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.

1. INTRODUCTION

Web applications have become integral to business, communication, finance, education, and digital services. The literature describes web applications as exposed to a broad and changing set of security weaknesses and emphasizes that vulnerabilities can remain even after security hardening and release. The reviewed material identifies SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), command injection, weak authentication, and emerging or zero-day attack patterns as important security concerns in web applications [1].

Traditional security scanners typically rely on predefined signatures, static payloads, static crawling, or rule-based detection. The studies indicate that such approaches can be limited by predictable request patterns, changing defenses, false positives, incomplete coverage, and difficulties in detecting new attack forms. Therefore, recent studies have increasingly incorporated artificial intelligence and machine learning to make scanning adaptive, prioritize risks, identify anomalous HTTP behavior, and generate remediation guidance.

This survey aims to organize and critically synthesize the research material around four themes: conventional automated scanning, intelligent and adaptive vulnerability discovery [4], AI/LLM-assisted security analysis, and proactive intelligence and penetration testing. This review also identifies common limitations and research opportunities.

2. CONTRIBUTION OF THE PAPER

The reviewed abstracts collectively demonstrate rapid progress in AI-assisted vulnerability assessment; however, they do not establish a common evaluation framework. Different studies use different tools, datasets, vulnerability classes, metrics and experimental environments. Some reports provide proof-of-concept results or experiments on deliberately vulnerable targets, while others describe frameworks without supplying sufficient comparative information for cross-study benchmarking.

Another gap is the integration of a complete security workflow. Individual studies address detection, crawling, anomaly analysis, risk prioritization, vulnerability chaining, threat intelligence, and remediation; however, the material provides limited evidence for a unified and reproducible pipeline that jointly evaluates these stages under realistic and continuously changing web application conditions.

Accordingly, this survey aims to (1) classify the approaches represented in the studies, (2) compare their principal techniques and reported outcomes, (3) identify common strengths and limitations, (4) synthesize the research gap, and (5) outline future directions for reliable, explainable, safe, and benchmarkable AI-enhanced web vulnerability assessment.

3. LITERATURE REVIEW / RELATED WORK / BACKGROUND STUDY

3.1 Securing Cross-Site Request Forgery Vulnerabilities in Web Applications Using Mutation Analysis

In the [2] 2024 study as published/presented in IEEE 2nd International Conference on Software Engineering and Information Technology (ICoSEIT). Mutation testing for CSRF security testing; eight mutation operators; weak versus robust test cases; mutation score increased from 0.09 to 0.65 after fixing the test case.

3.2 A Deep Learning-Based Approach to Intelligent Web Vulnerability Discovery and Risk Assessment

In the [2] 2026 study as published/presented in IEEE, 1st International Conference on Emerging Trends in Advancements and Applications of Computational Intelligence Techniques (ETAACT). It combines OWASP ZAP, Deep Q-Network crawling, LightGBM risk prioritization, and LSTM autoencoding, and reports improved false-positive reduction, prioritization accuracy, and scan coverage. GANs are discussed for adaptive payloads and zero-day discovery.

3.3 An Adaptive AI-Enhanced Automated Web Security Scanner with Multi-Vector Testing and Vulnerability Chaining

In the [3] 2026 study as published/presented at the 8th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA). It uses a multithreaded scanner, response-pattern anomaly analysis, adaptive encoding based on live blocking feedback, and vulnerability chaining. Synthetic tests indicated gains in coverage and prioritization while retaining scoping, throttling, and exclusion safeguards.

3.4 Intelligent Web Vulnerability Detection Using Self-Learning Artificial Intelligence Framework: Aegis AI Scanner Implementation

In the [4] 2026 study as published/presented at the International Conference on Emerging Technologies and Future Innovations (ETFI). Python framework integrating NMAP, web reconnaissance, AI response evaluation, and LLM-driven risk scoring; proof of concept for reflected XSS and SQL injection with automated remediation guidance [4].

3.5 Automated Vulnerability Scanning and Bug Detection for Secure Web Applications

In the [5] 2026 study as published/presented at the 6th International Conference on Expert Clouds and Applications (ICOECA). Automated URL-based scanning for OWASP Top 10-related vulnerabilities using rule-based detection and structured logging; emphasizes early-stage assessment, low computational overhead, responsible testing, and safe time-stamped reporting.

3.6 AI-based Custom Web Application Scanner and Bug Detection in Website using Docker

In the [6] 2026 study as published/presented at the 6th International Conference on Expert Clouds and Applications (ICOECA). A hybrid scanner combining manual payload scripts, an LLM, and Docker sandboxing targets SQL injection, XSS, CSRF, and command injection. Source material reports better detection, fewer false positives, and actionable developer information.

3.7 Large Language Models in Cloud Cybersecurity: Applications, Vulnerabilities, and Risk Mitigation Strategies

In the [7] 2026 study as published/presented at the Innovations in Machine, Engineering, and Digital Conference (IMED). Examines LLMs for cloud threat/anomaly detection, log analysis, and incident response; compares performance metrics; and discusses prompt injection, information leakage, and model contamination with mitigation measures such as filtering, adversarial training, encryption, and differential privacy [7].

3.8 A Web Scraping Driven Intelligence System for Proactive Detection of Web Application Vulnerabilities

In the [8] paper 2026, study as published/presented at the 6th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT). It uses real-time scraping of vulnerability databases, forums, blogs, and other sources, followed by NLP/ML processing and integration into SIEM for contextualized threat intelligence and proactive vulnerability response.

3.9 Automated Detection of Web Application Vulnerabilities

In The [9] paper 2026 study as published/presented at the 8th International Conference on Intelligent Sustainable Systems (ICISS). It uses web crawling, intelligent fuzzing, and an Adaptive Random Forest classifier with HTTP-request/response features and severity scoring. Source material reports improved accuracy, precision, recall, and F1-score, and adaptation to obfuscated and zero-day payloads.

3.10 The Role of Advanced Penetration Testing Techniques in Enhancing Cybersecurity: A Survey on Web Application Security

In The [10] reports this Not study as published/presented in Journal article; URL in the research paper. Survey of advanced penetration testing for web application security, emphasizing manual and automated testing with Burp Suite and Metasploit and vulnerabilities, including SQL injection, XSS, and weak authentication.

4. RESEARCH METHODOLOGY

This survey is based on research paper abstracts and bibliographic details contained in the research paper document, which represents ten studies addressing web application security, automated vulnerability detection, AI-assisted scanning, cloud cybersecurity, web-scraping-driven intelligence, and penetration testing. The material was organized according to the research problem, technical approach, target vulnerabilities or security function, and reported findings.

Because the source document provides abstracts rather than complete full-text papers for most studies, the synthesis was intentionally limited to claims supported by those abstracts. No unsupported performance comparisons or rankings were introduced. Where bibliographic information such as DOI, publication venue, or date was not research paper, it was marked as unavailable rather than inferred.

5. RESULTS AND DISCUSSION

The synthesis shows that automated vulnerability detection is progressing from static, signature-oriented inspection to adaptive and learning-driven assessment. Studies using deep learning and machine learning specifically target the limitations associated with traditional scanners, including false positives, incomplete scan coverage, and difficulty in handling changing application behavior. The reported results are encouraging; however, the abstracts do not provide a sufficiently common experimental protocol to conclude that one technique universally outperforms another.

[1] CSRF mutation analysis contributes a different perspective by evaluating the adequacy of security test cases rather than only searching for vulnerabilities. The reported increase in the mutation score from 0.09 to 0.65 demonstrates how mutation analysis can expose weaknesses in security test design. This complements automated scanning because effective security assessment depends not only on the scanner but also on the quality of the tests it performs.

[6],[7] LLM-oriented systems introduce stronger semantic analysis and remediation potential; however, the reviewed cloud cybersecurity study also highlights prompt injection, information leakage, and model contamination. Consequently, adding AI to security assessment creates a dual requirement: the AI system must improve vulnerability detection while being protected against AI-specific attacks.

The web scraping-driven approach extends vulnerability assessment beyond the target application by continuously monitoring external intelligence sources. [8] When combined with NLP, machine learning, and SIEM integration, this model supports proactive monitoring.

The common evaluation measures across the studies include accuracy, precision, recall, F1-score, mutation score, [2],[6] false-positive reduction, scan coverage, prioritization accuracy, detection latency, and adversarial robustness. A major opportunity is to standardize these metrics and evaluate the systems using common datasets and representative real-world applications.

6. CONCLUSION AND FUTURE SCOPE

This survey synthesizes ten research works covering mutation testing, automated scanning, artificial intelligence, deep learning, reinforcement learning, large language models, adaptive vulnerability testing, web-scraping-driven intelligence, intelligent fuzzing, and advanced penetration testing. The literature indicates a clear movement toward adaptive and hybrid security assessments in response to the limitations of static signatures, predictable payloads, and conventional scanning workflows. The reported findings suggest improvements in coverage, prioritization, detection metrics, false-positive reduction, and remediation support. Simultaneously, the reviewed evidence reveals a substantial research gap: the lack of a standardized, reproducible, end-to-end evaluation of AI-enhanced web vulnerability assessment in diverse and continuously changing real-world environments. Therefore, future studies should combine rigorous benchmarking with Comprehensibility, adversarial robustness, safe autonomous testing, continual learning, and operational scalability. Addressing these challenges can help transform AI-assisted vulnerability detection from isolated proof-of-concept systems into dependable security engineering platforms.

Future research should develop standardized datasets containing benign, vulnerable, obfuscated, and evolving web traffic, establish common experimental protocols, and compare rule-based, machine-learning, deep-learning, reinforcement-learning, and LLM-based methods under the same conditions. Research should also examine explainable vulnerability scoring so that security analysts can understand why a finding is prioritized. Another important direction is secure human-AI collaboration. Rather than fully autonomous exploitation, future

systems can emphasize controlled discovery, evidence generation, risk explanation, and remediation recommendations in explicitly authorized environments. Sandboxing and policy-based controls should be incorporated into the adaptive testing architecture.

Continual learning is also promising because new vulnerabilities and application behaviors appear after the deployment. Future systems should be evaluated for drift, adversarial robustness, false positive stability, detection latency, resource consumption, and safe updating. Finally, integration with development and operational workflows can connect vulnerability discovery with secure software development, issue tracking, remediation verification, and security monitoring.

7. CONFLICT OF INTEREST

The authors declare that there are no financial, commercial, institutional, or personal relationships that could have influenced the work reported in this research.

8. RESEARCH INTEGRITY STATEMENT

The authors declare that the manuscript is original, complies with the journal's plagiarism and AI usage requirements, has not been published or submitted elsewhere and that all applicable ethical guidelines have been followed in conducting, reporting, and publishing the research.

9. REFERENCES

[1] “Securing Cross-Site Request Forgery Vulnerabilities in Web Applications Using Mutation Analysis,” 2024 2nd International Conference on Software Engineering and Information Technology (ICoSEIT), IEEE, 2024. doi:10.1109/ICoSEIT60086.2024.10497499.

[2] “A Deep Learning-Based Approach to Intelligent Web Vulnerability Discovery and Risk Assessment,” 2026 1st International Conference on Emerging Trends in Advancements and Applications of Computational Intelligence Techniques (ETAACT), IEEE, 2026. doi:10.1109/ETAACT69135.2026.11542196.

[3] “An Adaptive AI-Enhanced Automated Web Security Scanner with Multi-Vector Testing and Vulnerability Chaining,” 8th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), 2026.

[4] “Intelligent Web Vulnerability Detection Using Self-Learning Artificial Intelligence Framework: Aegis AI Scanner Implementation,” International Conference on Emerging Technologies and Future Innovations (ETFI), 2026.

[5] “Automated Vulnerability Scanning and Bug Detection for Secure Web Applications,” 6th International Conference on Expert Clouds and Applications (ICOECA), 2026.

[6] “AI-based Custom Web Application Scanner and Bug Detection in Website using Docker,” 6th International Conference on Expert Clouds and Applications (ICOECA), 2026.

[7] “Large Language Models in Cloud Cybersecurity: Applications, Vulnerabilities, and Risk Mitigation Strategies,” Innovations in Machine, Engineering, and Digital Conference (IMED), 2026.

[8] “A Web Scraping Driven Intelligence System for Proactive Detection of Web Application Vulnerabilities,” 6th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), 2026.

[9] “Automated Detection of Web Application Vulnerabilities,” 8th International Conference on Intelligent Sustainable Systems (ICISS), 2026.

[10] “The Role of Advanced Penetration Testing Techniques in Enhancing Cybersecurity: A Survey on Web Application Security,” journal article, source URL: https://juti.if.its.ac.id/index.php/juti/article/view/1372.