International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0390
e ISSN: 2584-2854
Volume: 02
Issue: 08 August 2024
Page No: 2694-2698

Web Application Security: A Survey

Sayan Basak[1], Mayur Jadhav[2], Suraj Choudhary[3], Pranjal Kadam[4], Sheetal P. Gawande[5]
[1,2,3,4]Department of Information Technology, Pillai College of Engineering, New Panvel, Navi Mumbai, Maharashtra, India
[5]Department of Computer Engineering, Pillai College of Engineering, New Panvel, Navi Mumbai, Maharashtra, India
Emails: *sayan21it@student.mes.ac.in[1], mayur21it@student.mes.ac.in[2], suraj21it@student.mes.ac.in[3], pranjal21it@student.mes.ac.in[4], sheetalp@mes.ac.in[5]*

Abstract
Web applications play a crucial role in modern digital interactions by supporting a wide range of online activities, from social networking to e-commerce. However, the widespread use of web applications has also made security flaws visible and important. This article explores the complex topic of web application security, examining common attack paths, their effects, and the need for strong security measures. Phishing, XSS, and SQL Injection are some common web application attacks that provide a serious risk of financial loss, reputational loss, and privacy violations. The study emphasizes the importance of vulnerability discovery and mitigation techniques provided by organizations such as OWASP.
Keywords: *Clickjacking; Drive-By-Downloads; Phishing; XSS (Cross-Site Scripting)*

1. Introduction
Web applications, also known as web apps, are software programs that may be accessed by web browsers via a network like the internet. From social networking and online shopping to banking and productivity applications, they offer a vast array of features to its customers. But online apps are also very accessible and widely used, which makes them easy targets for cyberattacks. Web application threats come in a variety of forms, including as Phishing, Distributed Denial of Service (DDoS), Cross-Site Scripting (XSS), and SQL Injection. These assaults seek to take advantage of the loopholes in web applications to obtain private user data, interfere with services, or obtain unauthorized access to confidential information. The OWASP Top 10 has been referenced in this survey which provides a comprehensive list of the most critical security threats faced by web applications and valuable insights into common vulnerabilities and mitigation strategies. disrupt services, and compromise user privacy. The statistics presented in Fig 1.1 highlight the alarming frequency and variety of these threats, underscoring the urgent need for robust security measures.

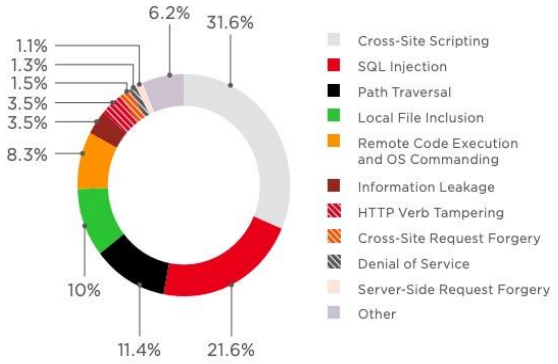

Figure 1 Web Application Attack Statistics

The data reflects the growth web application attacks have become increasingly prevalent, posing significant risks to both individuals and organizations. These attacks exploit vulnerabilities in web applications to steal sensitive data, disrupt services, and compromise user privacy. The statistics presented in Figure 1 shows the alarming frequency and variety of these threats, underscoring the urgent need for robust security measures. The data reflects the growth of cyberattacks, emphasizing the critical importance

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0390
e ISSN: 2584-2854
Volume: 02
Issue: 08 August 2024
Page No: 2694-2698

of enhancing web application security to protect against these pervasive and evolving threats. Web app attacks can have serious, far-reaching effects on people and businesses, including monetary losses, harm to one's reputation, and legal ramifications. Web application vulnerabilities are routinely ranked as one of the top security concerns that enterprises worldwide must deal with, according to studies undertaken by the Open Web Application Security Project (OWASP). To find common web app vulnerabilities, OWASP performs in-depth research and releases the OWASP Top 10 list, which acts as a standard for comprehending and reducing these risks. For web app developers and security experts, this list of common vulnerabilities—which includes Injection, Broken Authentication, and Sensitive Data Exposure—offers insights into the security issues that need to be addressed the most.

