A Systematic Review on Unified Reconnaissance and Vulnerability Assessment

Ashith Rajeev[1], B Harikeerthana[2], B Haritheertha[3], Muhammed Musthafa[4], Sr Reema Jose[5]
Department of Computer Science Cyber Security Vimal Jyothi Engineering College Chemperi, Kannur

***Abstract*—The discussed research centers on the improvement of Vulnerability Assessment and Penetration Testing (VAPT) as a process-oriented technique for identifying and addressing security vulnerabilities in networks, web applications, and operating systems. The focus is on the comparison of open-source and commercial penetration testing tools in terms of detection efficacy, false positive and negative detection, ease of use, scalability, and cost efficiency. Framework-based approaches are brought into the forefront for their potential to deliver organized, repeatable, and compliant test processes that enhance reporting and standardization in enterprise environments. Progress in areas of automation and machine learning is also discussed to facilitate smarter vulnerability detection, intelligent risk prioritization, and minimizing manual effort. Special focus is provided for web application vulnerabilities in line with OWASP Top 10 threats such as SQL injection, cross-site scripting (XSS), insecure session management, and misconfigurations. Experimental studies and case validations prove the usability and effectiveness of these methods in both simulated and real environments. Generally, the results reflect a shift away from solitary testing methods towards total, adaptive, and intelligent VAPT processes that present increased resistance against the ever-changing panorama of cyber-attacks.**

I. INTRODUCTION

The expanding reliance on web applications and networked environments has transformed cybersecurity into an essential research and practice field. Of the numerous methods used to protect systems, Vulnerability Assessment and Penetration Testing (VAPT) stands out as a key tool for discovering and preventing risks before they can be exploited. Past research has covered various facets of penetration testing ranging from the identification of SQL injection attacks against web applications to the comparative analysis of penetration testing tools under Linux operating systems, citing the advantages of opensource solutions in maintaining cost-effectiveness without loss of dependability.

Case studies of government websites have also been researched, highlighting the need to protect vital information infrastructure from increasingly sophisticated cyber-attacks.

Furthermore, the use of footprinting and reconnaissance methods has been researched extensively, as these initial steps reveal useful information about system weaknesses but also present ethical and juridical issues. A number of studies have contrasted penetration testing frameworks and methodologies, providing controlled strategies for organizations to undertake systematic security testing. Together, the body of work illustrates that although discrete tools and approaches help mitigate particular vulnerabilities, a comprehensive strategy integrating assessments, penetration testing, and robust security frameworks is necessary. This review synthesizes these contributions to provide an integrated awareness of existing penetration testing methodologies, point to critical issues, and provide direction for further research.

II. A SYSTEMATIC LITERATURE REVIEW

A. Research Methodology

This systematic literature review adopts a structured approach to identify, analyze, and classify studies related to Vulnerability Assessment and Penetration Testing (VAPT). The review process was conducted in several steps to ensure comprehensiveness and reliability.

1) Research Design: Relevant studies were searched using keywords such as “Vulnerability Assessment and Penetration Testing (VAPT),” “penetration testing tools,” “cybersecurity assessment,” “OWASP vulnerabilities,” and “machine learning in penetration testing.” Searches were conducted across reputable digital libraries, including IEEE Xplore, Springer, ACM Digital Library, ScienceDirect, and Google Scholar. *2) Inclusion Criteria:*

- Papers focusing on VAPT methodologies, penetration testing frameworks, and security evaluation tools.
- Studies proposing or implementing machine learning or intelligent agent-based solutions for vulnerability detection.
- Articles addressing OWASP Top 10 vulnerabilities, operating system security, and network/IoT penetration testing.
- Publications from peer-reviewed journals, conferences, or workshops between 2014–2024.

3) Exclusion Criteria:

- Research unrelated to vulnerability assessment, penetration testing, or system security.
- Papers lacking technical or experimental contributions.
- Duplicated studies or those with incomplete data.
- Non-peer-reviewed sources such as blogs, magazines, or non-academic reports.

