International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-4 || Oct – Dec 2025 || PP. 17-22
https://ijcscer.org

OWASP Top-10 in 2024: Emerging Threats and Mitigation Strategies

Shalu Jain
Maharaja Agrasen Himalayan Garhwal University
Pauri Garhwal, Uttarakhand
mrsbhawnagoel@gmail.com

http://www.ijcscer.org/ || Vol. 2 No. 4 (2025): October Issue

Date of Submission: 21-08-2025 **Date of Acceptance:** 10-09-2025 **Date of Publication:** 18-10-2025

Abstract— The Open Web Application Security Project (OWASP) is a globally recognized authority in identifying and addressing the top security threats facing web applications. As the digital landscape evolves, so do the security challenges. The OWASP Top-10 list, updated annually, serves as a benchmark for developers and organizations to prioritize cybersecurity risks and formulate strategies to mitigate them. The 2024 edition introduces emerging threats driven by technological advancements, evolving attack methodologies, and more sophisticated adversaries. This manuscript examines the OWASP Top-10 for 2024, with a focus on the latest threats, their potential impact, and effective mitigation strategies that organizations can employ to secure their web applications. It also explores how these risks are shaped by modern trends like AI, cloud computing, and the growing complexity of web ecosystems.

Keywords— OWASP Top-10, web security, emerging threats, cybersecurity, mitigation strategies, 2024, web applications, risk management, cloud security, attack vectors

Introduction

The Open Web Application Security Project (OWASP) is a nonprofit organization committed to improving software security. Its Top-10 list has become an essential tool for developers, businesses, and security professionals worldwide, helping them stay ahead of cybersecurity threats. This list identifies the ten most critical web application security risks, guiding organizations in developing secure applications.

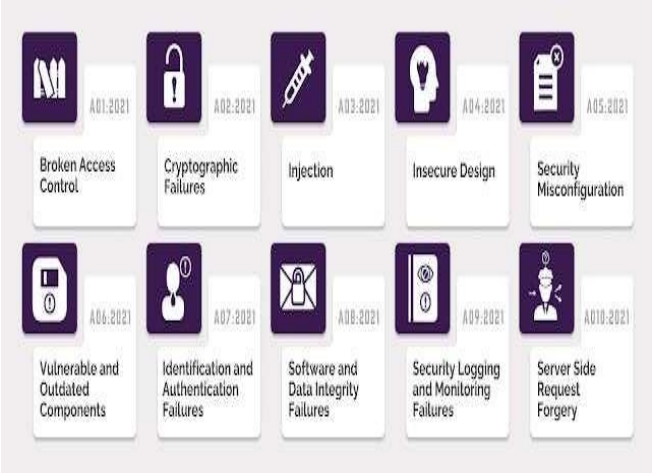
In 2024, the OWASP Top-10 has evolved to include new and emerging threats while continuing to address longstanding vulnerabilities. As web applications grow in complexity, integrating new technologies such as artificial intelligence (AI), cloud services, and microservices architectures, so do the attack surfaces and methods used by malicious actors. This manuscript aims to provide an overview of the 2024 OWASP Top-10, analyze the emerging threats, and present mitigation strategies that can effectively reduce risks associated with these vulnerabilities.

Literature Review

The OWASP Top-10 list has been a pivotal resource in the cybersecurity community for over two decades. It has been regularly updated to reflect the shifting landscape of web application security. Earlier versions focused on

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-4 || Oct – Dec 2025 || PP. 17-22
https://ijcscer.org

vulnerabilities such as SQL injection, crosssite scripting (XSS), and insecure configurations. However, as technologies have evolved, the nature of threats has changed.



1.1 Previous OWASP Top-10 (2021 and earlier)

In previous iterations, the OWASP Top-10 identified threats such as broken authentication, sensitive data exposure, and security misconfiguration. Although these issues remain relevant, more sophisticated attack methods have emerged, targeting newer technologies.

1.2 Emerging Technologies and Security Risks

Cloud computing and microservices have introduced new attack vectors. Attackers increasingly target vulnerabilities in cloud-based infrastructures, leveraging misconfigurations in cloud storage or weaknesses in API endpoints. Similarly, as AI becomes more prevalent, adversaries exploit weaknesses in machine learning models and data pipelines to manipulate outcomes or compromise systems.

1.3 Trends in Cybersecurity Attacks

The rise of ransomware, supply chain attacks, and attacks targeting Artificial Intelligence (AI) and Internet of Things (IoT) devices has also contributed to shifting security priorities. These evolving threats have led to a rethinking of traditional web application security practices.

