# Developing a Comprehensive Web Vulnerability Scanner for Enhanced Cybersecurity

**B.Nirmala,Student, Hyderabad Institute Of Technology And Management, Hyderabad, India, nirmalabigimalla@gmail.com**

**P.Arun,Student, Hyderabad Institute Of Technology And Management, Hyderabad, India, padigemarun123@gmail.com**

**T.Lahari, Student, Hyderabad Institute Of Technology And Management, Hyderabad, India, laharitubati@gmail.com**

**Bhaskar Das, Associate Professor, Hyderabad Institute Of Technology And Management, Hyderabad, India, bhaskardas.cse@hitam.org**

**G. Prabath Vishnu, Student, Hyderabad Institute Of Technology And Management, Hyderabad, India prabhathvishnug@gmail.com**

**SK. Asif, Student, Hyderabad Institute Of Technology And Management, Hyderabad, India, shaikasif.cs@gmail.com**

**Abstract- The research study describes how to improve cybersecurity in web applications by discovering and remedying errors within a complete web vulnerability scanner through its design and implementation. It considers providing an applicable and practical automated security scanning method that enhances features based on open-source tools. The scanner serves the purpose of proactive cybersecurity management; it classifies threats concerning their severity and optimizes operations while generating reportable information. This innovation spans the gap between theoretical vulnerabilities and real-world implementation. As such, it helps create an even safer digital ecosystem.**

***Keywords — Cybersecurity, Web Vulnerability Scanner, Automated Security, Open-Source Tools, Threat Classification, Proactive Management***

## I. INTRODUCTION

The rapid technological evolution has changed how individuals and organizations interact with digital systems, creating a highly interlinked world. This has been very advantageous but also introduced tremendous challenges for cybersecurity as attackers continually look for weaknesses in digital infrastructure. Web applications have become core to modern digital services, underpinning industries such as e-commerce, healthcare, and education. However, their widespread usage and openness make them inviting for cyberattacks. Common issues of SQL injection, cross-site scripting (XSS), and misconfigured systems frequently expose sensitive data and breach operational integrity. This requires proactive security measures where vulnerabilities are detected and mitigated before being exploited by attackers.

In the light of these challenges in cybersecurity, vulnerability scanners have emerged as essential tools for countering these issues. Such tools automatically discover possible vulnerabilities of the web applications and make those insights actionable for an organization for better strengthen its defense lines. Next-generation vulnerability scanners identify vulnerabilities as well as classify them on their critical level of impact so that a remediation action plan may be formulated to tackle security-related threats first. Thus, this kind of tool can create the perfect connection between discovery and eradication that enhances an organization's overall security posture. In an evolving environment, as depicted in today's high-tech digital world, comprehensive real-time analysis capability facilitates the response to emerging threats.

This paper develops an effective and comprehensive web vulnerability scanner. A combination of several open-

 DOI : 10.35291/2454-9150.2024.0417 

source tools is used, along with the integration of each other for the delivery of robust yet efficient security solutions. It's aimed to discover vulnerabilities across different levels in a web application- Network, Server, and even application code. These scanners feature dynamic threat categorization, streamlined workflows, and the generation of detailed reports to allow proper management of vulnerabilities. In addition, the study clearly puts the scanner into perspective for identifying common security challenges facing many organizations and its use as an instrument for strengthening an organization's defenses. This tool reduces the time and resources needed for manual assessments by automating key aspects of vulnerability management, offering a scalable and user-friendly solution to the ever-evolving challenges in cybersecurity.

## II. LITERATURE REVIEW

(Vieira, Antunes, and Madeira 2009)[1] Web services are an essential part of modern business but are often deployed with critical vulnerabilities that can be exploited. This study assessed 300 randomly selected Web services using four popular vulnerability scanners to identify security flaws. Results confirmed a significant number of vulnerabilities, demonstrating inadequate security testing in many services. The study also showed scanner performance variability, with different detection rates and false positives ranging from 35% to 40%, while two scanners showed low coverage below 20%. These findings highlight the limitations of Web vulnerability scanners in identifying threats comprehensively and underscore the need for more robust security assessment practices for Web services.

