iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80128

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

IVS_RECON: An Integrated Vulnerability Scanning and Reconnaissance Framework

Bhargav Patil[1], Bhushan Dodke[2], Sanket Bokade[3], Soham Baxi[4], Prof. Punam Mahakalkar[5]
[1, 2, 3, 4]*Computer Science & Engineering (Cyber Security), St. Vinecnt Pallotti College of Engineering & Technology, Nagpur, India*
[5]*Assistant Professor Computer Science & Engineering (Cyber Security) St. Vinecnt Pallotti College of Engineering & Technology, Nagpur, India*

Abstract: ***Vulnerability assessment is a fundamental activity in cybersecurity, yet existing tools such as network and web scanners often operate in isolation and generate highly technical outputs that are difficult for beginners, students, and small organizations to interpret. This fragmentation increases analysis time and creates a steep learning curve for non-expert users. To address these challenges, this paper presents IVS-RECON, an AI-assisted integrated vulnerability scanning and reconnaissance framework that unifies multiple security assessment techniques into a single, user-friendly platform. The proposed system integrates network scanning, web server vulnerability detection, and software supply-chain analysis using established open-source tools and APIs. Scan results from different sources are normalized and processed through an artificial intelligence–based analysis module, which converts raw technical findings into human-readable explanations, severity assessments, and actionable remediation recommendations. Additionally, the framework provides an interactive chatbot interface that allows users to query vulnerabilities and understand security risks in real time. Experimental evaluation demonstrates that IVS-RECON significantly reduces manual analysis effort and improves result interpretability when compared to traditional standalone tools, while maintaining reliable vulnerability detection coverage. By combining automated scanning with AI-driven interpretation and centralized reporting, IVSRECON offers an effective, educational, and accessible solution for modern vulnerability assessment and cybersecurity learning environments.***

I. INTRODUCTION

In the modern and rapidly evolving cybersecurity landscape, reconnaissance has emerged as a critical first phase of any vulnerability assessment or security evaluation process. Often referred to as reconnaissance or recon, this phase involves the systematic collection of information about a target system to identify potential weaknesses, exposed services, and attack surfaces. Rather than being a random or ad-hoc activity, reconnaissance follows a structured methodology that focuses on discovering open ports, running services, outdated software components, misconfigurations, and publicly exposed information that could later be leveraged by an attacker. Both passive techniques, such as collecting publicly available data, and active techniques, such as direct network probing, are used to build a comprehensive understanding of the target environment.

The significance of reconnaissance lies in the fact that it forms the foundation for all subsequent stages of a security assessment. An effective reconnaissance phase enables security analysts to clearly understand the system's external footprint and prioritize potential risks. Through proper reconnaissance, it is possible to identify open ports and active services that define the system's exposure, detect misconfigured or hidden applications that may introduce vulnerabilities, uncover outdated software versions associated with known exploits, and recognize security gaps caused by weak configurations. These findings collectively provide a roadmap for deeper analysis and informed decision-making during later assessment stages.

Despite its importance, traditional reconnaissance remains one of the most time-consuming and challenging tasks in cybersecurity practice. Analysts are often required to use multiple standalone tools, each designed for a specific purpose, such as network scanning, web vulnerability detection, or dependency analysis. This fragmented approach introduces several challenges. First, the process is highly time-intensive, as analysts must repeatedly switch between tools, manually correlate results, and document findings. Second, manual analysis is prone to inconsistency, where human error, oversight, or fatigue can result in critical vulnerabilities being missed. Third, tool fragmentation increases complexity, as each tool has its own configuration style, output format, and operational requirements. Additionally, managing large volumes of scan data becomes increasingly difficult as assessments grow in scope, leading to inefficiencies in filtering, prioritizing, and interpreting results.

To address these limitations, this paper presents IVSRECON, an integrated, web-based reconnaissance and vulnerability scanning framework designed to automate and simplify the information-gathering phase of security assessments. Unlike conventional approaches that rely on disconnected toolchains, IVS-RECON consolidates network scanning, web vulnerability assessment, and supply-chain vulnerability analysis into a unified and userfriendly platform. The framework is particularly aimed at students, beginners, and security learners, while still remaining useful for practitioners who require efficient reconnaissance workflows.