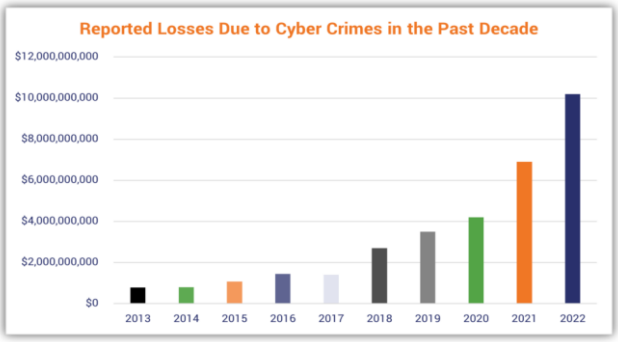

Figure 2 Losses Due to Cyber Attacks

Strong web app security mechanisms must be developed and implemented immediately due to the growing frequency and sophistication of web app assaults. These tools are essential for locating and fixing web application vulnerabilities, strengthening the applications' defenses against online attacks. Web app security technologies assist secure sensitive data, user privacy, and the integrity of online services by putting proactive security methods like threat detection, real-time monitoring, and vulnerability scanning into practice. The study highlights the importance of continuous research and innovation in web app security technologies for mitigating the changing threat landscape and securing the digital infrastructure that is fundamental to contemporary civilization.

2. Related Work

This study of the literature explores the topic of web application security by providing an in-depth analysis of academic papers. Web applications are the foundation of online activity in this day and age, therefore protecting them from emerging cyber threats is critical. Together, the surveyed papers provided insight into a number of web app security topics, such as prevalent attack routes, effective mitigation techniques, and new developments. The goal of this survey is to present a comprehensive picture of the state-of-the-art in web app security research by combining results from several sources. By examining the major ideas, approaches, and conclusions from the chosen papers, this study aims to add to the current discussion on web app security and provide guidance for future investigations in this important field. The 2022 International Conference on Recent Trends in Microelectronics, Automation, Computing, and Communications Systems hosted S. Akshay Kumar and Y. Usha Rani's paper et al. [1], which meticulously examines web application security through OWASP Guidelines. Amidst the surge in internet users, the paper highlights alarming data breaches, stressing the need for comprehensive vulnerability management. Referencing the OWASP Top 10, it underscores risks like injection attacks and cross-site scripting, advocating for robust defense mechanisms. Nick Rahimi's contribution to the 2021 International Conference on Computational Science and Computational Intelligence et al. [2] delves into the landscape of security issues in web applications. It emphasizes the urgency in addressing phishing attacks and proposes a data-driven approach using machine learning to classify websites. This approach aims to enhance detection accuracy and prevent online transaction fraud, emphasizing the importance of prediction and prevention in cybersecurity.

Muhamad Agreindra Helmiawan et al. [3] paper presented at the 2020 International Conference on Cyber and IT Service Management analyzes web security through the lens of the OWASP Top 10.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0390
e ISSN: 2584-2854
Volume: 02
Issue: 08 August 2024
Page No: 2694-2698

