INTEGRISCAN - A HIGH THROUGHPUT MULTI-SCANNER ECOSYSTEM FOR RAPID CYBER VULNERABILITY ANALYSIS

S Maruthuperumal, Thoram Sri Vidhya, Thati Shashi Vardhan, Thummanapally Shalini,

Thummanapally Rajashekar

Professor(CSE), UG Scholar, UG Scholar, UG Scholar, UG Scholar

Computer Science & Engineering

Bharath Institute of Higher Education and Research (BIHER)

Chennai, Tamil Nadu, India

Abstract : Cyberattacks are becoming increasingly common, and manual vulnerability assessments are becoming time-consuming and ineffective. IntegriScan overcomes this difficulty to automate vulnerability detection through a single framework that integrates multiple scanners. The framework scans networks, web applications, and databases across layers to expose threats such as SQL injection, cross-site scripting (XSS), and configuration errors. It includes various preprocessing techniques for data cleaning, normalization and analysis that ensure the accuracy of inputs before evaluation. With the rule-based detection algorithm, vulnerabilities are scanned, identified and classified according to their severity levels, including remediation hints. Regular scanning also strengthens security by ensuring that additional current threats are corrected immediately, minimizing errors while maximizing speed and accuracy.

IndexTerms **- Vulnerability Detection, Multi-Scanner Integration, Cybersecurity, Rule-Based Algorithm, Continuous Scanning**

I. INTRODUCTION

The rapid advancement of digital technologies has led to the widespread adoption of interconnected systems, including web applications, enterprise networks, databases, and cloud infrastructures. While this digital transformation enhances operational efficiency and scalability, it also significantly increases the attack surface for cyber threats. Vulnerabilities such as SQL injection, cross-site scripting (XSS), insecure configurations, and software flaws continue to be major causes of security breaches and data compromise [1], [10], [11]. Vulnerability detection has therefore become a critical component of modern cybersecurity strategies. Traditional vulnerability scanning tools are widely used to identify security weaknesses in systems before they can be exploited. Several studies have analysed different scanning tools and methodologies, highlighting their importance in proactive security assessment [11], [9]. However, these tools often operate in isolation and focus on specific domains such as web applications, networks, or databases, limiting their overall effectiveness [7], [13].

Existing research has explored various techniques for vulnerability detection, including static analysis, dynamic analysis, and pattern-based approaches. Pereira [5] emphasized the need for combining multiple detection techniques to improve accuracy and reduce false positives. Similarly, Cheng et al. [14] proposed pattern-driven approaches for automated vulnerability detection, while Li et al. [12] introduced integrated testing platforms to evaluate multiple detection methods. Despite these advancements, individual techniques still face challenges in handling complex and large-scale systems[16]. Recent studies have highlighted the advantages of automation and integration in vulnerability detection. Seara and Serrão [4] demonstrated that automated security tools can significantly improve efficiency and usability. Polónio et al. [3] proposed an automated framework integrating detection and mitigation capabilities, while Jain and Jain [2] introduced multi-threaded frameworks to enhance scanning performance. Additionally, Abdulghaffar et al. [1] showed that combining multiple vulnerability scanners can improve detection coverage and accuracy.

Comprehensive surveys and reviews further indicate that existing vulnerability detection methodologies suffer from limitations such as high false positive rates, incomplete coverage, and lack of real-time analysis [6], [16]. Chalvatzis et al. [9] demonstrated that individual scanners fail to provide a complete view of system security, emphasizing the need for integrated solutions. Moreover, domain-specific tools such as SQL injection detection systems [10] and network-based assessment tools [13] are effective only within limited scopes. Although several integrated and automated approaches have been proposed, many of them still face challenges related to scalability, continuous monitoring, result correlation, and ease of deployment in dynamic environments [3], [6]. Most existing solutions remain fragmented, requiring manual intervention and lacking a unified platform for comprehensive vulnerability assessment.

