Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 47 No. 03
March 2026

Unified Reconnaissance and Vulnerability Assessment

Ashith Rajeev[1], B Harikeerthana[2], B Haritheertha[3], Muhammed Musthafa[4], Sr Reema Jose[5]

[1, 2, 3, 4] Department of Computer Science Cyber Security Vimal Jyothi Engineering College, Chemperi, Kannur

[5] Assistant Professor, Department of Computer Science Cyber Security Vimal Jyothi Engineering College, Chemperi, Kannur

Email Id: [1] ashithrajeev20045@gmail.com, [2] harikeerthanabyju@gmail.com, [3] haritheerthabyju2@gmail.com, [4] muhmd.musthafa10@gmail.com, [5] srreemajose@vjec.ac.in

Abstract

Traditional cybersecurity assessment tools often rely on fragmented workflows, offer limited visualization and fail to communicate risks effectively to management, leading to gaps in enterprise risk assessment. To overcome these limitations, this paper introduces URVA (Unified Reconnaissance and Vulnerability Assessment), a unified cybersecurity platform that integrates artificial intelligence, interactive graph analysis and comprehensive reconnaissance. URVA follows a four-layer architecture that includes full-scale network reconnaissance with complete port coverage (1–65535), advanced OSINT collection and detailed vulnerability assessment covering over 25 common security checks such as XSS, SQL injection, LFI and CSRF. Its core innovation is the Intelligence Graph visualization system, which transforms complex security data into clear, actionable visual insights. The platform uses an interactive NetworkX-based graph to help security professionals identify attack paths, asset relationships and vulnerability correlations that are difficult to interpret through traditional reports. In addition, an AI-powered analysis engine (using the Groq API) automates business impact assessment, remediation planning and executive-level reporting, reducing report generation time from hours to minutes while maintaining accuracy. Evaluation results show that URVA provides deeper assessment coverage than conventional tools, while effectively bridging the communication gap between technical security teams and executive stakeholders. Its modular opensource design also supports future research in automated threat modeling, intelligent vulnerability prioritization and real-time security visualization, positioning URVA as a strong advancement in enterprise cybersecurity assessment.

Keywords: Cybersecurity assessment, vulnerability analysis, network reconnaissance, intelligence visualization, penetration testing, security automation.

1. Introduction

Modern cybersecurity assessments are severely challenged because of the fragmentation of existing security tools and the increasing complexity of enterprise network infrastructures. In practice, this means security professionals need to juggle numerous disparate tools for network reconnaissance, vulnerability scanning and threat analysis, which can result in inefficient workflow processes, incomplete assessments and missed security correlations. Traditional approaches require manual integration of results from tools like Nmap for network scanning, specialized subdomain enumeration utilities and web application security scanners such as OWASP ZAP, which has gaps in comprehensive security analysis.

The proliferation of web applications, microservices architectures and cloud-based infrastructures has exponentially increased the attack surface that security teams must assess and monitor. Current methodologies often fail to provide holistic visibility into asset relationships and vulnerability interdependencies, limiting the effectiveness of risk assessment and remediation prioritization. Besides, most of the existing tools also lack integrated visualization capabilities that allow the security analyst to intuitively understand complex network topologies and potential attack paths.

This work presents URVA, a unified cybersecurity assessment platform, designed to overcome the aforementioned limitations by providing integrated

automation and intelligent visualization. URVA chaining up network scanning, subdomain enumeration and web application vulnerability analysis into one workflow further eliminates the complexity of having to use several tools and manually correlates the results. The Intelligence Graph feature in this platform offers an interactive visualization of discovered assets and their relationships for the first time, thus enabling security professionals to pinpoint critical attack paths and prioritize remediation efforts more effectively.

The main contributions of this paper are: a common assessment framework that unifies several security testing methodologies; for the first time in the industry, an Intelligence Graph visualization system allows asset relationship mapping; completion of web application vulnerability analysis at a depth comparable to enterprise-grade security scanners; and generation of automated reports with actionable remediation. Experimental validation shows that URVA accomplishes assessment time reduction while improving accuracy in vulnerability detection and correlation compared to traditional approaches that require many tools.

The rest of the paper is organized as follows: Section II reviews related work in cybersecurity assessment tools. Section III presents the URVA system architecture and methodology. Section IV discusses the Intelligence Graph visualization approach. Section V presents results and performance evaluation. Section VI concludes with future research directions.

2. Related Work

A. Research Methodology

This systematic literature review follows a structured methodology to search, examine and categorize existing literature associated with the issue of Vulnerability Assessment (VA). This literature review follows a series of steps to increase its comprehensiveness and reliability.

1) Research Design: The relevant literature was searched for on the basis of keywords like “Vulnerability Assessment,” “cybersecurity assessment,” “vulnerability detection methodologies,” and “vulnerability prioritization.” Searching for the relevant literature was carried out on the best online libraries, like IEEE Xplore, Springer, ACM Digital Library, Science Direct and Google Scholar. In addition to peer-reviewed academic literature, authoritative cybersecurity knowledge bases and industry standards were also consulted to complement the research findings. These sources include globally recognized frameworks and vulnerability repositories such as OWASP, NIST and MITRE CVE, [9], [11], [12] which provide practical insights into real-world vulnerability classification, assessment standards and remediation practices. Incorporating these sources helps bridge the gap between theoretical research and practical vulnerability assessment implementations.

2) Inclusion Criteria:

- Vulnerability assessment papers that are based on methodologies, frameworks or security evaluation tools.
- Research papers relating to the development or use of automated or intelligent solutions.
- Articles on issues regarding network security, operating system security and application security.
- Publications in peer-reviewed journals, conferences or workshops between 2011 and 2025.

3) Exclusion Criteria:

- Research that is not related to vulnerability assessment and/or system security.
- Technical or experimental papers that lack contributions.
- Duplicated studies or those with incomplete data.
- Non-peer-reviewed literature sources, like blog sites, magazines or non-academic reports.

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

1) Yogi, M. K. (2023). *A Review of Cyber Vulnerability Assessment Methods* [19].
2) Nath, H. V. (2011). *Vulnerability Assessment Methods – A Review* [10].
3) Bennouk, K. (2024). *A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies* [4].
4) Jiang, Y. (2025). *A Survey on Vulnerability Prioritization: Taxonomy, Metrics and Research Challenges* [7].
5) Almuhaidib, A. S. (2025). *Weaponizing Language Models for Automating Vulnerability Assessment Report Validation* [1].

6) Ruotsalainen, A. (2024). *Literature Review of Vulnerability Management Best Practices in Cybersecurity* [14].

7) MDPI article (2024). *Comprehensive Assessment of Vulnerability Detection Approaches* [3]. 8) ScienceDirect article (2021). *Review of Cybersecurity Assessment Methods* [2].

B. Conclusions and Analysis

1) Purpose of the Review*:* The key aim of this review is to discuss and evaluate the present state-of-the-art research work being conducted on Vulnerability Assessment. It describes patterns of vulnerability identification, effectiveness of various methods and adopts new technology like artificial intelligence and automation in vulnerability assessment. It also evaluates frameworks of vulnerability prioritization and their significance in enhancing system security.

2) Source Selection: Eight peer-reviewed articles on research papers published between the years 2011 and 2025 were considered for selection on the topic of cybersecurity. The criteria chosen include:

- Research studies specifically targeting vulnerability assessment approaches/tools, frameworks or methodologies.
- Comparative analysis of methodologies used on different subject areas, such as web applications, operating systems and networks.
- Research into emerging trends like AI-assisted evaluation, automation and intelligent validation of reports.

C. Data Extraction and Collation

Key information on objectives, methodology, tools and frameworks, results and conclusions was systematically identified. The information was organized to facilitate crosstabulations to pick up trends, distinct approaches, as well as limitations within the studies.

1) Categorization and Analysis: The papers that were reviewed can be grouped into themes as follows:

- Methodologies and Frameworks: Traditional and modern vulnerability assessment methods, including host, network and application-based approaches.
- Prioritization Techniques: Approaches to ranking vulnerabilities based on risk and impact. [6]
- Emerging Technologies: Integration of AI, machine learning and automation in vulnerability detection and report validation.
- Vulnerability Management: Best practices for managing and mitigating discovered vulnerabilities. [8]

2) Evaluation Metrics: Detection accuracy, coverage, efficiency, scalability and ease of use are some of the metrics used to evaluate the effectiveness of the different approaches for vulnerability assessment across the reviewed studies [2]. While accuracy tells about correct identification of vulnerabilities, coverage provides insights on the breadth of various attack vectors assessed. Scalability addresses performance issues when working in large enterprise environments and ease of use reflects both deployment and operational complexity. These are some of the common challenges that were noted: a high rate of false positives, lack of standardized frameworks for assessment, limited correlation among the findings of vulnerabilities and deficient support for visualizations in complex infrastructures [3], [13].

3) Synthesis Approach: The approach for synthesizing these insights was comparative in nature. It helped to note the common trends, recurring methodologies and important findings in the research studies reviewed on vulnerability assessment. It also enabled the recognition of existing limitations and directions of emergence, thereby providing necessary insight into the current research landscape with conciseness yet comprehensively.

3. System Architecture and Methodology

URVA employs a four-layer architecture that ensures modularity and scalability. Every layer in URVA has a unique function to perform. The layering separates user interaction from vulnerability assessment tasks. This makes the system very organized and efficient. The layering also allows for the simultaneous execution of reconnaissance and vulnerability scanning tasks. The layering makes the system efficient. Communication between the layers is standardized.

A. Four-Layer Architecture Design

The four-tier model of URVA provides a structured and systematic data flow from raw input, converting it into security intelligence. The User Interface layer is the control mechanism of the system and lets the user set up parameters and view results in an intuitive interface.

The Reconnaissance phase identifies the attack surface of its target through collected intelligence from networks and publicly available information and it provides a basis for security analysis and intelligence.

Based on the outcome of the reconnaissance phase, the Vulnerability Analysis layer performs active and passive security assessments to reveal configuration errors, weaknesses and potential vulnerabilities against the discovered assets. The outcome of assessments produced during this phase are correlated and prioritized for risks and consequences. Finally, the Report Generation layer translates the technical outcome and produces a well-formatted security report on the assessments in the form of an executive summary and risk and remediation recommendations.

B. Layer-by-Layer Technical Implementation

1) Layer 1 - User Interface: The User Interface layer performs as the primary interaction point between the user and the system. PyQt5 [5] was chosen for its responsiveness and has implemented a graphical interface to handle the target specification, configuration and visualization of the scanning results. This layer also manages workflow execution with the ability to show progress updates in real-time and let the users monitor running assessments without performance degradation. It introduces multi-threading to protect the interface from long-running reconnaissance and vulnerability scans.

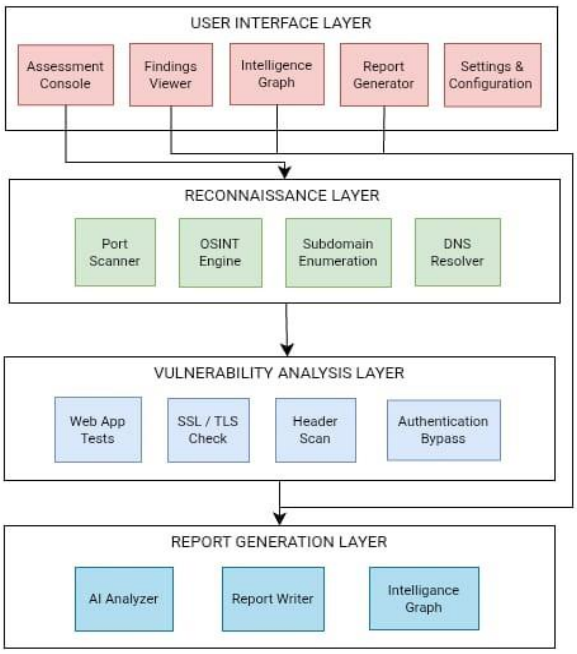

Fig. 1. Four-Layer Architecture Design

2) Layer 2 - Reconnaissance: The Reconnaissance layer is concerned with gathering detailed information on the target to build a whole profile of the attack surface. Network reconnaissance involves the use of Nmap in carrying out network scans for identification and determination of open ports, services running, service versions and operating system details. OSINT [18] techniques are put in place for publicly available intelligence gathering like domain information, technologies in use, DNS records and related digital footprinting. Moreover, subdomain enumeration is done through DNS brute forcing, certificate transparency logs and attempts at zone transfer; this increases the asset and entry point discovery scope by manifold.

3) Layer 3 - Vulnerability Analysis: The layer of Vulnerability Analysis aggressively tests discovered resources for vulnerabilities to exploit for different security vulnerabilities. It carries out comprehensive testing of web application for different aspects of security like analysing the configuration of SSL/TLS, verifying various security headers for proper implementation and finding various common injection vulnerabilities like XSS, SQL injection, Local File Inclusion and Command injection attacks. Authentication and session management mechanisms are tested to explore various problems existing in relation to CSRF protection, insecure cookies and unauthorized access paths. Various advanced tests include WAF detection [15], Clickjacking scan and sensitive file identification.

4) Layer 4 - Generating Reports: The Report Generation layer specializes in translating raw technology results into a structured form of meaningful security intelligence. An intelligence graph is then generated through graph-based analysis to represent relationships between host entities, services, vulnerabilities and attack paths. AI-based analysis is then incorporated to automatically calculate risk scores, determine potential Business Impact and provide recommendations based on a set of prioritized remedial actions. Eventually, professional PDF reports are created using industry-standard formats for executive summaries, technology results, risk matrices and mitigations.

C. Data Flow and Integration

URVA operates on a clearly identifiable data flow model, where user-submitted data triggers the

execution of Recon tasks, which run concurrently. The acquired data undergoes normalization and correlation among the various modules to remove redundancy and enhance accuracy. Vulnerability data is later related to assets and associations, which are represented in the Intelligence Graph. The correlated data is received by the AI Engine Analysis component for risk analysis and reporting.

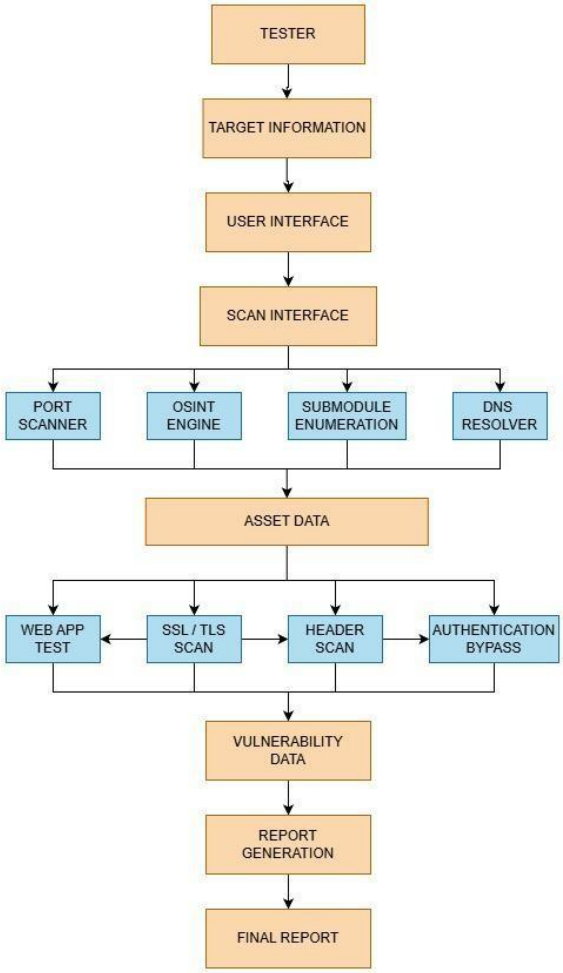

Fig. 2. Dataflow Diagram

D. Scalability and Performance Optimization

For efficient operation, URVA uses multi-threading approaches during scanning and asynchronous processing. The operation of modules in Reconnaissance and Vulnerability Testing is carried out in a multi-threaded manner to reduce the time taken during assessment. Memory-efficient data structures are also used during intelligence graph creation. Stream-based report processing is used to ensure stability in assessment of large-scale targets.

4. Intelligence Graph Visualization

A. Intelligence Graph Architecture and Implementation

Intelligence Graph is the primary visualization technique in the URVA tool, which demonstrates an intelligent graph theory approach to cybersecurity asset relationship mapping. Implemented for its robust graph-processing capabilities through the NetworkX library and its ability to provide real-time visualization through the PyQtGraph toolkit, Intelligence Graph generates an interactive network model G(V,E), where vertices are used to depict identified cybersecurity assets (target, domains, subdomains, IP addresses, ports, services and vulnerabilities) and edges are used to depict relationship mappings between the vertices (DNS resolution mapping, service binding mapping, vulnerability mapping and hierarchical dependency mapping). Varieties of layouts are used by this technique to organize vertices in different patterns. For instance, force layouts are allowed to tailor values to suitably demonstrate numeric spring values. Additionally, hierarchical multi-level layouts are used to optimize viewing patterns by allowing users to view comprehensive attack path layouts, while circular layouts are used to balance ass and location. Every cybersecurity asset label is given a distinct graphical representation through an intelligent coding system that allows different asset categories to have predefined graphical shapes. [17]

B. Interactive Analysis and Strategic Significance

The Intelligence Graph goes beyond traditional static reporting in that it offers real-time, interactive analysis tools, which allow for dynamic exploration of the highly complicated cyber-security environment. It allows user interaction with the graph through drag and drop positioning, multi-level zooming and filtering on the basis of severity, asset and user-defined parameters, with immediate access to technical-level analysis and remediation advice through hover and click-through functions. Also, critical network metrics, such as node density, graph component connectivity and the relationship clustering coefficient, are automatically calculated and made available, which allows for quick identification of high-value targets and single points of failure in the network that has undergone security assessment and analysis.

5. Result & Performance Evaluation

This section develops a detailed evaluation of the proposed URVA framework to ascertain its

effectiveness, performance and practical applicability. The evaluation is designed to assess how well URVA integrates multiple security assessment phases into a single unified platform and how it performs when compared with existing industry-standard security tools. Both qualitative and quantitative metrics are considered to provide a holistic understanding of the system's capability.

For this, the experimental analysis has targeted four key aspects of the experiment: functional coverage, capability strength, execution efficiency and vulnerability detection accuracy. URVA is evaluated against different network scales with respect to scalability and performance behaviour under various workloads. Moreover, the coverage of vulnerability detection by URVA is reviewed in accordance with OWASP Top 102021 in order to be compatible with current web application security needs.

Comparative studies performed using established platforms like Nmap, OWASP ZAP, Nessus, Burp Suite and OpenVAS [16] highlight the effectiveness of URVA's integrated workflow, intelligence-enabled analysis and automated reporting processes. The outcome indicates that URVA not only integrates different security-related tasks into a comprehensive platform but further strengthens the level of assessment by correlating, visualizing and leveraging AI-enabled risk assessment.

A. Feature Comparison with Existing Security Tools

Fig. 3 and Fig. 6 depict the comparative analysis of URVA with other widely utilized security scanning solutions including Nmap, OWASP ZAP, Nessus, Burp Suite and OpenVAS. It can be clearly observed from the analysis that URVA has a more unified scanning process with an encompassing security solution set.

Unlike conventional tools, which target particular phases of the assessment process, URVA enables network scanning, analysis of vulnerabilities in web environments, subdomain identification, intelligence graph creation, execution of the entire workflow, interaction-based graphing and automated report execution. Usually, it takes more than one tool chain or more manual integration efforts involving other tools in unison to accomplish the above-mentioned tasks. The intelligence graph, along with the entire workflow, makes it distinct from other tools.

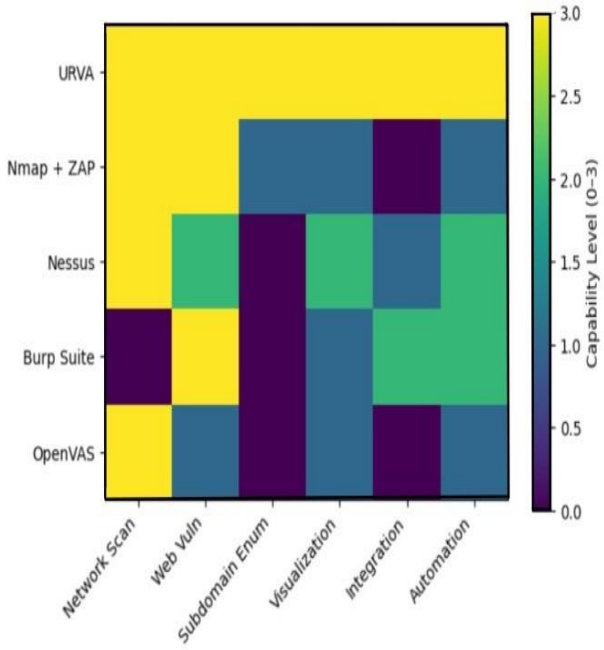

Fig. 3. Feature Comparison Heatmap of Security Assessment Tools

B. Capability-Level Evaluation

This capability assessment map using a heatmap reflects the strength of each capability within six broad domains of security assessment: network scan, web vulnerability, subdomain, visualization, integration and automation. URVA has scored the highest on each domain of capability assessment.

Although Nessus and Burp Suite prove useful in vulnerability scanning, they do not have the facility of reconnaissance and visualization. Nmap, being very efficient in scanning, fails to support web vulnerability analysis and reporting. All the above-described tools have been overcome by URVA, as it encompasses analysis, reconnaissance and visualization in its single auto main.

Overall, the capability level assessment proves that URVA has a more holistic, integrated and scalable assessment capability compared to the conventional security assessment tools. Consequently, it is very suitable for research as well as real world vulnerability scanning.

Vulnerability Type	Direction Method	Severity Levels	OWASP TOP 10	Coverage
SQL Injection	Payload Testing	Critical , High , Medium	A03 : 2021	Full
Cross - Site Scripting (XSS)	Script Injection	Critical , High , Medium	A03 : 2021	Full
SSL / TLS Issues	Certificate Analysis	High , Medium , Low	A02 : 2021	Full
Security Headers	HTTP Header Check	Medium , Low , Info	A05 : 2021	Full
Authentication Bypass	Access Testing	Critical , High	A07 : 2021	Full
Local File Inclusion	Path Traversal	High , Medium	A03 : 2021	Full
CSRF	Token Validation	Medium , Low	A01 : 2021	Full
Information Disclosure	Error Analysis	Medium , Low , Info	A01 : 2021	Full

Fig. 4. URVA Vulnerability Coverage Summary (OWASP Top 10 – 2021)

C. Performance and Scalability Analysis

Fig. 5 gives the analysis of execution time performed on URVA depending on the size of the networks, which can be considered to fall into three categories: small (1 to 50 hosts), medium (51 to 200 hosts) and large networks (200 or more hosts), as shown below. It can be seen that URVA is an efficient algorithm in terms

The discovery and subdomain scanning times are directly proportional to the target size, with optimal and consistent performance. Vulnerability analysis stands out as the component with the highest overall processing involved, given the in-depth analysis and testing for payload details. The creation of intelligence graphs and reporting has very low overhead, proving that optimized data structures and reporting methods are very efficient.

Assessment Phase	Small Network (1 - 50 hosts)	Medium Network (51 - 200 hosts)	Large Network (200+ hosts)
Network Discovery	2.3 min	8.7 min	23.1 min
Subdomain Enumeration	5.1 min	12.4 min	28.9 min
Vulnerability Analysis	8.9 min	22.3 min	45.7 min
Intelligence Graph	0.8 min	2.1 min	4.3 min
Report Generation	0.3 min	0.7 min	1.2 min

Fig. 5. URVA Execution Time Comparison Based on Network Size

Above results prove the effectiveness of the URVA protocol in both small research settings and enterprise networks.

D. Vulnerability Coverage and Security Effectiveness

Fig. 4 presents a summary of the categories found by URVA, their methods of detection, the levels of severity, alignment with OWASP Top 10 and overall coverage. URVA offers complete coverage for all major web vulnerabilities, including SQL Injection, Cross Site Scripting, Authentication Bypass, Local File Inclusion, CSRF, SSL/TLS Misconfigurations and Information Disclosure.

Each vulnerability is tied to appropriate categories in the OWASP Top 10 (2021) recommendations, thus meeting the highest levels of security standards. The software allows vulnerabilities to be classified based on various levels. The full spectrum illustrates the efficiency offered by the URVA software.

Feature	URVA	Nmap	OWASP ZAP	Nessus	Burp Suite
Network Scanning	✓	✓	✗	✓	✗
Web Vulnerability Analysis	✓	✗	✓	✓	✓
Subdomain Enumeration	✓	✗	✗	✗	✗
Intelligence Graph	✓	✗	✗	✗	✗
Unified Workflow	✓	✗	✗	✗	✗
Interactive Visualization	✓	✗	✗	✗	✗
Automated Reporting	✓	✗	✓	✓	✓

Fig. 6. Vulnerability Coverage and OWASP Top 10 Alignment in URVA

E. Discussion of Results

The results obtained have proven that URVA does indeed fill the gap that currently exists between standalone security solutions by creating an intelligent automated assessment platform. This is enhanced by the integrated process design, which minimizes tool dependency and offers enriched visualization by way of AI-driven analysis and reporting.

On the whole, URVA provides enhanced assessment completeness, simplified system operations and efficient performance scalability, which makes it quite

fitting for academic studies, pen-testing and real vulnerability assessment scenarios.

6. Conclusion

This paper proposes URVA as a holistic analysis platform for the domain of information technology and cybersecurity. This platform has numerous benefits as it overcomes flaws in current risk analysis. The primary benefits of URVA are the development of an intelligence graph solution using the NetworkX and PyQtGraph libraries. This tool helps in the generation of intelligence from the complex graph of information technology and cybersecurity. Furthermore, URVA has an automated risk analysis solution that uses the Groq API. This significantly saves time in the generation of reports for executives.

In addition, URVA has a modular four-layer stacked architecture that seamlessly weaves together extensive reconnaissance on the target networks, sophisticated OSINT collection, thorough vulnerability analysis (25+ security checks) and professional PDF report creation in a single, streamlined process. Results from experimental evaluations clearly show increased coverage, speed and transparency gains with URVA compared with traditional solutions available today. This openness and extensibility of URVA also makes it a solid platform for future research in automated threat modelling, vulnerability prioritization through machine learning algorithms, real-time security visualization and incorporation of upcoming threats intelligence platforms, verifying that incorporating traditional security methods and intelligent analysis and visualization can really help in improving current security analysis methods in cybersecurity.

References

[1] A. S. et al. Almuhaidib. Weaponizing language models for automating vulnerability assessment report validation. *IEEE Security & Privacy*, 2025.

[2] Various Authors. Review of cybersecurity assessment methods. *Journal of Information Security*, 2021.

[3] Various Authors. Comprehensive assessment of vulnerability detection approaches. *Sensors (MDPI)*, 2024.

[4] K. et al. Bennouk. A comprehensive review and assessment of cybersecurity vulnerability detection methodologies. *IEEE Access*, 2024.

[5] Martin Fitzpatrick. *Create GUI Applications with Python & Qt5 (PyQt5 Edition): The hands-on guide to making apps with Python*. Martin Fitzpatrick, 2020. Edition 4th, published June 25, 2020 or another edition.

[6] Y. Jiang, H. Zhang and X. Li. A survey on vulnerability prioritization: Taxonomy, metrics and research challenges. *arXiv preprint arXiv:2502.11070*, 2025.

[7] Y. et al. Jiang. A survey on vulnerability prioritization: Taxonomy, metrics and research challenges. *ACM Computing Surveys*, 2025.

[8] Xin Jin, Charalampos Katsis, Fan Sang, Jiahao Sun, Elisa Bertino, Ramana Rao Kompella and Ashish Kundu. Graphene: Infrastructure security posture analysis with ai-generated attack graphs. *arXiv preprint arXiv:2312.13119*, 2023.

[9] MITRE Corporation. Common vulnerabilities and exposures (cve), 2024.

[10] H. V. Nath. Vulnerability assessment methods – a review. *International Journal of Network Security*, 2011.

[11] NIST. Technical guide to information security testing and assessment (sp 800-115), 2020.

[12] OWASP Foundation. Owasp top 10 web application security risks, 2023. Available at https://owasp.org.

[13] OWASP Foundation. Owasp web security testing guide, 2023.

[14] A. Ruotsalainen. Literature review of vulnerability management best practices in cybersecurity. *Computers & Security*, 2024.

[15] Chad Russell. *Web Application Firewalls: Securing Modern Web Applications*. O'Reilly Media, Incorporated, 2018. books.google.com.

[16] Joao Pedro Seara and Carlos Serr˜ ao. Automation of system security˜ vulnerabilities detection using open-source software. *Electronics*, 13(5), 2024.

[17] Oleg Sheyner, Somesh Jha and Jeannette Wing. Automated generation and analysis of attack graphs. *IEEE Symposium on Security and Privacy*, 2002.

[18] Sabina Szymoniak and Kacper Foks. Open source intelligence opportunities and challenges: a review. *Advances in Science and Technology Research Journal*, 18:123–139, 06 2024.

[19] M. K. Yogi. A review of cyber vulnerability assessment methods. *International Journal of Cyber Security*, 2023.