| Volume 02 | Issue 04 | September 2026| ISSN: 3139-1737

International Journal of Advances and Applications in Convergent Studies & Transdisciplinary (IJ-AACST)

Bridging Disciplines, Bridging Knowledge

Aligned with the Vision of NEP 2020 and UGC Guidelines

Website: https://aacstij.org || Email: journaleditor@aacstij.org

AI-ENHANCED WEB APPLICATION'S VULNERABILITY DETECTION: A SURVEY

DOI: https://doi.org/10.5281/zenodo.22339274

***Kishor M. Supatkar*[1]*, *Dr. Varsha S. Tondre*[2]**

*Corresponding Author: [1]Department of Computer Science and Application,
Brijlal Biyani Science College,
Affiliated to SGBAU Amravati, Maharashtra, India 444605
kishore.supatkar@gmail.com

ORCID iD: *https://orcid.org/0009-0001-0291-4768*

[2] Department of Computer Science and Application,
Brijlal Biyani Science College,
Affiliated to SGBAU Amravati, Maharashtra, India 444605

ABSTRACT

Web applications remain critical components of modern digital services and continue to face evolving vulnerabilities, including cross-site scripting, SQL injection, cross-site request forgery [1], command injection, weak authentication, and previously unobserved attack patterns. This survey synthesizes the research abstracts on automated vulnerability scanning, mutation testing, artificial intelligence, deep learning [2], large language models, adaptive testing, vulnerability chaining [3], intelligent fuzzing, web-scraping-driven threat intelligence, and advanced penetration testing. The reviewed studies show a transition from signature and rule-based scanners to hybrid systems that combine crawling, machine learning, reinforcement learning, language models, anomaly detection, risk scoring, and automated remediation guidance. Across the reported studies, these approaches are associated with improved scan coverage, prioritization, detection performance, and reduced false positives, although the evidence is largely based on experiments, proof-of-concept implementations, synthetic datasets, and deliberately vulnerable targets. The survey identifies an important research gap in the unified, reproducible, and benchmarked evaluation of AI-enhanced web security systems across diverse real-world applications and continuously changing attack patterns. Therefore, future research should emphasize standardized datasets, explainable risk assessment, adversarial robustness, safe autonomous testing, and integrated evaluation of detection, prioritization, remediation, and operational costs.

KEYWORDS: Artificial intelligence, Automated vulnerability detection, Deep learning, Large language models, Web application security, Vulnerability scanning.