International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 6 Volume No.7 November - December – 2023
DOI:10.46647/ijetms.2023.v07i06.038 ISSN: 2581-4621

Evolving Trends in Web Application Vulnerabilities: A Comparative Study of OWASP Top 10 2017 and OWASP Top 10 2021

Devendra Upadhyay[1], Dr. Nilesh R. Ware[2]
[1] *PG – Technology Management, DIAT, Pune, Maharashtra**
[2] *Assistant Professor - Technology Management, DIAT, Pune, Maharashtra*
Corresponding Author Orcid ID: ORCID [0009-0001-6676-958X]

ABSTRACT
In today's digital era online services and interactions are present everywhere, which makes Web application security a primary concern. A global community that is serving to guide efforts toward web application security is the Open Web Application Security Project (OWASP)[1]. It achieves this target by releasing a periodic list of the security risks that are most critical from the point of view of web application security[2], this list is known as OWASP Top 10, This research paper aims to unveil the evolving nature of vulnerabilities present in web application through an in-depth comparative study of the OWASP Top 10 lists from 2017 and 2021 editions. It enlightens the continuously changing horizon going deep in ranking changes of threats, vulnerability descriptions, and identifying emerging trends. The comparative study enables organizations, security practitioners, and developers to adopt their security strategies and practices. It serves as a compass to address the ever-evolving challenges of web application security in the contemporary digital era.
Keywords—Authentication, Cybersecurity, Injection, OWASP, Vulnerability.

1. Introduction

Various aspects of our modern life involve web applications as an integral part of it, It includes e-commerce, communication, entertainment, or any other form of information exchange. This pervasive reliance on web applications has made them a cornerstone of the digital age. However, this ubiquity makes web applications the prime targets for cyberattacks, Malicious actors often seek to exploit the exposed vulnerabilities for financial gain, data theft, or service disruption[3].

The Open Web Application Security Project (OWASP) has played a pivotal role in handling the complex horizon of web application security. OWASP, a global community working at the forefront to enhancing web application security through dedicated efforts to identify, categorize, and mitigate web application vulnerabilities. Periodic compilation of the most critical web application security risks is one of its flagship initiatives which is published as OWASP Top 10[4].

The threats and vulnerabilities targeting web applications are evolving as a relentless pace as the digital ecosystem. Recognizing the imperative of staying ahead of these dynamic challenges, OWASP has periodically updated its Top 10 list. The latest edition, OWASP Top 10 2021[5], represents the organization's continued commitment to keeping pace with the evolving threat landscape. Fig. 1 represents the Top 10 vulnerabilities identified in OWASP 2021.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 6 Volume No.7 November - December – 2023
DOI:10.46647/ijetms.2023.v07i06.038 ISSN: 2581-4621

