Project Report: Web Application Vulnerability Scanner

Name: Sasi Kumar Medabalimi

Date: July 08, 2025

1. Introduction

This project focuses on building a basic yet functional web application vulnerability scanner using Python. The goal is to simulate real-world web penetration testing by detecting common flaws such as XSS and SQL Injection through payload-based testing. This tool is designed for educational and ethical hacking purposes.

2. Abstract

The scanner crawls the given URL for HTML forms and injects XSS/SQLi payloads to identify reflection-based vulnerabilities. It uses the requests and BeautifulSoup libraries for HTTP handling and parsing. Results are logged into a report file. This tool highlights the importance of secure form handling and validates how input validation failures can lead to critical vulnerabilities.

3. Tools Used

- Python 3
- Requests
- BeautifulSoup (bs4)
- Manual payloads
- Terminal for execution
- Notepad++ / VS Code for editing

4. Steps Involved

1. Built a Python script to fetch and parse forms from a target URL.
2. Created XSS and SQLi payload wordlists.
3. Injected payloads into all form fields (both GET and POST).
4. Analyzed responses for payload reflection.
5. Saved all findings in 'results/scan-report.txt'.
6. Tested the scanner on intentionally vulnerable web apps like:
   - http://testphp.vulnweb.com

- http://demo.testfire.net
- https://xss-game.appspot.com

5. Conclusion

This scanner simulates how attackers exploit basic form vulnerabilities. It provides awareness on how lack of validation can lead to XSS/SQLi. Although this is a lightweight tool, it mimics the early stages of real-world web vulnerability scanners and can be further extended to include CSRF, Open Redirects, and file upload flaws.