Focusing on cross-site scripting vulnerabilities, it proposes an innovative solution to fortify web applications. Their program maps internet applications efficiently, aiming to simplify vulnerability detection and remediation processes. Presented at the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, Michael A. Ivanov et al. [4] paper underscores the importance of web application security in Node.js development. It proposes a comprehensive approach drawing from OWASP guidelines to prevent common attacks like Denial-of-Service and NoSQL injection. The paper offers practical insights into securing front-end, middleware, and backend components. The 2022 International Conference on Trends in Electronics and Informatics hosted Saleem Raja A et al. [5] paper, which addresses the challenge of XSS attacks. Introducing ontology in cybersecurity, it advocates for a layered security approach to enhance web application protection. By elucidating exploitation techniques and presenting analysis tools, the paper emphasizes leveraging ontology models for effective defense against XSS vulnerabilities. Published in Electronics 2022, Mohammad Alsaffar et al. [6] paper expands on cyber threats, delving into phishing attacks, ransomware, and cryptojacking. It outlines stages and examples of phishing attacks, offering advice on protection measures and the need for heightened awareness. By highlighting evolving cybercriminal tactics, the paper underscores the importance of robust defense strategies. In J. Cybersecure. Priv. 2021, Jean Rosemond Dora and Karol Nemoga et al. [7] discuss the rampant use of malicious URLs by cybercriminals. They delineate common deception techniques and advocate for adaptive defenses against evolving attack vectors. Discussing detection techniques ranging from blacklist-based too deep learning-based approaches, the paper emphasizes the need for proactive cybersecurity measures. Kahksha Jalal and Sameena Naaz's paper, published in the Department of Computer Science and Engineering, School of Engineering Sciences and Technology et al. [8] focusing on malicious URL detection, stresses the importance of innovative solutions in combating increasing cybercrime. It discusses common features used by detection systems and encourages new research to enhance defense efficacy.

3. Related Tools

In the ever-evolving landscape of cyber threats, a variety of tools have been developed to help organizations and individuals protect their web applications and data. These tools range from phishing simulation platforms to automated vulnerability scanners, each designed to address specific aspects of web security. This section explores some of the widely used tools in the field, detailing their functionalities. GoPhish is a free, open-source tool that helps organizations combat phishing attacks through simulations and training. It allows users to design realistic phishing emails, target specific groups within a company, and launch campaigns to test their susceptibility. GoPhish tracks results, revealing who clicked on suspicious links or entered sensitive information, thereby providing valuable insights for improving organizational awareness and resilience against phishing attacks. [10] Acunetix Web Vulnerability Scanner is an automated security testing tool that helps identify vulnerabilities in web applications. It scans websites and web applications for weaknesses that attackers could exploit to steal sensitive data, such as passwords or credit card information. Acunetix offers comprehensive scanning capabilities, including SQL injection and cross-site scripting (XSS) detection, making it a crucial tool for proactive security management. [11] HTTPS Everywhere is a free browser extension that automatically forces websites to use HTTPS whenever possible. HTTPS, the secure version of HTTP, encrypted communication between your device and the website you are visiting, making it much more difficult for an attacker to eavesdrop on your traffic or steal your data. By ensuring secure connections, HTTPS Everywhere helps protect user privacy and data integrity. [12] NoScript is a popular extension that allows users to selectively enable and disable scripts on websites. This granular control over script execution can prevent malicious scripts

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0390
e ISSN: 2584-2854
Volume: 02
Issue: 08 August 2024
Page No: 2694-2698

from running, potentially thwarting drive-by downloads and other script-based attacks. No Script enhances security by allowing only trusted scripts to execute, thus reducing the attack surface available to malicious actors. [13] X-Frame-Options header is a server-side setting that instructs web browsers on how to handle a page when it is loaded within a frame or iframe. It offers three options: DENY, which prevents the page from being loaded in any frame or iframe; SAMEORIGIN, which allows the page to be loaded in a frame or iframe only if it is on the same domain; and ALLOW-FROM [uri], which permits the page to be loaded in a frame or iframe on a specified domain. This header helps mitigate clickjacking attacks by controlling how content is embedded in frames. [14]

4. Challenges

The objective of this survey paper is to explore the various aspects of protecting online applications from a wide range of cyber threats that researchers, developers, and security practitioners must deal with. Through a thorough analysis of the current literature and the synthesis of insights from various viewpoints, with the aim to obtain knowledge of the challenges that arise in improving web application security. Adaptability to New Threats: Staying ahead of emerging cyber threats requires constant vigilance and rapid adaptation. The capability to integrate new threat intelligence feeds and update detection algorithms accordingly. False Positives/Negatives: Achieving a balance between detecting genuine threats and avoiding false positives/negatives can be challenging. Overly aggressive detection may lead to frequent false alarms, while overly conservative approaches may miss genuine threats. Evasion Techniques: Sophisticated attackers may employ evasion techniques to bypass detection mechanisms, such as obfuscating malicious code or using polymorphic malware. Constantly refining detection techniques to counter evasion tactics is essential.

