Journal of KIIT. Vol. 23, No. 1, pp. 201-212, Jan. 31, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.1.201

ASM 솔루션을 활용한 공개 홈페이지 보안 취약점 분석 및 효율적인 대응방안 연구

최강석*, 이수진**

A Study on the Analysis of Vulnerabilities in Public Homepage using ASM Solution and Efficient Countermeasures

Kangsock Choi*, Soojin Lee**

요 약

민간기업의 온라인 활동이 증가하면서 웹사이트 및 웹 애플리케이션의 취약점을 겨냥한 공격이 급증하고 있다. 이에 본 연구에서는 공격표면관리(ASM) 솔루션인 Criminal IP를 활용하여 국내 10개 민간기업의 공개 홈페이지상에 존재하는 공개 취약점(CVE)을 분석하였다. 그 결과 10개 기업 모두에서 WEB/WAS, 네트워크 통신 및 보안 통신을 위한 암호화 라이브러리 등과 관련된 394개의 공개 취약점이 식별되었다. 394개의 공개 취약점 중 37.3%인 137건이 시급한 조치가 필요한 심각도 High 이상의 취약점이며, Critical 등급에 해당하는 취약점도 40개가 존재하였다. 식별된 핵심 취약점에 대해서는 그로 인해 발생 가능한 잠재적 위험을 제시하고, 위험 완화 및 안전한 공개 홈페이지 운영을 위한 기술적·정책적 차원의 대응방안들도 제시하였다.

Abstract

As private companies' online activities increase, cyber attacks targeting vulnerabilities in websites and web applications are increasing rapidly. In this study, we analyzed public vulnerabilities(CVEs) on the public websites of 10 domestic private companies using Criminal IP, an attack surface management solution. As a result, 394 CVEs related to WEB/WAS, network communication, and encryption libraries for secure communication were identified. Of the identified vulnerabilities, 137 CVEs(37.3%) were vulnerabilities with a severity level of High or higher that requiring urgent action, and 40 CVEs were Critical level vulnerabilities. For the identified core vulnerabilities, we presented potential risks that could arise from them, and suggested technical and policy-level countermeasures for risk mitigation and safe operation of public homepages.

Keywords

public homepage, attack surface management, CVE, risk, technical and policy-level countermeasures

* 국방대학교 국방정보관리전공 석사과정
- ORCID: https://orcid.org/0009-0008-0810-0272
** 국방대학교 사이버·컴퓨터공학학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-4117-407X

· Received: Oct. 12, 2024, Revised: Nov. 20, 2024, Accepted: Nov. 23, 2024
· Corresponding Author: Soojin Lee
Dept. of Cyber Security and Computer Engineering, Korea National Defense University, 1040, Hwangsanbul-ro, Nonsan-si, Chungcheongnam-do, Republic of Korea
Tel.: +82-41-831-5378, Email: cyberkma@korea.kr

Ⅰ. 서 론

코로나 팬데믹 이후 온라인을 통한 기업 활동이 이전보다 활발해지면서 기업 웹사이트와 웹 애플리케이션 취약점을 악용하는 사이버공격도 함께 증가하고 있다. Forbes에서 발표한 웹사이트 통계자료에 의하면, 3초에 1개씩 매일 250,000개의 새로운 웹사이트가 생성되고 있으며, 2023년 기준으로 71%의 기업이 웹사이트를 운영하고 있다[1].

그리고 Terranova Security社 발표자료에 의하면, 웹 애플리케이션의 98%가 악성코드 유포에 악용되거나 악성 웹사이트로의 리다이렉션을 유발하는 등 사이버공격에 취약하며, 전체 사이버공격의 17%가 이러한 웹 애플리케이션의 취약점을 겨냥한 공격인 것으로 확인되었다[2]. 과학기술정보통신부 발표자료에서도 24년 상반기 침해사고 신고 건수 899건 중 웹서버 해킹이 504건으로 가장 큰 비중을 차지하였다[3].

일반적으로 웹 해킹은 기업이나 공공기관이 공개적으로 운영하는 홈페이지에서 웹 스캐닝 툴 등을 통해 해킹에 필요한 취약점 정보를 수집하는 것으로부터 시작된다. 그리고 홈페이지 운영에 필수적인 상용 소프트웨어인 웹서버, WAS(Web Application Server) 및 DBMS 등은 매년 새로운 취약점이 공개되고 있어 간단한 정보수집 활동만으로도 취약점을 손쉽게 파악할 수 있다. 만약 공개된 취약점에 대한 보완이 적시에 수행되지 않는다면 해당 홈페이지는 사이버 공격자들의 손쉬운 공격목표가 되어 심각한 사이버 위협에 노출될 수도 있다. 웹사이트가 해킹되거나 공격자가 시스템이나 소프트웨어를 조작할 수 있는 경우에는 웹사이트는 물론 전체 네트워크까지 문제가 생겨 기업 운영이 중단될 수도 있다.

이러한 상황 인식하에 본 연구에서는 국내 주요 민간기업이 운영하는 공개 홈페이지 내에 존재하는 취약점을 공격표면관리(ASM, Attack Surface Management) 솔루션을 통해 파악하여 분석함으로써 공개 홈페이지로 인해 직면할 수 있는 위험의 심각성을 구체적으로 평가한다. 그리고 그 결과를 바탕으로 사이버 위협에 선제적으로 대응하기 위한 기술 및 정책적 측면의 조치사항을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 ASM 툴, 대외 공개 홈페이지 관리 기준 및 보안 위협, 사이버공격 동향을 살펴보고 공개 홈페이지 보안 관련 선행연구를 정리한다. 3장에서는 국내 주요 민간기업의 공개 홈페이지 운영 현황을 정리하고, 일부 민간기업의 공개 홈페이지에 대한 사이버 위협 실태를 파악한 결과를 분석한다. 4장에서는 공개 홈페이지의 보안성 강화에 필요한 기술적 및 정책적 차원의 대응방안을 제시한다. 마지막으로 5장에서 연구를 요약하고 결론을 맺는다.

Ⅱ. 관련 연구

2.1 공격표면관리(ASM)

공격표면(Attack surface)은 허가받지 않은 사용자가 시스템에 불법으로 접근하여 데이터를 탈취할 수 있는 모든 가능한 지점 또는 취약점(혹은 공격 벡터의 수)을 의미한다. 조직은 잠재적 위협을 최대한 빨리 식별하고 차단하기 위해 공격표면을 지속적으로 모니터링하고 최소화해야 한다[4].

