Evolution of Application Security based on OWASP Top 10 and CWE/SANS Top 25 with Predictions for the 2025 OWASP Top 10

Conference Paper · May 2025

DOI: 10.1109/ICICT64420.2025.11004742

2 authors, including:

Jinfeng Li
University of Cambridge
162 PUBLICATIONS **1,136** CITATIONS

SEE PROFILE

Proceedings of the International Conference on Inventive Computation Technologies (ICICT-2025)
IEEE Xplore Part Number: CFP25F70-ART; ISBN: 979-8-3315-1224-8

Evolution of Application Security based on OWASP Top 10 and CWE/SANS Top 25 with Predictions for the 2025 OWASP Top 10

Jinfeng Li*
Advanced Research Institute of Multidisciplinary Science
Beijing Institute of Technology
Beijing, China
*jinfengcambridge@bit.edu.cn. ORCID: 0000-0001-9462-2625

Haorong Li
School of Integrated Circuits and Electronics
Beijing Institute of Technology
Beijing, China
haorong.li@bit.edu.cn. ORCID: 0009-0001-3799-2707

2025 International Conference on Inventive Computation Technologies (ICICT) | 979-8-3315-1224-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICICT64420.2025.11004742

***Abstract*—The Open Web Application Security Project (OWASP) is widely recognized for its role in identifying and publishing the most critical vulnerabilities in the web application security domain through its OWASP Top 10 list. This study provides the first comprehensive evolutionary analysis of the OWASP Top 10, tracing its development from its inception to the most recent edition. By systematically analyzing historical trends, this research highlights key shifts in vulnerability patterns and emerging security challenges, offering a thorough perspective that expands upon existing literature on web application security. In particular, the study also presents a forward-looking projection for the upcoming 2025 OWASP Top 10, which is anticipated to be released later this year. This prediction is grounded in four primary factors influencing the evolving cybersecurity landscape: the increasing risks associated with artificial intelligence (AI) and machine learning (ML), the growing complexities of API and cloud security, the rising frequency of software supply chain attacks (SSCA), and the expanding impact of regulatory and compliance frameworks. The findings contribute significantly to the understanding of the dynamic threat environment, providing actionable insights for researchers, practitioners, and policymakers to enhance security strategies and mitigate future risks effectively.**

***Keywords*—Application Security, AI-based Security Risks, Broken Access Control, Cloud-native Security, CWE/SANS, Cybersecurity Threats, Injection Attacks, OWASP, OWASP Top 10, Software Supply Chain Security**

I. Introduction

Since 2020, our pioneering work [1] on vulnerability mapping, specifically focusing on the OWASP Top 10 and the SANS Common Weakness Enumeration (CWE), titled "Vulnerabilities Mapping based on OWASP-SANS: A Survey for Static Application Security Testing (SAST)," has garnered significant attention from developers, policymakers, industry professionals, and the academic community. The study [1] disseminated at Annals of Emerging Technologies in Computing provided valuable insights into the evolving landscape of application security, highlighting critical vulnerabilities and their implications for secure web/software development.

Five years after the initial publication, the current work serves as both a follow-up review and an updated prediction for the 2025 OWASP Top 10, which is slated for release later this year. According to the latest update from the OWASP project, the 2025 edition of the OWASP Top 10 is currently in the industrial survey phase. This follows the completion of the data collection process in December 2024. At present, the gathered data is undergoing a normalization process to ensure consistency and accuracy before the final list is compiled and released, followed by dedicated review and documentation updates.

Building on the state of the art in OWASP [2–12] as well as our previous analysis [1], this paper seeks to offer a forward-looking perspective on emerging threats and trends that are likely to shape the security priorities of the future. In addition to the evolving landscape of cybersecurity threats, new regulatory frameworks have introduced further complexity to the security environment. The introduction of the European Union's Network and Information Security Directive II (NIS2 Directive) [13][14] and the upcoming Cyber Resilience Act (set to come into full effect in December 2027) [15–17] are expected to have a profound impact on the way organizations approach cybersecurity, especially in relation to vulnerability management and risk mitigation. These legislative measures emphasize the need for heightened resilience and stricter oversight, adding further urgency to the ongoing discourse on securing digital infrastructures and applications. This paper explores the implications of these regulatory changes on the OWASP Top 10 and their potential influence on the cybersecurity landscape in the coming years. Through this work, we aim to provide an in-depth analysis of the evolving risks, while highlighting key areas for improvement and proactive adaptation in response to new and emerging security challenges.