(Makino and Klyuev 2015)[2] Indeed, in recent years, a lot of web applications have been released in the world. The diffusion of such services has occurred in parallel with increased cyber-attacks on web application vulnerabilities. In such a situation, one would want to increase the security of web applications. However, manual checking of each and every web vulnerability is a very cumbersome and time-consuming process. Thus, it is required to have a web application vulnerability scanner. In this work, we use two open-source vulnerability scanners, OWASP ZAP, and Skip fish, on two vulnerable web applications, DVWA and WAVSEP.

(Rexha et al. 2015)[3] Organizations are increasingly transitioning their daily operations to web-based platforms. This shift highlights the critical need for web developers to be well-versed in security techniques, such as defenses against SQL injection and Cross-Site Scripting (XSS) attacks, to safeguard sensitive data and prevent unauthorized access. This study evaluates the effectiveness of security practices employed by developers to address vulnerabilities in upcoming web applications. Based on practical observations, the research gathered data through surveys on security techniques and conducted penetration tests on over 110 local websites. Numerous vulnerabilities were identified, and the findings were correlated with survey responses for analysis.

(Kumar Singh and Roy 2012)[4] In the digital age, where information is just a click away, web applications play a pivotal role in expanding business operations globally. Most web applications follow a three-tier architecture, with the database at the core—a critical resource for any organization. However, as web applications continue to grow in adoption, they become increasingly vulnerable to threats, including SQL injection attacks, where hackers directly manipulate databases, making this one of the most severe threats. While various vulnerability scanners have been developed to detect such issues, existing tools face challenges such as low accuracy, high false positive rates, and slow scanning processes. To address these limitations, this study introduced a network-based vulnerability scanner that enhances coverage, eliminates false positives, and performs scans efficiently within a shorter timeframe.

(Chen and Wu 2010)[5] With the growing reliance on web applications as fundamental tools, the prevalence of web security issues has risen sharply. Many vulnerabilities, such as SQL injection and Cross-Site Scripting (XSS), stem from basic input validation flaws. Although these vulnerabilities are largely preventable, many web developers fail to prioritize security, leaving numerous websites susceptible to exploitation. To address this, the study implemented an automated vulnerability scanner focused on detecting injection vulnerabilities. The system was designed to identify SQL injection and XSS risks across web applications automatically. During its evaluation, the scanner successfully pinpointed vulnerabilities in multiple websites. The researchers tested the system on seven websites listed in the National Vulnerability Database to validate its effectiveness.

(Al Anhar and Suryanto 2021)[6]This paper discusses the effectiveness of several Web Application Vulnerability Scanners (WAVS) for the detection of vulnerabilities in NodeJS-based web applications, such as Damn Vulnerable NodeJS Application (DVNA) and NodeGoat. The study assesses four WAVS tools: OWASP ZAP, Wapiti, Arachni, and Burp Suite Professional, by obtaining that the highest True Positive (TP) and Recall rates occurred in the case of Burp Suite Professional, whereas the highest Precision was obtained in the case of Arachni. However, the study lacks consistency in the performance of f-measure across these tools; therefore, it leaves grounds for improvement. On the other hand, this paper differs from others because it does not only talk about cyber threat intelligence but considers a wider scope by including aspects beyond vulnerability scanning. It integrates threat analysis with the identified risk mitigation approaches to proactively increase security

 DOI : 10.35291/2454-9150.2024.0417 

awareness within an organization and is in itself more holistic than mere tool-based detection of vulnerabilities.

(P, S, and Srinivas 2023)[7] This paper introduces "CyberCheck," an open-source OSINT and Web Vulnerability Scanner, customizable and developed to suit penetration testers looking for the aspect of transparency and being in control regarding how their target endpoints are being scanned. Built on top of the Python language, CyberCheck can even let testers change several scan parameters ethically and flexibly without relying on third-party tools. This research contributes by offering transparency and customization in OSINT and scanning processes, but it mainly focuses on personal control and workflow optimization for penetration testers. Instead, the unique contribution of this research is to present a comprehensive framework of cyber threat intelligence that incorporates automated threat identification with organizational risk mitigation strategies. This would extend the scope far beyond mere endpoint customization to strategic security, allowing them to act preventively against impending threats, most likely outside of endpoint vulnerabilities.

(Sedaghat, Adibniya, and Sarram 2009)[8] This article focuses on software vulnerabilities and notes that about 70% of newly discovered vulnerabilities monthly are in application software, which is a significant concern for managers. The paper discusses two methods for testing such vulnerabilities: one while still in the development process, suggesting code review using static analysis tools, and one after deployment, using software scanners. A comparison reveals the advantages and disadvantages of the respective scenarios without having to go into technical details. The study will outline testing strategies, but in this case, it does not focus on integrating threat intelligence with vulnerability management. Instead, This research puts together a holistic approach toward cybersecurity by bridging threat intelligence with preemptive and post-deployment defenses, thereby enhancing the proactive risk management framework within an organization.

(Subramanian et al. 2010) [9] The proposed research work introduces a quantitative framework for improving web application vulnerability diagnosis and remediation by integrating confidence metrics from multiple scanners. This framework evaluates vulnerabilities and their variations based on the derived metrics in order to perform prioritized remediation steps for accuracy and reliability. Though the framework enhances the trustworthiness of the diagnostic outcomes, the concentration of the methodology lies in the aggregation of scanner outputs and not in dealing with the dynamically changing nature of cyber threats as a whole. While most such research goes beyond scanner diagnostics to the integrated space of cyber threat intelligence, the research here identifies emerging threats and advises on preventive strategies. In a way, this approach not only helps remediate but also arms any organization with an active defense mechanism in advanced threat defenses.

(Kumar Singh and Roy 2012) [10] It attempts to address the increasing menace of SQL injection attacks on databases that are embedded in the web application, criticizes current vulnerability scanners pertaining to low accuracy, costly false positives, and sluggish scanning rates, and promises a network-based vulnerability scanner with the hope that they can look out for SQLI faster with more accuracy and without false positives. Though implemented to enhance detection capabilities for SQLI, the scope of this methodology is rather narrow-specific improvement in technical performance on a single attack type. This research bridges these individual approaches to an attack vector through the provision of a cyber threat intelligence framework that covers the full spectrum of threats and offers actionable insight into organizational defense. This approach allows organizations to build robust defenses against emerging threats on diverse attack surfaces.

(Alptekin et al. 2020) [11] In this paper, the optimized approach of vulnerability assessment was proposed: accelerating vulnerability detection by scanning the least number possible while arranging security tests based on similarities of web pages, coming from the hypothesis that similar pages may have similar vulnerabilities. These scans considerably cut down the times and reach high predictive accuracy when actual vulnerabilities do appear in the top 8 and 15 predictions 86.9% and 98.4% of the time, respectively. This approach enhances scanning capabilities but remains more focused on technical optimization compared to widely spread security strategies. Conversely, this study brings out the first-ever integration of cyber threat intelligence into a holistic framework of understanding and preemption against a wide range of threats. It enhances the scope for organizations beyond mere vulnerability detection and building resilience against changing scenarios of security challenges.

(Joshi, Raturi, and Kumar 2022) [12] The paper states that third-party attacks on websites and web applications are persistent despite a higher change in their security measures. It points out the need for incorporating SEP from the early development stages, and the increasingly standard practice of VAPT, to provide comprehensive defense. This paper reviews different types of vulnerability analysis tools used in VAPT and analyses their effectiveness at different penetration testing levels. Although this research provides a very good foundation for applying VAPT tools, it remains somewhat tool-based risk management. In contrast, what sets the approach apart here is the holistic cyber threat intelligence framework. This enables a proactive, intelligence-led defense strategy extending further than just

 DOI : 10.35291/2454-9150.2024.0417 

a framework of vulnerability analysis tools to address overall organizational threats organizations

## III. METHODOLOGIES

### A. Methods

This study uses a qualitative research method based on an in-depth literature review and examination of existing knowledge regarding vulnerability scanners. This endeavor pursues understanding functionalities, advantages, and weaknesses in applying vulnerability scanners [13] in cybersecurity practice and their possible application in educational settings. Through a synthesis of available information gathered from credible sources, this methodology attempts to convey elaborate coverage in regard to how effectively vulnerability scanners may be used to identify and deal with security threats.

### B. Research Design

To understand the general trend and current state of the vulnerability scanning technology, the research was designed as a literature-based study on current scholarly papers, industry reports, technical documentation, and case studies related to this topic. All aspects of vulnerability management - scanner capabilities, its integration into network security systems, common challenges, and best practices - were reported in these sources, making them a basis for analyzing how vulnerability scanners apply in practice and how they are used as proactive measures in cybersecurity.

### C. Data Sources and Collection

The literature sources were retrieved from academic databases, online security journals, and reliable web resources. The retrieval process was restricted to government and industry reports. Only those publications that were five years old or less, dealt with vulnerability scanning in the domain of network security, and could be applied for colleges or equivalent organizations were selected. The sources would have to be within the last five years to ensure the data is up-to-date with the current trends in technology and security.

### D. Data Analysis

The literature data were critically reviewed systematically and classified based on themes dealing with the technical features of vulnerability scanners, practical uses, challenges, and current use trends. This thematic review presented an understanding of the strengths and weaknesses of various vulnerability scanning tools and common implementation issues that occurred. Comparison analysis was further conducted to consider some differences in effectiveness across kinds of scanners, say, network-based vs. host-based.

### E. Synthesis of Findings

Such insights from the analysis were synthesized into meaningful conclusions regarding vulnerability scanners' pivotal position in safe and secure networks. Key findings were used to present opportunities for improving special training requirements and incorporating them into educational cybersecurity curricula and draw final conclusions. The conclusions thereby extend actionable recommendations about the formative practices for effective and conscious vulnerability management and cybersecurity awareness within academia.

## IV. IMPLEMENTATION

The Web Vulnerability Scanner (Web Scanner) design would be a complete design involving integrating numerous open-source tools to develop an efficient yet all-inclusive security scan for a web application. This application is developed using Python. Therefore, it is configured to run on Kali Linux, an operating system with preinstalled utilities for network and application analysis. The modular architecture of this tool ensures smooth working and is capable of providing dynamic workflows, real-time feedback, and detailed reports. The Web Scanner performs a preliminary check for the availability of the integrated tools by ensuring that all necessary components are in place before starting a scan.

This pre-check process minimizes the interruption risk during the scanning process. Once operational, the scanner identifies vulnerabilities within the target application and categorizes them based on their severity — critical, high, medium, or low — using color-coded labels. This threat categorization allows users to focus on the most vital issues, making remediation easier. The scanning workflow is also adaptive to the availability of tools and the complexity of the target to ensure flexibility and scalability in usability. The tool integrates several open-source tools, each selected for its specific capabilities in vulnerability scanning. For example, Wapiti is used to identify the vulnerability of SQL injection and XSS.

Nmap helps in finding which ports are open, what service is running on those ports, or even the operating system being used. Tools like Nikto scan for older software versions installed on web servers and for harmful files. Additional tools, such as Dirb, the Harvester, SSL yze, What Web, and Uni scan, complement the scanner by scanning through different types. The user interface is designed to offer real-time feedback with progress indicators. It gives users visual updates during the scanning process.

This makes it interactive, allowing users to skip lengthy tests or dynamically adjust parameters to enhance the user experience. Upon completion of the scan, Web Scanner generates detailed PDF reports that include an executive

 DOI : 10.35291/2454-9150.2024.0417 

summary, the classification of vulnerabilities, and recommendations for remediation. These reports correlate findings with the OWASP Top 10 vulnerabilities, making them actionable insights for security professionals.

The tool has been tested on various web applications, and results have been impressive in terms of efficiency and reliability. The one-click installation makes it simple to deploy, and its light design makes it run smoothly in different environments. The option to replace unavailable tools with suitable alternatives guarantees that scanning continues without interruptions, making this a robust solution for proactive vulnerability management. Future development involves machine learning to improve detection accuracy and predictive analytics for emerging threats, further refining the capabilities of a scanner to remain at the heart of modern cybersecurity frameworks.

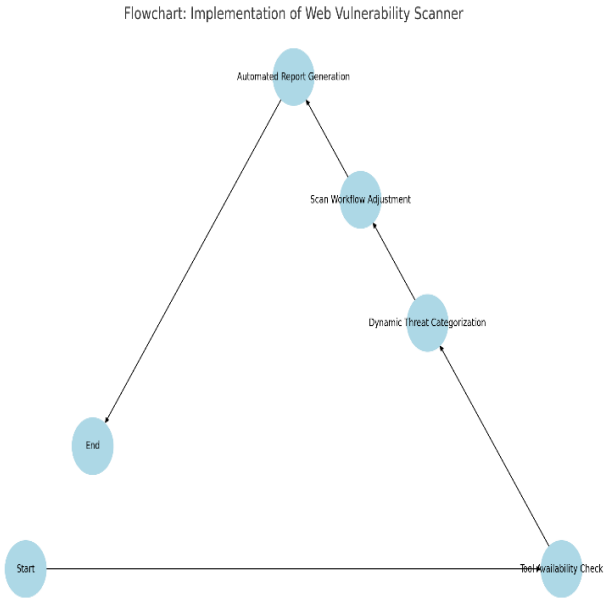


Fig1-Implementation of web vulnerability scanner

## V. MAIN COMPONENTS OF WEB SCANNER

Some important functionality that is contained in implementing Web Vulnerability Scanner, such as Web Scanner, will involve effective and exhaustive security reviews. Some include Tool Availability Checks, which have the role of scanning to first check that all essential free tools that are needed prior to making any scan for their absence are availed.

One of the most essential features of the scanner is its Threat Categorization, which dynamically classifies identified vulnerabilities into critical, high, medium, and low categories. The categorization is further enhanced with color codes to make it easier for security professionals to identify and prioritize critical issues quickly. The scanner also has Process Indicators for the Scan Workflow, which dynamically change based on the availability of tools and the complexity of the target application. Visual feedback such as spinners enhances user experience regarding real-time updates of the long scan process.

Once a scan is done, the Web Scanner provides Automated Reports detailing identified vulnerability analysis, severity level, and recommendable remedial actions. Automating the reports makes it simpler to address the security threat hence helping organizations respond quickly and precisely.

The Web Scanner combines a variety of tools, each chosen for a specific characteristic in vulnerability detection. Tools like Wapiti focus on SQL injection and XSS vulnerabilities, whereas What Web can identify technologies used in web applications, such as CMS platforms and server configurations. Nmap is used in network discovery and security auditing, so it provides information about open ports and operating systems. Golismero specializes in gathering information and finding web vulnerabilities. Uniscan specializes in finding file inclusion vulnerabilities, while Xsser specializes in XSS vulnerabilities.

There are additional tools that improve the scanner in different areas. For example, Dirb scans directory and file names through brute force. theHarvester and Dnsrecon are reconnaissance tools which collect subdomain and DNS-related information. Tools such as SSlyze scan SSL/TLS configurations to ensure that encryption standards are being met, and Nikto identifies outdated software and dangerous files on web servers. Utilities such as Dmitry, **Dnsenum, and **Dnsmap are used for comprehensive subdomain enumeration and mapping in domain-level scans. In addition, Wafw00f identifies web application firewalls, and Amass provides an extensive overview of target infrastructures. These tools collectively form a robust framework, enabling the Web Scanner to provide extensive vulnerability assessments. By incorporating a modular design, the scanner will ensure flexibility, scalability, and efficiency, making it an important tool for modern cybersecurity practice.

## VI. SCANNER AND OUR APPLICATION SCANNER DIFFERENCE

Web vulnerability scanners are essential for identifying and mitigating security flaws in web applications, and significant differences exist between traditional and modern scanners. Traditional scanners have a limited detection scope, focusing primarily on predefined vulnerabilities like SQL injection and cross-site scripting (XSS), whereas modern scanners provide a comprehensive range, including issues like outdated software and misconfigurations. Customization in older tools is restricted to pre-configured scans, while advanced scanners allow highly tailored scanning profiles to suit user needs.