공격표면을 구성하는 요소는 네트워크 자산(공개 IP 주소, 네트워크 서비스, 포트 및 프로토콜 등), 애플리케이션(웹 애플리케이션, API, 클라우드 서비스 등), 시스템(서버, 데스크톱, 모바일 장치 등), 데이터(데이터베이스, 파일 저장소, 데이터 전송 경로 등) 및 사용자(직원, 제3자 서비스 제공자, 파트너 등) 등이다[5].

ASM은 조직의 관리대상이 되는 IT 자산에 존재하는 공격표면을 식별하고 관리하는 보안관리의 한 분야이다. ASM을 통해 조직은 효율적으로 IT 자산을 관리하면서 취약점을 테스트할 고위험 영역과 공격자가 수행 가능한 공격 벡터를 식별하여 보안 사고를 예방할 수 있다. 그리고 시스템 각 부분에 접근할 수 있는 사용자 유형과 권한을 재설정하여 내부자 위협을 감소시킴은 물론 표적형 사이버공격까지도 완화할 수 있다[6].

이상과 같은 이유로 최근 ASM 솔루션을 적용하여 공격표면을 관리하려는 기업이 증가하고 있다.

특히 방어자 관점에서 위험을 관리했던 대부분의 사이버보안 솔루션들과 달리 ASM 솔루션은 공격자 관점으로 IT 시스템을 관찰할 수 있도록 지원하고 있어 도입이 계속 증가할 것으로 전망하고 있다.

ASM 솔루션이 제공하는 주요 기능은 ① 자산 발견(조직의 모든 IT 자산 자동 탐지 및 목록화), ② 취약점 분석(자산의 취약점 및 우선순위 식별), ③ 위협 인텔리전스(최신 위협정보 제공 및 공격자 패턴 분석), ④ 위험 평가(식별된 취약점 및 위협에 대한 위험 평가), ⑤ 자동화된 모니터링(지속적으로 공격표면을 모니터링하고 새로운 취약점 및 변화된 자산 탐지) 등이다[5]-[7].

2.2 공개 홈페이지 관리 기준

행정안전부에서 발표한 '행정·공공기관 웹사이트 구축운영 가이드'[8]는 행정 및 공공기관이 웹사이트의 구축·운영부터 폐기까지 준수 또는 참조해야 할 사항을 종합적으로 제공하는 안내서이다. 가이드 적용 대상은 행정기관 등이 웹 서비스를 목적으로 구축·운영하는 웹사이트이다.

가이드에서는 웹사이트의 구축 단계부터 보안을 고려하면서 사용자 인증, 권한 관리, 데이터 암호화 등 다양한 보안 설계를 적용하여 외부 공격에 대한 방어력을 강화할 것을 요구한다. 또한, 웹사이트의 취약점을 주기적으로 점검하고, 발견된 취약점에 대한 패치를 신속하게 적용하여 소프트웨어 및 시스템을 최신 상태로 유지할 것을 강조하고 있다.

2023년 12월 개정된 한국인터넷진흥원(KISA)의 '홈페이지 개인정보 노출방지 안내서'[9]는 웹사이트 운영 시 개인정보 보호를 위한 구체적인 지침을 제공한다. 이 안내서는 개인정보를 수집, 저장, 처리하는 과정에서 법적 요구사항을 준수하고, 암호화, 접근 제어, 로그 모니터링 등의 기술적 및 관리적 조치를 취할 것을 명시하고 있다.

2.3 대외 공개 홈페이지 사이버 공격 유형

공개 홈페이지에서 발생 가능한 대표적인 사이버 공격은 다음과 같이 4가지 형태로 구분할 수 있다.

첫째, 웹서버의 취약점을 악용하여 정보(개인정보 포함)가 유출될 수 있다. 기업이나 조직이 관리하는 기밀 정보 및 사용자 개인정보가 외부에 노출되는 경우 법적 책임이 부과되고, 신뢰도 하락을 초래할 수 있다.

2021년 8월부터 2022년 11월까지 1년 6개월 동안 6개 대학·단체에서 개인정보보호 조치 소홀로 학교 구성원의 주민등록번호 2만건 등 총 81만여 건의 개인정보가 유출되었다. 이 때 사용된 공격 기법은 파라미터 변조 공격, 웹셸 업로드 공격 및 관리자 계정 취약점을 이용한 공격이었다[10]. 2024년 1월에는 국내 인터넷 동영상 강의 사이트가 크리덴셜 스터핑(Credential stuffing) 공격과 크로스사이트 스크립팅(Cross site scripting) 취약점을 이용한 공격을 당해 회원 9만 5천여 명의 개인정보가 유출되기도 하였다[11].

둘째, 공격자에 의해 노출된 공개 취약점을 통해 서비스 거부 공격(DoS) 또는 시스템 비정상 작동을 유발할 수 있다. 이는 홈페이지의 가용성에 영향을 미치며, 사용자들에게 해당 조직에 대한 부정적인 이미지를 심어줄 수 있다.

러시아-우크라이나 전쟁 기간 중인 2022년 4월, 에스토니아 정부 웹사이트들이 DDoS 공격으로 몇 시간 동안 마비되었다. 이어서 8월에는 핀란드 의회 웹사이트가 의회 개회 중에 DDoS 공격을 받았다. 두 공격 모두 러시아 정부가 지원하는 해커집단의 소행으로 추정하고 있다[12].

셋째, 공격자는 원격 코드 실행 취약점을 악용해 서버를 완전히 장악할 수 있다. 이는 데이터 손실, 시스템 통제권 탈취, 악성코드 배포 등 심각한 보안 사고로 이어질 수 있다. 대표적인 사례로는 2021년 공개된 오픈소스 로깅 라이브러리인 Log4j 관련 취약점을 들 수 있다. 취약점이 공개된 이후 수많은 공격 시도가 발생했으며, 중국, 이란, 북한 및 튀르키예 등 국가 기반 사이버 공격자들도 이 취약점을 활용하였다[13].

넷째, SSL/TLS 관련 취약점을 통해 중간자 공격이 발생할 수 있다. 이는 암호화된 데이터의 노출 및 데이터 전송 과정에서의 정보 탈취로 이어질 수 있다. 하트 블리드(Heartbleed), 프리크(FREAK), 로그잼(LogJam) 및 푸들(POODLE) 등이 대표적인 취약점에 해당한다.

지난 2014년 캐나다 세무청은 하트 블리드 취약점으로 인해 900명의 사회보장번호가 유출되기도 하였다[14].

2.4 선행연구 고찰

공격표면관리와 관련된 연구는 조직의 전반적인 IT 자산에서부터 소프트웨어에 이르기까지 상당히 다양한 요소들을 대상으로 활발하게 진행되고 있다. 그리고 비교적 최근의 연구들은 사물인터넷[15]-[17] 또는 OT(Operational technology)[18][19]에 대한 공격표면관리를 주로 다루면서 새로운 공격표면이 되고 있는 신기술 적용 영역으로 연구가 확장되고 있다.그러나 본 절에서는 웹과 직접적으로 연관된 대표적인 공격표면관리 연구만을 간략하게 정리한다.

A. Yushko et al.[20]은 웹 애플리케이션을 보호하기 위한 SIEM(Security Information & Event Management) 기반의 접근방법을 제안하였다. 먼저 웹 애플리케이션의 가장 일반적인 취약점과 공격표면을 분석하였으며, 그 결과를 바탕으로 SIEM에서 생성되는 이벤트, 취약점 및 공격표면의 상호관계를 고려하여 분류 및 그룹화를 수행하였다.

D. Laksmiati[21]는 네트워크 기반 스캐너를 활용하여 최근 해커들에게 인기 표적이 되고 있는 WordPress 기반 웹사이트의 취약점을 분석하였다. 그 결과 즉시 수정하고 보완이 필요한 취약점이 확인되었으며, 식별된 취약점의 악용을 방지하고 공격표면을 줄이기 위해 WordPress 기반 웹사이트에 대한 정기적인 취약점 평가가 필요함을 강조하였다.

S. Temara[22]는 ChatGPT를 활용해 조직이 사용하는 인터넷 프로토콜(IP) 주소 범위, 도메인 이름, 네트워크 토폴로지, 공급업체 기술, SSL/TLS 암호, 포트 및 서비스, 운영체제 등 다양한 유형의 정보를 수집한 후 이를 바탕으로 잠재적 위험을 탐색하는 접근방법을 제안하였다. Y. H. Kwon et al.[23]은 프롬프트 AI 기술을 활용하여 웹 취약점을 자동으로 분석하고 탐지하는 도구를 제안하였다.

H. J. Park et al.[24]은 금융기관 공개 홈페이지 취약점을 분석하고 효율적인 대처 방안을 연구하였다. 감독규정에서 제시한 웹 서비스 취약점 항목을 중심으로 OWASP Top 10 2017 항목과 비교하여 설명하면서, 웹 서비스 취약점 점검 프로세스를 효과적으로 진행할 수 있는 방안도 제시하였다.

본 연구와 유사하게 민간기업의 외부 공격표면을 분석한 연구도 있었다. N. Gelernter et al.[25]은 유럽 100대 기업의 외부 공격표면을 분석한 결과 기업들이 서로 다른 IT 아키텍처를 적용하고 있어 노출되는 사이버보안 문제가 다르다는 점을 확인하였다. J. S. Yu et al.[26]은 방위산업 분야의 디지털 전환에 따른 공격표면 증가에 대응하기 위해 보안 위협을 공급망, 내부자 및 네트워크로 구분해 분석하였다. 그리고 신기술 도입 간 보안 내재화, 업체의 자체적인 공격표면 관리 지침 수립, 기술 발전을 반영한 방위산업 규정 개정 등의 대응 방안을 제시하였다.

선행 연구를 고찰한 결과, 앞서 정리한 연구들을 포함하여 웹 취약점 분석 및 공격표면관리를 수행했던 연구는 다수 확인되었다. 그러나 홈페이지를 직접적 대상으로 한 연구들은 WordPress 기반 웹사이트의 취약점 분석[21]과 금융기관 공개 홈페이지 대상의 취약점 분석[24] 2건뿐이었으며, 민간기업의 공개 홈페이지를 대상으로 취약점을 분석한 연구는 확인할 수 없었다.

III. 공개 홈페이지 취약점 분석

3.1 분석 대상군 선정

취약점 분석 대상군을 선정하기 위해 우선 공정거래위원회에서 2023년 4월에 공시한 ‘2023년 공시대상기업집단 지정 현황’을 참고하여 민간기업 84개를 선정하였다. 그리고 표 1에서 보는 바와 같이 공개 홈페이지 보안 상태 비교를 위한 대조군으로 정부기관 25개 및 군 관련 공공기관 11개를 추가로 선정해 ASM 솔루션을 통해 취약점을 점검하였다. 그 결과 정부기관 및 군 관련 공공기관은 특별한 취약점이 식별되지 않았다. 그러나 민간기업 84개 중 10개 기업의 공개 홈페이지에서는 다수의 취약점이 식별되었다.

이러한 결과를 바탕으로 본 연구에서는 다수의 취약점이 식별된 민간기업 10개를 대상으로 세부적으로 취약점을 분석한다.

표 1. 공개 홈페이지의 취약점이 노출된 기관의 수
Table 1. Number of institutions exposed to vulnerabilities on their public websites

Organization	Vulnerable	Secure	Total
Private companies	10	74	84
Government agencies	-	25	25
Public organizations related to military	-	11	11

3.2 취약점 분석 방법

우선 분석 대상 기업에서 운영하는 공개 홈페이지의 URL을 기반으로 IP 주소를 확인하기 위해 NSLOOKUP 명령어를 사용하여 도메인 이름을 IP 주소로 변환하였다. 이후, 대표적인 ASM 솔루션인 'Criminal IP'[6]를 활용하여 각 홈페이지의 취약점을 검사하였다.

Criminal IP는 IP 주소에 기반하여 데이터베이스 서버, 파일 서버, 관리 서버 및 사물인터넷 시스템 등 각 기업이나 조직이 보유하고 있는 IT 자산에 대한 취약점을 실시간으로 탐지하고 위협에 대한 선제적인 대응을 가능하게 해 주는 종합적인 위협 인텔리전스 검색엔진이다.

Criminal IP를 통해 수집되는 취약점은 그림 1에서 보는 바와 같은 형태로 출력된다. IP 주소를 기반으로 검색한 도메인을 5단계의 위험도 등급으로 분류해 제시하며, 가짜 도메인 및 피싱 도메인 여부, SSL 인증서의 유효성, 악성 링크 존재 여부 등의 정보를 종합적으로 파악할 수 있다. 또한, 악용되는 정보(Abuse record)와 오픈된 포트(Open ports), 그리고 홈페이지에 실제로 존재하는 모든 취약점을 확인할 수 있다.

식별된 취약점에 대해서는 공개 취약점(CVE, Common Vulnerabilities and Exposures) 정보[27]와 연계해 해당 취약점의 심각도(Severity), 취약점으로 발생 가능한 공격 양상이나 최신 발생 동향까지도 일괄적으로 파악할 수 있다. 심각도와 관련해서는 CVSS(Common Vulnerability Scoring System) v4.0이 최신 버전이기는 하나, 본 연구에서 활용한 Criminal IP가 v2.0 및 v3.1까지만 지원하고 있어 v3.1을 기준으로 분석하였다.

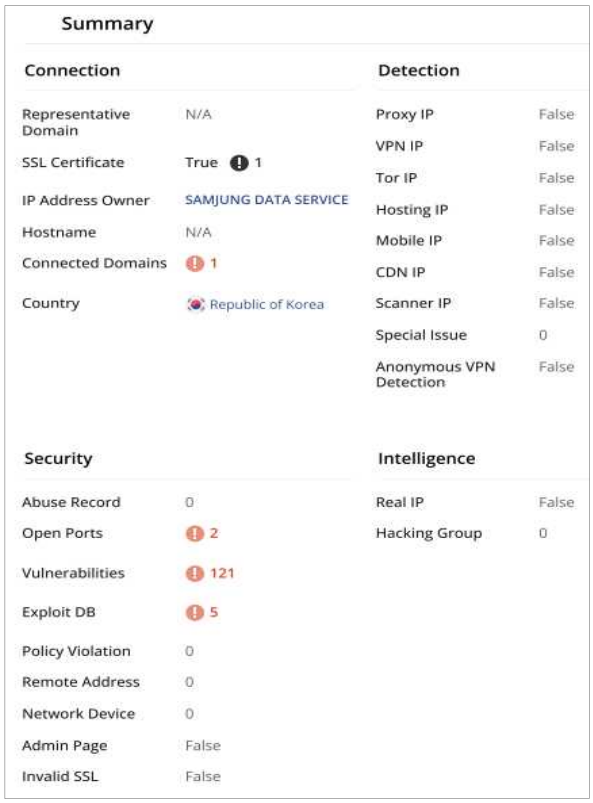


그림 1. Criminal IP를 통한 취약점 점검 결과
Fig. 1. Results of vulnerability check using Criminal IP

3.3 취약점 분석 결과

Crimial IP를 기반으로 10개 민간기업을 대상으로 취약점을 식별한 결과는 표 2에서 보는 바와 같다.

표 2. 10개 기업에 대한 취약점 점검 결과
Table 2. Results of vulnerability check for 10 companies

Vulnerability	None	Exist
CVE existence [①]	-	10
Use not valid SSL certificate [②]	7	3
Use vulnerable ports [③]	7	3
Allow remote access [④]	8	2

분석 대상 10개 기업의 공개 홈페이지 모두에서 공개 취약점이 발견되었으며, WEB 서버 및 WAS (Apache, nginx 등), 네트워크 통신(OPENSSH), 보안 통신을 위한 암호화 관련 오픈소스 라이브러리(OPEN SSL) 취약점 등이 주를 이루었다. 공개 취약점 외에도 해당 민간기업들에서는 SSL 인증서 만료 3건, 취약한 TCP 포트 사용 3건, 서버로의 원격 접속(OPENSSH) 허용 2건 등이 확인되었다.

홈페이지의 웹서버 공개 취약점(①)이 노출되면 디렉토리 탐색 공격을 통해 웹서버 내의 특정 파일이나 디렉토리에 접근할 수 있게 되어 중요한 정보들를 유출될 수 있다. 또한, 웹 애플리케이션 취약점을 통해 SQL 인젝션, 크로스 사이트 스크립팅 등의 공격이 가능해져, 데이터베이스나 사용자 정보유출로 이어지거나 웹 서버에 과도한 요청(서비스 거부 공격(DDoS))을 보내 다운시킬 수도 있다[28].

만료된 SSL 인증서(②)는 사용자 정보 유출이나 악성 사이트로의 접속을 유도하는 피싱 공격으로 이어질 수 있다. 그리고 중간자 공격(MITM)에 노출되어 공격자가 데이터 전송을 가로채고 민감정보를 탈취할 위험이 증가한다. 검색 엔진 최적화(SEO, Search Engine Opmization) 측면에서는 SSL 인증서가 만료되면 검색 순위에 부정적인 영향을 미칠 수 있으며, 이로 인해 웹사이트의 가시성이 저하되어 비즈니스에 부정적인 결과를 초래할 수 있다. 특정 산업에서는 데이터 보호와 관련된 법적 요구사항이 있을 수 있으며, 만료된 SSL 인증서로 인해 이러한 요구사항을 충족하지 못하면 법적 문제가 발생할 수도 있다.

취약한 포트 사용(③) 역시 다양한 위협을 초래할 수 있다. 21번 포트(FTP)가 오픈된 상태로 운영되는 경우, 기본적으로 데이터가 암호화되지 않고 전송되므로 중간자 공격(MITM)에 매우 취약하여 공격자가 데이터 전송을 가로채고, 민감한 정보를 탈취할 수 있는 위협이 발생할 수 있다. 53번 포트(DNS)가 오픈된 상태로 운영되면 DNS 스푸핑 공격에 노출되어, 잘못된 IP 주소로 사용자가 리디렉션되면서 정보가 탈취될 수 있다. 또한, DNS 요청과 응답은 쉽게 모니터링될 수 있어 내부 구조나 사용되는 도메인 정보가 유출될 위험도 존재한다.

마지막으로 원격 접속(OpenSSH)이 허용(④)된 경우에는 공격자가 비밀번호 기반 로그인 공격을 시도할 가능성이 높아진다. 사전(Dictionary) 공격이나 무작위 대입(Brute-force) 공격을 통해 사용자 계정의 비밀번호를 유출하려는 시도가 이루어질 수 있고, SSH 서비스가 오픈된 상태에서는 공격자가 과도한 요청을 서버에 보내어 자원을 소모시키면서 정상 사용자가 서비스를 이용하지 못하게 만드는 서비스 거부 공격의 대상이 될 수 있다.

분석 대상 10개 민간기업에서 발견된 공개 취약점(CVE)은 표 3에 나타난 바와 같이 총 394개이며, 이를 제품 기준으로 분류하면 WEB/WAS가 41.8%를 차지하였다. 나머지는 모두 보안 통신 프로토콜(59.2%)로 확인되었다.

표 3. 식별된 공개 취약점 구분 결과
Table 3. Classification results of identified CVEs

Category	WEB/WAS	Secure communication protocol	Total
# of CVE	106 (41.8%)	288 (59.2%)	394

식별된 394개 공개 취약점들의 심각도를 CVSS v3.1[27] 기준으로 분석한 결과는 그림 2에서 보는 바와 같다. Medium 이상의 취약점은 총 219건이었으며, 시급한 조치가 필요한 High 이상의 취약점이 전체의 37.3%인 137건으로 확인되었다.