This paper is structured into three key sections. Section II provides a detailed examination of the evolution of the OWASP Top 10 across its six editions since its inception, highlighting newly observed patterns derived from chronological statistical analysis. To broaden the scope and enhance benchmarking, the study extends its analysis to the CWE/SANS Top 25, offering additional insights into security vulnerabilities within the broader software development domain beyond web applications. Section III builds upon these observations, incorporating emerging trends—particularly the rising security risks associated with artificial intelligence (AI) and machine learning (ML)—to present a data-driven prediction of the forthcoming 2025 OWASP Top

10 list. This section also includes a critical discussion of the inherent limitations of the forecasting approach, addressing potential uncertainties and constraints. Finally, the study outlines promising future research directions, encouraging further exploration into evolving security challenges and mitigation strategies.

II. Methods and Results Based on Existing Data

A. Evolution of OWASP Top 10

As of now, six versions of the OWASP Top 10 can be found on the official OWASP website, corresponding to the years 2004, 2007, 2010, 2013, 2017 (RC2), and 2021. The formulation of the OWASP Top 10 list follows a structured lifecycle, as illustrated in Fig. 1, which outlines the key stages of its development and periodic updates.

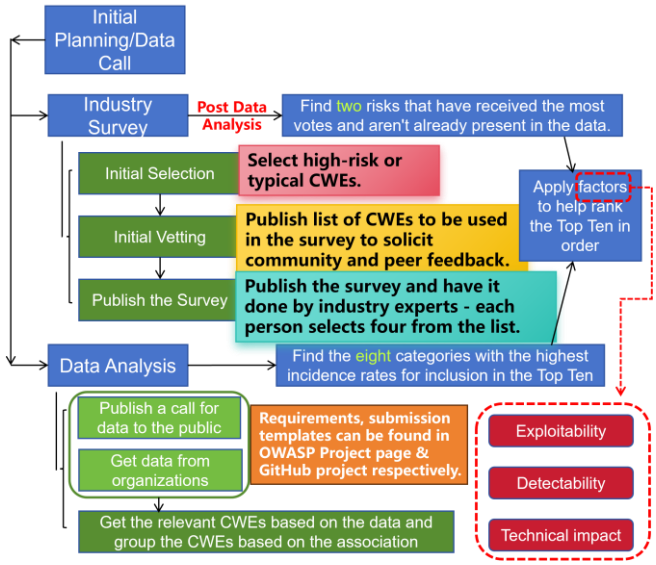

Fig. 1. Procedural flowchart of OWASP Top 10 formation.

Before presenting the evolution analysis of the OWASP Top 10, we first conduct a statistical examination to identify the most frequently occurring vulnerabilities across the six published versions. The findings of this analysis are visually represented in the pie chart shown in Fig. 2. The most frequently occurring security vulnerability is Injection, which appears in all six versions of the OWASP Top 10. It accounts for 10% of the total occurrences, appearing six times out of 60 recorded instances. This consistent presence across all versions highlights its critical and persistent nature in web security threats.

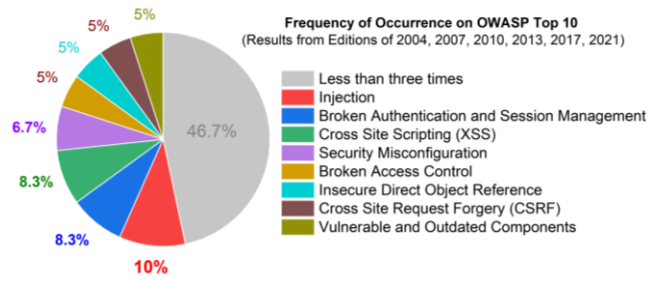

Fig. 2. Proportional distribution of most frequently occurring vulnerabilities across the six published versions (2004, 2007, 2010, 2013, 2017, and 2021) of OWASP Top 10 security vulnerabilities.

In a chronological manner, Figure 3 illustrates the ranking trends of common security vulnerabilities (those appearing at least three times as per the results analysis in Fig. 2) across the six versions of the OWASP Top 10. By examining the data points positioned at the top three high-risk areas (highlighted in red), several key observations can be made. Injection appears most frequently at these top positions, with a total of five occurrences. Following this, Broken Authentication and Session Management ranks second, appearing four times. Notably, Cross-Site Scripting (XSS) ranked within the top three in 2007, 2010, and 2013, but experienced a significant decline to seventh place in 2017 and was completely removed from the 2021 list. Broken Access Control, after appearing only once in 2004, disappeared from the rankings until it resurfaced in 2017. Its importance has since grown substantially, as it jumped from fifth place in 2017 to first place in 2021, highlighting its increasing significance as a security concern.

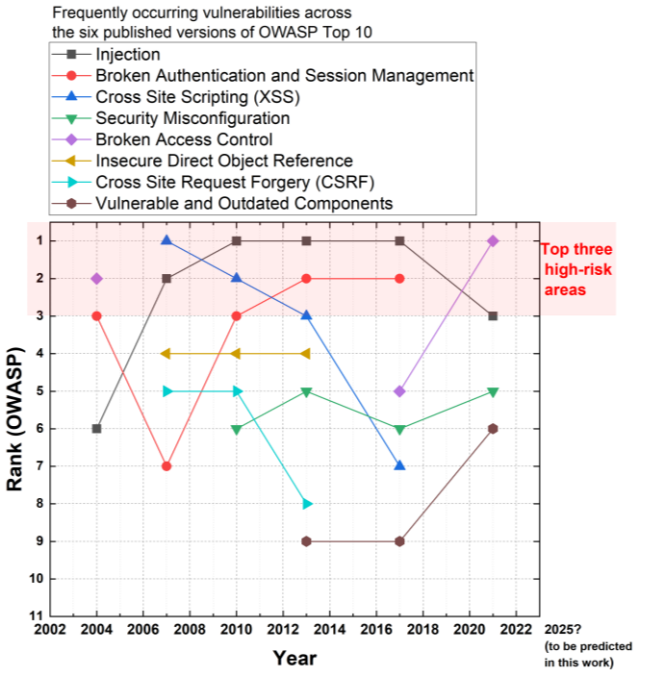

Fig. 3. Evolution of the ranking trends of common security vulnerabilities in the OWASP top 10 over different years.

B. Benchmark with the Evolution of CWE/SANS Top25

For benchmarking purposes, a comparable study was conducted on the CWE/SANS Top 25 risks, a collaborative effort between the MITRE Corporation's Common Weakness Enumeration (CWE) and the SANS Institute. While the OWASP Top 10 primarily focuses on vulnerabilities associated with web applications (with a separate list available for mobile applications [18]), the CWE/SANS Top 25 provides a broader scope. This list includes a wide range of weaknesses not only relevant to web applications but also applicable to various types of software systems across diverse platforms and environments. As such, the CWE/SANS Top 25 serves as a comprehensive resource for identifying and addressing security vulnerabilities that can affect the entire software development lifecycle, from design and coding to deployment and maintenance. This broader focus offers valuable insights into systemic security challenges [19] that transcend the specific domain of web applications [20][21].

Figure 4 illustrates the proportional distribution of various security vulnerabilities across the 2009, 2010, 2011, 2019, 2020, 2021, 2022, 2023, and 2024 versions of the CWE/SANS Top 25 rankings. It is evident that, for vulnerabilities occurring at least seven times, their frequencies are relatively

consistent across these years. In total, 12 such vulnerabilities are identified, representing recurring and significant issues in the software development lifecycle. These common vulnerabilities continue to pose substantial challenges in ensuring secure software design and development.

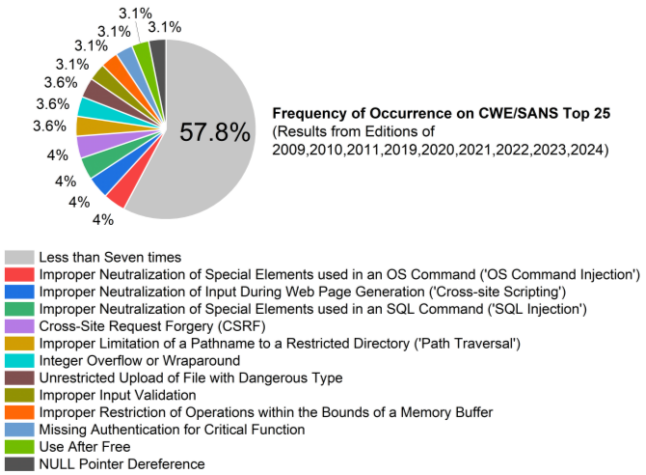

Fig. 4. Proportional distribution of common security vulnerabilities in the CWE/SANS top 25 rankings (across the nine editions of 2009, 2010, 2011, 2019, 2020, 2021, 2022, 2023 and 2024).

