Introduction

Web applications are increasingly targeted by cyber threats like SQL injection and cross-site scripting (XSS). This project aims to build a simple web vulnerability scanner that can identify such risks in websites by crawling, testing forms, and logging results. It helps understand how attackers exploit input fields and gives insights into basic web security testing.

Abstract

The WebVulnScanner project is a Python-based tool that scans web pages to find potential XSS and SQL injection vulnerabilities. It uses BeautifulSoup for parsing HTML, requests for making HTTP calls, and logs the output to a file. The scanner crawls links and forms, injects common payloads, and checks if the site reflects them unsafely, indicating a possible vulnerability.

Tools Used

- Python
- requests
- BeautifulSoup
- logging
- HTML test site: testphp.vulnweb.com

Steps Involved in Building the Project

1. Set up a basic Python script with BeautifulSoup and requests
2. Implement crawling to collect links and form data
3. Add XSS payload testing using <script> injections
4. Add SQL injection test using common payloads like ' OR '1'='1
5. Store results in logs/scan_log.txt
6. Package with README and requirements.txt for GitHub upload

Conclusion

This scanner is a starting point to understand web security flaws like XSS and SQL injection. While it does not cover all OWASP Top 10 vulnerabilities, it demonstrates how automated tools can assist in ethical hacking. In the future, this tool can be improved by adding a GUI, deeper crawling, and more vulnerability types.