 DOI : 10.35291/2454-9150.2024.0417 

Additionally, traditional scanners often rely on complex or command-line interfaces, making them less user-friendly, whereas modern solutions feature intuitive interfaces designed for ease of use. Scanning speed in older tools is typically slower due to manual configurations, whereas advanced scanners employ automated processes for efficiency. High false positive rates in legacy scanners hinder accuracy, but advanced tools use precise detection techniques to reduce such errors. Report generation has also evolved, with modern scanners providing detailed, actionable recommendations, unlike the basic reports of older systems. Furthermore, while traditional tools require technical expertise, advanced scanners are designed for both technical and non-technical users, ensuring accessibility.

Integration capabilities have also improved, with modern tools seamlessly connecting to various open-source security systems, unlike the limited integration in legacy scanners. Vulnerability classification has advanced from basic risk levels to detailed severity categories with specific remediation steps. Lastly, while traditional scanners are often restricted to specific environments, modern solutions are cross-platform compatible, supporting a wide range of operating systems like Linux and Windows. These advancements underscore the superior functionality and efficiency of modern web vulnerability scanners over their predecessors.

## VII. RESULT

Testing was done on multiple web applications and the following results came forth: A click installation coupled with scanning in one went side by side to minimize the assessment time. Real-time feedback and the skip feature of long tests lift the control of the user reporting: The PDF reports generated included an executive summary, association of the findings with OWASP Top 10, explanation of the vulnerabilities, and remediation guidance all provided a clean, actionable view of each scan Flexibility: On some instances, specific tools couldn't be used. Web Scanner has been flexible enough to deploy additional tools for similar checks in places where specific tools were not available, thus ensuring complete coverage but not.

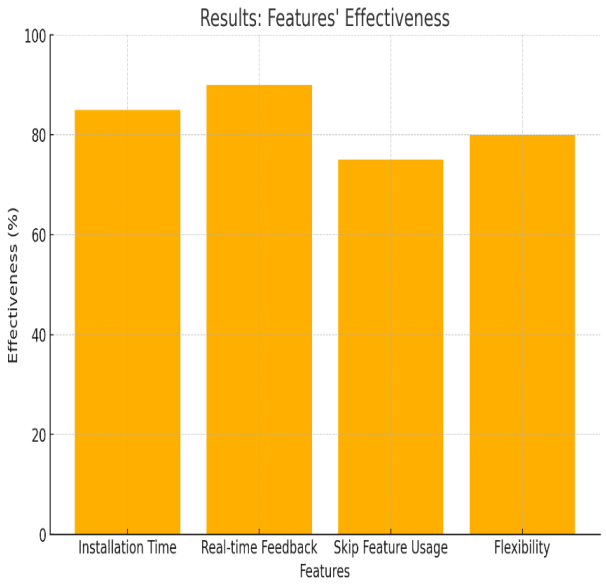


Fig2: Features Effectiveness

## VIII. CONCLUSION

Web Scanner is an all-in-one vulnerability assessment tool that has several open-source security tools built into it so users can get an all-around analysis of web applications and networks. With its friendly interface and one-click installation, it offers streamlined solutions for pinpointing and then classifying the vulnerabilities at one time, which would cut down on the time and resources that could be expended by security professionals on accomplishing their mission. It contains different tools for the firewall regarding applications on a website, detection of CMS, SSL checks, DNS vulnerabilities and injection attacks that detail across many categories of threats.

Due to its severity-based classification, along with features offering clear reporting, Web Scanner provides users with an option to prioritize critical issues. Each vulnerability, in this case, is described and shown how to remedy it. Its real-time feedback, skip options, and lightweight operation make it very versatile in scanning environments. Although this dependence on open-source tools restricts some of the advanced threat detection, efficient design, and mitigation of false positives make Web Scanner a useful tool in proactive vulnerability management. As future iterations evolve to include machine learning and targeted tool deployment, Web Scanner will have enormous potential to become the norm in web security assessments for use by users to protect applications against this ever-evolving landscape of cyber threats.

 DOI : 10.35291/2454-9150.2024.0417 

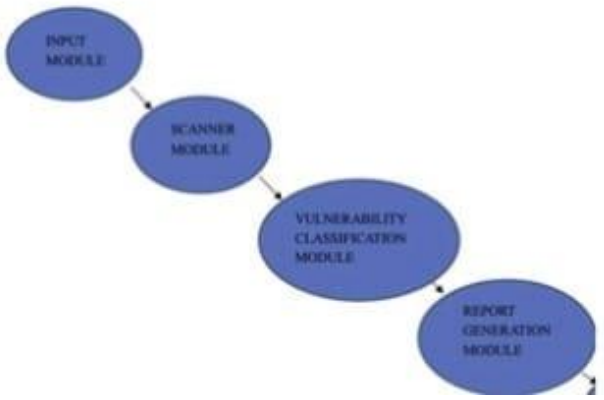


Fig3: Scanning process of vulnerability scanner

## REFERENCES

1. Al Anhar, Azwar, and Yohan Suryanto. 2021. "Evaluation of Web Application Vulnerability Scanner for Modern Web Application." Pp. 200–204 in *2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST)*. Yogyakarta, Indonesia: IEEE.

2. Alptekin, Halit, Simge Demir, Sevval Simsek, and Cemal Yilmaz. 2020. "Towards Prioritizing Vulnerability Testing." Pp. 672–73 in *2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. Macau, China: IEEE.

3. Chen, Haibo, Junzuo Chen, Jinfu Chen, Shang Yin, Yiming Wu, and Jiaping Xu. 2020. "An Automatic Vulnerability Scanner for Web Applications." Pp. 1519–24 in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. Guangzhou, China: IEEE.

4. Chen, Jan-Min, and Chia-Lun Wu. 2010. "An Automated Vulnerability Scanner for Injection Attack Based on Injection Point." Pp. 113–18 in *2010 International Computer Symposium (ICS2010)*. Tainan, Taiwan: IEEE.

5. Joshi, Ashish, Aditya Raturi, and Santosh Kumar. 2022. "An Analysis of Vulnerability Scanners in Web Applications for VAPT." Pp. 278–83 in *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*. Greater Noida, India: IEEE.

6. Kumar Singh, Avinash, and Sangita Roy. 2012. "A Network Based Vulnerability Scanner for Detecting SQLI Attacks in Web Applications." Pp. 585–90 in *2012 1st International Conference on Recent Advances in Information Technology (RAIT)*. Dhanbad, India: IEEE.

7. Makino, Yuma, and Vitaly Klyuev. 2015. "Evaluation of Web Vulnerability Scanners." Pp. 399–402 in *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. Warsaw, Poland: IEEE.

8. Mburano, Balume, and Weisheng Si. 2018. "Evaluation of Web Vulnerability Scanners Based on OWASP Benchmark." Pp. 1–6 in *2018 26th International Conference on Systems Engineering (ICSEng)*. Sydney, Australia: IEEE.

9. P, Shamunesh, Vinoth S, and L. N. B. Srinivas. 2023. "Cybercheck – OSINT & Web Vulnerability Scanner." Pp. 275–79 in *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*. Namakkal, India: IEEE.

10. Rexha, Blerim, Arbnor Halili, Korab Rrmoku, and Dren Imeraj. 2015. "Impact of Secure Programming on Web Application Vulnerabilities." Pp. 61–66 in *2015 IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS)*. Bhubaneshwar, Odisha, India: IEEE.

11. Sedaghat, Shahrzad, Fazlollah Adibniya, and MehdiAgha Sarram. 2009. "The Investigation of Vulnerability Test in Application Software." Pp. 1–5 in *2009 International Conference on the Current Trends in Information Technology (CTIT)*. Dubai, United Arab Emirates: IEEE.

12. Subramanian, Deepak, Ha Thanh Le, Peter Kok Keong Loh, and Annamalai Benjamin Premkumar. 2010. "Quantitative Evaluation of Related Web-Based Vulnerabilities." Pp. 118–25 in *2010 Fourth International Conference on Secure Software Integration and Reliability Improvement Companion*. Singapore, Singapore: IEEE.

13. Vieira, Marco, Nuno Antunes, and Henrique Madeira. 2009. "Using Web Security Scanners to Detect Vulnerabilities in Web Services." Pp. 566–71 in *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*. Lisbon, Portugal: IEEE.

 DOI : 10.35291/2454-9150.2024.0417 