Figure 5 presents the ranking trend of the 12 most frequent vulnerabilities in the CWE/SANS Top 25 over time. It is evident that vulnerabilities with higher rankings maintain a relatively stable order over the years. Specifically, Improper Input Validation and Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') have consistently held the top two positions over the past six years. Improper Neutralization of Special Elements Used in an OS Command ('OS Command Injection'), although a frequent presence in the Top 25 and consistently ranking within the top three, experienced a notable decline starting from 2021.

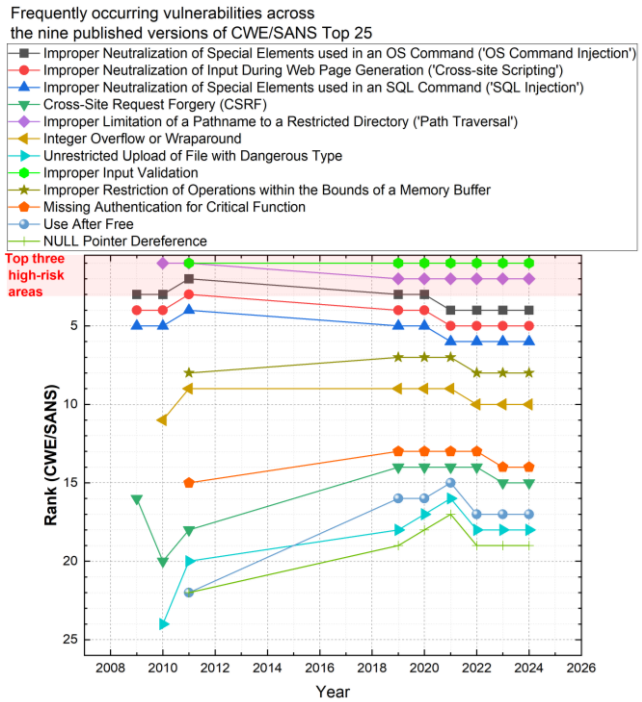

Fig. 5. Evolution of the ranking trends of common security vulnerabilities in the CWE/SANS top 25 lists over different years.

By 2024, the OS Command Injection had declined from its position among the top three high-risk vulnerabilities, reflecting a significant shift in the cybersecurity landscape. This change indicates the evolving nature of security threats, driven by advancements in secure coding practices, improved detection mechanisms, and the widespread adoption of mitigations such as input validation and command execution restrictions. The dynamic prioritization of vulnerabilities in the software development ecosystem highlights the continuous adaptation of both attackers and defenders, where new threats emerge as others become better understood and mitigated. This trend further reinforces the importance of proactive security strategies, ongoing vulnerability assessments, and the integration of robust security measures throughout the software development lifecycle.

III. Prediction of 2025 OWASP Top10 and Discussions

A. Prediction Mechanism and Results for 2025

Building upon the historical evolution of the OWASP Top 10 analysed in the previous section, and incorporating four newly identified pillars introduced in this study, the 2025 edition of the OWASP Top 10 is expected to reflect not only emerging threats but also evolving trends in the cybersecurity landscape. These trends, shaped by technological advancements and the lessons learned from past vulnerabilities, will play a crucial role in defining the next set of critical security risks. The four key pillars identified in this paper (Fig. 6)—artificial intelligence (AI) and machine learning (ML) security risks, API and cloud security, software supply chain attacks, and regulatory and compliance pressures—are anticipated to significantly influence the identification and prioritization of vulnerabilities in the forthcoming edition. This revised list will likely provide a comprehensive overview of the most pressing security challenges faced by organizations, helping to direct focus towards areas that are increasingly vulnerable as digital ecosystems continue to grow and evolve. In this context, the 2025 OWASP Top 10 will not only serve as a reflection of current cybersecurity concerns but also act as a guide for future preparedness and mitigation strategies. The newly predicted OWASP Top 10 for 2025, taking into account these critical factors, is presented in Table I.