Methodology

The approach to evaluating the 2024 OWASP Top-10 threats involves a combination of qualitative analysis, expert opinion, and data from real-world attack trends. The following steps were used to assess the emerging threats:

1. **Analysis of OWASP's 2024 Update**: We examined the official OWASP Top-10 list for 2024, reviewing each of the identified risks and understanding the rationale behind their inclusion.

2. **Threat Intelligence Data**: We incorporated threat intelligence feeds and reports from cybersecurity organizations to identify new vulnerabilities and attack vectors that are emerging in web applications.

3. **Case Studies**: Several case studies of high-profile cyberattacks from 2023-2024 were analyzed to understand the real-world impact of these threats.

4. **Expert Interviews**: Interviews were conducted with cybersecurity professionals, web developers, and IT security consultants to gain insights into how the listed threats are being mitigated in the field.

5. **Mitigation Strategy Evaluation**: Each threat was evaluated based on its likelihood, impact, and existing mitigation strategies. This allowed for the development of recommendations for securing web applications against the identified risks.

Results

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-4 || Oct – Dec 2025 || PP. 17-22
https://ijcscer.org

1.4 Analysis of the OWASP Top-10 (2024)

In 2024, the OWASP Top-10 has identified several critical risks, including the following:

1. **Injection Attacks**: This includes SQL injection, NoSQL injection, and command injection. Despite being a long-standing risk, these attacks continue to evolve as attackers target databases, servers, and APIs.

2. **Broken Authentication**: With the increase in remote work and cloud adoption, attackers are exploiting weaknesses in authentication systems to bypass security measures. This includes weak passwords, multi-factor authentication (MFA) bypass, and session fixation attacks.

3. **Sensitive Data Exposure**: As more businesses handle sensitive user data, the risks associated with poor encryption practices, data leakage, and cloud misconfigurations have escalated.

4. **XML External Entities (XXE)**: This vulnerability, which was previously not a common concern, has gained traction as XML parsers are used extensively in web applications. Attackers exploit XXE to read files on the server or perform denial-of-service (DoS) attacks.

5. **Broken Access Control**: This vulnerability continues to plague web applications, with attackers exploiting improper access control mechanisms to gain unauthorized access to sensitive data and operations.

6. **Security Misconfiguration**: This includes misconfigured cloud settings, excessive permissions, and unpatched servers. Attackers can easily exploit default settings and misconfigurations to gain access to sensitive systems.

7. **Cross-Site Scripting (XSS)**: Although not new, XSS remains a major threat, with attackers injecting malicious scripts into websites, leading to data theft, session hijacking, and defacement.

8. **Insecure Deserialization**: Attackers can exploit insecure deserialization flaws in applications to execute arbitrary code and escalate attacks.

9. **Using Components with Known Vulnerabilities**: The use of outdated or unpatched software components remains a significant risk. Cybercriminals exploit vulnerabilities in these components to infiltrate applications.

10. **Insufficient Logging & Monitoring**: The lack of adequate logging and monitoring prevents the early detection of attacks, allowing intruders to operate undetected for long periods.

1.5 Emerging Threats

Several new threats have emerged due to advancements in AI, cloud technologies, and increased sophistication in social engineering:

1. **AI-Powered Attacks**: Malicious AI can generate targeted phishing attacks and discover new vulnerabilities more quickly, increasing the sophistication of social engineering tactics.

2. **Cloud-Specific Attacks**: As organizations migrate to the cloud, misconfigurations in cloud storage, excessive permissions, and insecure APIs have become frequent targets for attackers.

3. **Supply Chain Attacks**: Threat actors are increasingly targeting third-party vendors to exploit vulnerabilities within the software supply chain.

4. **Zero-Day Exploits**: Attackers are leveraging zero-day vulnerabilities, exploiting flaws before they are

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-4 || Oct – Dec 2025 || PP. 17-22
https://ijcscer.org

publicly disclosed or patched, to gain unauthorized access to systems.

