Title: Web Application Vulnerability Scanner

Introduction:

This project involves creating a web application vulnerability scanner designed to identify common flaws such as XSS, SQL Injection, and CSRF in target websites. It uses automated crawling and testing techniques to detect input validation issues in web pages.

Abstract:

The scanner crawls target URLs, injects payloads into input fields, and analyzes the response. A Flask-based interface allows users to initiate scans and review detailed results, making it suitable for educational or ethical testing environments.

Tools Used:

- Python
- Flask (for UI)
- Requests & BeautifulSoup (for HTTP requests and HTML parsing)
- Regex (for pattern detection)

Steps Involved in Building the Project:

1. Built a crawler to gather URLs from a target site.
2. Implemented payload injection techniques for XSS and SQLi.
3. Analyzed server responses for vulnerability indicators.
4. Built a Flask UI for initiating scans and showing results.
5. Optionally checked CSRF protection tokens in HTML forms.

Conclusion:

The scanner provides a basic yet functional web vulnerability assessment framework.

It helps understand how input vulnerabilities arise and how to automate their detection.

This project builds both offensive and defensive awareness essential in cybersecurity.