Severity	Critical	High	Medium	Low	None	Total
# of CVE	40	97	82	13	162	394

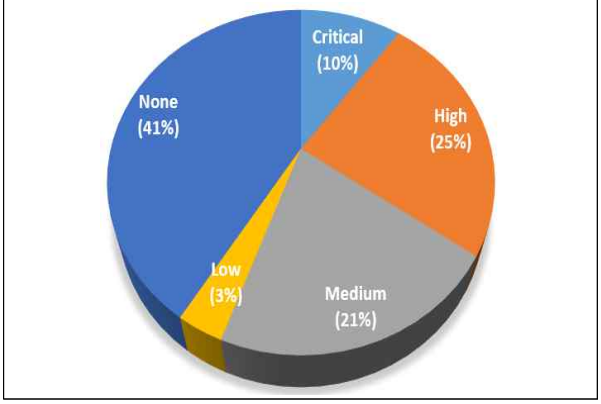


그림 2. CVSS v3.1을 기준으로 한 심각도 분석 결과
Fig. 2. Analysis result of severity based on CVSS v3.1

가장 높은 심각도를 가지는 Critical 등급에 해당하는 공개 취약점 40건을 제품군별로 구분한 결과, Apache 제품군과 연관된 취약점이 12건, OpenSSH 제품군과 연관된 취약점이 5건, 그리고 OpenSSL 제품군과 연관된 취약점이 23건으로 확인되었다.

Apache 제품군 중 Apache HTTP Server에서 발견된 CVE-2022-22720 취약점은 HTTP 요청 스머글링 공격(서버와 클라이언트 간의 통신을 가로채거나 변조하여 민감한 정보를 탈취하거나, 서버의 동작을 방해하는 등의 공격)을 가능하게 한다.

또한, CVE-2022-31813 취약점은 IP 기반 인증을 우회할 수 있는 취약점으로서, 공격자가 원본 서버나 응용 프로그램에 무단으로 접근할 수 있다[29].

OpenSSH 제품군의 CVE-2023-38408 취약점은 OpenSSH의 ssh-agent에서 발생하는 원격 코드 실행 취약점으로 PKCS#11 로드 요청 시 발생하며, 공격자가 악성 소프트웨어를 실행하거나 영향을 받은 시스템을 완전히 제어할 수 있는 위험이 있다. CVE-2023-28531 취약점은 제약 조건 없이 에이전트에 키가 추가되어 잠재적으로 무단 액세스 또는 키의 오용이 발생할 수 있다. CVE-2016-1908 취약점은 X11 서버의 구성 문제를 악용해 신뢰할 수 있는 X11 포워딩 권한을 얻을 수 있는 취약점으로, 공격자는 이 취약점을 통해 시스템의 중요 파일에 접근하거나 데이터를 수정할 수 있다[30].

OpenSSL 제품군의 CVE-2023-0464 취약점은 공격자가 악성 인증서 체인을 생성하여 컴퓨팅 리소스를 과도하게 소모하게 함으로써, 운영 중인 시스템에 치명적인 서비스 거부(DoS) 공격을 발생시킬 수 있다. CVE-2022-1292 취약점은 c_rehash 스크립트에서 쉘 메타 문자를 제대로 제거하지 않아 발생하는 명령 주입 취약점으로, 공격자는 악의적인 명령을 실행하여 시스템을 심각하게 손상시키거나 중요한 데이터를 유출할 수 있다. CVE-2022-2068 취약점은 CVE-2022-1292가 패치된 후 코드 리뷰 과정에서 추가로 식별된 원격 코드 실행 취약점으로 운영체제에서 공격자가 스크립트 권한으로 임의의 명령을 실행할 수 있는 위험을 내포하고 있다. 이는 시스템 전체에 심각한 보안 위협을 초래하며, 공격자는 악성코드를 실행하거나 데이터를 손상시키는 등의 공격을 감행할 수 있다. CVE-2016-6304 취약점은 다중 메모리 누수로 인해 원격 공격자가 서비스 거부를 유발할 수 있는 취약점으로 서버의 안정성을 크게 저해하는 요인이 될 수 있다[31].

이상과 같은 공개 취약점이 존재하는 상태로 홈페이지가 운영될 경우, 운영 중인 시스템이나 네트워크에 심각한 위험이 발생할 수 있다. 그리고 적시적인 조치가 이루어지지 않을 경우 기업이 비즈니스를 수행하기 어려운 상황으로 이어질 수도 있어 관련 내용에 대해서는 기술적·정책적 차원의 조치 방안을 강구하여 적용하는 것이 필수적이다.

Ⅳ. 안전한 공개 홈페이지 관리 방안

4.1 기술적 차원의 조치

진화를 거듭하고 사이버 공격에 효과적으로 대응하고 공개 홈페이지의 보안성을 강화하기 위해서는 다양한 도구와 기술을 효과적으로 활용하는 것이 필요하다.

4.1.1 ASM 솔루션을 활용한 조직의 공격표면관리

우선 최근 많은 민간기업에서 활용하는 공격표면관리(ASM) 솔루션은 IT 자산, 네트워크, 애플리케이션 및 데이터베이스 등 모든 가능한 공격표면을 체계적으로 식별하고 관리하는 데 도움을 준다. ASM 솔루션을 활용하면 자산을 자동으로 탐지하고 목록화하여 보안 관리자가 IT 자산의 보안 상태를 손쉽게 파악하고 취약점 분석 및 우선순위 설정을 효율적으로 수행할 수 있다. 또한, ASM 솔루션을 통해 식별된 취약점에 대해서 위험도를 평가한 후 문제 해결을 위한 패치 관리 및 보안 조치를 우선적으로 시행할 수 있다.

최신 위협정보를 제공하는 위협 인텔리전스 시스템을 ASM 솔루션과 통합하면 공격 패턴 및 동향을 분석하고, 새로운 공격 기법이나 취약점 등에 대한 조기 경고를 받을 수 있다.

ASM 솔루션을 적용함에 있어서는 단일 솔루션만을 적용하기보다는 다양한 솔루션의 복합적 사용이 필요하다. 상용 공격표면관리 솔루션들의 탐지 결과는 상당한 차이가 존재하기 때문에[18] 특정 솔루션의 단점을 보완하기 위해 가용예산 범위 내에서 서로 다른 ASM 솔루션의 동시 적용을 반드시 검토해야 한다.

4.1.2 네트워크 탐지 및 대응시스템 적용

네트워크 탐지 및 대응(Network Detection and Response, 이하 NDR) 시스템은 네트워크 내에서 발생하는 비정상적인 활동을 탐지하고 이에 대응하는 기능을 제공한다. NDR 시스템을 통해 네트워크 트래픽을 실시간으로 모니터링하고 비정상적인 활동이나 이상 징후를 탐지할 수 있다.

이를 통해 잠재적인 공격 시도를 조기에 발견하고 대응할 수 있다. NDR 시스템은 탐지된 위협에 대한 분석을 수행하고, 공격자의 행동 패턴을 분석하여 공격의 확산을 차단한다. 분석 결과를 바탕으로 자동화된 대응 조치를 시행하여 네트워크 보안을 강화한다. 또한, NDR 시스템은 네트워크 관련 로그와 이벤트를 수집하고 분석하여 공격의 발생 원인 및 경로를 파악하고, 사고 발생 후 원인 분석 및 포렌식 조사를 지원한다. 지능형 경고 기능을 제공하여 위협의 심각성을 평가하고 우선적으로 대응할 수 있도록 한다.

4.1.3 웹 방화벽 및 침입방지시스템 적용

이미 많은 민간기업 또는 공공기관에서 사용되고 있는 웹 방화벽과 침입방지시스템은 웹 애플리케이션과 네트워크를 보호하는 데 중요한 역할을 한다. 웹 방화벽은 웹 애플리케이션에 대한 공격을 필터링하고 차단하며, SQL 인젝션, 크로스 사이트 스크립팅(XSS), CSRF(Cross-Site Request Forgery) 등의 공격을 방어한다. 침입방지시스템은 네트워크 트래픽을 분석하여 실시간으로 악의적인 패턴이나 공격 시도를 탐지하고 자동으로 대응조치를 취하여 네트워크의 보안을 강화한다.

웹 방화벽과 침입방지시스템의 효과적인 활용을 위해서는 보안 정책을 설정하고 이를 지속적으로 관리해야 하며, 최신 위협 동향에 맞게 정책을 조정하고 규칙을 업데이트해야 한다. 통합보안관리 시스템을 통해 웹 방화벽과 침입방지시스템의 데이터를 종합적으로 분석한다면 보다 신속하게 위협에 대응할 수 있다.

4.1.4 시스템 및 소프트웨어 최신화

발견된 취약점에 대한 보안 패치는 공개된 즉시 적용해야 하며, 관리 대상 IT 자산의 펌웨어 또는 소프트웨어는 항상 최신화된 상태를 유지할 수 있도록 공급업체와 협조하여 정기적인 업데이트를 실시해야 한다. 그리고 보안 관리자 또는 시스템 관리자의 책임성을 강조하기 위해 기업 내부 규정 등을 통해 이러한 사항들을 명문화할 필요가 있다.

4.1.5 SSL 인증서 최신화 및 HTTPS 적용

SSL 인증서와 HTTPS 프로토콜은 전송되는 데이터의 보호에 있어 핵심적인 역할을 수행한다[32]. 따라서 데이터 전송 시 보안을 강화하기 위해 최신 버전의 SSL 인증서를 적용하고, HTTPS 프로토콜을 사용하여 클라이언트와 서버 간의 데이터 전송을 암호화함으로써 중간자 공격 및 데이터 유출 등을 방지해야 한다.

4.1.6 다단계 인증 적용 및 접근 권한 최소화

관리자 권한으로 홈페이지 서버에 접속하는 경우에는 다단계 인증 방식을 통해 사용자 인증 절차를 강화하는 것이 필요하다. 아이디 및 비밀번호 외에 추가적인 인증 수단(예: SMS 코드, 인증 앱 등)을 적용해야 하며, 방화벽 등에서 접근 가능한 IP를 최소화하여 관리해야 한다. 그리고 정기적으로는 중요 서버나 데이터에 대한 접근 권한 및 관리자 권한 등을 재검토하면서 불필요하게 부여된 권한은 과감하게 삭제해야 한다.

4.1.7 민감정보 수집 최소화 및 암호화 저장

최소한의 민감정보만 수집하고, 이를 서버 내에 저장할 경우에는 적절한 암호화 방법을 적용하며, 불필요한 정보를 저장하지 않도록 하여 데이터 유출 시 피해를 최소화해야 한다.

4.2 정책적 차원의 조치

금융회사 및 전자금융업자는 관련 법규에 따라 주기적으로 취약성 점검을 수행하고 그 결과를 금융위원회에 보고해야 한다. 이러한 요구사항은 전자금융거래법 제21조의 3(전자금융기반시설의 취약점 분석평가)과 전자금융감독규정 제37조의 2(전자금융기반시설의 취약점 분석·평가 주기 내용 등)에 명시되어 있다. 그리고 주요정보통신기반시설은 종합적인 위험 진단을 통하여 관리적·물리적·기술적 점검 항목들에 대한 취약점을 점검하고, 모의 해킹이나 침투 테스트 등을 수행해야만 한다.

그러나 주요정보통신기반시설에 해당하지 않는 민간기업의 경우, 법령에 따라 취약점 점검 및 조치를 반드시 수행하여야 할 법적 의무가 없기에, 최소한 상장 민간기업에서 운영하는 공개 홈페이지만이라도 취약점 점검 대상에 포함될 수 있도록 법률 개정이 필요하다. 그리고 기업 내부적으로 다음과 같은 조치들을 취할 필요가 있다.

4.2.1 포괄적인 보안정책 수립 및 시행

기업에서는 보안 목표와 방향성을 명확히 하기 위해 포괄적인 보안정책의 수립이 필요하다. 이러한 정책에는 정보보호 대상, 사용자 접근 권한, 데이터 관리 및 사고 대응 절차, 임직원에 대한 보안 교육(개인정보 포함) 등의 내용을 포함하여야 한다.

4.2.2 사이버보안 교육 강화

임직원들의 보안 의식을 높이기 위한 교육활동은 매우 중요하며, 교육 내용에는 최신 사이버 동향 및 사고 사례, 법령 개정 현황을 포함하여 최소 년 1회 이상 정기적으로 실시하는 것이 필요하다. 최대한 직관적이고 객관적 사실에 근거한 사례 위주 교육으로 임직원들이 보안 위협을 체감할 수 있도록 준비해야 하며, 비밀번호 관리 및 데이터 보호 등의 중요성을 이해하고 일상생활 속에 자연스럽게 내재화될 수 있도록 유도해야 한다.

4.2.3 IT 담당 부서 임직원에 대한 관리 강화

주요 서버나 상용 소프트웨어 등을 관리하는 IT 담당 부서의 임직원들에 대한 보다 강력한 관리가 필요하다. 접근 제어 및 권한 관리를 위해 중요 데이터와 시스템에 대한 접근을 최소한으로 제한하고, 불필요한 권한의 부여 여부를 수시로 확인해 즉시 회수할 수 있는 절차를 실행해야 한다.

4.2.4 사고 대응 계획 수립 및 시행

보안 사고 발생 시 신속하게 대응할 수 있도록 사고 대응 계획을 수립해야 한다. 사고 탐지, 대응 절차, 복구 방법 및 사후 분석이 포함될 수 있도록 하고, 최소 년 1회 이상 정기적인 모의훈련을 통해 실효성을 검증하면서 담당자의 업무 숙련도도 향상되도록 발전시켜 나가야 한다. 서버나 상용 소프트웨어 등에 대한 공개 취약점이 발표될 경우 조속한 개선 조치가 시행될 수 있도록 명문화하여 높은 보안 수준을 꾸준히 유지하는 것은 매우 중요하다.

4.2.5 외부 전문업체를 통한 홈페이지 점검

일반적으로 민간기업의 공개 홈페이지는 대국민 서비스를 제공하는 주요한 창구이다. 따라서 정기적으로 전문보안업체를 통해 외부 감사와 침투 테스트를 수행하는 것이 필요하며, 이를 통해 기업 내부 조직에서 발견하지 못한 취약점을 사전에 식별하고 개선해 나가야 한다. 또한, 필요에 따라서는 ISMS-P나 ISO-27001:2023과 같은 대외 보안인증과 연계하여 사이버 대응과 관련된 역량을 향상시키는 것을 고려할 필요가 있다.

4.2.6 운영 조직과 보안 조직의 분리

여전히 많은 민간기업이 사이버보안 업무영역을 IT 담당 운영 부서에 할당하고 있다. 이는 사이버보안에서 요구하는 사항들이 IT 운영의 효율을 저해한다는 시각과 비즈니스 사업 측면에서 인력/예산 소요가 과다하다는 인식에 기인한다. 그러나 보안사고가 발생하면 기업의 생존까지 위협받을 수도 있기 때문에 사이버보안은 별도의 전문조직을 통해 관리되도록 하면서 IT 운영조직과는 상호 견제가 될 수 있도록 하고, 운영과는 차별화된 접근을 통해 사이버보안이 실행될 수 있도록 책임과 권한을 부여하는 것이 필요하다.

4.2.7 데이터 보호, 복구 및 백업전략 수립

민간기업의 비즈니스 연속성 계획 측면에서 사이버공격 등으로 대규모 데이터 손실이 발생할 경우를 대비하여 업무 연속성이 필요한 핵심 서버군을 자체적으로 분류하고 그에 맞는 관리방안을 수립하여 시행해 나가야만 한다.

그리고 각 기업에 필요한 RTO(Recovery Time Objective)와 RPO(Recovery Point Objective)을 설정하고, 데이터 보호 및 복구 전략을 수립, 백업 복구 모의훈련과 연계하여 관리될 수 있도록 해야 한다.

Ⅴ. 결론 및 향후 연구

현대사회에서 사이버보안의 중요성이 날로 증대되는 가운데, 공개 홈페이지의 보안 취약점을 효과적으로 관리하고 운영하는 것은 필수적이다.

그러나 분석 결과에서도 확인한 바와 같이, 민간기업의 공개 홈페이지는 기업의 규모 대비 여전히 관리가 미흡한 경우가 많았다. 분석 대상으로 선정한 10개 민간기업의 공개 홈페이지 모두에서 WEB 서버 및 WAS, 네트워크 통신 및 보안 통신을 위한 암호화 오픈소스 라이브러리와 관련된 총 394개의 공개 취약점이 식별되었다. 또한, SSL 인증서 만료, 취약한 TCP 포트 사용 및 원격 접속 허용 등의 취약점도 존재하는 것으로 확인되었다.

식별된 394개 공개 취약점의 심각도를 CVSS v3.1을 기준으로 분석한 결과, 시급한 조치가 요구되는 High 이상의 취약점이 전체의 37.3%인 137건이었으며, 가장 높은 심각도인 Critical 등급에 해당하는 공개 취약점도 40건이나 존재하였다.

이처럼 온라인 기업 활동의 중심이 되는 기업의 공개 홈페이지에 치명적인 취약점들이 존재하는 상황은 국가적 또는 사회적으로 심각한 문제를 초래할 수 있어 기업의 책임성을 고취하기 위해 기술적 및 정책적 차원에서의 조치가 시급하다.

기술적 차원에서는 ASM 솔루션, NDR 시스템, 웹 방화벽 및 침입방지시스템 적용, 정기적인 보안 패치 적용을 통한 시스템 및 소프트웨어 최신화, SSL 및 HTTPS 적용, 다단계 인증 도입 및 데이터 접근 권한 재검토, 민감정보 수집 최소화 및 암호화 저장 등의 조치가 필요하다.

정책적 차원에서는 민간기업의 책임을 강화하기 위해 법령 개정이 선행되어야 한다. 기업 자체적으로는 포괄적인 보안정책을 수립·시행하면서 구성원들에 대한 보안교육과 IT 담당 직원에 대한 관리를 강화할 필요가 있다. 그리고 사고 발생 시 신속한 대응을 위한 계획과 데이터 보호·복구 및 백업전략 등을 마련하여 모의훈련과 병행하면서 업무 담당자들의 숙련도를 향상시켜야 한다.

본 연구는 상용 ASM 솔루션에서 제공하는 공개 취약점을 기능 위주로 표면적으로 분석하였다. 그러나 향후에는 공개 홈페이지의 소스코드에서 발견되는 보안 취약점을 체계적으로 분석하고, 근본적인 보안 문제에 대한 해결책을 모색해 보고자 한다. 또한, 서로 다른 보안 솔루션들이 생성해 내는 실증적 데이터를 활용하여 종합적인 관점에서 해당 솔루션들의 효율성을 평가해 볼 예정이다.

References

[1] Forbes, "Top Website Statistics For 2024", https://www.forbes.com/advisor/in/business/software/website-statistics/ [accessed: Sep. 18, 2024]

[2] Terranova Security, "130 Cyber Security Statistics: 2024 Trends and Data", https:// www.terranova security.com/blog/cyber-security- statistics [accessed: Sep. 20, 2024]

[3] Ministry of Science and ICT, "Analysis of major cyber threats in the private sector in the first half of 2024", https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&bbsSeqNo=94&nttSeqNo=3184766 [accessed: Sep. 20, 2024]

[4] Gartner Research, "Emerging Tech: Security—The Future of Attack Surface Management Supports Exposure Management", Apr. 2023.

[5] Palo Alto Networks, "Attack Surface Management for dummies", 2022.

[6] Criminal IP Blog, https://www.criminalip.io [accessed: Sep. 10, 2024]

[7] IBM, "What is attack surface management?", https://www.ibm.com/think/topics/attack-surface-management#:~:text=Attack%20surface%20management%20(ASM)%20is,up%20an%20organization's%20attack%20surface. [accessed: Sep. 25, 2024]

[8] Ministry of the Interior and Safety, "Guide to the establishment and operation of websites of

administrative and public institutions", Mar. 2021.

