DESIGN AND IMPLEMENTATION OF WEB SECURITY SCANNING SYSTEM

Junjie Hao, Panchenko V.I.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv

With the growing dependency on web-based services and applications across industries, the attack surface for modern IT systems has expanded significantly. Web applications, being frequently exposed to the public internet, are now a primary target for attackers exploiting misconfigurations, outdated components, and software vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure direct object references (IDOR). According to OWASP's Top Ten list [1], such vulnerabilities continue to pose major threats to organizational security. Traditional scanning methods are often rigid, heavyweight, or expensive, leaving gaps for attackers to exploit. Therefore, the development of an adaptable, efficient, and extensible web vulnerability scanner has become an increasingly relevant research topic [2, 3].

This work presents the design and implementation of a modular web security scanning system built using the Go programming language. The system is structured into independent yet cooperative modules that cover the entire reconnaissance and vulnerability detection workflow.

For vulnerability detection, two approaches are combined: template-based scanning using the Nuclei engine [4], which applies predefined payloads against known attack vectors such as SQLi, XSS, LFI, and RCE; and a crawler-based detection module that simulates user behavior, submits contextual payloads in dynamic input fields, and analyzes response anomalies in real time. The crawler supports DOM interaction through headless browsing, enhancing the detection of event-driven vulnerabilities like DOM-based XSS or client-side logic flaws.

The final system has been tested against real-world targets and synthetic environments, demonstrating its ability to detect a wide range of vulnerabilities with a low false positive rate. Compared to traditional scanners, the proposed solution shows significant improvements in scan efficiency and modular extensibility.

References:

1. "OWASP Top Ten Web Application Security Risks", available at : https://owasp.org/www-project-top-ten/ (last accessed 11.04.2025)

2. "Web Security Academy. PortSwigger", available at : https://portswigger.net/ (last accessed 11.04.2025)

3. Stuttard, D., & Pinto, M. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Wiley, 2011. 912 p.

4. "Nuclei: A fast and customizable vulnerability scanner", available at : https://github.com/projectdiscovery/nuclei (last accessed 11.04.2025)