To address these limitations, this paper proposes IntegriScan, a high-throughput multi-scanner ecosystem designed for rapid and comprehensive cyber vulnerability analysis. The proposed framework integrates multiple security scanning tools into a unified platform, enabling cross-layer vulnerability detection across network, web, and database domains. By incorporating automation, parallel execution, and rule-based correlation, IntegriScan aims to improve detection accuracy, reduce false positives, and enhance overall security assessment efficiency.

II. RELATED WORK

Vulnerability detection has been extensively studied in the cybersecurity domain, with researchers proposing various automated scanning and analysis techniques to improve detection accuracy and coverage. Existing literature highlights both the strengths and limitations of current vulnerability assessment approaches.

Abdulghaffar et al. [1] proposed an automated penetration testing framework that integrates multiple web vulnerability scanners to improve detection accuracy. Their approach demonstrated that combining results from different tools significantly enhances vulnerability coverage while reducing false negatives.

Trapti Jain and Nakul Jain [2] developed a multi-threaded vulnerability scanning framework that integrates multiple scanners into a single system. Their work highlighted the benefits of parallel execution in reducing scanning time and improving efficiency.

Polónio et al. [3] introduced an automated cybersecurity framework that integrates detection, classification, and mitigation of vulnerabilities using software-defined networking and orchestration techniques. Their system demonstrated improved scalability and proactive threat mitigation.

Seara and Serrão [4] proposed an automated vulnerability detection system using open-source tools. Their study emphasized the importance of automation in simplifying security audits and improving usability for non-expert users.

Pereira [5] explored advanced techniques for software vulnerability detection, focusing on combining multiple analysis approaches to improve detection rates while reducing false positives.

Bennouk et al. [6] presented a comprehensive survey of vulnerability detection methodologies, highlighting key challenges such as data inconsistency, high false positive rates, and limitations of existing approaches.

Chen et al. [7] developed an automatic web vulnerability scanner that integrates information gathering with vulnerability detection, improving scanning coverage and effectiveness.

Aldea et al. [8] proposed an integrated vulnerability management system that combines detection, analysis, and reporting within a unified platform, enhancing overall security management.

Chalvatzis et al. [9] evaluated various vulnerability scanners and demonstrated that individual tools often fail to provide complete security coverage, emphasizing the need for integrated solutions.

Zhang and Guo [10] focused on SQL injection detection methods and developed a specialized tool that achieves high accuracy in detecting database-related vulnerabilities.

Despite these advancements, the existing body of work indicates that many current solutions remain fragmented, domain-specific, or difficult to scale in real-world. These limitations motivate the development of a unified, high-throughput multi-scanner framework such as the proposed IntegriScan system.

III.PROPOSED WORK

To overcome the challenges identified in existing studies, this work proposes IntegriScan, a unified multi-scanner framework for vulnerability assessment. The primary objective of IntegriScan is to integrate multiple open-source security scanners into a single platform to provide comprehensive and accurate security analysis. Unlike traditional tools that focus on specific domains or require manual configuration, IntegriScan offers an automated, scalable, and user-friendly solution for vulnerability detection. The proposed system is based on the following key components:

a. **Multi-Engine Integration:** IntegriScan integrates multiple widely used security scanners, including Nmap for network analysis, Nikto and Wapiti for web vulnerability detection, SQLMap for database security testing, and SSLScan for cryptographic assessment. This integration enables broader vulnerability coverage compared to standalone tools.

b. **Result Correlation and Prioritization:** The system correlates outputs from all integrated scanners and applies a severity-based evaluation model using CVSS scoring. This approach reduces duplicate findings, minimizes false positives, and prioritizes vulnerabilities based on their impact and urgency.

c. **Automation:** IntegriScan automates the entire scanning process and supports parallel execution of multiple scanners. This significantly reduces scanning time and enables continuous security monitoring in line with modern enterprise security requirements.

d. **Usability and Reporting:** In order to make it easier to use, IntegriScan provides an easy command line interface with automatically generated reports in formats such as CSV, JSON and PDF. This design makes it easier for clients to interpret and share the findings at the same time, which emphasized the improvement of tool usability.

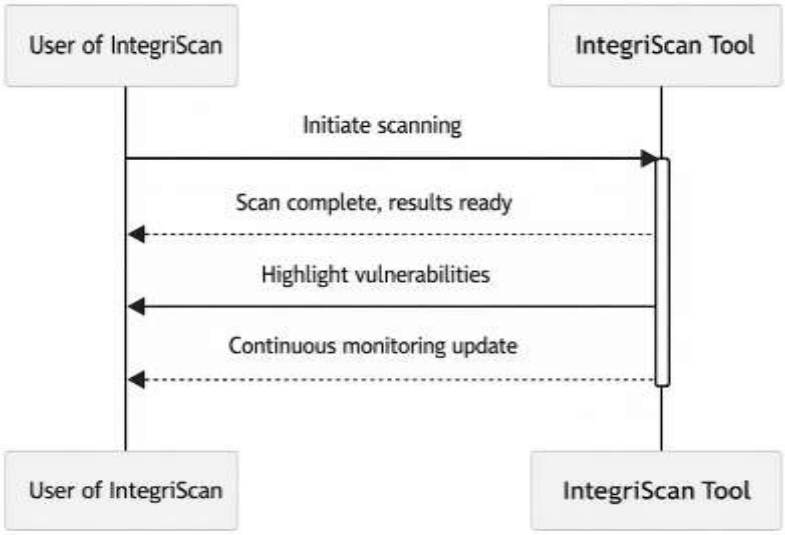

Fig. 1 User Interface of a High Throughput Multi-Scanner Ecosystem

As illustrated in Fig. 1, the user interface enables seamless interaction between the user and the vulnerability scanning system. The user initiates the scanning process, after which the system performs automated analysis and presents the results by highlighting detected vulnerabilities. Additionally, the interface supports continuous monitoring, ensuring sustained security awareness and real-time tracking of potential threats

IV.DESIGN AND METHODOLOGY OF THE INTEGRISCAN FRAMEWORK

IntegriScan's design is based on modular and layered architectures to ensure flexibility, scalability and seamless integration of several vulnerability scanners. Each module is responsible for a specific stage within the workflow, starting with the user's input and ending with the appropriate vulnerability testing. The entire method is divided into important phases.

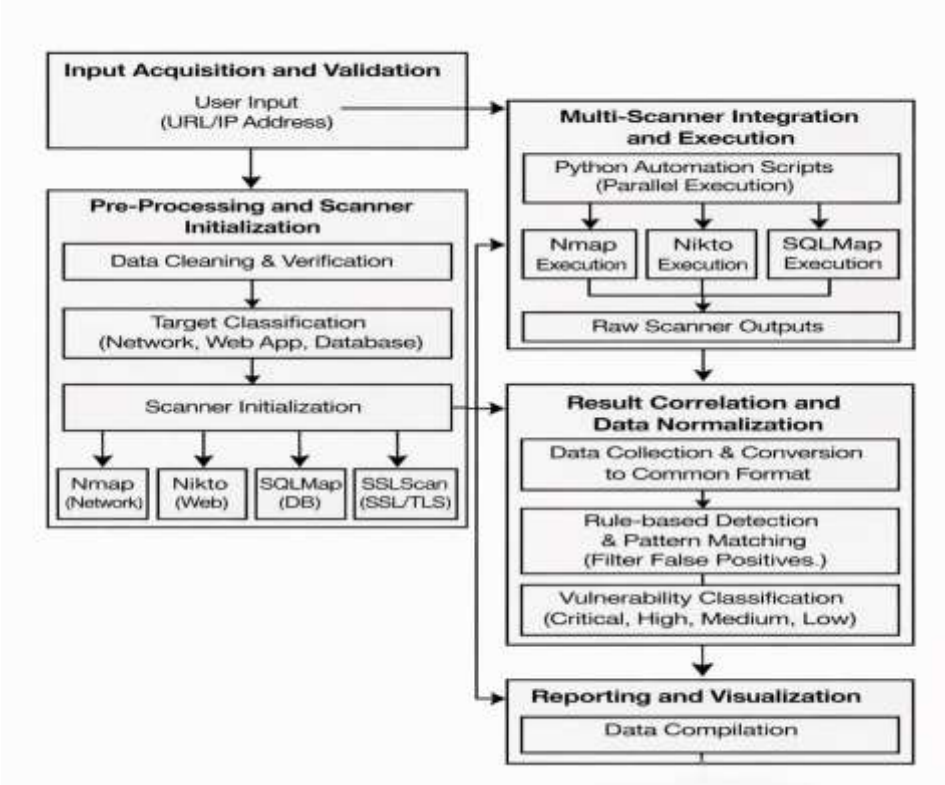

Fig. 2 Workflow Architecture of the IntegriScan Vulnerability Assessment Framework.

As shown in Fig. 2, the IntegriScan architecture enables comprehensive vulnerability detection through continuous scanning. The framework integrates several security tools to identify vulnerabilities and generate actionable insights, thus improving overall system security.

A. Input Acquisition and Validation:

The system starts when the user provides a target input with an Internet application URL or system IP address. The system then validates the input to ensure that it is very accurate in format and safe to test. This step prevents errors and ensures that the most valid objectives are analyzed by the scanner.

B. Pre-Processing and Scanner Initialization:

In this stage, the system prepares the input information with the aim of cleaning and verifying it. It determines whether the goal belongs to a network, web application or database. Once labeled, the framework initializes the corresponding scanners — which include Nmap for community scanning, Nikto for internet vulnerabilities, SQLMap for database protection, and SSLScan for SSL/TLS scanning.

C. Multi-Scanner Integration and Execution:

The scanner is incorporated using Python automation scripts. All scanner can be performed in parallel through the Python subprocess library, allowing faster and more efficient scanning. Every scanner performs its specific task and produces structured outputs that could be collected by the system.

D. Result Correlation and Data Normalization:

After scanning, the results of all systems are collected and converted into a common layout. This level helps eliminate the duplicate or irrelevant conclusions and filters out false positives. With the help of rule-based detection algorithm and pattern matching, vulnerabilities are then characterized according to their severity levels, which consist of vital, high, medium or low.

Algorithm: Multi-Scanner Vulnerability Correlation
Input: Scanner outputs S = {S1, S2, S3…Sn}
Output: Prioritized vulnerability report
Step 1: Collect outputs from all scanners
Step 2: Convert outputs to normalized format
Step 3: Identify duplicate vulnerabilities
Step 4: Apply rule-based filtering
Step 5: Assign severity using CVSS score
Step 6: Rank vulnerabilities based on severity
Step 7: Generate final report

E. Reporting and Visualization:

In the final phase, all related data is compiled into clean and established reports. The system generates reviews in unique formats, making them easy to share and review. These reports help organizations assess their security posture and take immediate action to address critical vulnerabilities.

V.EXPERIMENTAL RESULTS

The proposed IntegriScan framework has been tested on special web packages and network systems to measure its universal performance, accuracy and speed. The experiments were conducted in the Linux environment, using Python 3.10, and integrated scanners including Nmap, Nikto, SQLMap and SSLScan. For the tests, multiple URLs and local IP addresses have been used as inputs to verify the effectiveness with which the system can discover different vulnerabilities such as SQL injection, cross-website scripting (XSS), SSL/TLS configuration problems and open network ports.

The results confirmed that IntegriScan is capable of effectively locating a wide variety of vulnerabilities in multiple layers of the target environment. The integration of multiple scanners provides a wider coverage and higher accuracy than the use of a single system.

In addition, the rule-based correlation technique contributed to limiting false positives, ensuring that the problems suggested were more reliable and applicable, the system also tested a significant improvement in performance due to its parallel scanning approach, which reduced the overall scanning time by approximately 40–50% compared to sequential scanning. The generated reports labelled the vulnerabilities detected as critical, high, medium and low levels, giving customers a clear and prepared view of security risks.

Evaluation Metrics:
Detection Accuracy = (TP + TN) / (TP + TN + FP + FN)
False Positive Rate = FP / (FP + TN)
Performance Gain = Sequential Scan Time / Parallel Scan Time

Table I. Comparison of Vulnerability Assessment Tools

Tools/ Framework	Detection Accuracy	False Positives	Average Scan Time(min)	Vulnerability Coverage
Nmap	**72%**	**12%**	**8.2**	**Network-based only**
Nikto	**68%**	**15%**	**10.5**	**Web server only**
Wapiti	**74%**	**11%**	**12.1**	**Web app Vulnerabilities**
SQLMap	**80%**	**9%**	**14.3**	**Database Injections**
SSLScan	**77%**	**10%**	**6.7**	**SSL/TLS only**
IntegriScan	**91%**	**5%**	**15.2**	**Comprehensive (Network + Web + DB + SSL/TLS)**

TABLE I provides a comprehensive comparative analysis of the proposed IntegriScan framework against five industry-standard security tools: Nmap, Nikto, Wapiti, SQLMap, and SSLScan. The evaluation is based on four key metrics: Detection Accuracy, False Positive rate, Average Scan Time, and Vulnerability Coverage.

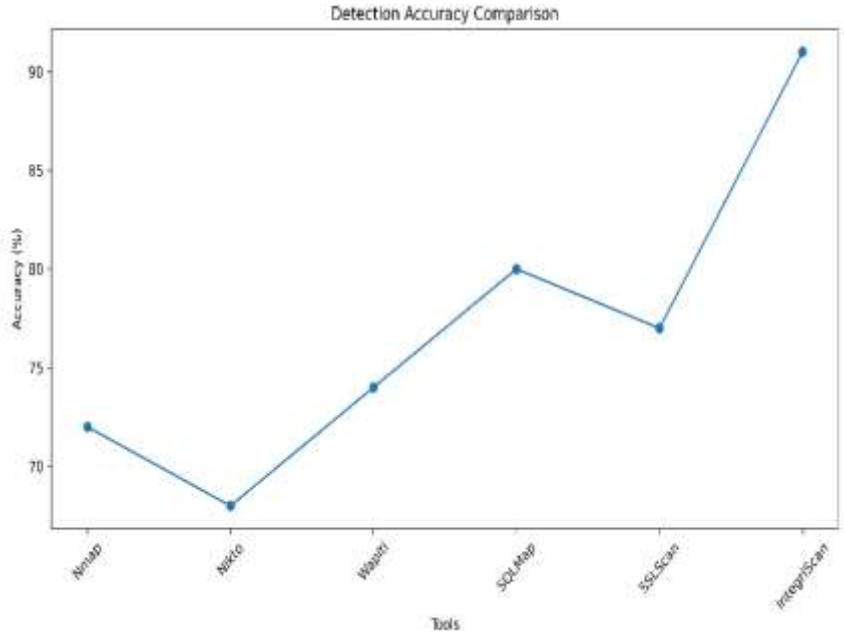

FIG. 3. Comparative Analysis of Detection Accuracy Across Various Security Scanning Tools

The experimental results, as illustrated in Fig. 3, provide a comparative performance metric of the proposed IntegriScan framework against established tools such as Nmap, Nikto, Wapiti, SQLMap, and SSLScan. The graph indicates that:

1. Baseline Performance: Traditional tools exhibit detection accuracies ranging between 68% and 80%.
2. Leading Competitors: SQLMap shows a peak accuracy of 80% among the existing tools, followed by SSLScan at approximately 77%.
3. Proposed System: The IntegriScan framework demonstrates measurable improvement in controlled testing with a detection accuracy of approximately 91%, outperforming the nearest competitor by a margin of 11%.

This improvement can be attributed to the integrated orchestration discussed in the workflow. Also, the reduced false positive rate indicates improved precision and more accurate vulnerability classification. Lower misclassification minimizes unnecessary alerts and reduces analyst workload, enhancing the overall reliability of the proposed framework. These results demonstrate that IntegriScan shows better detection performance.

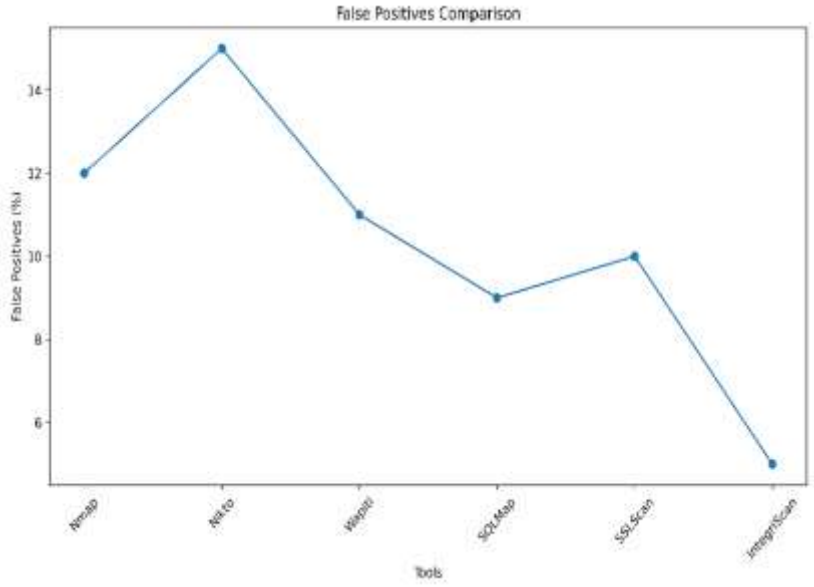

FIG. 4. Comparative Analysis of False Positive Rates Among Evaluation Tools

Fig. 4 illustrates the comparative False Positive (FP) rates of various scanning tools. A critical metric for any security framework is the minimization of false alarms to reduce manual verification overhead.

1. High Variance in Existing Tools: Conventional tools like Nikto and Nmap demonstrate higher FP rates, peaking at 15% and 12% respectively.
2. Optimized Performance: The proposed IntegriScan framework shows a significant reduction in false positives, achieving a low of 5%.

This 50%–60% reduction compared to standard tools proves that IntegriScan's rule-based algorithm and continuous scanning logic effectively filters out non-critical or incorrect detections, ensuring higher reliability in production environments.

Experimental Setup:

The experiments were conducted on Ubuntu Linux environment with Python 3.10. The system was evaluated using vulnerable test applications including DVWA and intentionally vulnerable local servers.

Overall, the results demonstrate that the proposed framework shows better precision and operational robustness compared to existing tools, thereby strengthening its applicability in real-world cybersecurity deployments.

VI. CONCLUSION

This study presented IntegriScan, a multi-engine vulnerability scanning framework designed to address the limitations of current commercial and open-source tools. IntegriScan integrates network, web and database scanners into a unified framework, ensuring comprehensive security coverage in multiple layers of an organization's IT infrastructure. The inclusion of automated correlation of results and severity-based priority mechanisms significantly reduces false positives and false negatives, allowing security teams to focus on high-impact vulnerabilities and improve remediation efficiency.

Experimental evaluations were carried out in controlled environments, including DVWA, custom vulnerable servers and SQL-based database systems. The results show that IntegriScan has achieved high detection accuracy while maintaining efficient scanning performance and continuous monitoring capabilities. Compared to independent tools, the proposed framework showed clear advantages in terms of automation, centralized management, usability and scalability. The multi-engine integration approach has enabled a wider vulnerability coverage without extensive manual intervention.

In addition, the continuous scanning mechanism has contributed to the progressive identification of vulnerabilities over time and validates the effectiveness of proactive surveillance in dynamic environments. The framework has also simplified vulnerability reporting and analysis, reduced operational complexity, and improved overall security posture. Although current implementations focus primarily on web, network and database infrastructures, future work may expand the framework to support cloud-based architectures, IoT ecosystems and containerized environments. Furthermore, the integration of machine learning-based anomaly detection and real-time adaptive scanning technology could further improve the detection of intelligence and system response.

In summary, IntegriScan provides a scalable and efficient solution for integrated vulnerability management, bridging the gap between existing tools and real-world security needs.

REFERENCES

[1] K. Abdulghaffar, N. Elmrabit, and M. Yousefi, "Enhancing web application security through automated penetration testing with multiple vulnerability scanners", Computers, vol. 12, no. 11, p. 235,2023, Doi: 10.3390/computers12110235.
[2] T. Jain and N. Jain, "Framework for web application vulnerability discovery and mitigation by customizing rules through ModSecurity",In Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN), 2019,pp. 643–648.
[3] J. Polónio, J. Moura, and R. N. Marinheiro, "Toward automatic detection and mitigation of high-risk cybersecurity vulnerabilities at networked systems", IEEE Access, vol. 13, pp. 181957–181976,2025, Doi: 10.1109/ACCESS.2025.3622497.
[4] J. P. Seara and C. Serrão, "Automation of system security vulnerabilities detection using open-source software", Electronics,vol. 13, no. 5, p. 873, 2024, Doi: 10.3390/electronics13050873.
[5] J. D. Pereira, "Techniques and tools for advanced software vulnerability detection", in Proc. 2020 IEEE Int. Symp. Softw. Rel.Eng. Workshops (ISSREW), 2020, pp. 123–126, Doi:10.1109/ISSREW51248.2020.00049.
[6] K. Bennouk, N. Ait Aali, Y. El Bouzekri El Idrissi, B. Sebai, A. Z.Faroukhi, and D. Mahouachi, "A comprehensive review and assessment of cybersecurity vulnerability detection methodologies",J.Cybersecur. Priv., vol. 4, pp. 853–908, 2024, Doi :10.3390/jcp4040040.
[7] H. Chen, J. Chen, J. Chen, S. Yin, Y. Wu, and J. Xu, "An automatic vulnerability scanner for web applications", In Proc. 2020 IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom), 2020, pp. 1519–1524, Doi: 10.1109/TrustCom50675.2020.00207.
[8] M. Aldea, D. Gheorghică, and V. Croitoru, "Software vulnerabilities integrated management system", In Proc. 2020 IEEE Int. Symp.Softw. Rel. Eng. Workshops (ISSREW), 2020, pp. 97–102.
[9] I. Chalvatzis, D. A. Karras, and R. C. Papademetriou, "Evaluation of vulnerability scanners for small and medium enterprises business networks resilience towards risk assessment," in Proc. Int. Conf.Information, Intelligence, Systems and Applications (IISA), 2019.
[10] T. Zhang and X. Guo, "Research on SQL injection vulnerabilities and its detection methods", in Proc. 2020 4th Annu. Int. Conf. Data Sci. Bus. Anal. (ICDSBA), 2020, pp. 251–254, Doi:10.1109/ICDSBA51020.2020.00071.
[11] A. I. Mohaidat and A. Al-Helali, "Web vulnerability scanning tools:A comprehensive overview, selection guidance, and cyber security recommendations", Int. J. Res. Stud. Comput. Sci. Eng. (IJRSCSE),vol. 10, no. 1, pp. 8–15, 2024, Doi: 10.20431/2349-4859.1001002.
[12] J. Li, J. Chen, M. Huang, M. Zhou, L. Zhang, and W. Xie, "An integration testing platform for software vulnerability detection method", in Proc. 2017 IEEE Trustcom/BigDataSE/ICESS, 2017,pp. 984–989, Doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.341.
[13] Q. Guo, P. Xie, F. Li, X. Guo, Y. Li, and L. Ma, "Research on linkage model of network resource survey and vulnerability detection in power information system", in Proc. 2019 IEEE 3rd Int. Conf. Inf.Technol., Netw., Electron. Autom. Control (ITNEC), 2019, pp.1068–1071.
[14] S. Cheng, J. Wang, J. Wang, J. Yang, and F. Jiang, "PDVDS: A pattern-driven software vulnerability detection system", in Proc.2010 IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput. (EUC),2010, pp. 536–541, Doi: 10.1109/EUC.2010.88.
[15] M. A. Aarya, A. Rajan, K. P. S. Sachin, and R. Gopi, "Web scanning:Existing techniques and future," in Proc. Int. Conf. Intelligent Computing and Control Systems (ICICCS), 202
[16] A. Ben Said, A. Lahami, and M. Abid, "Dynamic vulnerability detection approaches and tools: State of the art," in Proc. IEEE Int.Conf. Software Engineering and Applications (ICSEA), 2020.