Project Report: Web Vulnerability Scanner

Introduction

Web applications are increasingly targeted by attackers due to weak security practices. Common vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), and open ports pose significant risks. To address this, a lightweight Web Vulnerability Scanner has been developed to help detect and analyze such issues.

Abstract

This project focuses on building a simple yet effective Web Vulnerability Scanner using Python and Flask. The tool allows users to scan websites for potential vulnerabilities, such as SQL Injection, XSS, and insecure open ports. Results are displayed on an interactive web interface along with severity levels to guide security improvements.

Tools Used

Programming Language: Python 3
Framework: Flask
Frontend: HTML, CSS, Bootstrap
Libraries: requests, socket, BeautifulSoup, flask

Steps Involved in Building the Project

1. Designed a Flask-based web interface.
2. Implemented scanning functions to detect SQL Injection, XSS, and open ports.
3. Integrated results into a structured output with severity levels.
4. Displayed results in an interactive and user-friendly web page.
5. Tested on multiple websites for validation.

Conclusion

The Web Vulnerability Scanner successfully identifies common web vulnerabilities and provides results in an easy-to-understand format. It can be extended in the future to cover advanced vulnerabilities such as CSRF and directory traversal. This project highlights the importance of proactive web security testing.

Made by: Swapnil Magar