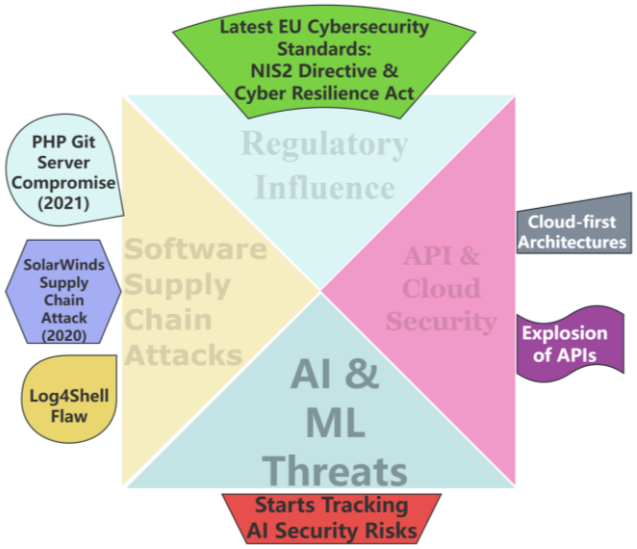

Fig. 6. The four new pillars identified in this work that underline our latest prediction of the OWASP Top 10 to be announced in 2025, highlighting the emerging cybersecurity challenges that are expected to shape the evolving threat landscape.

TABLE I. PREDICTED OWASP TOP 10 FOR 2025 AND ONWARDS

Rank	Predicted OWASP 2025 Risk	Reason for Inclusion
1	Broken Access Control	Remains a leading cause of security breaches, allowing unauthorized access to sensitive data and functionalities.
2	AI/ML-Based Security Risks	Growing adoption of AI/ML introduces threats like adversarial attacks, model poisoning, and prompt injection in AI-driven applications.
3	Injection (including Prompt Injection)	Classic SQL and command injections persist, and new forms like prompt injection in AI applications are emerging.
4	Insecure Design	Poor security practices at the design stage continue to lead to exploitable vulnerabilities.
5	Security Misconfiguration	Misconfigured cloud settings, container vulnerabilities, and automation errors remain common attack vectors.
6	Vulnerable and Outdated Components	Third-party dependencies, open-source vulnerabilities, and unpatched software create significant risks.
7	Identity and Authentication Failures	Weak authentication, credential stuffing, and MFA bypass attacks continue to threaten user security.
8	Software Supply Chain Vulnerabilities	Attacks on CI/CD pipelines, package repositories, and dependencies are increasing in frequency and impact.
9	Security Logging and Monitoring Failures	Lack of proper logging and detection mechanisms delays breach responses and forensic investigations.
10	Cloud and API Security Issues	Rapid cloud adoption has led to API misconfigurations, excessive permissions, and serverless security flaws.

The top three threats identified in the 2025 OWASP Top 10 (predicted) reflect the increasingly complex and dynamic nature of the cybersecurity landscape. As per the envisioned Top 10 list, Broken Access Control (BAC) continues to be a major concern, as unauthorized access remains a persistent attack vector, often resulting in data breaches and exploitation of sensitive information. This challenge is exacerbated by the growing sophistication of cyberattacks and the expanding attack surface of modern applications, which include web, mobile, and cloud environments.

A newly emerging concern is AI/ML-based security risks. As artificial intelligence and machine learning technologies become more integrated into applications, they introduce new vulnerabilities. Adversarial attacks targeting AI models, data poisoning, and model theft are anticipated to become more prevalent, especially as organizations increasingly rely on AI-driven systems. These novel threats present significant challenges for cybersecurity, as traditional defense mechanisms struggle to address the unique complexities of machine learning environments, calling for the development of specialized security measures.

While traditional injection threats, such as SQL [22] and command injection, remain prevalent, a growing trend is the rise of prompt injection attacks, particularly targeting AI-driven applications. These attacks exploit the unique characteristics of AI models, highlighting the need for tailored defenses that can effectively protect against these emerging vulnerabilities. The continued reliance on third-party libraries, open-source components, and outdated software remains a critical security weakness. When these dependencies are not properly managed, updated, or patched, they can serve as entry points for attackers exploiting known vulnerabilities. This issue underscores the importance of rigorous dependency management and regular software updates to mitigate security risks. In addition, weak authentication practices, credential stuffing, and inadequate multi-factor authentication (MFA) implementations persist as major facilitators of unauthorized access, reinforcing the need for stronger, more robust authentication protocols.

The threat of software supply chain attacks is likely to grow, as vulnerabilities in dependencies, package repositories, and CI/CD pipelines become increasingly targeted by attackers. As organizations embrace automation in development and deployment, ensuring the security of these pipelines becomes critical. The growing complexity of modern infrastructure further highlights the need for enhanced detection and response capabilities, particularly in cloud environments and AI-driven systems. With the rise of cloud-native applications, API security misconfigurations, excessive privileges, and vulnerabilities in serverless architectures are expected to dominate the threat landscape. These emerging concerns indicate a shift toward securing decentralized systems and emphasize the importance of rigorous access control and configuration management in increasingly complex cloud environments.

Overall, the 2025 OWASP Top 10 highlights the evolving nature of security threats, with a clear shift toward addressing risks in AI, the software supply chain, and modern cloud architectures. The rapid pace of technological advancement underscores the need for adaptive, proactive security strategies to safeguard applications and systems in this increasingly complex digital landscape.

B. Limitations and Opportunities for Future Work

Despite providing valuable insights into the evolving landscape of cybersecurity, this study has several limitations.

Firstly, while the analysis of the OWASP Top 10 and CWE/SANS Top 25 provides a comprehensive overview of the most prevalent vulnerabilities, it primarily focuses on well-established threats and may not fully capture emerging risks, such as those related to AI/ML-based security or advanced persistent threats. As these new challenges are not yet universally understood or consistently catalogued in mainstream vulnerability databases, there is a risk that they may not be adequately represented in the study.

Secondly, the study predominantly relies on historical data from the OWASP Top 10 and CWE/SANS Top 25, which reflect trends from previous years but may not account for the most recent shifts in attack methods or evolving security strategies. As cybersecurity threats evolve rapidly, especially with the rise of cloud-native applications and AI-driven systems, the findings may not fully capture the most current threat landscape. Additionally, the study does not delve deeply into the specifics of how various organizations are implementing security measures or the effectiveness [23] of current mitigation strategies against these vulnerabilities. While it highlights key areas of concern, such as broken access control, prompt injection attacks, and supply chain risks, the analysis does not assess the practical application of security measures in real-world scenarios, which can vary significantly based on industry, organization size, and technological environment.

Finally, while the study discusses trends across different versions of the OWASP Top 10 and CWE/SANS Top 25, it does not include a comprehensive analysis of regional or sector-specific variations in security risks. Vulnerability patterns may differ across different industries (e.g., big data and sentiment analysis [24], electronic engineering and wireless communications [25]) or geographic regions, and a more targeted investigation could provide deeper insights into the unique challenges faced by specific sectors. In summary, while this study offers a broad view of the key security vulnerabilities shaping the cybersecurity landscape, its findings are limited by the scope of the datasets used, the exclusion of emerging threats, and the lack of detailed context regarding the practical application of security measures. Future research could build on these insights by incorporating more up-to-date data and focusing on the real-world implementation of security strategies tailored for different sectors [26–28] and applications [29–31], based on which iteratively optimized protocols shall follow, aiming for enhanced detection process (featuring improved reliability and reduced complexity) specified for each sector.

IV. Concluding Remarks

The predicted 2025 OWASP Top 10 will undoubtedly reflect the rapidly changing cybersecurity landscape, with both longstanding vulnerabilities and emerging threats coming to the forefront. While traditional concerns such as broken access control and injection flaws remain critical, new challenges driven by the integration of AI/ML technologies, the increasing reliance on cloud-native architectures, and the growing complexity of software supply chains are reshaping the way organizations must approach security. The predictions outlined in this work serve as a call to action for researchers, practitioners, and policymakers to adapt and respond to these evolving threats by strengthening security practices and developing more resilient systems. As cybersecurity continues to evolve, proactive measures are essential to mitigate risks and protect the integrity of digital infrastructures.

