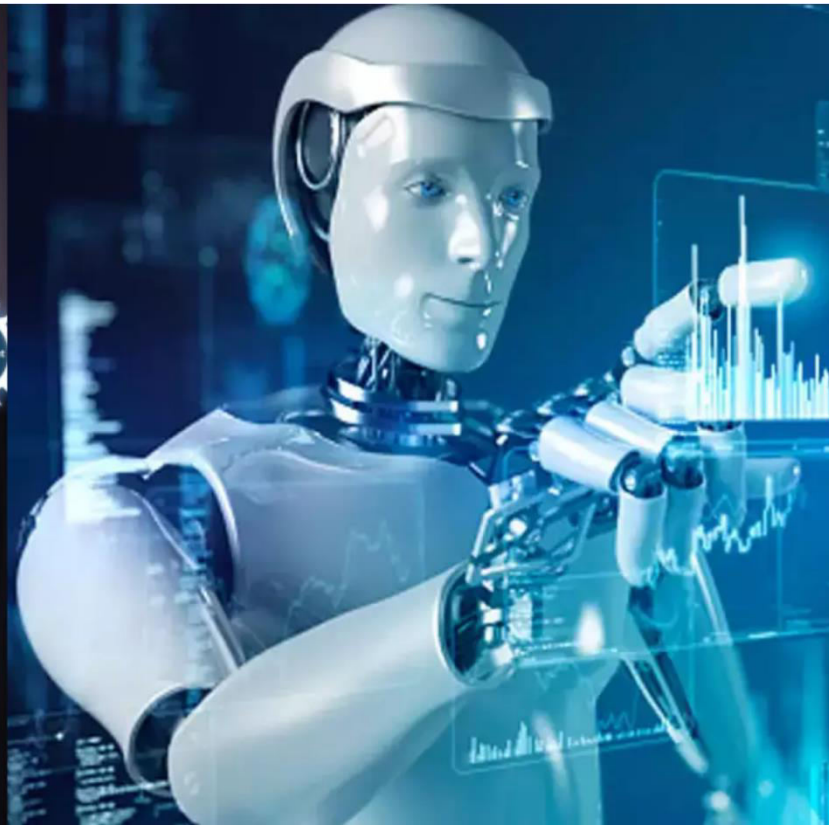
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Special Issue 1, January 2026

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

A Review of AI-Powered Web Vulnerability Scanning Methodologies

Kunj Bhatia, Ayush Patil, Vishal Surwase, Prathamesh Bhojankar, Prof. Chandrakant Rane

U.G. Student, Department of Information Technology, Indala College of Engineering, Kalyan, Maharashtra, India

U.G. Student, Department of Information Technology, Indala College of Engineering, Kalyan, Maharashtra, India

U.G. Student, Department of Information Technology, Indala College of Engineering, Kalyan, Maharashtra, India

U.G. Student, Department of Information Technology, Indala College of Engineering, Kalyan, Maharashtra, India

Professor, Department of Information Technology, Indala College of Engineering, Kalyan, Maharashtra, India

ABSTRACT: Maintaining the security of web applications is a significant challenge as modern cyber threats continue to avoid traditional defense methods. This research offers a detailed look at the shift to AI-supported scanning systems, which use machine learning algorithms for intelligent, real-time threat detection. We examine how Large Language Models (LLMs) currently identify security weaknesses and look into advanced visualization tools like vulnerability heatmaps. Additionally, the study reviews how automated remediation strategies work and the need for multi-format reporting across different development environments. By bringing together recent academic and industry advancements, this paper lays the groundwork for implementing AI-based security protocols.

KEYWORDS: AI, Web Security, Vulnerability Scanning, Large Language Models (LLMs), Review, Vulnerability Heatmap, Automated Mitigation, Threat Intelligence.

I. INTRODUCTION

As global digital infrastructure becomes more decentralized, web applications have become the main target for complex cyberattacks. Traditional security scanners have relied on fixed signature databases and strict rule-based systems. While these methods can effectively identify known exploits, they fall short against polymorphic "zero-day" attacks and the complex logic flaws present in modern microservices.

Integrating Artificial Intelligence (AI) helps fill these gaps by enabling systems to learn from large collections of code and historical attack data. This change allows for a more context-aware analysis, where the scanner can understand the developer's intent instead of only looking for string matches. This paper examines the methods that let AI evolve from a passive detection tool into an active security asset.

II. RELATED WORK

The use of AI in cybersecurity has shifted from theory to real-world application in the industry.

- Semantic Code Analysis: Traditional pattern matching is giving way to semantic analysis driven by Large Language Models (LLMs). These models can spot structural weaknesses in code logic that don't trigger standard signature alerts.
- Industry Standards: Platforms like Acunetix and Netsparker have started using machine learning to improve their validation processes. These updates aim to lower the "noise" from false positives, which is a big hurdle for security teams.
- Adversarial Simulation: Tools like ArmoScan use AI to take on an "attacker mindset," simulating multi-stage exploit chains to discover vulnerabilities that only show up under certain operational conditions.
- Hybrid Intelligence: Solutions like Detectify combine AI automation with data from ethical hacking communities. This ensures that the machine learning models are kept up to date with the latest exploit variants.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

- Advanced Penetration Testing: New tools that integrate LLMs, such as BurpGPT and Rogue, have made it possible to automate complex manual tasks. This includes generating targeted test payloads and bypassing automated bot-detection systems.

III. METHODOLOGY

The proposed AI-driven framework uses a modular structure to move beyond traditional signature-based detection methods. The methodology is arranged into three main phases:

- Semantic Detection Layer: The system uses Large Language Models (LLMs) to perform semantic code analysis. It identifies complex logical vulnerabilities that traditional scanners often miss. These models help automate penetration testing by generating relevant test datasets and simulating human-like interactions with applications.
- Risk Assessment and Visualization: Confirmed vulnerabilities are integrated into a color-coded heatmap. This map shows threat distribution and severity across the system. It plots the likelihood of a successful exploit against its potential impact. This allows security teams to focus on high-risk areas for prompt action.
- Automated Mitigation and Integration: The framework includes a decision engine and knowledge base that create tailored mitigation plans. These plans specify code adjustments and configuration changes. To support the development lifecycle, results are exported in different formats, such as JSON, XML, and SARIF, ensuring they work with existing security APIs and toolchains.

IV. EXPERIMENTAL RESULTS

Methodology	Core Strength	Primary Limitation
Traditional Rule-Based	High speed and efficiency for known risks.	High rate of false positives; blind to zero-day threats.
AI-Enhanced Systems	Superior accuracy and deep contextual awareness.	High computational requirements and data dependency.
LLM-Integrated	Human-like reasoning and complex logic testing.	Vulnerable to prompt injection and API latency.

V. CONCLUSION

The shift to AI-powered web security is an important step in protecting against new digital threats. By leaving behind static signatures and adopting systems that learn and adapt, organizations can build stronger security measures. Future improvements should aim to make LLM-based scanners more efficient to minimize delays. It is also essential to set standard criteria to assess how well AI-driven solutions work.

REFERENCES

[1] ArmoLogic. (2023). A Comprehensive Review of AI-Powered Web Vulnerability Scanning.
Retrieved from https://armologic.com/news/a-comprehensive-review-of-ai-powered-web-vulnerability-scanning/
[2] Mend.io.(2023).AI-Powered Web Vulnerability Scanning.
Retrieved from https://www.mend.io/resources/blog/ai-powered-web-vulnerability-scanning/
[3] Security(2023).TheRise of AI-Powered Vulnerability Scanners.
Retrieved from https://www.getastra.com/blog/security-audit/ai-powered-vulnerability-scanner/
[4] Balbix. (2023). What is a Vulnerability Heatmap?
Retrieved from https://www.balbix.com/insights/vulnerability-heatmap/
[5] Netmaker. (2023). A Guide to Vulnerability Heat Maps.
Retrieved from https://www.netmaker.io/blog/a-guide-to-vulnerability-heat-maps/

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details