4) Reviewed Papers: The following 15 papers were selected for detailed review:

1) Lamba (2014). *Cyber Attack Prevention Using Vulnerability Assessment and Penetration Testing Tools* [10].

2) Goel & Mehtre (2015). *Vulnerability Assessment and Penetration Testing as a Cyber Defence Technology* [7].

3) Gurline & Gurpreet (2016). *Penetration Testing: Attacking Oneself to Enhance Security* [8].

4) Bhingardeve & Franklin (2018). *Comparison Study of Open-Source Penetration Testing Tools* [4].

5) Zachariah & Roy (2019). *Comparison Study of Penetration Testing Tools in Linux* [15].

6) Jasper, Amritha & Sethumadhavan (2020). *Penetration Testing on WPA2* [9].

7) Almaarif & Lubis (2020). *VAPT Framework: Case Study of Government's Website* [2].

8) Bhatia . (2021). *Vulnerability Assessment and Penetration Testing (VAPT)* [3].

9) Alanda . (2021). *Web Application Penetration Testing Using SQL Injection Attack* [1].

10) Kek & Selvarajah (2022). *Footprinting and Reconnaissance: Impact and Risks* [13].

11) Fatima . (2023). *Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat* [6].

12) Softic & Vejzovi´ c (2023).´ *Impact of VAPT on Operating System Security* [14].

13) Shehab (2024). *Improving Port Scan Cybersecurity Risks Detection Using Machine Learning* [12].

14) Sakthivel (2024). *Ensuring Web Application Security: An OWASP Driven Development Methodology* [11].

15) Fasha . (2024). *Mitigating the OWASP Top 10 for LLM Applications Using Intelligent Agents* [5].

Refer table 1 shows, summarizing the evaluation criteria used across the reviewed studies, which compares their methodologies, datasets and evaluation metrics.

B. Conclusions and analysis

1) Purpose of the Review: The primary objective of the review is to analyze the current state of research on Vulnerability Assessment and Penetration Testing (VAPT). It identifies trends in penetration testing, evaluates the usability of tools and frameworks, and highlights emerging technologies such as machine learning and intelligent agents. Additionally, it assesses compliance with security standards like the OWASP Top 10 and their role in strengthening web application security.

2) Source Selection: Fifteen peer-reviewed research articles and conference papers published between 2014 and 2024 were chosen. The selection was based on relevance, authenticity, and contribution to cybersecurity. The main criteria included:

- Studies focused on vulnerability testing and penetration testing frameworks.
- Comparative analysis of open-source and commercial penetration testing tools.
- Case studies covering web application, operating system, and network security.
- Research on emerging techniques like machine learningbased threat detection.

3) Data Extraction and Collation: Key information such as objectives, methodology, tools and frameworks used, results, and conclusions were extracted from each study. The data were systematically organized to enable cross-comparison. Special emphasis was placed on identifying common themes, unique approaches, and study limitations.

4) Categorization and Analysis: The reviewed papers were categorized into the following themes:

- Penetration Testing Tools: Comparative studies analyzing efficiency and adaptability of tools in different environments.
- Frameworks and Methodologies: Structured VAPT approaches for corporations, government portals, and web applications.
- Web Application Security: Detection of OWASP Top 10 vulnerabilities and implementation of preventive measures.
- Operating System and Network Security: Studies on configuration assessments, authentication, and network vulnerability analysis.
- Emerging Technologies: Integration of machine learning, intelligent agents, and automation in VAPT processes.

5) *Evaluation Metrics:* Research outcomes were measured based on detection accuracy, depth of testing, costeffectiveness, usability, and scalability. The review also identified research gaps, real-world implementation challenges, and ethical/legal issues associated with penetration testing practices.

6) *Synthesis Approach:* A comparative synthesis approach was used to integrate insights across the selected studies. Patterns, trends, and major findings were extracted to provide a consolidated understanding of the VAPT research landscape. This method helped highlight the strengths and weaknesses of current tools and practices while identifying directions for future research.

III. RELATED WORKS

Vulnerability Assessment and Penetration Testing (VAPT) has emerged as the most successful methodology in the field of cybersecurity, which aims to detect system vulnerabilities and exploit them within a controlled environment to provide improved security. The initial works, including [10] and [7], underlined the significance of VAPT in cyber defense by applying vulnerability scanning and penetration tactics to enterprise systems and test networks. These researches showed how proactive vulnerability detection minimizes security threats by unveiling attack surfaces prior to exploitation. This 2016 work [8] also increased the emphasis on the efficacy of manual penetration testing, where human-initiated examinations tend to reveal security loopholes that automated software might miss, thus making system strength more increased. As illustrated in Figure 1, the methodology generally follows sequential phases, ensuring both systematic detection and controlled exploitation of vulnerabilities.

Paper Title	Methods/Approaches	Datasets	Evaluation Metrics
CyberAttack Prevention Using VAPT Tools (Lamba, 2014)	VAPT implementation, vulnerability scanning	Simulated network and web applications	Number of vulnerabilities detected, risk severity
Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology (Goel & Mehtre, 2015)	VAPT methodology, case study analysis	Enterprise systems	Detection efficiency, system security improvement
Penetration Testing: Attacking Oneself to Enhance Security (Gurline & Gurpreet, 2016)	Manual penetration testing, security assessment	Web applications, networks	Vulnerability coverage, penetration success rate

AComparisonStudy of OpenSource Penetration Testing Tools (Bhingardeve & Franklin, 2018)	Comparative analysis of open-source tools	Linux platforms, web applications	Tool effectiveness, ease of use, accuracy
A Comparison Study of Penetration Testing Tools in Linux (Zachariah & Roy, 2019)	Tool comparison, penetration testing	Linux-based systems	Vulnerability coverage, performance metrics
Penetration Testing on WPA2 (Jasper ., 2020)	Wireless network penetration testing	WPA2 secured networks	Success rate of attacks, security loopholes identified
VAPT Framework: Case Study of Government Website (Almaarif & Lubis, 2020)	VAPT framework implementation	Government website systems	Vulnerabilities detected, framework efficiency
Vulnerability Assessment and Penetration Testing (Bhatia ., 2021)	Structured VAPT framework	Web applications, enterprise networks	Risk mitigation effectiveness, detection accuracy
Web Application Penetration Testing Using SQL Injection Attack (Alanda ., 2021)	SQL injection testing, web app assessment	Web application datasets	Number of vulnerabilities detected, impact severity
Footprinting and Reconnaissance: Impact and Risks (Kek & Selvarajah, 2022)	Network reconnaissance, footprinting	Simulated network environment	Accuracy of discovered vulnerabilities, risk assessment
Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat (Fatima ., 2023)	Penetration testing, threat analysis	IoT devices, enterprise networks	Detection rate, threat coverage, security improvement
Impact of Vulnerability Assessment and	OS security assessment, VAPT	Operating systems	Vulnerabilities detected, security improvement metrics

Penetration Testing on Operating System Security (Softic & Vejzovi´ c, 2023)´			
Improving Port Scan Cybersecurity Risks Detection Using ML Algorithms (Shehab ., 2024)	Machine learning-based port scan detection	Port scan logs, network traffic	Detection accuracy, false positive/negative rates
Ensuring Web Application Security: OWASP Driven Development Methodology (Sakthivel ., 2024)	OWASP Top 10 guided VAPT	Web applications	Vulnerabilities mitigated, adherence to OWASP standards
Mitigating the OWASP Top 10 for Large Language Models Applications using Intelligent Agents (Fasha ., 2024)	Intelligent agent-based security testing	LLM applications	Detection accuracy, mitigation success, system security

TABLE I EVALUATION MATRIX OF REVIEWED PAPERS

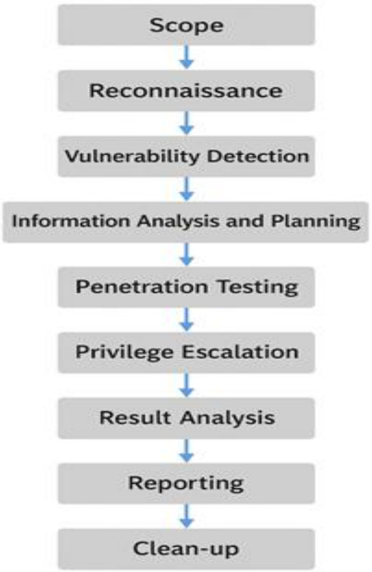

Fig. 1. Phases of Vulnerability Assessment Penetration Testing

With the heightened development of open-source software, studies in 2018 and 2019 [4], [15] compared analyses of pentesting tools, especially for Linux environments and web applications. They compared detection precision, user-friendliness, and vulnerability support, presenting information on which tools are most useful for actual use. Parallel studies in 2020 focused on particular security areas: [9] studied penetration testing of wireless networks with WPA2 protection, revealing major vulnerabilities in Wi-Fi security, while [2] created a systematic VAPT process implemented on a government website, demonstrating its efficiency in identifying actual vulnerabilities in crucial infrastructures. The 2021 works of [1], [3] furthered the systematic use of VAPT in enterprise and web application environments.

One paper provided a formal VAPT framework for enterprise networks, while another utilized SQL injection attacks to assess the security stance of web applications. Likewise, in 2022, reconnaissance and footprinting attacks were investigated by [13] highlighting the dangers introduced by attackers in the information-gathering phase of an attack. Their research highlighted how precise footprinting lays the foundation for effective exploitation attempts. Current studies (2023–2024) have moved in the direction of resolving new-age technological issues and the integration of cutting-edge methods like artificial intelligence and OWASP-governed methodologies. [6] and [14] validated VAPT's efficacy on IoT devices and operating system security, revealing the extent of its utility in securing varied platforms.

Rami Shehab [12] incorporated machine learning for identifying cybersecurity threats in port scanning in 2024, with greater accuracy of detection and lower false positives. In complement to the above, Sakthivel . [11] offered an OWASPinspired approach to strengthen web application security by preventing the most widespread vulnerabilities. Lastly, Fasha [5] utilized intelligent agents to protect large language model (LLM) applications from OWASP Top 10 vulnerabilities, exploring new paths in penetration testing through attacks on AI-based systems. Collectively, these works capture the evolution of VAPT from conventional network and system testing to contemporary AI-based methodologies, showcasing its resilience to adapt to changing cybersecurity threats in enterprise systems, IoT devices, wireless networks, and emerging applications like LLMs.

IV. RESULT

A. What are the Problems Targeted? (RQ1)

Here, we present an answer to Research Question 1 (RQ1). To answer this question, it was required to study the main security issues addressed by the analyzed studies in the domain of Vulnerability Assessment and Penetration Testing (VAPT). From these studies, we determined six general categories of issues:

1) Web Application Vulnerabilities:

- SQL Injection and Cross-Site Scripting (XSS): Injectionbased attacks are still among the most severe threats, taking advantage of weak input validation and inadequate sanitization mechanisms.
- Insecure Session Management: Session hijacking, fixation, and token manipulation risks are posed when secure cookies and tokens are implemented improperly .
- Authentication and Authorization Flaws: Weakened login systems, malfunctioning access controls, and defeatable authorization mechanisms are commonly abused .
- OWASP Top 10 Risks: Most studies directly map their analysis onto OWASP Top 10, focusing on problems like misconfigured headers, insecure deserialization, and lack of logging/monitoring .

2) Network and Wireless Security Problems:

- WPA2 Vulnerabilities: Wireless penetration testing identified weaknesses against dictionary attacks, rogue access points, and handshake manipulation .
- Port Scanning Threats: Misprotected services reveal sensitive information, enabling attackers to scan the attack surface .
- Misconfigured Network Devices: Default passwords, open ports, and old firmware on routers/switches are easy targets .
- Denial-of-Service (DoS) Threats: Enterprise and campus networks are still vulnerable to flooding and disruption attacks .

3) Operating System Security Flaws:

- Unauthorized Access and Weak Passwords: Password reuse, poor policies, and default system passwords continue to be used extensively .
- Outdated or Unpatched Software: Old operating systems with patch missing expose exploitable vulnerabilities .
- OS Misconfigurations: Incorrect file permissions, unwanted services, and insecure registry keys enhance attack surfaces .
- Privilege Escalation Opportunities: Weak privilege management and kernel vulnerabilities enable the escalation of rights and system compromise .

4) Shortcomings in Penetration Testing Tools:

- False Positives and Incomplete Coverage: Research indicates tools tend to mistakenly flag harmless behaviors or miss serious flaws .
- Lack of Automation and Reporting: Most tools lack automated reporting capabilities or support for integration with enterprise systems .
- Limited Platform-Specific Effectiveness: Tools optimized for Linux perform suboptimally in Windows or IoT setups
- Usability Challenges: Steep learning curves associated with open-source tools restrict adoption among novice testers .

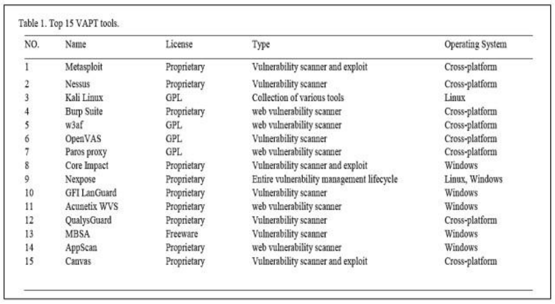

Table 1. Top 15 VAPT tools.

NO.	Name	License	Type	Operating System
1	Metasploit	Proprietary	Vulnerability scanner and exploit	Cross-platform
2	Nessus	Proprietary	Vulnerability scanner	Cross-platform
3	Kali Linux	GPL	Collection of various tools	Linux
4	Burp Suite	Proprietary	web vulnerability scanner	Cross-platform
5	w3af	GPL	web vulnerability scanner	Cross-platform
6	OpenVAS	GPL	Vulnerability scanner	Cross-platform
7	Paros proxy	GPL	web vulnerability scanner	Cross-platform
8	Core Impact	Proprietary	Vulnerability scanner and exploit	Windows
9	Nexpose	Proprietary	Entire vulnerability management lifecycle	Linux, Windows
10	GFI LanGuard	Proprietary	Vulnerability scanner	Windows
11	Acunetix WVS	Proprietary	web vulnerability scanner	Windows
12	QualysGuard	Proprietary	Vulnerability scanner	Cross-platform
13	MBSA	Freeware	Vulnerability scanner	Windows
14	AppScan	Proprietary	web vulnerability scanner	Windows
15	Canvas	Proprietary	Vulnerability scanner and exploit	Cross-platform

Fig. 2. VAPT Tools

5) Emerging Threats in Contemporary Systems:

- Zero-Day Exploits: Unannounced vulnerability detection is still a problem .
- IoT Security Gaps: Weak encryption, weak authentication, and resource-starved devices render IoT extremely susceptible .
- AI/ML and LLM Applications: New risks are prompt injection, adversarial manipulation, and insecure API integration in AI-based systems .
- Advanced Persistent Threats (APTs): Advanced, multistage attacks question the boundaries of traditional VAPT

.

6) Compliance and Standardization Challenges:

- Lack of Adherence to Standards: Organizations rarely align testing procedures with OWASP, NIST, or ISO 27001 .
- Fragmented Assessment Practices: Security testing methodologies are highly variable and result in nonuniform vulnerability identification .
- Limited Regulatory Integration: Sectors like healthcare, finance, and government do not have industry-specific penetration testing regulations .

Generally, the studies reviewed indicate that while there is considerable advancements in VAPT methods, there are still gaps remaining in web applications, networks, operating systems, and newly emerging AI-based systems. This highlights the need for adaptive, standardized, and intelligent penetration testing methods on an immediate basis.

B. What are the methods employed in the studies? (RQ2)

- Vulnerability Assessment and Penetration Testing (VAPT) VAPT is the basic approach utilized in the majority of the studies, integrating automated scanning for vulnerabilities with manual penetration tests to provide an overall security review. Automated tools identify vulnerabilities in systems, networks, and web applications like misconfigurations, old software, open ports, and poor authentication protocols. Manual penetration testing subsequently takes advantage of these vulnerabilities to mimic actual attacks and estimate potential effects. The hybrid method allows organizations to detect top-priority vulnerabilities, prioritize them in terms of severity, and make wise security enhancement decisions. Further, some studies incorporate continuous VAPT, whereby automated scanning occurs regularly alongside manual inspections, and vulnerabilities within dynamic environments (e.g., cloud or DevOps pipelines) are tackled in a timely manner.

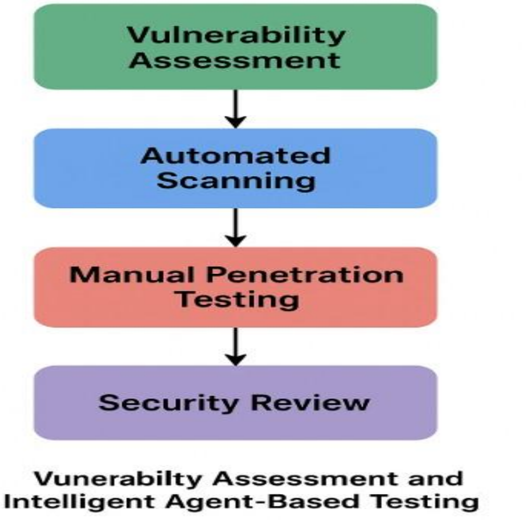
Vulnerability Assessment
Automated Scanning
Manual Penetration Testing
Security Review
Vunerabilty Assessment and Intelligent Agent-Based Testing

Fig. 3. Vulnerability Assessment And Intelligent Agent-Based Testing

- Comparative Tool Analysis
  A few studies focus on comparing open-source and proprietary penetration testing tools on criteria such as effectiveness, detection rate, false positives/negatives, ease of use, cost, and compatibility (Linux, Windows, web applications). Controlled experiments or case studies identify the strengths and weaknesses of each of these tools. These comparisons assist organizations in choosing the most appropriate tools based on their security requirements and environments. Other research takes extensions in comparisons by experimenting with multi-tool combinations, where multiple tools are combined to minimize blind spots. Tests also involve performance testing in resourcelimited environments, including IoT devices or embedded systems.

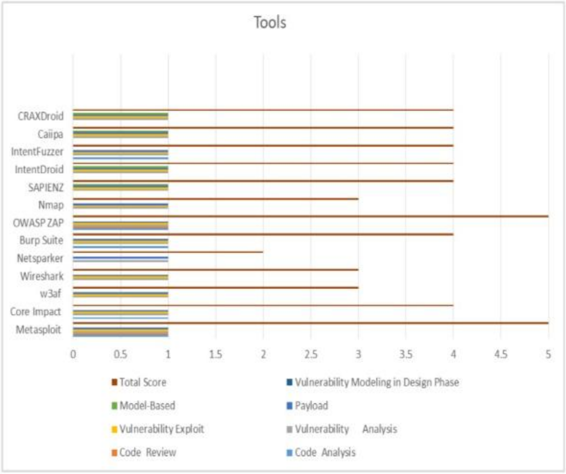

Fig. 4. Comparison of VAPT Tools across Capabilities

- Framework-Based Methods

Framework-based approaches are a systematic, step-bystep methodology for VAPT, such as planning, scanning, exploitation, reporting, and mitigation. They can be used best in enterprise or government environments to facilitate systematic testing, uniformity, and security standard compliance. Uniform reporting enables organizations to monitor over time how vulnerabilities are improving. Recent research also presents frameworks mapping vulnerabilities to regulatory requirements (e.g., ISO 27001, GDPR, HIPAA) and providing automated remediation recommendations, enhancing compliance as well as efficiency.

- Machine Learning and Intelligent Agent-Based Approaches

Recent work combines machine learning (ML) and intelligent agents to improve threat analysis and vulnerability detection. ML-based algorithms scan network traffic, logs, and system information to identify anomalies and attacks, and intelligent agents, especially in LLM usage, can recognize vulnerabilities automatically and suggest mitigations. These techniques minimize false positives, enhance real-time detection, and enable predictive analysis with minimal human effort. Other research investigates reinforcement learning to dynamically adjust scanning approaches, and federated learning to allow organizations to exchange ML models for more effective detection without revealing sensitive data.

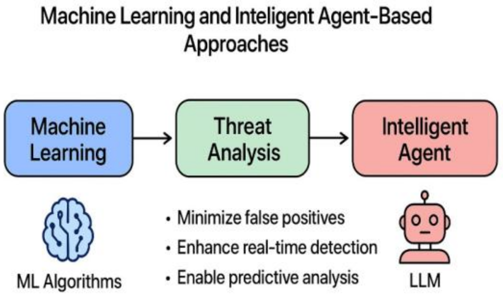
Machine Learning and Inteligent Agent-Based Approaches
Machine Learning
Threat Analysis
Intelligent Agent
ML Algorithms
• Minimize false positives
• Enhance real-time detection
• Enable predictive analysis
LLM

Fig. 5. Machine Learning and Intelligent Agent-Based Approaches for Automated Vulnerability Detection and Mitigation

- OWASP Top 10-Guided Testing

Some studies match testing techniques with OWASP Top 10 standards to target high-risk web application vulnerabilities like SQL injection, XSS, broken authentication, and security misconfigurations. Automated scanners and manual exploitation methods are utilized to make web applications conform to industry-approved security guidelines. More sophisticated techniques go beyond OWASP Top 10, tackling API-specific flaws, cloud misconfigurations, and business-impact prioritization, making security testing context-aware.

- Case Studies and Simulated Environments Most studies employ case studies or simulated testbeds to mimic enterprise networks, IoT devices, wireless networks, or web applications. Testbeds provide an environment controlled by the researchers that can be used to measure tool effectiveness, detect advanced or upcoming threats, and suggest targeted security improvements. Some testbeds simulate cyber ranges for training sec teams while testing. Others employ cloud-based simulation environments to build scalable, repeatable test scenarios for VAPT tool validation.
- Techniques for Risk Prioritization and Reporting Post-assessment activities such as vulnerability scoring, risk ranking, and dashboards enable organizations to prioritize high-risk vulnerabilities and remediate them in an effective manner. Visualization and reporting enable findings to become actionable and facilitate ongoing cybersecurity improvement. Latest approaches incorporate threat intelligence feeds within risk scoring to take into account actively exploited vulnerabilities. Apart from that, predictive

dashboards predict probable breaches in case vulnerabilities are not patched.

- Hybrid Methods

Certain research fuses more than one method, blending VAPT, ML-based scanning, framework testing, and intelligent agents. Hybrid approaches broaden detection coverage, minimize false positives, automate rote tasks, and offer actionable security feedback, demonstrating a shift towards adaptive and comprehensive cybersecurity assessment. Sophisticated hybrid systems also incorporate red-teaming methods, mimicking actual attacker actions, and promote human-AI collaboration, leveraging the pace of automation with the richness of expert insight.

Year	Technology / Technique Used
2014	Vulnerability Assessment & Penetration Testing (VAPT)
2015	VAPT Methodology & Case Study Analysis
2015	Manual Penetration Testing & Security Assessment
2016	Comparative Analysis of Open-Source Penetration Testing Tools
2020	Penetration Testing Tools Evaluation in Linux
2020	Wireless Network Penetration Testing (WPA2)
2021	Framework-Based VAPT for Government Websites
2021	Structured VAPT Framework
2021	SQL Injection Penetration Testing for Web Applications
2023	Penetration Testing & Network Threat Analysis
2023	AI-Powered VAPT on Operating Systems
2023	ML-Assisted Port Scan Detection
2024	OWASP Top-10 Guided Web Application Security
2024	Agent-Based Vulnerability Mitigation for LLMs

TABLE II TECHNOLOGIES AND TECHNIQUES USED IN REVIEWED VAPT STUDIES (2014–2024)

V. CONCLUSION

This review highlights the transformational potential of blockchain in secure messaging, addressing critical challenges such as data privacy, decentralization and security The analyzed studies identify various approaches, including cryptographic development, decentralized frameworks and including machine learning integration The most important barriers are the same. Future research will focus on optimizing blockchain networks to support real-time transactions and seamlessly integrate with existing systems. By addressing these challenges, blockchain technology can lay a solid foundation for secure and reliable networks across applications.

REFERENCES

[1] A. Alanda, D. Satria, M. I. Ardhana, A. A. Dahlan, and H. A. Mooduto. Web application penetration testing using sql injection attack. JOIV International Journal on Informatics Visualization, 5(3):320, September 2021.

[2] Ahmad Almaarif and Muharman Lubis. Vulnerability assessment and penetration testing (vapt) framework: Case study of government's website. International Journal on Advanced Science, Engineering and Information Technology (IJASEIT), 10(5):1874–1880, October 2020.

[3] Gaurav Bhatia, Om Bhatia, Aryan Bhandare, Vishnu Bagde, and Alka Prayagkar. Vulnerability assessment and penetration testing. International Journal of Engineering Research & Technology (IJERT), 10(05), May 2021. First published online 17 May 2021.

[4] Nilesh Bhingardeve and Seeza Franklin. A comparison study of open-source penetration testing tools. International Journal of Trend in Scientific Research and Development, 2(4):2595–2597, June 2018. Published June 2018.

[5] Mohammad Fasha, Faisal Abul Rub, Nasim Matar, Bilal Sowan, Mohammad Al Khaldy, and Hussam Barham. Mitigating the owasp top 10 for large language models applications using intelligent agents. In 2024 2nd International Conference on Cyber Resilience (ICCR), pages 1–9, 2024.

[6] Areej Fatima, Tahir Abbas Khan, Tamer Mohamed Abdellatif, Sidra Zulfiqar, Muhammad Asif, Waseem Safi, Hussam Al Hamadi, and Amer Hani Al-Kassem. Impact and research challenges of penetrating testing and vulnerability assessment on network threat. In 2023

International Conference on Business Analytics for Technology and Security (ICBATS), pages 1–8, 2023.

[7] Jai Goel and Babu Mehtre. Vulnerability assessment penetration testing as a cyber defence technology. Procedia Computer Science, 57:710–715, 12 2015.

[8] Gurpreet Kaur2 Gurline Kaur1. Penetration testing: Attacking oneself to enhance security. International Journal of Advanced Research in Computer and Communication Engineering, 5(4), April 2016.

[9] R. Sam Jasper, P. P. Amritha, and M. Sethumadhavan. Penetration testing on WPA2. International Journal of Recent Technology and Engineering (IJRTE), 8(6):3003, March 2020. Published March 30, 2020.

[10] Anil Lamba. Cyber attack prevention using vapt tools (vulnerability assessment & penetration testing). Cikitusi Journal for Multidisciplinary Research, 1(2), 2014. Posted: February 1, 2020.

[11] M. Sakthivel, S. Sivanantham, N. Bharathiraja, N. Bala Krishna, R. Kamalraj, and V. Saravana Kumar. Ensuring web application security: An owasp driven development methodology. In 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), volume 1, pages 1–7, 2024.

[12] Rami Shehab, Rana Alrawashdeh, Romel Al-Ali, Tayseer Alkh'dour, and Mohammed Amin Almaiah. Improving port scan cybersecurity risks detection using feature selection techniques with machine learning algorithms. Journal of Theoretical and Applied Information Technology (JATIT), 102(16):6094–6113, August 2024. Published 31 August 2024.

[13] Kek Shye Lianq and Vinesha Selvarajah. Footprinting and reconnaissance: Impact and risks. In 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pages 1–5, 2022.

[14] Jasmin Softic and Zanin Vejzovi´ c. Impact of vulnerability assesment´ and penetration testing (vapt) on operating system security. In 2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH), pages 1–6, 2023.

[15] Lijo Zachariah and Sudeshna Roy. A comparison study of penetration testing tools in linux. International Journal of Scientific and Engineering Research, 10(4), April 2019. Pilot comparative study of open-source Linux penetration testing tools.