While this study provides a comprehensive analysis of the evolution of the OWASP Top 10 and offers predictions for the 2025 edition, several areas warrant further exploration. Future research should focus on empirical validation of the predicted vulnerabilities through large-scale security incident data, industry case studies, and penetration testing results. This would help refine the accuracy of the predicted rankings and assess the real-world impact of emerging threats. Another critical avenue for future work is developing defensive strategies tailored to address new and evolving security risks. As AI/ML-based security threats become more prominent, further investigation into adversarial machine learning defence mechanisms and robust AI model security frameworks is essential. Similarly, advancements in cloud security best practices, particularly in securing serverless architectures, containerized environments, and API-driven infrastructures, require continuous research and refinement.

Additionally, with increasing regulatory pressures such as the NIS2 Directive and the Cyber Resilience Act, future studies should explore how these frameworks influence security policies and vulnerability mitigation strategies in both public and private sectors. The role of automated security solutions, including AI-driven security monitoring, automated compliance enforcement, and real-time anomaly detection, also presents a promising direction for improving resilience against evolving threats. Lastly, as the OWASP Top 10 continues to evolve, maintaining an adaptive vulnerability assessment framework that incorporates real-time threat intelligence, industry feedback, and academic insights will be essential. This will ensure that security professionals and policymakers remain well-equipped to address the dynamic nature of cybersecurity risks, enhance resilience, and strengthen the overall security posture of digital systems in an increasingly interconnected world.

Acknowledgment

This work was inspired by our project under the partial support from the National Natural Science Foundation of China (Grant 62301043), and the Fundamental Research Funds for the Central Universities (Beijing Institute of Technology Research Fund Program for Young Scholars).

References

[1] J. Li, “Vulnerabilities Mapping based on OWASP-SANS: A Survey for Static Application Security Testing (SAST),” Ann. Emerg. Technol. Comput., vol. 4, no. 3, pp. 1–8, July 2020.

[2] F. Tudela, J. Higuera, J. Higuera, J. Montalvo, and M. Argyros, “On Combining Static, Dynamic and Interactive Analysis Security Testing Tools to Improve OWASP Top Ten Security Vulnerability Detection in Web Applications,” Appl. Sci., vol. 10, 24, 9119, December 2020.

[3] V. Damanik and S. Sunaringtyas, “Secure Code Recommendation Based on Code Review Result Using OWASP Code Review Guide,” 2020 International Workshop on Big Data and Information Security (IWBIS), Depok, Indonesia, November 2020, pp. 153–158.

[4] B. Kiruba, V. Saravanan, T. Vasanth, and B. Yogeshwar, “OWASP Attack Prevention,” 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, September 2022, pp. 1671–1675.

[5] S. Budiyanto, L. Silalahi, A. Hakim, A. Hamid, and D. Hanafi, “Vulnerability Analysis on Internet of Things (IoT) Networks using Raspberry Pi and Open Web Application Security Project (OWASP),”

2024 FORTEI-International Conference on Electrical Engineering (FORTEI-ICEE), Badung, Indonesia, January 2025, pp. 58–63.

[6] M. Idris, I. Syarif, and I. Winarno, "Development of Vulnerable Web Application Based on OWASP API Security Risks," 2021 International Electronics Symposium (IES), Surabaya, Indonesia, November 2021, pp. 190–194.

[7] A. Khanum, S. Qadir, and S. Jehan, "OWASP-Based Assessment of Web Application Security," 2023 18th International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, January 2024, pp. 240–245.

[8] S. Lala, A. Kumar, and T. Subbulakshmi, "Secure Web development using OWASP Guidelines," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, May 2021, pp. 323–332.

[9] S. Kumar and Y. Rani, "Implementation and analysis of Web application security measures using OWASP Guidelines," 2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC), Hyderabad, India, April 2022, pp. 182–187.

[10] A. Abdurrahman and E. Husni, "A Secure Digital Image Marketplace: Microservices and OWASP API Security Using Spring Boot," 2024 International Conference on ICT for Smart Society (ICISS), Bandung, Indonesia, November 2024, pp. 1–8.

[11] D. Akbar, R. Purwoko, Arizal, and M. Syahral, "IoT System Design and Implementation Based on OWASP IoT Security Verification Standard," 2024 8th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, October 2024, pp. 274–279.

