

The Use of Artificial Intelligence Techniques for Detecting Web Application Security Vulnerabilities and Improving Penetration Testing Efficiency: An Applied Study

Problem Statement

With the fast digitalization of business, government, healthcare, education, finance, and other sectors that are vital to society, there is a greater dependence than ever on web applications to provide the essential services. With the increasing amount of sensitive information being stored and processed on the web, web applications have emerged as one of the most enticing targets for cybercriminals. SQL injections, cross-site scripting (XSS), authentication bypass, remote code execution, and other web-based vulnerabilities are still the most common forms of cyberattacks that compromise the confidentiality, integrity, and availability of organizational information systems. As a result, there is an increasing need for organizations to conduct frequent vulnerability assessments and penetration testing to uncover any vulnerabilities before malicious parties can leverage them.

One of the most effective ways of assessing the security of a web application is by using penetration testing. But traditional penetration testing has been based on manual interpretation and the knowledge of cybersecurity experts. Manual penetration testing can be tedious, time-consuming, and costly, and may be hard to scale in large and rapidly changing Web environments. Furthermore, traditional testing methods can be time-consuming and may not be able to identify advanced or unknown vulnerabilities within a reasonable time, especially in the context of increasingly complex and dynamic web applications (Sanchez Collado et al., 2024).

The evolution of Artificial Intelligence (AI), especially machine learning, deep learning, intelligent automation, reinforcement learning, and Large Language Models (LLMs) has presented interesting possibilities for making vulnerability detection and penetration testing (VDP) processes more efficient. AI-powered tools can manage extensive security data,

detect patterns in attacks, prioritize vulnerabilities by risk level, automate reconnaissance and vulnerability identification, and assist with making informed choices in penetration testing. These capabilities can contribute to higher accuracy of detection, faster testing process, less human effort, and more effective cyber security assessments (Malkawi & Alhajj, 2026).

The advantages of AI in cybersecurity have been validated by a number of recent studies. According to Sanchez Collado et al. (2024), AI has a significant positive impact on the automation, vulnerability discovery, and the effectiveness of penetration testing, and it also decreases cybersecurity professionals' workload. Likewise, Saber et al. (2025) have shown that an AI-driven vulnerability scanning framework significantly cut down on the time needed for vulnerability assessment while sustaining around 95% detection accuracy. A similar study conducted by Radanliev (2025) supported the argument that incorporating AI with several security assessment methods can enhance the identification of vulnerabilities, speed up remediation efforts, and improve cyber resilience. Additionally, Agale et al. (2026) highlighted that AI and Large Language Models (LLMs) can streamline the process of reconnaissance, vulnerability assessments, exploitation planning, and decision-making in penetration testing.

While all this progress is encouraging, there are areas that still need to be explored more in-depth. Very few of the available literature are applied experimental studies, so most of it is systematic literature review. Many empirical studies only examine the penetration testing process at specific phases, including vulnerability scanning, without considering AI throughout the entire penetration testing lifecycle. Additionally, the explainability, transparency, adversarial robustness, scalability, benchmark availability, and integration of the model into the real-world enterprise cybersecurity environment have been reported as challenges in the past (Malkawi & Alhajj, 2026; Agale et al., 2026).

Furthermore, there are few studies that compare multiple AI techniques in the context of real-world web application scenarios while assessing the performance measures, including vulnerability detection accuracy, execution time, automation efficiency, and the overall effectiveness of the penetration test. Additionally, there is no standardized evaluation framework to support the practical implementation of AI-based cybersecurity solutions in various organizational settings (Sanchez Collado et al., 2024; Radanliev, 2025).

Hence, there is a clear need for an applied study that can systematically evaluate effectiveness of the Artificial Intelligence techniques to detect web application security vulnerabilities and enhance the efficiency of penetration tests. The aim of this study is to determine if AI technologies are able to deliver superior detection accuracy, quicker vulnerability assessment, higher levels of automation, and better operational efficiency than traditional pen testing techniques. The results will offer real-world practical evidence to support the adoption of AI-based cybersecurity solutions and recommendations to improve intelligent penetration testing frameworks in real-world web application security environments.

Research Question

What is the effectiveness of Artificial Intelligence techniques in detecting vulnerabilities in Web Applications and in the efficiency of the penetration testing when compared to the traditional method of penetration testing?

Research Objectives

The Objective of this research is to evaluate the performance of the Artificial Intelligence (AI) methods to detect security vulnerabilities in web applications and to enhance the efficiency of penetration testing.

To achieve this objective, the study aims to:

- 1- To evaluate the utility of the methods of Artificial Intelligence to identify security vulnerabilities of web applications.
- 2- To compare traditional penetration testing methods and techniques with AI-based penetration testing methods and techniques.
- 3- To quantify the effect of Artificial Intelligence (AI) on the penetration testing efficiency, both regarding the accuracy of detecting vulnerabilities and time taken to complete the penetration test.
- 4- To gain insights into the advantages, constraints, and obstacles of applying AI in the field of penetration testing to actual cybersecurity scenarios.
- 5- Offer actionable tips for more successful implementation of penetration testing AI frameworks to secure web applications.

References

- Agale, A., Kadam, A., Poyeraker, V., & Deshpande, R. (2026). *Review of AI-assisted and automated penetration testing techniques. International Journal of Advanced Research in Science, Communication and Technology*, 6(4).
- Malkawi, M., & Alhajj, R. (2026). AI-powered vulnerability detection and patch management in cybersecurity: A systematic review of techniques, challenges, and emerging trends. *Machine Learning and Knowledge Extraction*, 8(1), Article 19.
- Radanliev, P. (2025). Collaborative penetration testing suits emerging generative AI algorithms. *Applied Intelligence*, 55, Article 1030.
- Saber, V., Bahaa-Eldin, A. M., ElSayad, D., & Fayed, Z. T. (2025). Exploring the correlation between vulnerability scanning and Nmap. *International Journal of Intelligent Computing and Information Sciences*, 25(1), 41–50.
- Sanchez Collado, G., Olayinka, O., & Pasikhani, A. (2024). Web application penetration testing with artificial intelligence: A systematic review. In *Proceedings of the 22nd International Symposium on Network Computing and Applications (NCA 2024)*. IEEE.