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.2026.80000

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

Penetration Testing Tool

Ashit Tagde[1], Himanshu Pathrabe[2], Rudra Masram[3], Ishant Fule[4], Sahil Meshram[5], Dr. Sapna Waghmare[6]
[1, 2, 3, 4, 5]*Students, Department of Computer Science and Engineering, Guru Nanak Institute of Technology, Nagpur, India*
[6]*Associate Dean (CSE & Allied Branches), Guru Nanak Institute of Technology, Nagpur, India*

Abstract: ***The increasing number of cyber-attacks and system vulnerabilities has created a strong need for automated penetration testing solutions. This project focuses on developing a web-based Penetration Testing Tool that integrates multiple open-source security scanners, including Nmap, Nikto, and Burp Suite, to identify vulnerabilities in web applications and networks. The system aims to provide a single, interactive platform for ethical hackers, cybersecurity researchers, and administrators to assess potential security weaknesses. The proposed tool automates scanning, performs vulnerability assessment, and generates comprehensive real-time reports. This approach minimises manual effort, reduces testing time, and improves vulnerability-detection accuracy compared to traditional manual testing methods.***
Index Terms: Penetration Testing, Vulnerability Scanning, Cybersecurity, Network Security, Ethical Hacking.

I. INTRODUCTION

Protecting organisational infrastructure in the current digital age makes cybersecurity an absolute necessity. Due to fast-paced technological advancements, cybercriminals frequently exploit system vulnerabilities, which puts data integrity, confidentiality, and availability at serious risk. A vital method for testing an organisation's strength against such cyber threats is Penetration Testing. This approach uses controlled attacks to locate weak points before actual attackers have the chance to misuse them. The primary objective behind the Penetration Testing Tool introduced in this research is to automate the entire testing process. By bringing together several open-source scanners, this system provides an all-in-one platform created with PHP, SQL, and shell scripting. Major functionalities offered by the tool include network scanning, identification of web application flaws, phishing attack detection, and automated generation of reports. With the help of centralised oversight and live result streaming, the platform greatly improves the speed and user-friendliness of penetration testing, making it suitable even for people who lack advanced technical skills.

II. NEED OF THE STUDY

Manual penetration testing is time-consuming, requires deep technical expertise, and often fails to cover all possible attack surfaces. Additionally, using separate tools for different vulnerability tests can be inefficient. Hence, there is a need for a multi-functional penetration testing platform that consolidates all major testing features into a single environment. The proposed system addresses these issues by integrating multiple tools and automating the scanning process, making it suitable for small organisations, educational institutions, and cybersecurity learners.

III. RESEARCH METHODOLOGY

The project adopts an experimental and development-based methodology. The workflow includes:

1) Requirement Analysis: Identify major penetration testing functionalities such as network scanning, web vulnerability scanning, and phishing detection.
2) Tool Integration: Integrate open-source tools — Nmap for network discovery, Nikto for web vulnerability scanning, and Burp Suite for advanced security testing.
3) Backend Development: Use PHP and MySQL to manage test configurations, store results, and generate reports.
4) Frontend Interface: Develop an interactive web dashboard allowing users to select tools, input target URLs/IPs, and view live scan progress.
5) Testing & Validation: Perform test runs on sample networks and web applications to evaluate detection efficiency, speed, and reliability.

IV. RESULTS AND DISCUSSION

The developed system successfully detects various network and web-based vulnerabilities, including open ports, outdated software versions, insecure headers, and potential injection points. The real-time reporting feature displays scan progress dynamically and stores results for future analysis.

©IJRASET: All Rights are Reserved

The tool simplifies complex testing procedures into a single, user-friendly interface and provides accurate, actionable insights for system administrators. Performance evaluation shows that automated testing using this tool significantly reduces the time and manual effort required compared to traditional methods. The integration of multiple scanners ensures comprehensive vulnerability coverage, while the modular design allows easy addition of future tools and functionalities.

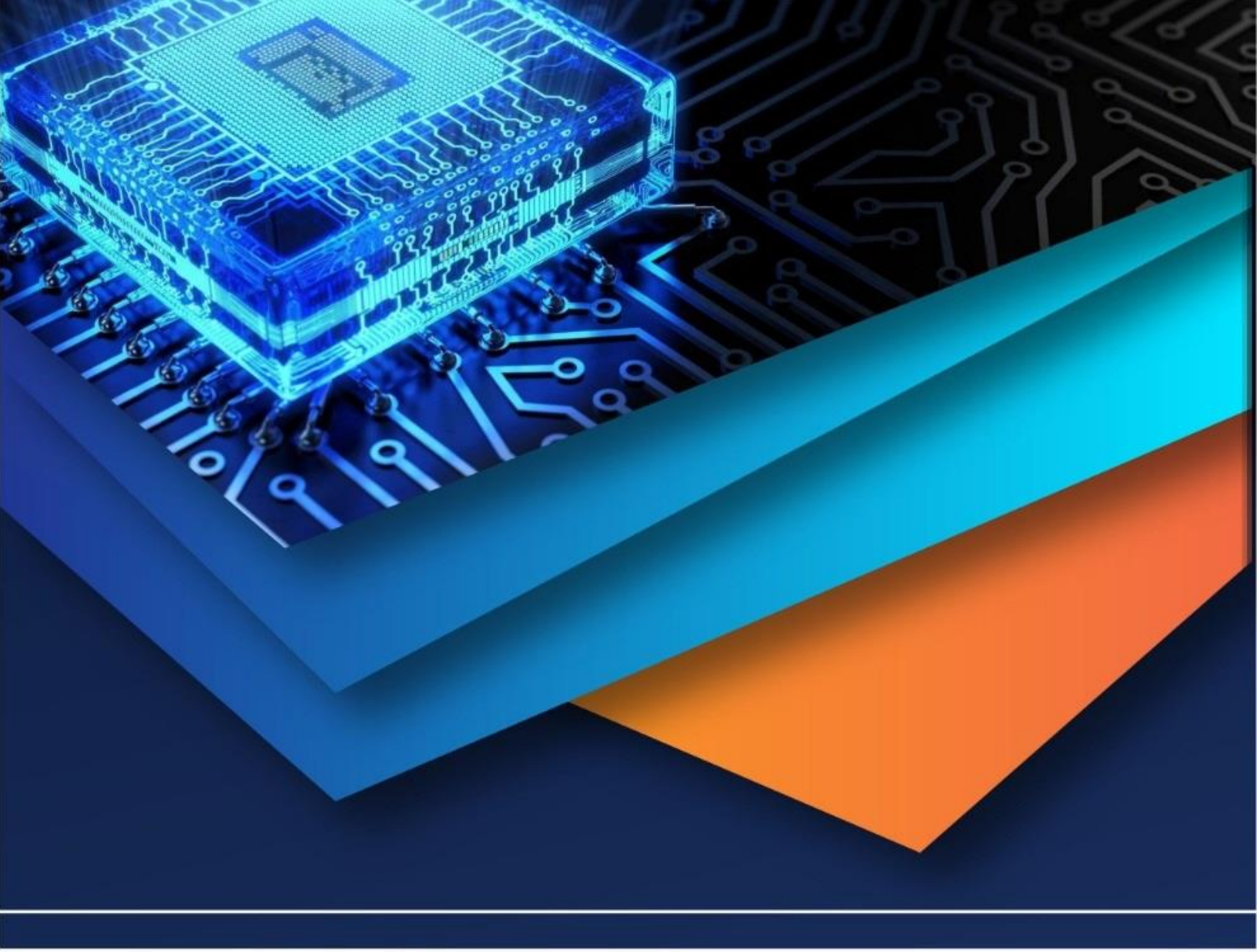
V. ACKNOWLEDGMENT

The researchers wish to offer their heartfelt thanks to their project guide and departmental mentors for their skilled direction, constructive input, and unwavering assistance during the course of this research work, named "Penetration Testing Tool." The authors further wish to acknowledge the Department of Computer Science for making available the necessary facilities and resources that were crucial for the proper completion of this project. In addition, deep appreciation is extended to family members and fellow students for their steady encouragement, patience, and inspiration throughout the entire research journey.

REFERENCES

[1] OWASP Foundation. 2023. OWASP Testing Guide for Web Application Security. OWASP.
[2] Nmap Security Scanner. n.d. Network Exploration and Security Auditing Tool. Insecure.org.
[3] CIRT.net. n.d. Nikto Web Scanner – Open Source Web Server Scanner.
[4] PortSwigger. 2024. Burp Suite Professional Documentation.
[5] Stallings, W. 2022. Network Security Essentials: Applications and Standards. Pearson Education.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)