



Florida International University

Fall Semester - 2024 - Senior Design Project

Nuclei – Vulnerability Scanner

Students: Xavier Rodriguez, Alejandro Hernandez, Frederick Gonzalez, Jonathan Rizo, Jean Bagnis
Instructor/Faculty: *Masoud Sadjadi*, Florida International University

PROBLEM

Inaccessibility or High Cost: Many vulnerability scanners are expensive and require extensive technical knowledge to maintain and operate them.¹ Thus, making them inaccessible largely to smaller organizations or individuals.

Inefficiency and Inaccuracy: Many tools produce false positives, delaying patching and increasing risks. Reliable detection, like Nuclei's minimal-error approach, is vital for timely fixes and effective bug bounties.

Database Security Risks: Threats like SQL injection and poorly secured databases present significant risks.

Weak Encryption Practices: Insufficient encryption or data leakage compromises sensitive information, leaving systems open to exploitation.

CURRENT SYSTEM

Commonly used vulnerability scanners, such as Nessus, OpenVAS, and Qualys have paved the way for automated vulnerability detection but are not without limitations:

Cost: Many tools are prohibitively expensive for smaller organizations.

Usability: A steep learning curve and overly technical interfaces deter wider adoption.

Compatibility: Some tools lack integration with modern workflows or platforms.

Effectiveness: Issues with false positives/negatives and limited customization impede the efficiency of these tools.

REQUIREMENTS

Reducing False Positives: Enhanced algorithm focused on accuracy and minimizing time spent investigating non-issues through URL manipulation and key word scanning.

Customization and Flexibility: Provide a modular, YAML-based template system to adapt scanning to specific needs.

Ease of Use and Scalability: Ensure an intuitive interface and scalability across networks, regardless of size or complexity.

Detailed Vulnerability Insights: Deliver granular details about detected vulnerabilities, including affected hosts, systems, and specific risks.

SYSTEM DESIGN

Our system uses Nuclei, a powerful open-source vulnerability scanner, Nuclei allows us to use:

YAML Templates: Define reusable and customizable scanning rules, making it easy to adapt to various environments.

Frequent CVE Updates: Ensures the system stays up-to-date with the latest vulnerability information.²

OBJECT DESIGN

Scanning Engine: The primary module that interacts with YAML templates to execute multi-threaded vulnerability scans, adaptively generating rules and collecting results for efficiency and organization.

Template Parser: A sub-module that reads and validates YAML templates, ensuring compatibility with CVEs and enabling dynamic, user-customized scanning rules using pre-built or custom templates.

Database Module: Provides secure, encrypted storage and retrieval of scan results, system logs, and metadata, supporting trend analysis, reporting, and regular backups for data integrity.

IMPLEMENTATION

System Diagram: Visual representation of the architecture, highlighting secure connections between the scanner, target hosts, and the network.

Codebase: Developed in YAML, utilizing the Nuclei Scanner and custom YAML templates for adaptability.

Database Integration: Centralized logging of detected vulnerabilities for analysis and reporting.

VERIFICATION

Testing: Validating the scanner against real-world vulnerabilities to ensure accuracy and reliability.

Penetration Testing: Conduct controlled tests on various systems to evaluate performance and effectiveness.

Metrics: Measuring the tool's success in terms of reduced false positives, detection time, and comprehensive reporting.

SUMMARY

Our **System Vulnerability Scanner** offers a cutting-edge solution for identifying and mitigating vulnerabilities across systems, databases, and hosts on networks.

By using **Nuclei** and using YAML-based customed templates, it ensures detailed reporting of vulnerabilities with minimal false positives.

The scanner provides an accessible, cost-effective, and scalable alternative to existing tools while integrating seamlessly into modern security workflows.

REFERENCES

[1] <https://www.tenable.com/buy>
[2] <https://github.com/projectdiscovery/nuclei>

ATTENTION: Subheadings shown above is a recommended structure for a research/scientific poster. Main elements of a poster are Introduction, Research and Conclusion. Researchers can customize the section headers based on their projects’ needs. REMOVE THIS TEXT ONCE YOU START WORKING ON YOUR POSTER