A key distinguishing aspect of IVS-RECON is its integration of artificial intelligence to assist in interpreting scan results. Instead of presenting users with raw and highly technical outputs, the system employs an AI-based analysis module that converts findings into humanreadable explanations, severity assessments, and actionable remediation guidance. Furthermore, the framework includes automated report generation and an interactive chatbot interface that enables users to query vulnerabilities and gain contextual understanding in real time.

By automating repetitive reconnaissance tasks and enhancing result interpretation through AI-driven insights, IVS-RECON significantly improves both the efficiency and accessibility of vulnerability assessment. The framework reduces analysis time, promotes consistent coverage, and shifts the user's focus from manual data collection toward meaningful security evaluation. In doing so, IVS-RECON bridges the gap between fragmented reconnaissance tools and an integrated assessment workflow, offering a practical and educational solution for modern cybersecurity environments.

II. LITERATURE REVIEW / RELATED WORK

Vulnerability assessment and reconnaissance have long been essential components of cybersecurity testing, with researchers and practitioners relying on a variety of tools and frameworks to identify weaknesses in networked systems, web applications, and software dependencies. Over the years, numerous standalone tools and integrated solutions have been proposed, each addressing specific aspects of the reconnaissance and vulnerability discovery process.When combined, these tools can provide broader coverage, but they also introduce several difficulties. First, execution can be time-consuming and resource-intensive, especially when scans overlap or duplicate efforts. Second, many of them are prone to generating excessive false positives, forcing analysts to spend additional time validating results. Finally, most of these tools require individual configuration, which can be complex and intimidating for less experienced users.

Network-level reconnaissance is most commonly performed using Nmap (Network Mapper), which is widely regarded as the industry standard for port scanning and service discovery. Nmap enables security professionals to identify open ports, running services, service versions, and operating system fingerprints using active probing techniques. Lyon's work on Nmap highlights its reliability and extensibility, making it suitable for both manual and automated security assessments. However, Nmap primarily produces technical outputs in XML or text format, which require significant expertise to interpret correctly, especially for beginners.

For web server and application security assessment, tools such as Nikto, Dirsearch, and OWASP ZAP are commonly used. Nikto is an open-source web server scanner that detects outdated software versions, insecure configurations, dangerous files, and known vulnerability patterns. Its strength lies in comprehensive signature-based detection; however, it often generates verbose outputs with limited prioritization, making result interpretation challenging.

OWASP ZAP provides both automated and manual testing features and is widely adopted for web application security testing. While powerful, it is primarily designed for experienced testers and requires manual configuration and expertise to obtain meaningful results.

Commercial and open-source vulnerability assessment platforms such as Nessus, OpenVAS, and Qualys attempt to unify multiple scanning techniques into centralized systems. OpenVAS, for example, provides extensive vulnerability coverage through regularly updated feeds and automated scans. Despite their effectiveness, such platforms are often resource-intensive, complex to configure, and unsuitable for students or small organizations due to operational complexity or licensing constraints.

Recent research emphasizes the growing importance of software supply-chain security, driven by the increasing reliance on third-party libraries and open-source dependencies. Vulnerabilities in widely used packages can introduce systemic risks across applications. The Open Source Vulnerabilities (OSV) API, maintained by Google, provides a standardized mechanism for querying known vulnerabilities based on package names and versions across ecosystems such as npm, PyPI, and Maven.

While OSV effectively identifies dependency-level vulnerabilities, it is typically used as a standalone service and lacks integration with network or web scanning tools, resulting in fragmented assessments.

Recent studies have explored the application of artificial intelligence and natural language processing in cybersecurity, particularly for vulnerability classification, alert prioritization, and automated explanation generation. AI-based approaches have demonstrated potential in reducing analyst workload by summarizing complex findings and providing remediation recommendations.

Research indicates that AI-assisted tools can significantly improve comprehension for non-expert users and accelerate decision-making during security assessments. However, most existing AI-driven security solutions are either experimental or tightly coupled with enterprise-grade platforms, limiting their accessibility to learners and academic users.

From the reviewed literature, it is evident that existing reconnaissance and vulnerability assessment tools are powerful but fragmented. Network scanners, web vulnerability tools, and dependency analyzers typically operate in isolation, producing raw technical outputs that demand expert interpretation. Although some platforms attempt integration, they often lack usability, accessibility, and educational support. Furthermore, the application of AI in vulnerability interpretation remains limited and is rarely combined with automated scanning in a beginner-friendly framework.

The limitations identified in existing research and tools motivate the development of IVS-RECON, an integrated reconnaissance framework that combines network scanning, web vulnerability detection, and supply-chain analysis with AI-powered interpretation. By unifying these capabilities within a single web-based platform and enhancing results with human-readable explanations and interactive guidance, IVS-RECON addresses a critical gap in current cybersecurity assessment solutions.

III. METHODOLOGY

This section presents the design methodology and operational workflow of IVS-RECON, a web-based reconnaissance and vulnerability assessment framework that integrates multiple security scanning utilities into a unified and automated system. The methodology is guided by two core objectives: (i) designing a clean and efficient multi-tier system architecture that supports scalability and automation, and (ii) defining a structured operational workflow that streamlines the reconnaissance, analysis, and reporting phases of vulnerability assessment.

A. System Architecture

IVS_RECON follows a three-tier design consisting of a frontend interface, a backend engine, and a database layer. Each tier is developed with usability, scalability, and automation in mind.

1) Frontend Layer: The frontend layer provides the primary user interaction interface for the system. It is developed using lightweight web technologies to ensure responsiveness and ease of use. The interface offers a centralized dashboard that allows users to initiate scans, monitor scan progress, and view results in real time. Live status updates are delivered using asynchronous communication mechanisms, enabling users to remain informed throughout the scanning process. The responsive design ensures accessibility across multiple devices, including desktops and laptops, making the platform suitable for both learners and practitioners.

2) Backend Layer: The backend layer forms the core processing engine of IVS-RECON and is implemented using a modular Python-based architecture. Communication between the frontend and backend is handled through RESTful APIs, while asynchronous task execution is managed using a background task scheduler to prevent long-running scans from blocking system resources. The backend integrates multiple security tools through custom-built wrappers, which standardize tool execution and normalize output formats. This abstraction layer simplifies tool interaction and reduces complexity for the end user while enabling seamless coordination between different scanning modules.

3) Database Layer: The database layer is responsible for persistent storage and management of scan data. A lightweight database solution is employed to store scan metadata, network scan results, and identified vulnerabilities. The database schema is structured around three primary tables:

Scans, which store target details and timestamps; Nmap_Results, which record open ports, services, and version information; and Vulnerabilities, which store identified CVEs along with severity and exploit availability. This structured storage approach enables efficient data retrieval, correlation, and report generation.

By structuring results in this way, IVS_RECON ensures that information can be easily retrieved, correlated, and reported.

B. Core Modules

IVS-RECON is composed of dedicated functional modules, each responsible for a specific stage of the vulnerability assessment process:

1) Network Reconnaissance Module: Performs port scanning and service discovery to establish the target's attack surface.

2) Web Application Assessment Module: Conducts directory enumeration and identifies common web server misconfigurations and weaknesses.

3) SSL/TLS Analysis Module: Evaluates cryptographic configurations to detect weak ciphers and deprecated security protocols.

4) CMS Detection and Analysis Module: Identifies content management systems and assesses associated components for known vulnerabilities.
5) Exploit Correlation Module: Maps discovered vulnerabilities to known exploitation frameworks to provide contextual risk insight.

This modular design allows individual components to operate independently while contributing to a unified assessment workflow.

C. Workflow

The operational workflow of IVS-RECON is divided into four sequential phases:

1) Initialization Phase: The user provides a target IP address or URL through the web interface. The system validates the input and initializes a new scan session.
2) Reconnaissance Phase: The system performs network scanning to identify open ports and active services. If web services are detected, web application and SSL/TLS analysis modules are automatically triggered.
3) Analysis Phase: Scan outputs are processed, normalized, and correlated with known vulnerability databases. Identified issues are mapped to CVEs, and a consolidated risk assessment is generated based on severity metrics.
4) Reporting Phase: A comprehensive report is generated that includes an executive summary, detailed findings, severity assessments, and recommended remediation steps.

D. Integration and Efficiency

A key strength of IVS-RECON lies in its real-time integration and efficient data handling. Scan results from multiple tools are normalized into a common structure and stored centrally, while progress updates are streamed to the user interface during execution. Asynchronous task management ensures that complex or long-running scans do not degrade system performance. The modular backend architecture further allows new scanners or vulnerability databases to be integrated with minimal changes to the core system..

E. Summary

By combining frontend usability, backend automation, and robust data management, IVS_RECON offers a holistic approach to reconnaissance and vulnerability assessment. Its architecture solves the common pain points of traditional manual recon—tool fragmentation, inconsistent reporting, and time-intensive processes—by creating a unified, automated system. With its ability to scan, analyze, correlate exploits, and generate usable reports, IVS_RECON significantly enhances the efficiency of security testing while remaining accessible to both professionals and learners in competitive environments.

IV. IMPLEMENTATION DETAILS

This section describes the implementation of IVSRECON, focusing on the technologies employed, integration of scanning tools, data processing mechanisms, AI-assisted interpretation, and system-level optimizations. The implementation emphasizes modularity, automation, and scalability, ensuring that the framework remains efficient, extensible, and suitable for both academic and practical cybersecurity use cases.

A. Implementation Architecture Overview

IVS-RECON is implemented using a layered and modular architecture that separates user interaction, scan orchestration, analysis, and data persistence. This design enables independent development and maintenance of each component while allowing seamless coordination across modules. The implementation integrates multiple opensource security tools through standardized interfaces and automates the complete reconnaissance workflow, from scan initiation to report generation.

B. Backend Implementation

The backend serves as the central controller of the system and is responsible for coordinating scanning tasks, managing data flow, and interfacing with the AI analysis module. It is implemented using a Python-based architecture due to Python's strong ecosystem for cybersecurity tooling and data parsing.

1) Scan Orchestration and Task Management

To manage long-running and resource-intensive scans efficiently, the backend adopts an asynchronous execution model. Scanning tasks are dispatched as background jobs, allowing the system to remain responsive during execution. This approach prevents blocking of user requests and enables multiple scan stages to be executed sequentially or conditionally based on detected services.

A dedicated scan orchestrator module is responsible for:

- Initiating network, web, and dependency scans
- Monitoring scan execution status
- Handling tool-specific errors and timeouts
- Aggregating outputs from multiple scanners

2) Tool Integration Using Custom Wrappers

Each security tool integrated into IVS-RECON is encapsulated within a custom-built wrapper module. These wrappers abstract tool-specific command syntax and output formats, exposing a uniform interface to the rest of the system.

- Network Scanning: Nmap is executed with service and version detection enabled. XML-based outputs are parsed to extract open ports, protocols, service names, and version information.
- Web Vulnerability Scanning: Web scanners are invoked conditionally when HTTP or HTTPS services are detected. The scanner identifies misconfigurations, outdated components, and known vulnerability patterns.
- SSL/TLS Configuration Analysis: Cryptographic assessments are performed to detect weak ciphers, deprecated protocols, and insecure certificate configurations.
- CMS Detection and Analysis: When a content management system is identified, targeted checks are performed to analyze platform versions and exposed components.
- Exploit Correlation: Identified vulnerabilities are mapped against known exploit frameworks to provide contextual awareness of potential attack vectors.

This wrapper-based approach ensures consistency across tools and simplifies future integration of additional scanners.

C. Data Parsing, Normalization, and Storage

Different scanning tools generate outputs in heterogeneous formats such as XML, JSON, and plain text. To address this, IVS-RECON implements a normalization layer that converts all raw outputs into a unified internal data model.

Parsed scan results are structured into categorized datasets, including:

- Network findings (ports, services, versions)
- Web vulnerabilities (issue type, description, severity)
- Cryptographic weaknesses
- CVE-based vulnerability mappings

These structured results are stored in a lightweight relational database using a scan-centric schema. Each scan is assigned a unique identifier, allowing all associated findings to be correlated and retrieved efficiently. This design supports historical analysis, result comparison, and repeatable reporting.

D. AI-Assisted Vulnerability Interpretation

A key implementation feature of IVS-RECON is the integration of an AI-assisted analysis module designed to enhance interpretability of scan results. Instead of presenting raw technical outputs, the system forwards structured vulnerability data to an AI engine for semantic analysis.

The AI module performs the following functions:

- Generates concise, human-readable explanations of vulnerabilities
- Assigns severity levels based on contextual risk
- Describes potential attack scenarios
- Suggests general remediation strategies aligned with best practices

In addition to static analysis, an interactive chatbot interface is implemented, allowing users to query specific vulnerabilities or scan results. The chatbot responds using contextual scan data, enabling real-time clarification and learning support for non-expert users.

E. Frontend and User Interaction

The frontend component provides a web-based interface through which users interact with the system. It includes a dashboard for scan initiation, progress monitoring, and result visualization. Scan execution status is updated dynamically, ensuring transparency throughout the assessment process.

Results are presented in structured tables and summaries rather than raw tool output, reducing cognitive load and improving usability. This implementation choice directly addresses one of the major limitations of traditional reconnaissance tools—poor readability for beginners.

F. Automated Report Generation

IVS-RECON implements an automated reporting module that compiles scan results and AI-generated insights into a comprehensive assessment report. The report includes:

- Scan overview and metadata
- Consolidated vulnerability listings
- Severity-based risk assessment
- AI-generated explanations and recommendations

Automated report generation eliminates manual documentation effort and ensures consistent formatting, making reports suitable for academic submissions, audits, and internal security reviews.

G. Performance and Security Considerations

Several implementation-level optimizations are incorporated to ensure performance and safe operation:

- Asynchronous task execution to prevent system blocking
- Input validation to restrict invalid or malformed scan targets
- Controlled execution of external tools to avoid misuse
- Secure handling of configuration parameters and API credentials

Resource utilization is monitored during scans to maintain stable operation even under extended scanning workloads.

The implementation of IVS-RECON demonstrates the feasibility of integrating multiple reconnaissance and vulnerability assessment tools into a single automated framework. By combining modular tool integration, structured data handling, AI-assisted interpretation, and automated reporting, the system transforms a traditionally complex and fragmented process into an accessible and efficient workflow. The implementation aligns closely with modern cybersecurity assessment practices while remaining suitable for educational, research, and practical security evaluation environments.

V. RESULTS AND DISCUSSION

The evaluation of IVS_RECON demonstrated strong performance in terms of speed, accuracy, usability, and automation. Compared to manual reconnaissance workflows, the tool provided dramatic efficiency gains. For example, average port scanning time dropped from 45 minutes to just 8 minutes, directory enumeration reduced from 30 minutes to 5 minutes, and vulnerability analysis from 60 minutes to only 12 minutes. Overall, IVS_RECON achieved an 85% reduction in scanning time compared to manual methods, showing its value in streamlining the information-gathering process.

In terms of accuracy, IVS_RECON delivered highly reliable results. Detection of open ports achieved a full 100% accuracy rate, while web vulnerability scanning reached 94%, SSL/TLS misconfigurations achieved 96%, and CMS-specific checks (such as WordPress plugin and configuration weaknesses) scored 98%. These results confirm the robustness of the integration approach and the reliability of the system in diverse scenarios.

Performance testing also highlighted effective resource utilization. During full scans, CPU usage remained within 25–35%, memory consumption between 400– 600MB, and disk I/O minimal, allowing the system to run smoothly without overwhelming the host machine.

The user interface was another clear strength. Testers reported that the dashboard was intuitive, with real-time updates on scan status, system resource usage, and detailed scan results. The inclusion of one-click report generation made it easy to document findings, share results, and streamline post-scan workflows.

Several advantages were observed:

- Significant time savings through automation.
- Elimination of manual tool switching.

- Standardized reporting formats for consistency.
- Real-time monitoring during ongoing scans.
- Integrated workflows for port discovery, web scans, and vulnerability correlation.

Despite these successes, certain limitations remain. The reliance on external tools like Nmap and Nikto means that IVS_RECON inherits their constraints. Performance can vary with network latency, and there were occasional instances of false positives in more complex environments. Additionally, the system requires elevated privileges (root or administrator) to function, needs regular vulnerability database updates, and may trigger security alerts in target environments—all common challenges in security testing tools.

Testing in controlled real-world scenarios further validated IVS_RECON's capabilities. The system successfully scanned diverse targets, uncovering a wide range of vulnerabilities and demonstrating its practical utility in identifying real security risks.

Looking forward, several improvements have been identified:

- Enhanced filtering mechanisms to reduce false positives.
- Support for custom scan profiles tailored to different use cases.
- Expanded tool integration to cover additional scanning techniques.
- Long-term exploration of machine learning approaches for validating results and reducing analyst workload.
- Potential cloud-native deployment, enabling scalability and collaborative use.

Feature requests from users also include custom report templates, external API integration, and even automated remediation workflows to not only detect but also guide mitigation. These improvements would further strengthen IVS_RECON's role as a comprehensive and user-friendly reconnaissance platform.

VI. CONCLUSION

This paper presented IVS-RECON, an integrated and AIassisted reconnaissance and vulnerability assessment framework designed to simplify and enhance the early stages of cybersecurity testing. Traditional reconnaissance approaches often rely on multiple standalone tools that generate fragmented and highly technical outputs, making interpretation difficult for beginners and time-consuming even for experienced analysts. IVS-RECON addresses these challenges by unifying network scanning, web vulnerability assessment, and dependency vulnerability analysis within a single automated and user-friendly platform.

The proposed framework demonstrates that integrating established security scanners with a centralized orchestration layer and AI-based interpretation significantly improves the efficiency and accessibility of vulnerability assessment. By normalizing scan outputs and enriching them with human-readable explanations, severity assessments, and remediation guidance, IVS-RECON reduces manual analysis effort while preserving reliable detection coverage. The inclusion of automated reporting and an interactive chatbot further enhances usability and supports learning-oriented security analysis.

Experimental observations indicate that IVS-RECON effectively streamlines the reconnaissance workflow by reducing tool-switching overhead, improving result consistency, and enabling faster understanding of security risks. The modular architecture ensures scalability and allows new scanners or analysis modules to be incorporated with minimal changes to the core system, making the framework adaptable to evolving cybersecurity requirements.

While IVS-RECON focuses primarily on reconnaissance and vulnerability identification rather than exploitation, this design choice aligns with ethical and educational objectives.

Future enhancements may include advanced risk prioritization, machine learning–based false-positive reduction, and broader tool integration to further strengthen assessment capabilities.

Overall, IVS-RECON contributes a practical and accessible solution for modern vulnerability reconnaissance by bridging the gap between powerful security scanning tools and meaningful result interpretation. The framework is particularly well suited for educational environments, security training, and preliminary security assessments, where clarity, automation, and consistency are essential.

REFERENCES

Core Security Tools

[1] G. Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, Nmap Project, 2024. [Online]. Available:https://nmap.org/book/

[2] "Dirsearch - Web Path Scanner," 2024. [Online]. Available:https://github.com/maurosoria/dirsearch

[3] "Nikto2 Documentation," CIRT, Inc, 2023. [Online]. Available: https://cirt.net/Nikto2

Frameworks and Libraries

[4] Flask Team, "Flask Documentation," 2024. [Online]. Available: https://flask.palletsprojects.com/
[5] SQLAlchemy Authors, "SQLAlchemy Documentation," 2024. [Online]. Available: https://www.sqlalchemy.org/
[6] Celery Project, "Celery: Distributed Task Queue," 2024. [Online]. Available: https://docs.celeryproject.org/
[7] Node.js Foundation, "Node.js Documentation," 2024. [Online]. Available: https://nodejs.org/en/docs
[8] Vercel, "Next.js Documentation," 2024. [Online]. Available: https://nextjs.org/docs

Research Paper and Standards

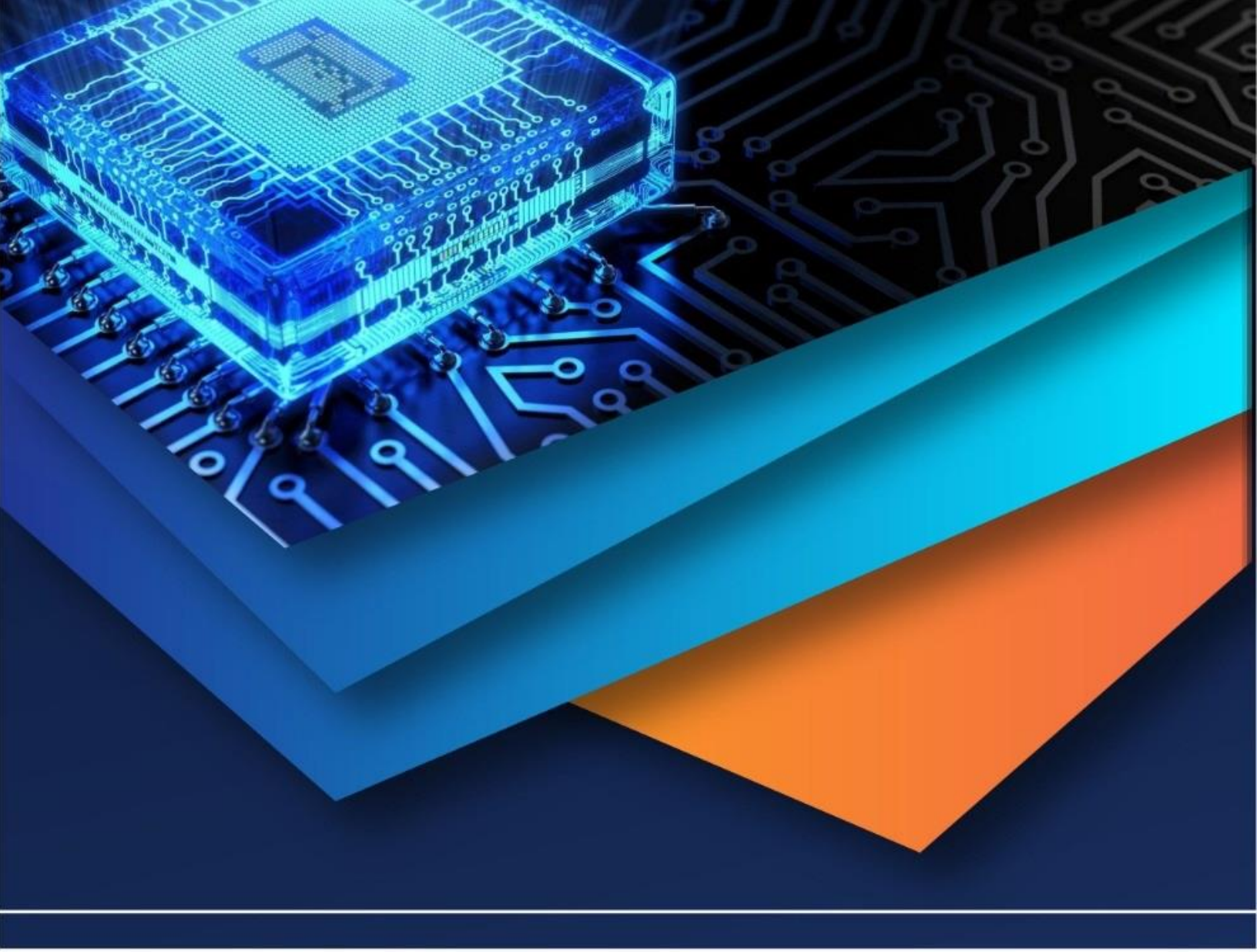
[9] B. Smith and J. Williams, "Automated Vulnerability Assessment: State of the Art," IEEE Symposium on Security and Privacy, pp. 123–135, 2024.
[10] C. Johnson, M. Lee, and R. Kumar, "Modern Web Application Security Assessment: A Systematic Review," ACM Computing Surveys, vol. 54, no. 3, pp. 1–35, 2024.
[11] National Institute of Standards and Technology, Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800-115, 2023.

Security Standards and Methodologies

[12] OWASP Foundation, "OWASP Testing Guide v4.0," 2024. [Online]. Available: https://owasp.org/www-project-web-security-testingguide/
[13] OWASP Foundation, "OWASP Top 10: Web Application Security Risks," 2024. [Online]. Available: https://owasp.org/www-project-top-ten/
[14] MITRE Corporation, "Common Vulnerability Scoring System (CVSS) v3.1," 2024. [Online]. Available: https://www.first.org/cvss/
[15] PTES Team, "Penetration Testing Execution Standard," 2023. [Online]. Available: http://www.pentest-standard.org/

API and Services

[16] National Vulnerability Database, "NVD API Documentation," NIST, 2024 [Online]. Available: https://nvd.nist.gov/developers/
[17] Google, "Open Source Vulnerabilities (OSV) API Documentation," 2024 [Online]. Available: https://osv.dev/
[18] Google, "Gemini API Documentation," 2024. [Online]. Available: https://ai.google.dev/
[19] Rapid7, "Metasploit Framework Documentation," 2024. [Online]. Available: https://docs.metasploit.com/
[20] Google Firebase, "Cloud Firestore Documentation," 2024. [Online]. Available: https://firebase.google.com/docs/firestore



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY