. 항목별로 위험도를 분류할 필요가 있으며, 분류된 취약점은 위험도에 따라 조치 계획을 수립할 필요가 있다[5].

본 논문에서는 해당 점검 항목을 활용할 것이며, 각 항목은 상위 개념인 OWASP Top 10 기준에 따라 분류한다. 또한 각 항목의 위험도는 OWASP에서 산정한 위험도를 사전 위험도로 지정한다.

2.2.3 홈페이지 취약점 진단・제거 가이드(2013)

한국인터넷진흥원은 국내에서 운영되는 홈페이지의 수가 증가함에 따라 자체적인 홈페이지 취약점 진단 및 조치를 취할 수 있도록 가이드를 제작하였다[6]. 취약점 항목은 OWASP Top 10보다 상세하며, 기반시설 취약점 항목과 유사하다. 앞서 설명한 가이드라인과 차이점은 취약점 항목에 따른 공격 피해를 정의하고 있으나, 취약점의 위험도를 정의하고 있지 않다. 기반시설 취약점 분석·평가 가이드와 동일하게 발견된 모든 취약점을 조치해야 한다는 전제로 가이드가 제작되었다. 하지만 시스템 운영자 입장에서는 위험도를 식별하고, 우선 순위에 따른 이행 계획을 수립하기에는 부적절하다.

본 논문에서는 취약점 항목 및 공격 피해 항목을 사용할 것이다. 취약점 항목은 기반시설 취약점 항목과 통합할 것이며, 공격 피해는 웹 취약점 공격시 발생하는 1차 공격 결과로 활용한다.

Table 4. KISA Homepage Vulnerability Diagnosis/Removal Guide Items

Vulnerability item	Attack damage
OS command injection	Control of the system
SQL injection	DB information leakage
XPath injection	User authentication bypass
Information leakage	Server information exposure
Malicious content	Malware infection
Cross Site Script (XSS)	Session Hijacking Malware spread
Weak string strength	User account hijacking
Inadequate certification and accreditation	Taking over administrator privileges
Weak password recovery	User account hijacking
Insufficient Session Management	Stealing user rights
Cross-site request forgery	Stealing user rights
Automated attack	System overload
File upload	Control of the system
Path tracking and file download	Expose web server information
Data plain text transmission	Disclosure of sensitive information
Cookie tampering	Stealing user rights
URL/parameter tampering	Stealing user rights
Directory indexing	Exposing system files
Admin page exposure	Web site information disclosure
Location disclosure	Web site information disclosure
Web service method configuration attack	Control of the system

2.2.4 국가정보원 8대 취약점(2005)

국가정보원은 2005년 국내 홈페이지를 대상으로 발생하는 해킹사고 중 빈번하게 발생하는 취약점 상위 8개를 발표하였다[7]. 발생 빈도를 기준으로 취약점의 위험도를 평가하고 있다는 점에서는 OWASP Top 10과 같이 통계에 따른 사전 위험도를 정의하고 있다. 하지만 해당 항목은 2005년도 통계를 바탕으로 제작되었기에, 현재도 동일한 취약점 위험도로 평가하기에는 부적절하다. 예로 제로보드 및 테크노트 취약점의 경우에는 2000년대 초반에 홈페이지 제작에 다수 이용되었으나, 현재는 사양되어 가는 추세이며, 워드프레스 등의 신규 프레임워크로 이동하는 추세이다. 또한 취약점 항목에 대한 2005년 이후로 업데이트가 이루어지지 않고 있기 때문에 현재에도 해당 취약점의 통계 및 항목을 그대로 반영하기에는 다소 부족한 점이 있다.

본 논문에서는 OWASP Top 10 하위 항목 세부 취약점으로 주요정보통신기반시설 가이드 및 홈페이지 취약점 진단·제거 가이드, 국가정보원 취약점 항목 3가지를 통합한다.

앞서 살펴본 웹 취약점 가이드별 활용 필드는 다음과 같으며, 다음 절의 공격 결과 기반의 위험도 평가 모델 웹 취약점 통합시 활용한다.

- OWASP Top 10 : 위험, 점수
- 주요정보통신기반시설 : 취약점 항목
- 홈페이지 취약점 가이드 : 취약점 항목, 공격 피해
- 국정원 8대 취약점 : 취약점 항목

Table 5. NIS 8 Vulnerability Items

Rank	Vulnerability
1	Directory Listing
2	File Download
3	Cross Site Script
4	File Upload
5	WebDAV -Remote Execution
6	Technote
7	Zeroboard
8	SQL Injection

2.3 사이버 킬체인

2.3.1 통상 개념

타격 순환 체계를 의미하는 군사 용어 킬체인은, 적군의 공격 과정과 그 요소를 파악하여 선제 타격을 하는 적극적 방어 체계이다. 킬체인은 탐지, 확인, 추적, 조준, 교전, 평가의 6가지 단계로 구성되며, 적의 공격 중 초기 단계에서 예방하는 것이 효과적이라는 개념이다. 예로 적이 탐지할 수 있는 정보가 적으면 적을수록 다음 공격을 성공할 확률이 낮아진다.

군수 업체인 록히드 마틴社는 이러한 개념에 착안하여 사이버 킬체인 모델을 제안하였다[8]. 록히드 마틴사에 의해 제안되었으나, 현재는 다양한 사이버 킬체인 모델이 존재하고 있으며, 각 회사는 특성에 맞게 대응 모델을 개선·발전시켜 나아가고 있다.

사이버 킬체인은 공격의 각 단계를 파악하여 예방하는 것이 기본 개념이다. 이는 지능형 지속적 위협(APT)에 특화된 대응 모델로 공격 프로세스를 단계별로 정의하고, 이에 대한 대응 방안을 마련하였다[9]. 해당 모델은 공격자의 목적 달성까지 한 단계만이라도 차단을 할 수 있다면, 공격의 지연 또는 실패시키는 것에 목적을 두고 있다[10]. 하지만 해당 모델은 보안 장비에 의존적이라는 점과 내부 위협에는 대응하지 못한다는 한계가 존재한다[11].

Table 6. Cyber Kill Chain Model[12]

Step	Cyber Kill Chain	Explanation
1	Reconnaissance	Attack target and target selection
2	Weaponization	Preparing Cyber Weapons
3	Delievery	Delivering cyber weapons to target systems
4	Exploitation	Using vulnerabilities to operate cyber weapons
5	Installation	Install malicious programs on the target system
6	Command and Control	Build a channel for remote operation
7	Actions on Objectives	Achieving the intended purpose

2.3.2 개념 적용 방안

본 논문에서는 웹 애플리케이션에서 발생할 수 있는 취약점을 단계별로 사이버 킬체인 모델에 접목 시켜서 위험도를 평가할 것이다. 사이버 킬체인은 지능형 지속적 위협(APT)을 기준으로 제안된 모델로서, 웹 취약점 공격 과정과는 상이할 수 있다. 하지만 공격이 최선의 방어라는 킬체인 개념과 공격자 입장에서 사전에 취약점을 도출·조치하는 웹 취약점 및 모의해킹 진단 등의 침투 테스트와 개념이 유사하다.

웹 취약점 점검의 형태는 공격자의 입장에서 대상 시스템을 점검하는 방식으로 진행되기 때문에 사이버 킬체인 모델에 따라 취약점 점검 결과가 도출 가능하다. 이러한 과정을 통해 시스템 운영자는 취약점에 대한 일련의 공격 과정을 파악 가능하며, 소스코드 수정, 보안 장비 도입, 정책 수정 등 보안대책을 유연하게 수립할 수 있다. 또한 취약점 조치시 산정된 위험도에 따라 조치 우선 순위를 쉽게 파악 가능하다.

III. 공격 결과 기반의 위험도 평가 모델

3.1 웹 취약점 통합

- 대분류 및 상세 취약점

국내에서 웹 취약점 점검시 주로 사용되고 있는 통신기반시설 웹 취약점 점검 항목, 한국인터넷진흥원 홈페이지 취약점 진단·제거 가이드, 국정원 8대 취약점 항목을 취합하였다. 취약점 항목 중 불충분한 인증과 불충분한 인가는 OWASP Top 10의 취약한 인증과 취약한 접근 통제로 상위 개념으로 재분류하였다.

- 공격 방법

각 취약점들은 공격 방식이 다르기 때문에 취약점별 공격 방식을 분석하여 공격 방법 필드를 새로 구성하였다. 파라미터에 대한 입력값, 정보 노출, 특정 기능, 세션 공격, 인증 무력화, 웹 서버 설정 및 소프트웨어 공격으로 정의하였다[13].

- 결과

한국인터넷진흥원 홈페이지 취약점 진단 가이드의 공격 피해는 정보 노출, 인증 우회, 데이터 베이스 장악, 시스템 장악, 권한 탈취, 계정 탈취로 간략하게 구분 하였다. 그 결과는 다음 표와 같다. 이중 내부 시스템 침투가 가능한 시스템 장악, 데이터 베이스 장악에 한하여 목적 달성 단계로 평가한다. 이외의 결과는 명령 및 제어 단계에서 평가한다.

- 사전 위험도

취합된 항목과 OWASP Top 10의 항목에 매핑을 시켰으며, 각각의 매핑된 취약점은 OWASP 위험도를 반영하여 사전 위험도로 정의하였다.

Table 7. Integrated web vulnerabilities

Category (Prerisk)	Attack method	Vulnerability	Attack damage
A1: Injection (8)	Input-base	SQL	Control of the DB
		OS Command	Control of the system
		Buffer Overflow	Information disclosure
		Format String	
	Specific feature	LDAP	Bypass auth
		XPath	
		SSI	Control of the system
A2: Authentication (7)	Disable authentication	Weak string strength	Account takeover
		Weak password recovery	
		Automated attack	
	Session management	Session prediction	Hijacking authority
		Session pinning	
		Insufficient session expiration	
		Cookie tampering	
A3: Sens. Data Exposure (7)	Information disclosure	Information leak	Information disclosure
		Admin page exposure	
	Session management	Data plain text transmission	
A4: XXE (7)	Specific feature	XXE	Control of the system
A5: Broken Access Control (6)	Access control	Missing process validation	Hijacking authority
		URL/param tampering	
	Input-base	Path trace	Information disclosure
		File download	
		File upload	Control of the system
A6: Security Misconfiguration (6)	Web server config	Directory indexing	Information disclosure
		Location disclosure	
		Web method	Control of the system
		WebDAV	
A7: XSS (6)	Input-base	XSS	Hijacking authority
		CSRF	
A9: Vuln-Components (4.7)	Web server S/W	Tech note	Corresponding result
		Zero board	
		etc	

3.2 웹 공격 사이버 킬체인 모델

사이버 킬체인 개념도는 다음 그림과 같으며, 각 단계별 주요 구성 요소를 설명한다.

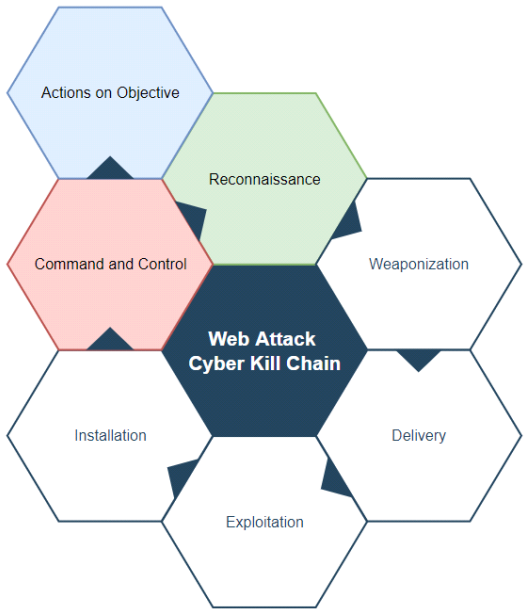

Fig. 2. Cyber Kill Chain Concept

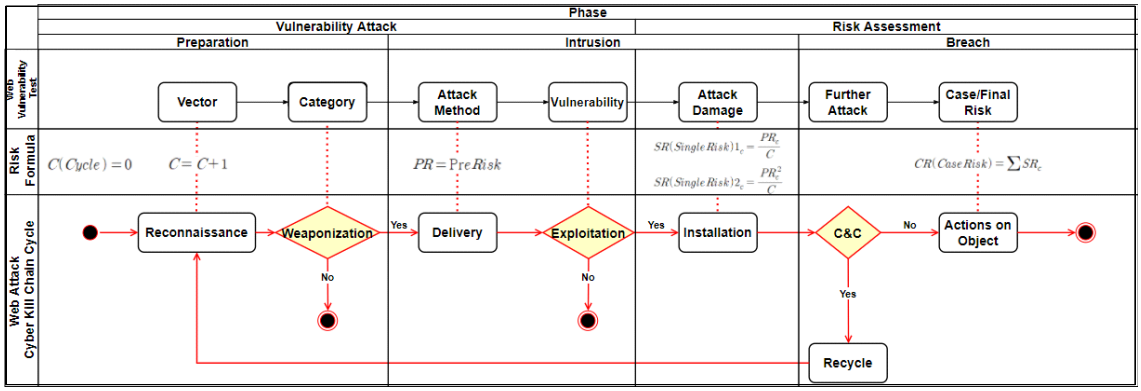

Fig. 3. Web Attack Cyber Kill Chain Algorithm

3.2.1 웹 공격 사이버 킬체인 구성 요소

- 구성 기호

Table 8. Description of configuration symbols

Figure	Symbol name	Explanation
	Starting terminal	The start of an attack
	End Terminal	The end of the attack
	Treatment symbol	Handling point for attack
	Judgment symbol	Branch point by situation condition

- 사이클
  - 정찰(Reconnaissance) 단계에서 목적 달성(Actions on Object) 전까지 일련의 과정이 되며, 위험 평가시 설치(Installation) 단계에서 도출된 단일 취약점의 총합이 된다. 사이클이 재귀하는 부분은 명령 및 제어(Command and Control) 단계에서 다른 취약점과 연계하여 추가 공격이 가능할 경우 정찰(Reconnaissance) 단계로 넘어가면서 N번째 사이클이 시작된다.
- 처리 기호 : 정찰, 전달, 설치, 목적 달성 단계
  - 취약점 공격을 위한 행위를 표현한다. 공격 가능성을 확인하기 위한 행위 및 공격 행위, 취약점 확인, 공격 성공의 행위가 단계별로 정의된다.
- 판단 기호 : 무기화, 공격, 명령 및 제어
  - 취약점 공격 중 처리 기호에 대한 확인 절차에 해당 된다. 보안 수준으로 인하여, 해당 공격 또는 추가 공격에 대한 성공 및 실패를 통해 분기한다.

3.2.2 웹 공격 사이버 킬체인 단계별 정의

상위 개념으로 준비(Preparation), 침입(Intrusion), 침해(Breach) 3단계로 구분하였다[14]. 록히드 마틴社의 사이버 킬체인 모델 7단계는 하위 세부 단계로 정의하였으며, 3.1. 절에서 정의한 통합 웹 취약점은 사이버 킬체인의 무기화 단계부터, 설치 단계까지 매칭하였다. 또한 공격 성공시 해당하는 침해 구간의 명령 및 제어, 목적 달성 단계는 본 논문에서 제시하는 위험 평가 방법을 적용하였다. 이로써 웹 취약점 공격 위험도 평가 모델에 대한 기본 개념을 도출하였다.

Table 9. Web Attack Cyber Kill Chain

Web Attack Cyber Kill Chain			
Phase	Kill Chain	Web Vul[1)]	Division
Prepare	Recon	Vector	Vulnerability Attack
	Weaponize	Category	
Intrusion	Delivery	Attack Method	
	Exploit	Vulnerability	
	Install	Attack Damage	Risk Assess
Breach	C&C	Further Attack	
	Actions on Objectives	Case/Final Risk	

1) Vul = Vulnerability

- 준비(Preparation) : 공격자(점검자)가 공격 대상(점검 대상)의 취약점을 악용할 수 있는 방법을 알아내는 단계
  - 정찰(Reconnaissance) : 웹 애플리케이션에서 발생 가능한 취약점들의 공격 지점 탐색 단계로 Attack Vector로 구분
  - 무기화(Weaponization) : 공격 지점을 통하여 공격 가능 취약점을 통합 웹 취약점 대분류의 OWASP Top 10 항목과 매핑
- 침입(Intrusion) : 공격자(점검자)가 악용할 수 있는 취약점을 발견했고, 그것을 전달하여 보안 통제를 거쳐 취약점 공격까지 성공하는 단계
  - 전달(Delivery) : 무기화 단계에서 정의된 대분류 기준으로 공격 방식에 따른 세부 취약점 항목 정의
  - 공격(Exploitation) : 공격 방식에 따라 취약점 공격 성공 여부를 확인하는 조건 분기점으로, 해당 단계에서 보안 대책 제시 및 조치를 통하여 향후 공격자의 킬체인을 종료시키는 단계
  - 설치(Installation) : 공격 지점에 대한 취약점 공격 성공 단계로 통합 웹 취약점에서 정의한 사전 위험도로 단일 취약점을 산정하며, 아래 표와 같이 공격 결과에 따라 취약점 차수 적용[15]

Table 10. Attack Damage Division

Degree	State	Attack Damage
1	Front-End	Information disclosure Bypass authentication Account takeover Hijacking authority
2	Back-End	Control of the DB Control of the system

- 침해(Breach) : 준비 ~ 침입 단계로부터 확인된 취약점의 추가 공격 가능 여부 확인 및 목적 달성 최종 단계에서 조건에 따라 최종 위험도를 산정
  - 명령 및 제어(Command And Control) : 해당 취약점이 다른 취약점과 연계하여 추가 공격 가능이 가능할 경우 정찰 단계로 분기하거나, 추가 공격이 불가능할 경우 목적 달성 단계로 이동
  - 목적 달성(Actions on Objective) : 시스템 장악 또는 데이터 베이스 장악 등 취약점 공격의 목적 달성시 킬체인 종료 및 유형별 취약점 위험도를 합산하여 비교

3.3 위험 평가 모델

3.3.1 결과 기반 위험 평가

취약점 공격 구간은 공격의 성공 여부를 판단하고, 평가하는 구간이다. 정찰 단계에서는 사이버 킬체인의 사이클 수치가 증가되며, 전달 단계에서 통합 웹 취약점에서 정의한 사전 위험도가 할당된다.

- 정찰(Reconnaissance) : 사이클이 카운트 되는 구간으로 처음 시작 또는 명령 및 제어 단계에서 추가 공격을 위해 정찰단계로 회귀 및 사이클 증가

$$C(Cycle) = C+1 \tag{1}$$

- 전달(Delivery) : 통합 웹취약점 대분류에 따라 집계된 점수 사전 위험도 지정

$$PR = \mathrm{Pre}Risk \tag{2}$$

위험 평가(Risk Assessment) 구간에서는 단일 취약점 및 사이버 킬체인의 사이클 위험도를 합산하여 유형별 위험도(Case Risk)를 산정하고, 최종 위험도(Final Risk)를 평가한다.

- 설치(Installation) : 단일 취약점에 대한 위험 평가 구간으로 다음 표와 같이 공격 결과에 따라 단일 위험도를 평가하며, 최종 위험도 산출시 사용

Table 11. Attack Damage Division

Degree	Formula
1	$SR(SingleRisk)1_c = \frac{PR_c}{C}$ (3)
2	$SR(SingleRisk)2_c = \frac{PR_c^2}{C}$ (4)

- 명령 및 제어(Command and Control) : 일련의 공격 과정 중 발생 가능한 취약점의 총합을 나타내며, 추가 공격과 목적 달성을 분기하는 지점

Table 12. Branch additional attacks

C&C[2)]	Decision	Next Step
Further Attack	Yes	Recycle
	No	Actions on Object

- 목적 달성(Actions on Objectives) : 일련의 목적 달성시, 공격 과정에서 발생한 단일 취약점 위험도를 합산하여 유형별 위험도를 산출

$$CR(CaseRisk) = \sum SR_c \quad (5)$$

- 최종 위험 평가(Final Risk) : 점검 대상의 유형별 위험도에 따라 유형 우선순위(Case Priority)를 산정하고, 단일 취약점 위험도를 유형 우선순위에 따라 최종 위험도를 평가

$$FinalRisk = \frac{SingleRisk}{CasePriority} \quad (6)$$

IV. 위험 평가 모델 검증

4.1 사전통계와 결과 기반 위험 평가 비교

평가는 실제 웹 취약점 점검 결과를 바탕으로 진행하였으며, 발견된 취약점 위험도를 분류하였다. 사전 위험도는 OWASP 기준을 따랐으며, 결과 기반 위험도는 본 논문에서 제시한 모델에 따라 반영하였다.

유형 1. **다운로드 취약점(6)**을 통하여, 관리자 세션 쿠키 정보 획득, **쿠키 변조(7)** 후, **SQL 삽입 공격(8)**을 통하여 웹 관리자 권한 탈취, 관리자 메뉴를 통하여 **파일 업로드(6)** 후 시스템 권한 획득

Table 13. Case 1 Compare

Cycle	Vulnerability	Risk(Priority)	
		Pre	Result
1	File download	6(3)	6(2)
2	Cookie tampering	7(2)	3.5(3)
3	SQL Injection	8(1)	2.6(4)
4	File upload	6(3)	9(1)

유형 2. **웹 메소드 공격(6)** PUT 메소드를 통한 악성 파일 업로드를 통하여 시스템 권한 획득

Table 14. Case 2 Compare

Cycle	Vulnerability	Risk(Priority)	
		Pre	Result
1	Web method	6(1)	36(1)

유형 3. 웹 응용 프로그램 서버 관리자 페이지 **위치 공개(6)** 및 **약한 문자열 강도(7)** 취약점으로 관리자 권한 탈취, 배포 메뉴의 **취약한 컴포넌트 취약점(4.7)**으로 악성 파일 업로드 후 시스템 권한 획득

Table 15. Case 3 Compare

Cycle	Vulnerability	Risk(Priority)	
		Pre	Result
1	Location disclosure	6(2)	6(2)
2	Weak string strength	7(1)	3.5(3)
3	Vuln-Components	4.7(3)	7.36(1)

유형 4. **크로스 사이트 스크립팅(6)** 공격으로 세션 탈취, **세션 관리 미흡(7)**으로 사용자 권한 탈취

Table 16. Case 4 Compare

Cycle	Vulnerability	Risk(Priority)	
		Pre	Result
1	XSS	6(2)	6(1)
2	Insufficient session expiration	7(1)	3.5(2)

이와 같이 결과 기반 위험 평가 모델은 취약점에 따라 발생 결과 및 연계 가능 여부에 따라 위험도 순위를 평가할 수 있다. 결과 기반 위험도 평가를 통해 담당자는 운영 중인 시스템에서 발견된 취약점의 위험도에 따라 우선 순위를 식별할 수 있다.

4.2 취약점 점검 결과 통합 위험 평가

4.1. 절에서 확인한 바와 같이 사이버 킬체인에 따라 목적 달성 유형별 위험도 평가가 가능하였으며, 식별된 위험을 통하여 우선 순위를 산정할 수 있었다. 실제 점검 대상 및 환경에서는 4.1 절과 같이 다양한 유형의 취약점이 발견된다. 여러 유형으로 구성

2) C&C = Command & Control

된 웹 취약점을 위험도를 구분하고, 최종적인 위험 평가를 진행한다.

우선, 4.1 절에서 도출된 결과 기반 단일 위험도를 합산하여 유형 위험도를 구하였으며, 유형별 유형 위험도에 따라 다음 표와 같이 유형 우선순위를 산출하였다. 유형 2의 경우 시스템 권한을 첫 번째 사이클에서 획득하였기에, 해당 공격 유형의 우선순위가 가장 높음을 알 수 있다.

Table 17. Case Priority

Case	SUM	Case Priority
1	21.1	2
2	36	1
3	16.86	3
4	9.5	4

여러 취약점의 최종 위험도를 구하기 위하여, 설치 단계에서 정의된 단일 취약점(Single Risk)을 유형 우선 순위에 따라 나누어 주었다. 이에 따라 다음과 같이 시스템 내에서 발견된 취약점들의 위험도 및 조치 우선순위를 평가할 수 있었다.

Table 18. Final Risk

Rank	Vulnerability	SR[3]	CP[4]	FR[5]
1	Web method	36	1	36
2	File upload	9	2	4.5
3	File download	6	2	3
4	Vuln-Components	7.36	3	2.45
5	Location disclosure	6	3	2
6	Cookie tampering	3.5	2	1.75
7	XSS	6	4	1.5
8	SQL Injection	2.6	2	1.3
9	Weak string strength	3.5	3	1.17
10	Insufficient session expiration	3.5	4	0.88

V. 결 론

본 논문에서 제안한 위험 평가 모델은 공격자의 목적 달성 상황이 여러 취약점과 함께 발생 가능할 경우에 취약점의 위험도는 낮아진다는 관점에서 시작되었으며, 연구 성과는 다음 4가지로 분류할 수 있다.

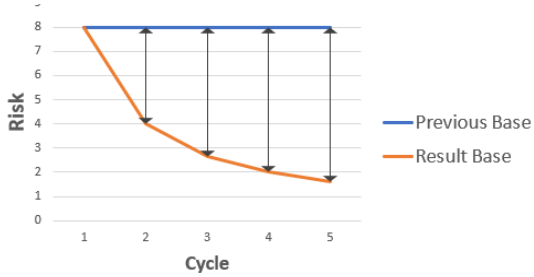

Fig. 4. Previous-based versus results-based comparison

첫째, 국내·외 웹 취약점 점검 항목 통합.

국내·외 존재하는 웹 취약점 점검 항목을 바탕으로 통합 웹 취약점 항목을 구성하였다. OWASP Top 10 기준으로 해당되는 상세 취약점을 분류하였으며, 해당 취약점은 OWASP에서 통계 기반으로 위험도를 산정한 점수치를 사전 위험도라 칭하였다. 또한 공격 결과에 따른 위험 평가를 정의하여, 사용자·시스템 권한으로 나누어 공격 결과에 대한 위험도를 세분화하여 평가 가능토록 하였다.

둘째, 웹 취약점 위험 모델링.

웹 취약점 항목들에 대하여, 공격 지점부터 공격 결과까지 위협 모델링을 수행하였다. 해당 각 결과를 바탕으로 지능형 지속적 위협(APT)에 특화된 사이버 킬체인 모델을 웹 취약점 공격에 응용할 수 있는 방법을 도출하였다.

셋째, 결과 기반 위험도 평가.

웹 취약점 점검을 통하여, 도출한 웹 취약점 결과를 바탕으로 공격 결과 및 공격 사이클에 따른 단일 위험도 평가 모델을 제시하였으며, 점검 대상에서 발생하는 전체 취약점에 대해서 또한 개별 최종 위험도를 산출 할 수 있는 방법론을 제시하였다. 기존에는 웹에서 발생 가능한 웹 취약점을 모두 도출하여, 취약점에 해당하는 위험도를 통계적으로 측정하는 기준이 강하였다. 하지만 본 논문에서는 취약점의 위험도가 중점이 아닌, 점검 대상에서 발생하는 취약점의 위험도 우선 순위를 중점적인 관점으로 재해석하여, 위험 평가 모델을 제시하였다.

넷째, 사이버 킬체인에 따른 웹 취약점 공격 대응.

사이버 킬체인 모델은 공격자의 공격 단계를 파악

3) SR(Single Risk) 설치 단계의 단일 취약점 위험도
4) CP(Case Priority) 유형별 위험도 순위
5) FR(Final Risk) SR÷CP를 통한 최종 위험도

함으로써, 각 단계별 대응 방안을 수립하여 공격자의 공격을 차단 또는 지연시키는데 목적을 두고 있다. 웹 취약점 공격용 사이버 킬체인 또한 웹 서비스를 바탕으로 발생할 수 있는 공격을 단계별로 정의하여 위험도를 측정하여 우선 순위별 조치할 수 있도록 하였다. 또한 해당 킬체인 모델을 사용하여, 연결 고리를 제거함으로써 공격자가 최종 목적 달성까지의 공격을 성공할 수 없도록 능동적 사이버 보안이 가능하도록 하였다.