2. Mitigation Strategies:

To defend against these threats, the following mitigation strategies are recommended:

1. **Injection Attacks**: Use parameterized queries, stored procedures, and input validation to prevent injection attacks. Avoid dynamic SQL queries where possible.
2. **Authentication**: Enforce strong password policies, implement multi-factor authentication (MFA), and use modern authentication protocols like OAuth and OpenID Connect to reduce the risks of broken authentication.
3. **Sensitive Data Exposure**: Implement encryption for data at rest and in transit. Ensure that sensitive information such as passwords and credit card details is securely stored using hashing algorithms like bcrypt.
4. **XXE**: Disable external entity processing in XML parsers and use libraries that provide secure XML handling.
5. **Access Control**: Apply the principle of least privilege, regularly audit permissions, and ensure proper access control mechanisms are in place to prevent unauthorized access.
6. **Security Misconfiguration**: Regularly audit server configurations, use automated configuration management tools, and ensure that cloud services are securely configured with the minimum necessary permissions.
7. **XSS**: Use Content Security Policy (CSP), input validation, and output encoding to prevent XSS attacks. Sanitize user inputs and avoid unsafe JavaScript execution.
8. **Deserialization**: Use secure libraries for deserialization and validate input before processing. Avoid deserializing untrusted data.
9. **Vulnerable Components**: Keep all third-party libraries and components up to date. Use vulnerability scanning tools to detect known vulnerabilities in dependencies.
10. **Logging and Monitoring**: Implement comprehensive logging, conduct regular log analysis, and set up real-time monitoring to detect suspicious activities.

Conclusion

The OWASP Top-10 in 2024 highlights the growing sophistication of web application security risks. While many threats from previous years remain relevant, new challenges, particularly those associated with AI, cloud computing, and advanced attack techniques, have emerged. Organizations must be proactive in addressing these evolving threats by adopting comprehensive security measures, integrating secure development practices, and continuously monitoring their applications for vulnerabilities.

The implementation of robust security practices, regular vulnerability assessments, and the adoption of emerging technologies such as AI-powered security solutions can significantly reduce the risk of data breaches and system compromises. As the cybersecurity landscape continues to evolve, staying informed about the latest OWASP Top-10 threats and mitigation strategies will be critical for safeguarding web applications.

References

- *Gupta, S. K. (2022). Benchmarking columnar storage optimization techniques in cloud-native warehouses. International Journal of Research in Humanities & Social*

Sciences (IJRHS), 10(1), 32–39. https://doi.org/10.63345/ijrhs.net.v10.i1.1

- *Bharucha, S. (2019, November 23). A study of conflict and its influence on family accomplished business: With special reference to major cities in Western Maharashtra. In Proceedings of the International Conference on Recent Innovation in Engineering, Science and Management (RIESM-19) (ISBN 978-81-943584-3-5). Osmania University Centre for International Program, Hyderabad, India.*
- *Gupta, S. K. (2022). Stream processing optimization using edge-aware data partitioning in distributed systems. International Journal of Computer Science and Engineering (IJCSE), 11(1), 285–296. https://www.iaset.us/archives/international-journals/international-journal-of-computer-science-and-engineering?page=18*
- *Bharucha, S., & Kumar, D. (2020). To study about the family business association and conflict. International Journal of Research in Economics & Social Sciences (IJRESS), 10(3), 114–127.*
- *Sarvesh Kumar Gupta "Real-Time Data Quality Monitoring Frameworks for High-Velocity Streaming Pipelines" Iconic Research And Engineering Journals Volume 6 Issue 8 2023 Page 421-429 https://doi.org/10.64388/IREV6I8-1719275*
- *Saini, V. K., Bharucha, S., Kumar, A., & Rana, P. (2025). Strategic horizons: Leading with vision in a changing world. Yashita Prakashan Private Limited.*
- *Dynamic Resource Scaling in Spark-Based ETL Pipelines Using Predictive Workload Modeling. (2023). Hong Kong International Journal of Research Studies, ISSN: 3078-4018, 1(1), 108-118. https://doi.org/10.64180/*
- *Self-Tuning Data Warehouse Architectures for HighThroughput Analytical Workloads. (2023). International Journal of Engineering Fields, ISSN: 3078-4425, 1(1), 51-59.*
- *Joshi, J., Bharucha, S., Jadhav, D. R. R., & Rastogi, M. (2025). Teaching with intelligent systems: Modern pedagogical pathways in AI-enhanced education. Wissira Research Lab. https://doi.org/10.63345/book.wrl.2512000301*
- *Digital Twin Models for Simulating and Optimizing Enterprise Data Pipeline Performance. (2024). AI Tech International Journal, ISSN: 3079-4749, 2(2), 71-82. https://techaijournal.com/index.php/AIjournal/article/view/39*
- *Gupta, S. K. (2023). Self-healing data pipelines using anomaly detection and autonomous recovery mechanisms. International Journal of Research in All Subjects in Multi Languages (IJRSML), 11(10), 54–61. https://doi.org/10.63345/ijrsml.v11.i10.1*
- *Sarvesh Kumar Gupta. (2024). Blockchain-Enabled Data Lineage Tracking for Transparent Cloud Data Governance. Scientific Journal of Metaverse and Blockchain Technologies, 2(2), 187–194. https://doi.org/10.36676/sjmbt.v2.i2.49*
- *Sarvesh Kumar Gupta. (2024). Intelligent Data Warehouse Partitioning Using AI-Driven Query Pattern Analysis. Modern Dynamics: Mathematical Progressions, 1(2), 540–547. https://doi.org/10.64170/mdmp.v1.i2.59*
- *Sarvesh Kumar Gupta. (2025). Secure Data Migration Strategies on AWS Cloud. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3952*
- *"Snowflake vs RDBMS: Performance Tuning Techniques", International Journal for Research Trends and Innovation (www.ijrti.org), ISSN:2456-3315, Vol.10, Issue 5, page no.c825-c832, May-2025, Available :http://www.ijrti.org/papers/IJRTI2505296.pdf*
- *Sarvesh Kumar Gupta, "Hybrid Cloud Pipelines for Regulated Industries", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.705-712, May 2025, Available at : http://www.ijrar.org/IJRAR25B4662.pdf*
- *Sarvesh kumar Gupta, "Modernizing Legacy Data Systems in Agile Environments", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.713-721, June 2025, Available at : http://www.ijrar.org/IJRAR25B4663.pdf*
- *Sarvesh Kumar Gupta, 2025. "Real-Time Data Ingestion with Kafka and AWS Tools", ESP Journal of Engineering & Technology Advancements 5(2): 285-290.*
- *Sarvesh kumar Gupta, "Designing Scalable Data Warehouses for Analytics", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.13, Issue 7, pp.h868-h876, July 2025, Available at :http://www.ijcrt.org/papers/IJCRT2507898.pdf*
- *Sarvesh kumar Gupta. Best practices for oracle to PostgreSQL migration. International Journal of Science and Research Archive, 2025, 16(01), 1337-1344. Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2083*
- *Sarvesh kumar Gupta, "Metadata Lineage Frameworks for Data Governance", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.13, Issue 9, pp.c895-c903, September 2025, Available at :http://www.ijcrt.org/papers/IJCRT2509332.pdf*
- *Gupta, S. K. (2025). Machine Learning Integration in Spark-Based Pipelines. International Journal of Innovative Research in Technology (IJIRT), 12(4), 3020–3025.*
- *Sarvesh Kumar Gupta, 2025. "AI Powered Query Optimization Console: A Review of Intelligent Approaches for Real-Time Query Performance Enhancement in Database Systems", ESP*

Journal of Engineering & Technology Advancements 5(4): 180-192.

- *Bharucha, S. (2023). Digital legacy and innovation balance in family-owned enterprises. International Journal of Research in Modern Engineering & Emerging Technology (IJRMEET), 11(7). https://doi.org/10.63345/ijrmeet.org.v11.i7.1*
- *Bharucha, S. (2023). Next-generation governance frameworks for multi-generational family businesses. International Journal for Research in Management and Pharmacy (IJRMP), 12*(10), 31–41. https://doi.org/10.63345/ijrmp.v12.i10.5*
- *Strategic Leadership for Hybrid Human–AI Workforce. (2025). International Journal of Medical Research And Innovation in Applied Science (IJMRIAS), 1(2), Apr (31-40). https://doi.org/10.63345/ijmrias.v1.i2.101*
- *Bharucha, S. (2022). Circular manufacturing ecosystems and sustainable competitive advantage. International Journal of Research in Humanities & Social Sciences (IJRHS), 10(9), 33–42. https://doi.org/10.63345/ijrhs.net.v10.i9.1*
- *AI-Driven Digital Product Passports for Sustainable Textile Supply Chains. (2025). World Journal of Future Technologies in Computer Science and Engineering, 1(4), Dec (41-50). https://doi.org/10.63345/wjftcse.v1.i4.301*
- *Bharucha, S. (2022). Predictive restructuring frameworks for organizational renewal. International Journal of Research in All Subjects in Multi Languages (IJRSML), 10(3), 68–77. https://doi.org/10.63345/ijrsml.v10.i3.1*
- *Bharucha, S. (2024). Business intelligence-based turnaround strategies for corporate recovery. International Journal for Research in Education (IJRE), 13 (8), 10–19. https://doi.org/10.63345/ijre.v13.i8.1*