[9] Korea Internet & Security Agency, "Personal Information Disclosure Prevention Guide on the Home Page", Apr. 2024.

[10] Personal Information Protection Commission Homepage, https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9230 [accessed: Sep. 22, 2024]

[11] Boannews, https://www.boannews.com. [accessed: Sep. 22, 2024]

[12] The European Centre of Excellence for Countering Hybrid Threats, "Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage", Hybrid CoE Working pp. 32, May 2024.

[13] T-A. Santiago, "What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what's at stake", Dec. 2021.

[14] Canada Revenue Agency, "2022-2023 Annual Corporate Research - Qualitative Component Final Report", Oct. 2023.

[15] S. Rizvi, RJ Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, "Identifying the attack surface for IoT network", Internet of Things, Vol. 9, pp. 100162, Mar. 2020. https://doi.org/10.1016/j.iot.2020.100162.

[16] A. Barnawi, S. Gaba, A. Alphy, A. Jabbari, I. Budhiraja, V. Kumar, and N. Kumar, "A systematic analysis of deep learning methods and potential attacks in internet-of-things surfaces", Neural Computing and Applications, Vol. 35, pp. 18293-18308, Jun. 2023. https://doi.org/10.1007/s00521-023-08634-6.

[17] G. Nzeako, C. D. Okeke, M. O. Akinsanya, O. A. Popoola, and E. G. Chukwurah, "Security paradigms for IoT in telecom networks: Conceptual challenges and solution pathways", Engineering Science & Technology Journal, Vol. 5, No. 5, pp. 1606-1626, May 2024. https://doi.org/10.51594/estj. v5i5.1111.

[18] T. Ashley, S. N. G. Gourisetti, N. Brown, and C. Bonebrake, "Aggregate attack surface management for network discovery of operational technology", Computers & Security, Vol. 123, pp. 102939, Dec. 2022. https://doi.org/10.1016/j.cose.2022.102939.

[19] S. Hollerer, et al., "Challenges in OT Security and Their Impacts on Safety-Related Cyber-Physical Production Systems", Digital Transformation, Springer, pp. 171-202, Feb. 2023. https://doi.org/10.1007/978-3-662-65004-2_7.

[20] A. Yushko, R. Shevchuk, K. Łopaciński, M. Leszczynska, O. Yashchyk, and T. Yurchyshyn, "Shielding Web Application against Cyber-Attacks using SIEM", 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland, pp. 393-396, Sep. 2023. https://doi.org/10.1109/ACIT58437.2023.10275630.

[21] D. Laksmiati, "Vulnerability Assessment with Network-Based Scanner Method for Improving Website Security", Journal of Computer Networks, Architecture and High Performance Computing, Vol. 5, No. 1, pp. 38-45, Jan. 2023. https://doi.org/10.47709/cnahpc.v5i1.1991.

[22] S. Temara, "Maximizing Penetration Testing Success with Effective Reconnaissance Techniques using ChatGPT", arXiv:2307.06391, Jul. 2023. https://doi.org/10.48550/arXiv.2307.06391.

[23] Y. H. Kwon, G. E. Kim, H. Y. Kim, G. M. Lee, G. H. Jin, Y. J. Moon, and M. K. Choi, "Automated web vulnerability analysis tool with Prompt AI", Proc. of the KIIT 2024 Summer Conference, Jeju, Korea, pp. 779-783, May 2024.

[24] H. J. Park and I. S. Kim, "Effective Countermeasures against Vulnerability Assessment for the Public Website of Financial Institution", Journal of The Korea Institute of Information Security & Cryptology, Vol. 27, No. 4, pp. 885-895, Aug. 2017. https://doi.org/10.13089/JKIISC.2017.27.4.885.

[25] N. Gelernter, H. Schulmann, and M.

WaidnerAuthors, "External Attack-Surface of Modern Organizations", Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, Singapore, pp. 589-604, Jul. 2024. https://doi.org/10.1145/3634737.3656295.

[26] J. S. Yu and J. H. Park, "Analysis and Countermeasures of Security Threats to Digital Transformation in Defense Industry", Journal of Korea Academia-Industrial cooperation Society, Vol. 24, No. 10, pp. 682-689, Oct. 2023. https://doi.org/10.5762/KAIS.2023.24.10.682.

[27] NIST, "National Vulnerability Database", https://www.nist.gov/programs-projects/national-vulnerability-database-nvd [accessed: Sep. 02, 2024]

[28] S. S. Nair, "Securing Against Advanced Cyber Threats: A Comprehensive Guide to Phishing, XSS, and SQL Injection Defense", Journal of Computer Science and Technology Studies, Vol. 6, No. 1, pp. 76-93, Jan. 2024. https://doi.org/10.32996/jcsts.2024.6.1.9.

[29] Apache.org, "Apache HTTP Server Project", https://httpd.apache.org [accessed: Sep. 5, 2024]

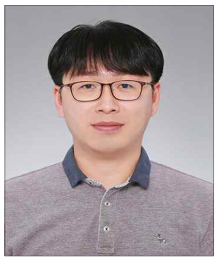
[30] OpenSSH.com, "OpenSSH Security", https://www.openssh.com/security.html [accessed: Sep. 08, 2024]

[31] Openssl.org "OpenSSL Library", https://openssl-library.org/news/vulnerabilities/ [accessed: Oct. 24, 2024]

[32] D. D. Kumar, J. D. Mukharzee, C. V. D. Reddy, and S. M. Rajagopal, "Safe and Secure Communication Using SSL/TLS", 2024 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, pp. 1-6, Apr. 2024. https://doi.org/10.1109/ESCI59607.2024.10497224.

저자소개

최 강 석 (Kangsock Choi)



2005년 2월 : 인천대학교 컴퓨터공학과(공학사)
2005년 1월 ~ 2012년 3월 : (주)LG CNS 대리
2012년 4월 ~ 2017년 5월 : ㈜삼성엔지니어링 과장
2017년 6월 ~ 2024년 4월 : ㈜한국국방연구원 전문위원
2024년 4월 ~ 현재 : ㈜HL홀딩스 프로
관심분야 : 사이버보안 정책, 침입탐지 시스템, ASM, EDR, XDR, SOAR, 취약점 분석 및 대응

이 수 진 (Soojin Lee)

1992년 3월 : 육군사관학교 전산학과(이학사)
1996년 2월 : 연세대학교 컴퓨터과학과(이학석사)
2006년 2월 : 한국과학기술원 전산학과(공학박사)
2006년 3월 ~ 현재 : 국방대학교 국방과학학부 사이버·컴퓨터공학학과 교수
관심분야 : 국방 사이버보안 정책, 사이버전, 침입탐지 시스템, 암호 이론 및 응용