Internship Project Report

Author: DHANUSH S

Internship: Elevate Lab Cybersecurity Program

Introduction

This project focuses on developing a Python-based Web Application Vulnerability Scanner capable of detecting common security flaws in modern web applications. It automates scanning for OWASP Top 10 vulnerabilities and provides an interactive dashboard for users to manage scans and view reports.

Abstract

The Web Application Vulnerability Scanner is designed to identify critical security issues such as SQL Injection, Cross-Site Scripting (XSS), Open Redirects, Security Header misconfigurations, and CSRF weaknesses. It features a modular plugin-based scanning engine, Flask-based web interface, and evidence-based reporting system.

Tools Used

- Python 3
- Flask Framework
- Requests Library
- BeautifulSoup
- Regex Pattern Matching
- HTML/CSS/JavaScript
- JSON-based configuration
- Docker (Optional)

Steps Involved

1. Project setup and dependency installation.
2. Designing the Flask web interface with login authentication.
3. Implementing the scanning engine with modular vulnerability plugins.
4. Developing detection modules for SQL Injection, XSS, CSRF, Open Redirect, and Security Headers.
5. Integrating API endpoints for scan execution.
6. Creating detailed vulnerability reporting with payload evidence.
7. Testing the scanner on controlled web applications.
8. Final debugging and UI improvements.

Conclusion

The Web Application Vulnerability Scanner successfully demonstrates the fundamental concepts of cybersecurity, specifically vulnerability detection, secure coding practices, and web security analysis. It is an effective internship project that reflects practical knowledge of offensive security and web application testing.