Project Report

Web Application Vulnerability Scanner

Introduction

Web applications are frequent targets for cyberattacks due to their accessibility and the sensitive data they handle. To help developers and security professionals identify and mitigate common vulnerabilities, this project implements a Web Application Vulnerability Scanner using Python. The tool provides both a command-line and a web interface for scanning web applications for critical security flaws.

Abstract

The Web Application Vulnerability Scanner is designed to detect common vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), and Open Redirects. It leverages pattern matching and regular expressions to analyze web responses for signs of exploitation. The scanner logs each finding with evidence and severity, and presents results in a user-friendly format. The project also includes a checklist for the OWASP Top 10 security risks, promoting awareness of industry-standard threats.

Tools Used

- **Python 3.8+** : Core programming language
- **Flask** : Web framework for the user interface
- **Flask-WTF** : CSRF protection for web forms
- **Requests** : HTTP requests and response handling
- **BeautifulSoup4** : HTML parsing
- **Regex** : Pattern matching for vulnerability detection
- **Git** : Version control

Steps Involved in Building the Project

1. **Project Setup** : Initialized a Python project with virtual environment and Git for version control.
2. **Dependency Installation** : Installed required libraries (`flask`, `flask-wtf`, `requests`, `beautifulsoup4`).
3. **Scanner Logic** : Developed `scanner.py` to send crafted requests and use regex to detect SQLi, XSS, and Open Redirect vulnerabilities.
4. **Web Interface** : Built a Flask app (`app.py`) with a Bootstrap-based form for user input and results display. Integrated CSRF protection.
5. **Logging & Reporting** : Enhanced the scanner to log each vulnerability with evidence and severity, and display results in both CLI and web UI.
6. **OWASP Top 10 Checklist** : Added a reference checklist to the web interface for user awareness.
7. **Testing & Documentation** : Tested the tool on sample URLs and documented usage in `README.md` and this report.

Conclusion

The Web Application Vulnerability Scanner provides a practical solution for quickly identifying critical security issues in web applications. By combining automated detection with clear reporting and OWASP guidance, it helps users improve their security posture. While not a replacement for professional penetration testing, this tool is valuable for education, awareness, and initial assessments.