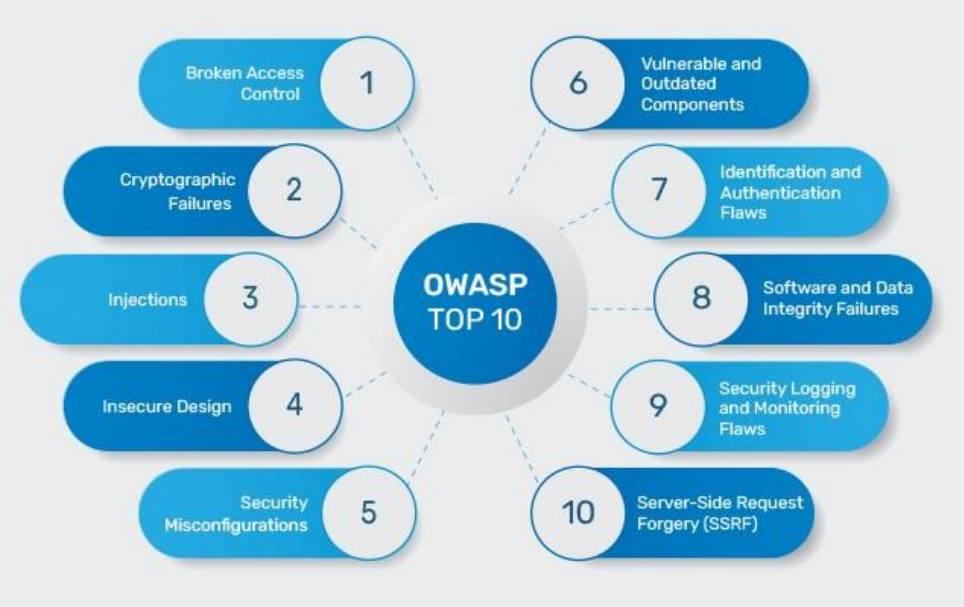

Fig 1. Top 10 vulnerabilities identified in OWASP 2021

The intention of this research paper is to guide into the evolving trend of vulnerabilities in web applications by comparing and analyzing the 2017 edition and the 2021 edition of OWASP Top 10. It has an objective of exploring the transformation in the horizon of web application vulnerabilities over this period by delving into emerging security strategies, evolving risks, and changing priorities. Understanding and mitigating their vulnerabilities is of paramount importance in the era where web applications are integral components of our digital lives rather than merely tools. Through the journey of exploration and analysis, we are looking to provide necessary knowledge and insights to security practitioners, developers, and organizations so that they may adapt their strategies and practices effectively[6]. The comparative study guides us through the ever-evolving landscape of web application vulnerabilities and serves as a beacon pointing the way toward a more secure digital future.

2. Background

2.1 Web Application Security Landscape

In today's digital age web applications have redefined how we communicate, transact, and access information, serving as the backbone of online services and interactions. On the other hand, web applications have also been exposed to an ever-evolving landscape of security threats in this digital transformation.

With the proliferation of web applications, they become an attractive target for cybercriminals seeking to exploit security weaknesses for various malicious purposes. Hence it become an essential discipline in the realm of cybersecurity to practice protecting web applications from vulnerabilities and attacks, which is called Web application security.

2.2 The Role of OWASP

These challenges require an organization dedicated to improving the security of web applications and software as a beacon of knowledge and guidance. the Open Web Application Security Project (OWASP) fulfils this purpose as a global non-profit organization. Under OSWAP organizations, security experts, and developers operate as a collaborative community with a shared commitment of enhancing web application security[7].

Publication of the document to provide insight into the most critical web application security risks is one of OWASP's flagship initiatives which is known as OWASP Top 10. For organizations, security practitioners, developers, and those striving to secure their web applications effectively the OWASP Top 10 serves as a reference point and a roadmap.

2.3 The Evolution of the OWASP Top 10

DOI:10.46647/ijetms.2023.v07i06.038 ISSN: 2581-4621

Web application security is a field characterized by its constant evolution. As new technologies emerge and attack vectors evolve, the nature of web application vulnerabilities changes. To reflect these shifts in the threat landscape and provide up-to-date guidance, OWASP periodically updates its Top 10 list[8].

The focus of this research review paper is a comparative analysis of two significant editions of the OWASP Top 10: the 2017 edition and the 2021 edition. By examining the changes and trends between these two editions, we aim to shed light on how web application vulnerabilities have evolved over this critical period.

The comparative study conducted in this paper acknowledges OWASP's pivotal role in shaping web application security practices. To gain an in-depth understanding of the evolving trends in web application vulnerabilities, the expertise, and insights of the global cybersecurity community towards the previous editions of the OWASP Top 10 have been used.

The methodology employed for this analysis will be discussed in the following sections which will explore the changes in rankings and emerging threats that have shaped the landscape of web application security along with vulnerability descriptions. Our aim is to provide valuable insights for security practitioners which will help them adapt in a rapidly changing digital world by fortifying their web application security strategies[9].

3. Methodology

A comparative study of the OWASP Top 10 2017 and OWASP Top 10 2021 was the methodology employed to ensure rigor, comprehensiveness, and objectivity. The research methodology consisted of several key steps:

3.1. Data Collection

The first step involved gathering the primary data sources for the study:

3.1.1. OWASP Top 10 2017 Report:

The 2017 edition of the OWASP Top 10 served as a foundational document for understanding web application security vulnerabilities prevalent at that time. This document was obtained directly from the official OWASP website.