[12] M. Aljabri, M. Aldossary, N. Homeed, B. Alhetelah, M. Althubiany, and O. Alotaibi, "Testing and Exploiting Tools to Improve OWASP Top Ten Security Vulnerabilities Detection," 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN), Al-Khobar, Saudi Arabia, January 2023, pp. 797–803.

[13] P. Wanecki, R. Jašek, and I. Drofova, "The Contribution of the European NIS2 Directive to the Design of the Cyber Security Model," 2023 International Conference on Information and Digital Technologies (IDT), Zilina, Slovakia, August 2023, pp. 149–154.

[14] A. Jara, I. Martinez, and J. Sanchez, "CyberSecurity Resilience Act (CRA) in Practice for IoT Devices: Getting Ready for the NIS2," 2024 IEEE Smart Cities Futures Summit (SCFC), Marrakech, Morocco, October 2024, pp. 56–60.

[15] M. Shaffique, "Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark?" Computer Law & Security Review, vol. 54, 106009, July 2024.

[16] M. Kikelj and I. Sabic, "Strengthening the Digital Ecosystem: Effects of the Cyber Resilience Act (CRA) on Open-Source Software," 2024 IEEE International Conference on Cyber Security and Resilience (CSR), London, United Kingdom, September 2024, pp. 557–561.

[17] L. Colonna, "The end of open source? Regulating open source under the cyber resilience act and the new product liability directive," Computer Law & Security Review, vol. 56, 106105, April 2025.

[18] K. Qian, R. Parizi, and D. Lo, "OWASP Risk Analysis Driven Security Requirements Specification for Secure Android Mobile Software Development," 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, January 2019, pp. 1–2.

[19] J. Shahid, M. Hameed, I. Javed, K. Qureshi, M. Ali, and N. Crespi, "A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions," Appl. Sci., vol. 12, 8, 4077, April 2022.

[20] K. Abdulghaffar, N. Elmrabit, and M. Yousefi, "Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners," Computers, vol. 12, 11, pp. 235, October 2023.

[21] H. Huang, Z. Zhang, H. Cheng, and S. W. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls," Computer, vol. 50, 6, pp. 81–85, June 2017.

[22] A. Rai, M. Miraz, D. Das, H. Kaur, and Swati, "SQL Injection: Classification and Prevention," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, June 2021, pp. 367–372.

[23] T. Petranović and N. Žarić, "Effectiveness of Using OWASP TOP 10 as AppSec Standard," 2023 27th International Conference on Information Technology (IT), Zabljak, Montenegro, March 2023, pp. 1–4.

[24] J. Li, Ed., Advances in Sentiment Analysis - Techniques, Applications, and Challenges. London, U.K.: IntechOpen, 2024.

[25] J. Li and H. Li, "Passive-active crosstalk beyond low-frequency breakdown in mathematical-physical models of liquid crystal phase shifters at low-frequency applications," IET Conference Proceedings, vol. 2024, 30, pp. 592–596, January 2025.

[26] J. Li and H. Li, "Susceptibility to Low-Frequency Breakdown in Full-Wave Models of Liquid Crystal-Coaxially-Filled Noise-Shielded Analog Phase Shifters," Electronics, vol. 13, 23, 4792, December 2024.

[27] J. Li and H. Li, "Assessing Vulnerabilities in Line Length Parameterization and the Per-Unit-Length Paradigm for Phase Modulation and Figure-of-Merit Evaluation in 60 GHz Liquid Crystal Phase Shifters," Symmetry, vol. 16, 10, 1261, September 2024.

[28] J. Li, "Optically Inspired Cryptography and Cryptanalysis: A Survey and Research Directions," Emerging Technologies in Computing, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), Springer, 2020, vol. 332, pp. 98–110.

[29] J. Li, "Taking Flow Characterization to New Heights by Fiber Bragg Gratings Array," Energies, vol. 16, 10, 4218, May 2023.

[30] V. Dehalwar, A. Kalam, M. L. Kolhe and A. Zayegh, "Review of web-based information security threats in smart grid," 2017 7th International Conference on Power Systems (ICPS), Pune, India, December 2017, pp. 849–853.

[31] S. Alazmi and D. Leon, "A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners," IEEE Access, vol. 10, pp. 33200–33219, March 2022.