OWASP 위험도 산정식 및 CWSS, CVSS와 같이 사전에 정의된 취약점 위험도가 불필요한 것은 아니지만, 실제 점검 환경에서 도출된 취약점 결과의 위험도를 사전에 평가된 것으로 평가하기에는 다소 무리가 있었다. 하지만 본 연구를 통하여, 사이버 킬체인에 따른 위협 모델링과 위험 평가가 가능하였으며, 공격 연결 고리를 단절시켜 공격자의 공격을 단계별로 차단 가능하게 되었다. 이와 같이 본 연구를 통하여, 웹 취약점 위험도 평가에 대한 사전 통계 위주 방식에서 벗어나 새로운 관점을 제시할 수 있을 것으로 기대한다.

References

[1] European Union Agency for Network and Information Security(ENISA), "ENISA Threat Landscape 2020 - List of top 15 threats," Oct. 2020.

[2] Korean Statistical Information Service(KOSIS), "Status of Informatization Statistics Survey Websites (Homepage, etc.)," May. 2020.

[3] OWASP, "OWASP Top 10 - 2017," Apr. 2017.

[4] Ministry of Science and ICT, "Detailed Guide to Analysis and Evaluation Method of Technical Vulnerability of Major Information and Communication Infrastructure," Mar. 2021.

[5] Autumn Byeon, Jong In Lim and Kyong-Ho Lee, "A Study On Advanced Model of Web Vulnerability Scoring Technique," Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 25(5), pp. 1217-1224, Oct. 2015.

[6] Korea Internet & Security Agency(KISA), "Guide to Homepage Vulnerability Diagnosis and Removal for Information System Developers and Operators," Dec. 2013.

[7] National Cyber Security Center(NCSC), "Homepage Security Management Manual," May. 2005.

[8] Eric M Hutchins, Michael J Cloppert and Rohan M Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Leading Issues in Information Warfare & Security Research. vol. 1, no. 1, pp. 113-125, Apr. 2011.

[9] Kyuyong Shin, Kyoung Min Kim and Jongkwan Lee, "A Study on the Concept of Social Engineering Cyber Kill Chain for Social Engineering based Cyber Operations," Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 28(5), pp. 1247-1258, Oct. 2018.

[10] Eun-hye Han and Kim In-Seok, "Efficient Operation Model for Effective APT Defense," Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 27(3), pp. 501-519, Jun. 2017.

[11] Kwang-Je Kim, Tae-Shin Kang, Jae-Hong Kim, Seunghoon Jung and Jong-Bae Kim, "Cyber Defense Development Plan based on Cyber Kill Chain," Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology (AJMAHS), 7(1), pp. 277-285, Jan. 2017.

[12] Jung-sik Lee, Sung-young Cho, Heang-rok Oh and Myung-mook Han, "A Study on Defense and Attack Model for Cyber Command Control System based Cyber Kill Chain," Journal of Internet

Computing and Services (JICS), 22(1), pp. 41-50, Feb. 2021.
〔13〕 Dafydd Stuttard and Marcus Pinto, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws," Wiley, pp. 999-1078, Sep. 2011.
〔14〕 Wilson Bautista, "Practical Cyber Intelligence," Packt, pp. 64-65, Mar. 2018.
〔15〕 Sungyoung Cho, Suyeon Yoo, Sang-hun Jeon, Chae-ho Lim and Sehun Kim, "A Web application vulnerability scoring framework by categorizing vulnerabilities according to privilege acquisition." Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 22(3), pp. 601-613, Jun. 2012.

〈저자소개〉

진 희 훈 (Hui Hun Jin) 정회원
2012년 2월: 서울과학기술대학교 컴퓨터공학과 학사
2011년 11월~2014년 09월: SK인포섹 모의해킹
2014년 10월~2015년 06월: 롯데정보통신 보안컨설팅
2014년 3월~현재: 사이버보안전문단
2015년 7월~현재: 한국광물자원공사 정보보안
2019년 9월~현재: 고려대학교 정보보호대학원 사이버보안학과 석사과정
〈관심분야〉 보안 아키텍처, 침투 테스트, 취약성 분석·평가, 네트워크 보안

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경학학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장. Technical Director
2010년 3월~2014년 12월: 고려대학교 정보보호대학원 조교수
2015년 1월~2020년 2월: 고려대학교 정보보호대학원 부교수
2020년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 온라인게임 보안, 자동차 보안, 침입탐지시스템, 네트워크 보안