3.1.2. OWASP Top 10 2021 Report:

The 2021 edition of the OWASP Top 10, which represents the most recent snapshot of web application security risks, was also sourced from the official OWASP website.

3.2. Data Analysis

3.2.1. Comparative Analysis of Rankings:

•A detailed comparison was made between the rankings of web application security risks in the 2017 and 2021 editions of the OWASP Top 10.

•Each vulnerability's ranking was assessed to identify changes in priority. A focus was placed on understanding which vulnerabilities gained or lost prominence over the years.

3.2.2. Evolution of Vulnerability Descriptions:

•The vulnerability descriptions provided in both editions were meticulously analysed.

•Differences, updates, and changes in the descriptions were noted. Particular attention was given to identifying new terminology, concepts, or explanations introduced in the 2021 edition to reflect evolving attack techniques or security considerations.

3.2.3. Emerging Trends:

•The comparative analysis also aimed to identify emerging trends and vulnerabilities introduced or emphasized in the OWASP Top 10 2021.

•A qualitative assessment was conducted to understand the relevance and significance of these trends in the contemporary web application security landscape.

3.3. Ethical Considerations

Throughout the research process, ethical considerations were paramount. The research review paper is based solely on publicly available and authorized documents from the official OWASP website. We have avoided utilizing any sensitive or confidential information in this study.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 6 Volume No.7 November - December – 2023
DOI:10.46647/ijetms.2023.v07i06.038 ISSN: 2581-4621

3.4. Limitations

The primary limitation of this study is that it relies on the content and categorizations presented in the OWASP Top 10 reports. The completeness and accuracy of the information provided in these reports also affect the findings of the comparative analysis.

The results derived from the methodology of comparative analysis outlined here will be presented and discussed in the subsequent sections which provide valuable insights into evolving trends in web application vulnerabilities. Organizations, security practitioners, and developers who are looking to enhance their web application security strategies can use the result to get practical insights into the changing landscape of web application vulnerabilities.

4. Comparative Analysis

Fig. 2 presents an overview of comparative analysis between the OWASP Top 10 2021 and 2017, We found that 3 new categories have been introduced, the Scope and names are changed for 4 vulnerability categories, and consolidation for a few categories in the Top 10 for 2021. The intention behind changing names is to focus on the root cause rather than the symptom.

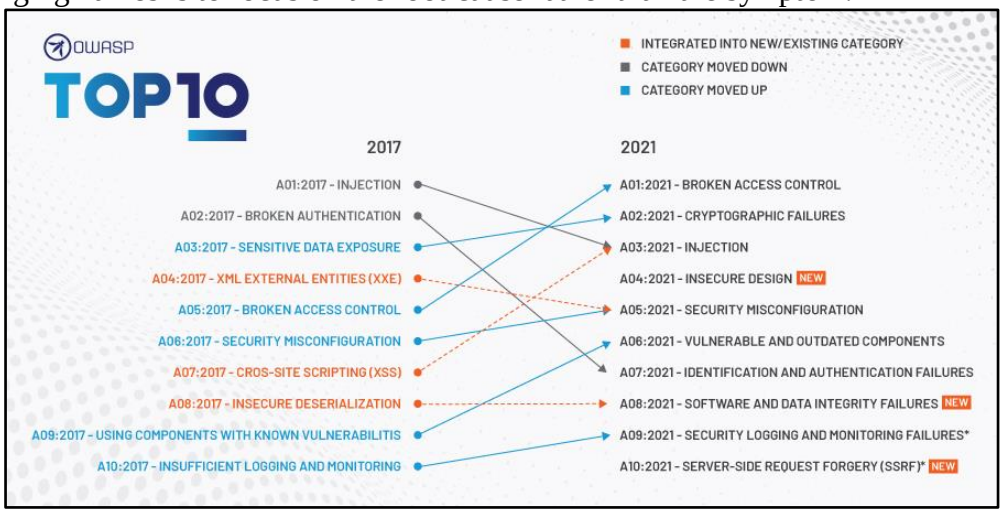

Fig 2. Top 10 vulnerabilities identified in OWASP 2021

4.1. Result: Changes in the Top 10 for 2021

Detailed Analysis for comparison of both reports has been made in line with the previous studies in this field. The analysis summary has been presented in the form of Table 1.

Table.1. Summary of Comparative Analysis

Rank in OWASP 2021	Vulnerability Name	Rank in OWASP 2017	Change	Remarks
A01	Broken Access Control	5th	Up 4	Moves up from the fifth position to the category with the most serious web application security risk.
A02	Cryptographic Failures	3rd	Up 2 (& Renamed)	Previously known as A03:2017-Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed name focuses on failures related to cryptography as it has been implicitly before. This category often leads to sensitive data exposure or system compromise.
A03	Injection	1st	Down 2 + A07	Cross-site Scripting is now part of this category in this edition.
A04	Insecure Design	-	New	Insecure Design is a new category for 2021, with a focus on risks related to design flaws. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.
A05	Security Misconfiguration	6th	Up 1 + A04	The former category for A4:2017-XML External Entities (XXE) is now part of this risk category
A06	Vulnerable and Outdated Components	9th	Up 3 (& Renamed)	Previously titled Using Components with Known Vulnerabilities and was #9 in the Top 10 community survey
A07	Identification and Authentication Failures	2nd	Down 5 (& Renamed)	Was previously Broken Authentication and is sliding down from the second position, and now includes CWEs (common weakness enumeration) that are more related to identification failures
A08	Software and Data Integrity Failures	-	New	New category for 2021, focusing on making assumptions related to software updates, and critical data, without verifying integrity.
A09	Security Logging and Monitoring Failures	10th	Up 1 (Expanded & Renamed)	Was previously A10:2017-Insufficient Logging & Monitoring moving up from #10 previously. This category is expanded to include more types of failures. However, failures in this category can directly impact visibility, incident alerting, and forensics.
A10	Server-Side Request Forgery	-	New	Server-Side Request Forgery is added newly. It is a web security vulnerability that allows an attacker to cause the server-side application to make requests to an unintended location. This could leak sensitive data, such as authorization credentials.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 6 Volume No.7 November - December – 2023
DOI:10.46647/ijetms.2023.v07i06.038 ISSN: 2581-4621

4.2. Key Findings

- Injection vulnerabilities, broken access control and sensitive data exposure remain significant threats in both versions.
- The removal of XXE vulnerability from the 2021 list indicates a decreasing prevalence of this vulnerability.
- Insecure deserialization is a new addition to the 2021 list, highlighting the growing recognition of its risks.
- Both versions emphasize the importance of strong authentication, access control, and protection of sensitive data.
- Insufficient logging and monitoring can hinder the detection and response to security incidents in web applications.

5. Discussion

The comparative analysis of the 2021 & 2017 version of OWASP Top 10 2017 reveals several critical insights into the evolving trends in web application vulnerabilities. These insights have far-reaching implications for security practitioners, developers, and organizations seeking to bolster their web application security measures in the face of a dynamic threat landscape.

5.1. Consistency in Top Priority Vulnerabilities

One of the striking findings of this comparative study is the continuity in the top 3 vulnerabilities in 2021 are from the Top 5 of the 2017 edition. It indicates that these vulnerabilities persist as a major threat to web application security. As there is consistency in top vulnerabilities, it is important to address these vulnerabilities as a foundational step in achieving of web application security. Organizations must make it a priority to prevent and mitigate injection attacks, Broken Access Control, and Cryptographic Failures[10].

5.2. Updated Vulnerability Descriptions

The 2021 edition underwent updates and refinements in the vulnerability descriptions while there is a relatively stable nature of core vulnerabilities. To adopt the continuous change in the landscape of threats these updates and refinements were essential so that it may accommodate modern application architectures. The revised descriptions direct toward effective mitigation strategies by focusing more on a deeper understanding of each vulnerability, offering context on how attackers use it. This evolution of the OWASP Top 10 list helps individuals and organizations better grasp the complexities present in web application vulnerabilities.

5.3. Recognition of Emerging Trends

The 2021 edition of the OWASP Top 10 introduced "Software and Data Integrity Failures " and "Insecure Design" as new additions that demonstrated a keen awareness of emerging trends in web application security[11]. It reflects the importance of addressing security concerns at the design stage itself and emphasizes the increasing prevalence of data Integrity in modern applications. Through this, it guides to incorporation of corresponding measures into security practices for handling the emerging trends.

5.4. Adaptability is Key

The comparative study strongly reinforces that continuous adoption for web application security is required because of the evolving threat landscape as it is not a static discipline and insists that development practices, security strategies, and risk mitigation efforts must also evolve with time. Organizations should adopt an agile and adaptive approach to web application security, staying informed about the latest trends and vulnerabilities. This adaptability is crucial for effectively countering new and emerging threats.

5.5. Role of OWASP in Shaping Security Practices

Practices of web application security are guided by the OWASP Top 10 over the years. Its influence extends beyond the list itself, as it serves as a reference point and educational resource for the global cybersecurity community[12]. The updates and enhancements introduced in the 2021 edition underscore OWASP's commitment to reflecting the evolving threat landscape accurately. Security

DOI:10.46647/ijetms.2023.v07i06.038 ISSN: 2581-4621

professionals and organizations can continue to rely on OWASP as a valuable source of guidance and knowledge.

6. Recommendations & Scope for future work

6.1. Recommendations

On the basis of the analysis carried out from the above study we recommend a few important points to be taken care of by organisations and Individuals.

6.1.1. Implement Comprehensive Web Application Security Training

To address the persistent vulnerabilities highlighted in this study, organizations should prioritize ongoing training and awareness programs for their development and security teams. Comprehensive training on secure coding practices, vulnerability detection, and secure design principles can empower teams to identify and mitigate vulnerabilities effectively. This proactive approach helps prevent common security pitfalls.

6.1.2. Embrace Automation and Security Tools

The use of automated security testing tools and vulnerability scanners should be a fundamental part of the development lifecycle. These tools play a vital role early in the development process as they can assist in identifying and addressing vulnerabilities, which in turn reduces the risk of security issues reaching production environments.

6.1.3. Address Design Flaws from the Start

"Insecure Design" as another emerging trend highlights the importance of addressing security concerns at the design stage of web applications[13]. Organizations should incorporate security by design principles into their development processes, emphasizing threat modelling, secure architecture, and risk assessments early in the project lifecycle.

6.1.4. Stay Updated and Adaptable

Web application security is a constantly evolving field. Security practitioners and organizations need to be vigilant and updated about emerging threats and vulnerabilities and should adapt accordingly to their security strategies. Regularly reviewing and implementing the recommendations provided by OWASP and other security organizations is crucial to maintaining robust security practices.

6.1.5. Collaborate and Share Insights

The security community thrives on collaboration and knowledge sharing. Organizations should encourage their security teams to actively participate in security communities, attend conferences, and engage in information exchange. Sharing insights and experiences can help collectively address evolving threats more effectively.

6.2. Scope for Future Work

Though valuable insights into the evolving trends of vulnerabilities in a web application have been provided by this comparative study, still there is a need for future research and exploration in a few arenas:

6.2.1. In-Depth Analysis of Emerging Trends

It is required to understand the challenges and mitigation strategies specifically associated with emerging trends like "API Security" and "Insecure Design" to provide practical guidance for security practitioners.

6.2.2. Longitudinal Studies

To look more comprehensive evolution view of web application vulnerabilities over time studies over several years are needed. Analysing multiple editions of the OWASP Top 10 and other sources over the years is a must to identify long-term trends.

6.2.3. Real-World Case Studies

Examining real-world case studies can be valuable learning resources for web application vulnerabilities and breaches and can provide concrete examples of how vulnerabilities are exploited and their real-world impact[14].

DOI:10.46647/ijetms.2023.v07i06.038 ISSN: 2581-4621

6.2.4. Quantitative Analysis

To assess the impact and severity of any specific vulnerabilities over time future research involving quantitative data can be explored which may involve data from security incident reports, breach statistics, and vulnerability databases.

Conclusion

This comparative study of the OWASP Top 10 2017 and OWASP Top 10 2021 provides valuable insights into the evolving trends in web application vulnerabilities. The continuity in certain vulnerabilities, updated descriptions, recognition of emerging trends, and the importance of adaptability all point to the dynamic nature of web application security. Security practitioners and organizations should leverage these insights to enhance their web application security measures and navigate the ever-changing digital landscape effectively[15]. By doing so, they can contribute to the ongoing effort to secure web applications and protect user data in an increasingly interconnected world. Incorporating the recommendations mentioned and pursuing future research avenues can contribute to a more secure web application landscape and enhance the resilience of organizations against evolving web application vulnerabilities.

References

[1]A. Kashniyal, “OWASP TOP 10 VULNERABILITIES,” *VeraCode*, Jan. 2019, Accessed: Oct. 23, 2023. [Online]. Available: https://www.academia.edu/40899265/OWASP_TOP_10_VULNERABILITIES
[2]“ScienceDirect Full Text PDF.” Accessed: Oct. 23, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S131915782100269X/pdfft?md5=41d273aa61a10fd014433b572c25516a&pid=1-s2.0-S131915782100269X-main.pdf&isDTMRedir=Y
[3]S. Rafique, M. Humayun, Z. Gul, A. Abbas, and H. Javed, “Systematic Review of Web Application Security Vulnerabilities Detection Methods,” *Journal of Computer and Communications*, vol. 03, pp. 28–40, Jan. 2015, doi: 10.4236/jcc.2015.39004.
[4]O. B. Fredj, O. Cheikhrouhou, M. Krichen, H. Hamam, and A. Derhab, “An OWASP Top Ten Driven Survey on Web Application Protection Methods,” in *Risks and Security of Internet and Systems*, J. Garcia-Alfaro, J. Leneutre, N. Cuppens, and R. Yaich, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2021, pp. 235–252. doi: 10.1007/978-3-030-68887-5_14.
[5]“A Study on Top 10 Web Application Vulnerabilities.” Accessed: Oct. 23, 2023. [Online]. Available: https://www.jetir.org/view?paper=JETIRAI06049
[6]“Top Web Application Security”.
[7]“OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation.” Accessed: Oct. 23, 2023. [Online]. Available: https://owasp.org/
[8]“OWASP Top Ten | OWASP Foundation.” Accessed: Oct. 23, 2023. [Online]. Available: https://owasp.org/www-project-top-ten/
[9]“preparing-for-the-new-owasp-top-10-and-beyond.pdf.” Accessed: Oct. 23, 2023. [Online]. Available: https://www.f5.com/pdf/article/preparing-for-the-new-owasp-top-10-and-beyond.pdf
[10] K. Rahman and C. Izurieta, “A Mapping Study of Security Vulnerability Detection Approaches for Web Applications,” in *2022 48th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, Aug. 2022, pp. 491–494. doi: 10.1109/SEAA56994.2022.00081.
[11] S. Disawal, “A Study on Top 10 Web Application Vulnerabilities,” vol. 6, no. 3, 2019.
[12] M. Bach-Nutman, “Understanding The Top 10 OWASP Vulnerabilities”.
[13] P. Sane, “Is the OWASP Top 10 List Comprehensive Enough for Writing Secure Code?,” in *Proceedings of the 2020 International Conference on Big Data in Management*, Manchester United Kingdom: ACM, May 2020, pp. 58–61. doi: 10.1145/3437075.3437089.
[14] D. N. J. Patel and D. Pandya, “OWASP TOP 10 VULNERABILITY ANALYSES IN GOVERNMENT WEBSITES”, Accessed: Oct. 23, 2023. [Online]. Available:

DOI:10.46647/ijetms.2023.v07i06.038 ISSN: 2581-4621

https://www.academia.edu/26117399/OWASP_TOP_10_VULNERABILITY_ANALYSES_IN_GOVERNMENT_WEBSITES
[15] J. Joshi, W. Aref, A. Ghafoor, and E. Spafford, "Security models for Web-based applications," *Commun. ACM*, vol. 44, pp. 38–44, Feb. 2001, doi: 10.1145/359205.359224.