Conclusion

In conclusion, our survey emphasizes the importance of web applications and their security in modern digital environments. We have examined the complex field of web application security through a thorough examination of numerous research papers, illuminating the wide range of risks and weaknesses present in these online platforms. Our research highlights the strong need of web application security and controls are needed to defend against changing cyberthreats and preserve user privacy and data. We have clarified the intricate interactions between attackers and defenders in the dynamic cybersecurity landscape by combining insights from many research sources, opening the door for well-informed plans and proactive defenses to successfully reduce risks.

References

[1]. S. Akshay Kumar, Y. Usha Rani, “Implementation and analysis of Web application security measures using OWASP Guidelines”, in 2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC), Hyderabad, India, Dec. 28-30,2022.[Online].Available:https://ieeexplore.ieee.org/document/10093657

[2]. Nick Rahimi, “A Study of the Landscape of Security Issues, Vulnerabilities, and Defense Mechanisms in Web Based Applications” in 2021 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, Dec. 15-17 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9799261

[3]. Muhamad Agreindra Helmiawan, Esa Firmansyah; Irfan Fadil, Yanvan Sofivan, Fathoni Mahardika, Agun Guntara, “Analysis of Web Security Using Open Web Application Security Project 10” in 2020 8th International Conference on Cyber and IT Service Management (CITSM), Pangkal, Indonesia, Oct. 23-24 2020.[Online].Available: https://ieeexplore.ieee.org/document/9268856

[4]. Michael A. Ivanov, Bogdana V. Kliuchnikova, Ilya V. Chugunkov, Anna M.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0390
e ISSN: 2584-2854
Volume: 02
Issue: 08 August 2024
Page No: 2694-2698

Plaksina, "Phishing Attacks and Protection Against Them", in 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia, Jan. 26-29 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9396693

[5]. Saleem Raja A, Madhubala R, Rajesh N, Shaheetha L, Arulkumar N, "Survey on Malicious URL Detection Techniques", in 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, Apr. 28-30 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9777221

[6]. Mohammad Alsaffar, Saud Aljaloud, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi, Tariq S. Almurayziq, Gharbi Alshammari and Abdullah Alshammari, "Detection of Web Cross-Site Scripting (XSS) Attacks", in Electronics 2022, 11(14), 2212, Qusay H. Mahmoud, Jul. 2022. [Online]. Available: https://doi.org/10.3390/electronics11142212

[7]. Jean Rosemond Dora and Karol Nemoga, "Ontology for Cross-Site-Scripting (XSS) Attack in Cybersecurity" in J. Cybersecure. Priv. 2021, 1(2), 319-339, Nour Moustafa, May 2021. [Online]. Available: https://doi.org/10.3390/jcp1020018

[8]. Kahksha Jalal and Sameena Naaz, "Detection of phishing website using machine learning approach" in Department of Computer Science and Engineering, School of Engineering Sciences and Technology, New Delhi, Feb. 2021. [Online].Available:https://www.researchgate.net/publication/332573776_Detection_of_phishing_website_using_machine_learning_approach

[9]. Shubham Verma, Kaustubh Giri, Sourabh Kshirsagar, Sheetal Gawande, "Web Application Security using Machine Learning" in International Journal of Engineering Science and Computing (IJESC) May 2022.

[10]. X-Frame-Options header. Available: https://developer.mozilla.org/enUS/docs/Web/HTTP/Headers/X-Frame-Options