iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83650

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 VI June 2026- Available at www.ijraset.com

A Survey of Vulnerability Assessment Tools for Cyber Security

Himanshu Sharma[1], Sanjeev Kumar[2], Manushi Khatri[3], Anshul[4]
[1, 2, 3]*Computer Science & Engineering Department, GRD Institute of Management Technology (GRDIMT), Dehradun*
[1, 4] *IILM University, Greater Noida*

Abstract: ***Vulnerability scanning tools are rapidly becoming integral to organizational cybersecurity. These tools aid in the identification and assessment of system and application weaknesses. Given the complexity of modern cyberattacks, the automation of these tools aids in the security of cyber assets. This survey provides an overview of the scanning tools, their architectures, methodologies, capabilities, strengths, weaknesses, and the domains where they are applied. This study surveys scanners in the environments they are built for and provides a summary of major scanning tools such as Nmap, Nessus, OpenVAS, Nikto, Burp Suite, OWASP ZAP, Acunetix, Qualys, Nexpose. This survey discusses the nascent trends such as the use of artificial intelligence for automated vulnerability assessment, the security scanning of cloud-native applications, and the DevSecOps paradigm.***

Keywords: Vulnerability Assessment, Cybersecurity, Vulnerability Scanning Tools, AI-Powered Security Analysis,

I. INTRODUCTION

Organizations experience unending attempts to breach data and exploit systems due to the ever changing cyber threats, including Ransomware, Privilege Escalation, and System Compromise. Applications, Operating Systems, Network Devices, and Cloud Services, used by most organizations, are still potential targets for cyber attackers. An example of an emerging trend includes vulnerability scanning as seen in Fig. 1, as well as the classification of some available assessment tools by their vulnerabilities.
Vulnerability scanning involves searching for system weaknesses that are already known and documented. Vulnerability scanning is achieved by using databases that list these system vulnerabilities. Sample databases of this nature are illustrated in Table 1:

Table1: Different types of Vulnerabilities

Vulnerability	Description
Common Vulnerabilities and Exposures (CVE)	public list of known cybersecurity vulnerabilities and cyber threats by standard identifiers. Identified vulnerabilities receive a CVE ID (e.g., CVE-2025-12345).
Common Weakness Enumeration (CWE)	A catalog of software and hardware security weakness and threats by the community. Occasional security threats are due to lack of quality coding. Examples are SQL Injection, Buffer Overflow, etc.
National Vulnerability Database(NVD)	A vulnerability information database by the U.S. government. Vulnerability records are enriched by severity, impacts, and remediation. The database is maintained by the National Institute of Standards and Technology.
Common Vulnerability Scoring System (CVSS)	A common scoring system by standards to rate the severity of security vulnerabilities. The score is in the range of 0.0 to 10.0.

Vulnerability scanners assist security professionals in performing:

- Assessing Risk
- Auditing for Compliance
- Preparing for Penetration Tests
- Monitoring Security
- Prevention of Incidents

Fig.1 A Survey of Vulnerability Scanning Tools

II. PROCESS FOR VULNERABILITY ASSESSMENT

The process for conducting a vulnerability assessment usually entails the following steps:

Step 1: Discovery of Targets

- Finding hosts, servers, applications, and services.
- Discovering live hosts on a network.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Step 2: Collection of Information
- Detect operating systems.
- Enumerate services.
- Conduct port scanning.
- Conduct banner grabbing.

Step 3: Vulnerability Identification
- Match services with known vulnerabilities.
- Match software versions to vulnerabilities on CVE.

Step 4: Risk Evaluation
- Determine severity levels.
- Prioritize vulnerabilities.

Step 5: Reporting
- Generate reports.
- Recommend remedial actions.

III. CLASSIFICATION OF VULNERABILITY SCANNERS

A. Network Vulnerability Scanners

These scanners detect vulnerabilities in network devices, servers, routers, firewalls and operating systems. Examples:
- Nmap
- Nessus
- OpenVAS
- Qualys VMDR
- Nexpose

Key Features:
- Port scanning
- Service detection
- Operating system fingerprinting
- CVE matching

B. Web Application Vulnerability Scanners

Concerned about finding vulnerabilities in web applications.
Examples:
- OWASP ZAP
- Burp Suite
- Acunetix
- Netsparker

It detects SQL Injection, Cross-Site Scripting (XSS), CSRF, Command Injection and File Inclusion

C. Database Vulnerability Scanners

Evaluate database security setups and weaknesses.
Examples:
- IBM Guardium
- AppDetectivePro
- Scuba Database Scanner

It can detect Weak passwords, misconfigurations and unauthorized privileges.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

D. Cloud Vulnerability Scanners

For cloud infrastructures and containerized environments.

Examples:

- Prisma Cloud
- Wiz
- Lacework
- AWS Inspector.

It can identify Misconfigured cloud resources, Container vulnerabilities, IAM issues and Exposed storage buckets.

IV. SURVEY OF POPULAR VULNERABILITY SCANNING TOOLS

A. Nmap (Network Mapper):

Nmap is an open source network scanning utility that is widely used.

Features

- Host discovery
- Port scanning
- OS fingerprinting
- NSE scripting engine Advantages
- Fast scanning
- Highly customizable
- Extensive community support.

Limitations:

Lack of ability to assess the vulnerability of the system.

- Requires expertise

Best Use Case: Network Reconnaissance, or Enumeration.

B. Nessus

Nessus is a Tenable-developed commercial vulnerability scanner.

Features:

- Comprehensive vulnerability database
- Compliance checks
- Configuration auditing
- Patch assessment

Advantages:

- High detection accuracy
- User-friendly interface
- Regular updates Limitations:
- Commercial licensing
- Resource intensive

Best Use Case: Vulnerability management in Enterprise.

C. OpenVAS

OpenVAS is an open source Vulnerability Assessment framework.

Features:

- Vulnerability scanning
- Threat intelligence feeds
- Detailed reporting

Advantages:
Open source and free.
• Large vulnerability database
Limitations:
• Slower scanning
• Complex setup
Best Use Case: Academic research and small organisations.

D. Qualys VMDR

Qualys VMDR (Vulnerability Management, Detection, and Response) is a cloud vulnerability management platform. Features:
• Continuous monitoring
• Asset discovery
• Patch management
• Risk prioritization
Advantages:
• Scalable
• Cloud-native architecture

Limitations:
• Subscription cost
• Internet dependency
Ideal Use Case: Enterprise environments with large number of users.

E. Rapid7 Nexpose

Nexpose provides real-time vulnerability assessment and risk scoring.
Features
- Live vulnerability monitoring
- Risk-based prioritization
- Compliance reporting

Advantages
- Dynamic risk scoring
- Excellent dashboards

Limitations
- Higher cost
- Learning curve

Best Use Case: Security Operations Centers (SOC).

F. Nikto

Nikto is an open source web server scanner. Features
• Detects outdated software
• Identifies dangerous files
• Server misconfiguration analysis Advantages
• Lightweight
• Fast deployment Limitations
• Generates false positives
Limited modern Web Application test is performed.
Limited modern Web Application test is conducted.
Best use Case: urity assessment

G. OWASP ZAP

OWASP Zed Attack Proxy (ZAP) is a free OWASP maintained web application security testing tool.
Features:
• Automated scanning
• Proxy interception
• Active and passive testing
• API security testing Advantages:
• Free and open source
• Beginner friendly
• CI/CD integration Limitations: Lacking of advanced enterprise features is limited. The best use case is for Web application security testing.

H. Burp Suite

PortSwigger has created Burp Suite, a professional web security testing platform.
Features:
• Intercepting proxy
• Automated scanner
• Intruder testing
• Repeater module
Advantages:
• Industry standard
• Extensive plugins
Limitations: A commercial version is needed for advanced scanning.
Best Use Case: Penetration testing and Bug Bounty Programs.

I. Acunetix

Acunetix specializes in automated web application vulnerability scanning.
Features:

- Deep crawling
- Authentication testing
- Vulnerability verification

Advantages:

- High accuracy
- Easy setup

Limitations:

- Expensive licensing

Best Use Case: Enterprise web security.

V. COMPARATIVE ANALYSIS

Tool	Type	Open Source	Web App Testing	Network Testing	Enterprise Support
Nmap	Network	Yes	No	Yes	Limited
Nessus	Network	No	Partial	Yes	Excellent
OpenVAS	Network	Yes	Partial	Yes	Good
Qualys	Cloud/Network	No	Yes	Yes	Excellent
Nexpose	Network	No	Partial	Yes	Excellent
Nikto	Web	Yes	Yes	No	Limited
OWASP ZAP	Web	Yes	Yes	No	Good
Burp Suite	Web	Partial	Yes	No	Excellent
Acunetix	Web	No	Yes	No	Excellent

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

VI. EMERGING TRENDS IN VULNERABILITY SCANNING

A. AI-Powered Vulnerability Assessment

Artificial Intelligence is increasingly being integrated into vulnerability scanners for:

- Intelligent prioritization
- False-positive reduction
- Automated risk assessment
- Attack path analysis

Examples:

- AI-assisted vulnerability triage
- Security Copilot systems
- Agentic AI security platforms

B. DevSecOps Integration

Modern scanners integrate directly into:

- GitHub Actions
- GitLab CI/CD
- Jenkins
- Azure DevOps

Benefits:

- Shift-left security
- Continuous vulnerability assessment
- Faster remediation

C. Cloud-Native Security

Modern scanners now support:

- Containers
- Kubernetes
- Serverless environments
- Multi-cloud deployments

D. Attack Surface Management (ASM)

Organizations are moving from periodic scanning toward continuous attack surface monitoring. Its capabilities include:

- Asset discovery
- External exposure analysis
- Shadow IT detection
- Continuous monitoring

VII. RESEARCH CHALLENGES

Current vulnerability scanners face several challenges:

1) High false-positive rates
2) Limited zero-day detection
3) Incomplete asset visibility
4) Cloud complexity
5) Large-scale scan management
6) Correlation of multi-tool findings
7) Vulnerability prioritization

Future research directions include:

- Agentic AI-driven scanners
- Automated exploit chain analysis

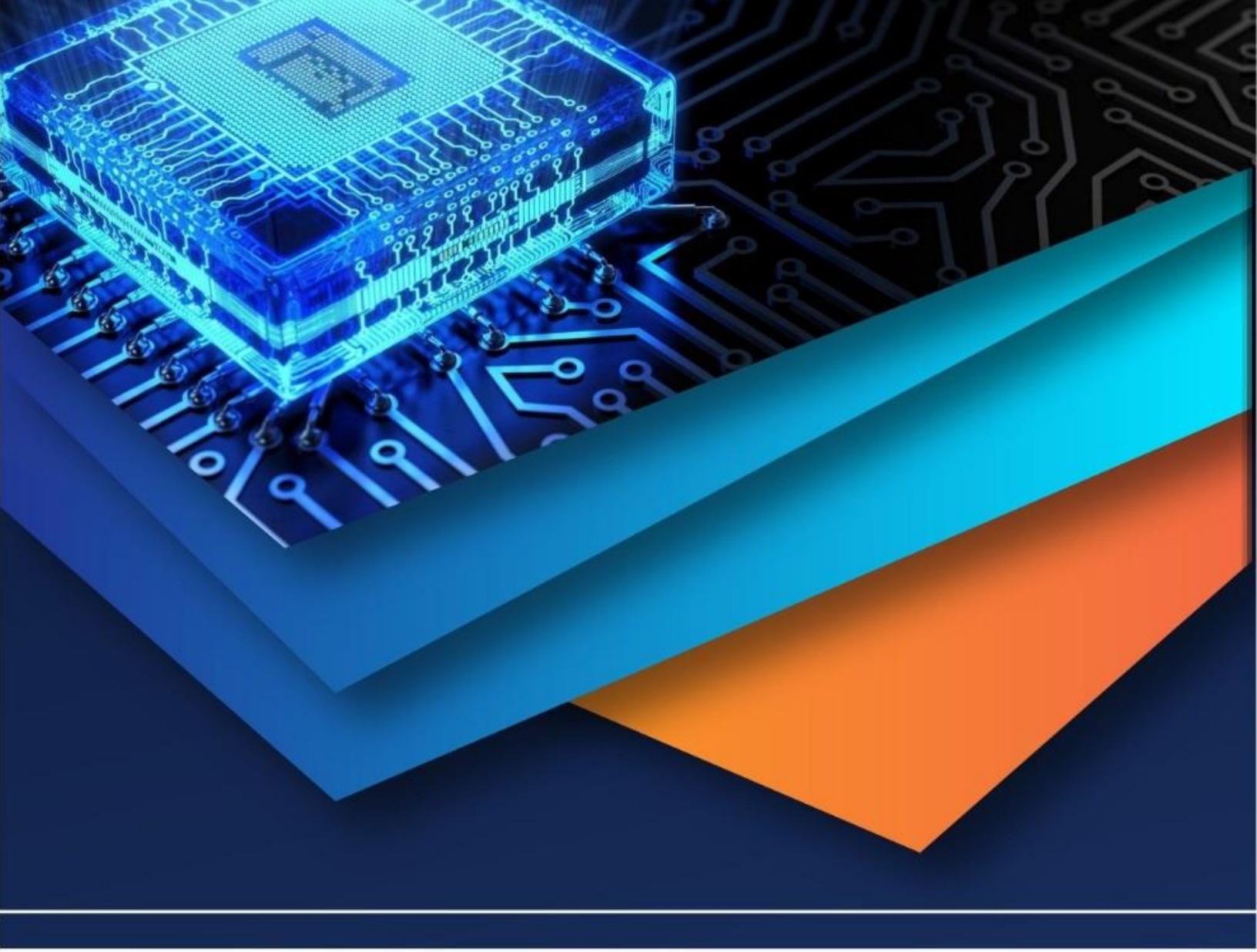
- Autonomous remediation systems
- Real-time threat intelligence integration
- Explainable AI for vulnerability assessment.

VIII. CONCLUSION

Vulnerability scanning tools play a critical role in modern cybersecurity defense strategies. Open-source tools such as Nmap, OpenVAS, Nikto, and OWASP ZAP provide cost-effective solutions, while enterprise platforms such as Nessus, Qualys, Nexpose, Burp Suite Professional, and Acunetix offer advanced detection and management capabilities. As cyber threats continue to evolve, the future of vulnerability assessment is moving toward AI-enabled, cloud-native, and continuously integrated security platforms capable of autonomous vulnerability discovery, prioritization, and remediation.

REFERENCES

[1] OWASP (2025). OWASP Web Security Testing Guide.
[2] MITRE Corporation (2025). Common Vulnerabilities and Exposures (CVE) Database.
[3] National Institute of Standards and Technology (2024). National Vulnerability Database (NVD).
[4] Akinyemi, A. M., & Sims, S. (2025). Role of artificial intelligence in modern cybersecurity vulnerability management practices. World Journal of Advanced Research and Reviews, 26(1), 555–584. https://doi.org/10.30574/wjarr.2025.26.1.1028
[5] Black, P. E., Fong, E., Okun, V., & Gaucher, R. (2008). Software assurance tools: Web application security scanner functional specification version 1.0. National Institute of Standards and Technology (NIST).
[6] Bodipudi, A. (2022). Integrating vulnerability scanning with continuous integration/continuous deployment (CI/CD) pipelines. European Journal of Advances in Engineering and Technology, 9(2), 49–55.
[7] Guhan Prasad, K., & Sai Krishna, P. (2022). Automatic web security scanner (Bachelor's Project Report). Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India.
[8] Intruder Security Ltd. (2024). The ultimate guide to vulnerability scanning. Intruder. Retrieved from https://www.intruder.io
[9] Kais, S., Kirda, E., Kruegel, C., & Jovanovic, N. (2006). A web vulnerability scanner. In Proceedings of the 15th International Conference on World Wide Web (WWW).
[10] Krishna, P. M., Abhinaya Sri, G., Vishnu, G. N., Vijay Kumar, B., & Sai, K. N. (2025). Vulnerability scanners are automated tools that scan web applications to look for security vulnerabilities. Fuzzy Systems and Soft Computing, 20(1), 253–259.
[11] Nagananthini, T. S., Baruni, M. K., & Laksitha, N. R. G. (2025). Web vulnerability scanner. International Journal of Research Publication and Reviews, 6(10), 3899–3906. https://doi.org/10.55248/gengpi.06.1025.3706
[12] OWASP Foundation. (2024). OWASP Top 10: The ten most critical web application security risks. Retrieved from https://owasp.org/www-project-top-ten/
[13] Patil, H. P., & Gosavi, P. B. (2018). Web vulnerability scanner by using HTTP method. International Journal of Computer Applications.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY