iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2026 **Issue:** Conference **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82958

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 V May 2026- Available at www.ijraset.com
National Conference on Innovation in Engineering and Technology-(NCIET2026)

Darkblend: An Integrated Automated Vulnerability Scanner With AI Powered Reporting

Suriyakala A V[1], Chaitanya Sawant[2], Bhumesh Patil[3], Purva Salgaonkar[4], Manali Bhuvad[5]
[1]*Professor,* [2, 3, 4, 5]*Student Department of Artificial Intelligence And Data Science, ACPCE, Kharghar*

Abstract: ***Cyberattacks are growing at a pace that makes traditional, manual vulnerability assessments increasingly inadequate. Organizations of all sizes struggle to keep up with threats because most available tools are either too narrow in scope, too complex for non-expert users, or too expensive to deploy at scale. This paper introduces DarkBlend, a web-based automated vulnerability scanner that unifies network scanning, web application analysis, and local system assessment under a single user-friendly platform. The system is built on Python and Flask, uses Nmap for port-level analysis, and generates intelligent, actionable security reports. Authentication is handled through a one time password (OTP) mechanism, and all scan data is persisted in a PostgreSQL database. Experimental evaluations show that DarkBlend reliably detects open ports, missing HTTP security headers, SSL certificate issues, DNS misconfigurations, and exposed subdomains. The results establish DarkBlend as a practical and accessible cybersecurity tool suited for educational settings, small organizations, and individual practitioners who need proactive, automated threat detection without deep domain expertise.***

Keywords — Vulnerability scanner, automated security, network scanning, web application security, OTP authentication, AI-powered reporting, Flask, Nmap, PostgreSQL.

I. INTRODUCTION

The rapid expansion of internet-connected systems has fundamentally altered the threat landscape for organizations around the world. Networks, web applications, and local machines face relentless probing by automated bots and human attackers who exploit weaknesses ranging from open ports and misconfigured servers to missing security headers and expired SSL certificates. In 2024 alone, the number of publicly disclosed vulnerabilities reached record levels, reinforcing the urgency for faster and more comprehensive security assessment workflows. Manual penetration testing has long been the gold standard for security evaluation. However, it demands expert practitioners, carries a high cost, and cannot realistically keep pace with the speed at which modern infrastructure changes. This gap creates a window ofexposure that attackers are consistently able to exploit. Automated scanning tools partially address this problem, but most existing solutions are fragmented, addressing only web security or only network enumeration, rarely both. Furthermore, many tools present their findings in a format that is inaccessible to beginners or non-technical stakeholders, limiting their real-world usefulness. DarkBlend was conceived to close these gaps. It is a unified, open-source vulnerability scanning platform that combines three scanning modules IP/network scanning, web application scanning, and local system scanning into one coherent web interface. Users authenticate via OTP, submit scan targets through a simple dashboard, and receive structured reports enriched with AI-generated remediation guidance. By democratizing access to automated security assessment, DarkBlend aims to help individuals, students, and small organizations take a proactive stance against cyber threats without needing expensive tools or specialist staff.

II. LITERATURE REVIEW

Automated vulnerability scanning has attracted considerable research attention over the past decade, producing tools and platforms with varying strengths and limitations. Verma et al. [1] presented XploitGuard, a modular automated scanner that targets SQL injection, cross-site scripting (XSS), and open port enumeration. The tool correlates multiple vulnerability signals before generating a report, which reduces the false-positive rate significantly compared to single-signal scanners. While XploitGuard demonstrates strong performance in controlled test environments such as DVWA and Metasploitable, it lacks a persistent authentication layer and does not provide AI-augmented reporting. Moreira et al. [2] proposed a microservices-based platform for automated web vulnerability detection that is specifically designed to serve organizations without in house security expertise. The system achieves a detection rate above 85% on known vulnerabilities by combining static and dynamic analysis techniques.

However, its architecture is complex to deploy and the platform concentrates solely on web applications, leaving network and system-level risks unaddressed. [3] developed a Web Vulnerability Scanner (WVS) that crawls target applications to build a structural model before initiating injection tests. This context-aware approach reduces false positives and improves relevance. The tool also integrates with CI/CD pipelines, enabling security checks as part of the software development lifecycle. Its primary limitation is the absence of network level scanning and user-friendly reporting for non technical audiences. Zhang et al. [4] introduced IMap, which offloads scanning logic to P4-programmable network switches to achieve line-rate throughput up to 40 Gbps. While IMap is technically impressive for enterprise and campus network monitoring, its dependency on specialized hardware places it beyond the reach of most small-scale deployments Patel et al. [5] presented a sophisticated network scanning tool that correlates detected service versions with the National Vulnerability Database (CVD) to flag hosts running known-vulnerable software. Features such as OS fingerprinting and stealth scanning make it well-suited for authorized penetration testing. Like IMap, however, it is positioned for expert practitioners and does not serve non technical users well. A consistent theme across the literature is fragmentation: tools excel within a specific domain but do not provide holistic coverage. None of the surveyed systems offers a single platform combining network, web, and system scanning alongside a beginner-friendly interface, secure OTP authentication, persistent storage, and reporting. DarkBlend directly addresses this research gap.

III. METHODOLOGY

The methodology used in this research focuses on developing an automated vulnerability scanning platform called DarkBlend that is simple, efficient, and user-friendly. The system was developed using Python and the Flask framework because they support fast development and easy integration with cybersecurity tools. The platform was designed in a modular structure so that network scanning, web scanning, and system monitoring could work independently while being connected through a single dashboard.The first stage involved implementing a secure OTP-based authentication system. Instead of traditional passwords, users receive a six-digit verification code through email using Flask-Mail. This approach improves both security and user convenience. After successful login, user details and scan history are stored in a PostgreSQL database.

DarkBlend consists of three main scanning modules. The Network/IP Scanning Module uses Nmap to detect active hosts, open ports, and running services within a network. The Web Application Scanning Module checks websites for security issues such as missing HTTP security headers, SSL certificate problems, DNS misconfigurations, and exposed subdomains. The System Scanning Module monitors the local machine using Python libraries like psutil and platform to collect information about CPU usage, memory, disk status, processes, and system health.After scanning, all results are combined into a structured JSON format. An AI-based reporting system then analyzes the findings, prioritizes vulnerabilities according to severity, and provides simple remediation suggestions. The final reports are displayed on the dashboard and can also be exported as PDF documents.To test the effectiveness of the system, scans were performed on local devices, IPs, and real-world websites. The results showed that DarkBlend could successfully identify vulnerabilities such as open ports, SSL issues, missing security headers, DNS problems, and unusual system activities, proving that the methodology provides a reliable and automated security assessment solution.

IV. RESULTS AND DISCUSSION

DarkBlend was successfully deployed and tested in a controlled environment using local network devices, public IP addresses, and real-world websites. The platform demonstrated reliable performance across all scanning modules and provided accurate vulnerability detection with simplified reporting.The OTP-based authentication system worked efficiently by delivering verification codes to registered email addresses within 5 to 15 seconds under normal network conditions. Invalid or expired OTPs were consistently rejected, confirming the reliability of the access control mechanism. The use of TLS-encrypted SMTP communication and Flask secure session management further strengthened the platform’s security.Performance testing showed that the system responded quickly during scans. Network/IP scans generally completed within 15 to 45 seconds depending on firewall restrictions and target complexity. Web application scans took around 2 to 8 seconds, while local system scans returned results in less than one second because the data was collected directly from the host machine. Report generation and dashboard rendering required an additional 1 to 3 seconds, making the complete user experience smooth and responsive.The Network/IP Scanning Module accurately identified open ports and running services on tested hosts. For example, when scanning a public DNS resolver, the system correctly detected ports 53 and 443 as open. During internal network testing, the scanner also discovered an unnoticed HTTP administrative interface running on port 80, showing its usefulness for practical security auditing.The Web Application Scanning Module produced detailed and informative results.

When tested on a deliberately misconfigured website, the platform detected an invalid SSL certificate, multiple missing HTTP security headers, an exposed FTP port, and missing SPF/DMARC records. The AI-powered reporting system categorized these vulnerabilities into Critical, High, and Medium severity levels and provided remediation guidance with suggested commands and fixes.

From a security perspective, DarkBlend itself was designed with secure implementation practices. Input validation and sanitization were applied to IP addresses and URLs before processing them through Nmap or HTTP libraries, reducing the risk of malicious injection attacks. The OTP mechanism, with one million possible combinations and short expiry duration, made brute-force attacks impractical.When compared with existing tools such as Nessus and OpenVAS, DarkBlend offers a lightweight and user-friendly alternative. Although it does not provide the extensive vulnerability database available in commercial tools like Nessus, it removes licensing costs and simplifies deployment. Unlike OpenVAS, which often requires complex setup and dedicated infrastructure, DarkBlend can run as a standard Flask application with minimal configuration.A major advantage of DarkBlend is the integration of network scanning, web application testing, system monitoring, OTP-based authentication, database storage, and AI-powered reporting within a single platform. This combination makes the system especially suitable for educational environments, small organizations, and users with limited cybersecurity expertise. Overall, the results confirmed that DarkBlend provides an effective, reliable, and practical automated vulnerability assessment solution.

Table No. 1 :Key Findings with existing systems.

Feature	Nessus	OpenVAS	Acunetix	DarkBlend
Cost	Paid	Free	Paid	Free
Scan Scope	Network + Web	Network	Web only	Network + Web + System
Setup	Medium	Complex	Medium	Easy
Authentication	Password	Password	Password	Email OTP
Dashboard	Advanced	Basic	Advanced	Interactive
Database	Proprietary	Proprietary	Proprietary	PostgreSQL
Beginner Friendly	Partial	No	Partial	Yes
History Tracking	Yes	Yes	Yes	Yes
Open Source	No	Yes	No	Yes

V. CONCLUSION

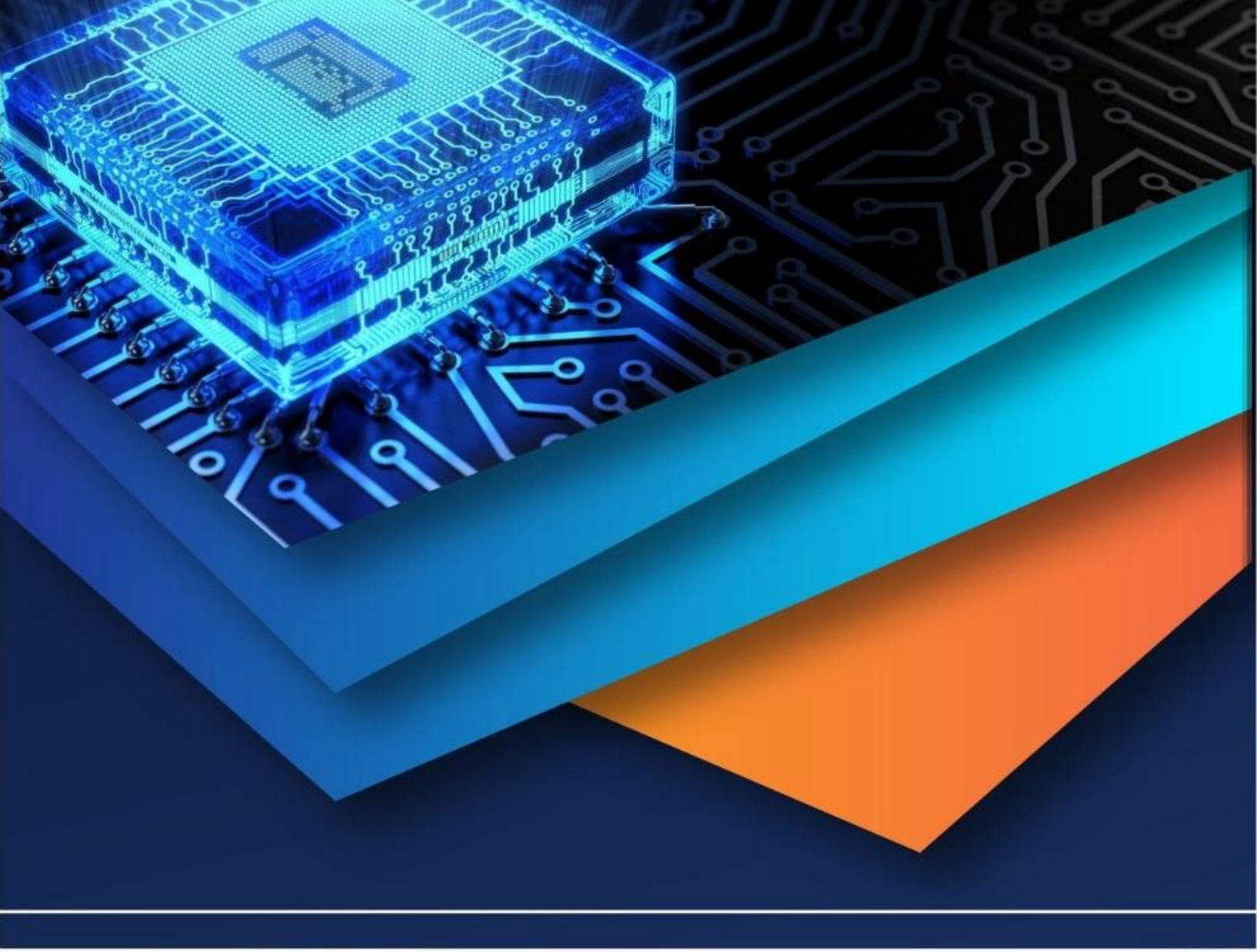
This paper presented DarkBlend, an integrated automated vulnerability scanner that addresses a persistent gap in the cybersecurity tool landscape: the absence of a single, open-source platform that combines multi-layer scanning with accessibility for non-expert users. By uniting IP/network scanning, web application analysis, and local system assessment under a Flask-based web interface secured by OTP authentication and supported by AI powered reporting, DarkBlend demonstrates that professional-grade security assessment does not need to be expensive or technically forbidding. Evaluation results confirm that the platform reliably detects open ports, missing security headers, SSL certificate problems, DNS misconfigurations, and exposed subdomains. Scan latencies are practical for regular use, and the AI-generated reports provide actionable remediation steps that users at any skill level can follow. Future work will prioritize several high-value enhancements. NVD and Shodan API integration will enable automatic CVE correlation, elevating DarkBlend from a configuration scanner to a vulnerability intelligence platform. Active web vulnerability testing using safe, non-destructive payloads will extend detection to OWASP Top 10 injection categories. A Celery-based job scheduler will support continuous and scheduled scanning. Machine learning models trained on historical scan data will enable anomaly detection for emerging threats. Finally, Docker containerization and cloud deployment will simplify installation and enable globally accessible, scalable operation. DarkBlend establishes a strong and extensible foundation for these future contributions, and the team intends to continue its development as an open-source project aligned with the curriculum of the Department of Artificial Intelligence and Data Science at A.C. Patil College of Engineering.

VI. ACKNOWLEDGEMENT

The authors express their sincere gratitude to Prof. Suriyakala A V for her consistent guidance, constructive feedback, and encouragement throughout this project. They also thank the Department of Artificial Intelligence and Data Science, A.C. Patil College of Engineering, for providing the resources and environment necessary to carry out this research. Finally, the authors acknowledge the support of their families and colleagues whose encouragement made this work possible.

REFERENCES

[1] A. Verma, A. K. Singh, D. Shukla, R. Sharma, and S. Laroiya, "XploitGuard: Automated Vulnerability Scanning Tool," International Journal of Computer Science and Security, vol. 15, no. 2, pp. 45–58, 2025.
[2] D. Moreira, J. P. Seara, J. P. Pavia, and C. Serrão, "Intelligent Platform for Automating Vulnerability Detection in Web Applications," IEEE Access, vol. 12, pp. 34201–34215, 2024.
[3] P. Patel, R. V. Reddy, D. S. Kiran, J. S. S. Harsha, and A. M. P. Reddy, "Enhancing Web Application Security: A Comprehensive Approach with WVS," International Journal of Advanced Computer Science and Applications, vol. 15, no. 3, pp. 102–115, 2024.
[4] M. Zhang, G. Li, C. Guo, H. Bao, M. Xu, H. Hu, and F. Li, "IMap: Toward a Fast, Scalable and Reconfigurable In-Network Scanner With Programmable Switches," IEEE Transactions on Network and Service Management, vol. 21, no. 2, pp. 1987–2001, 2024.
[5] S. Patel, P. Christian, K. Mistry, K. Raj, and H. Raithatha, "Enhancing Network Security with Advanced Network Scanning Tools," International Journal of Network Security and Its Applications, vol. 16, no. 1, pp. 23–37, 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY